Black Tulip

Report of the investigation into the DigiNotar Certificate Authority breach

Classification	**PUBLIC**
Customer	Ministry of the Interior and Kingdom Relations
Project no./Ref. no.	PR-110202
Date	13 August 2012
Version	1.0
Team	Hans Hoogstraaten (Team leader) Ronald Prins (CEO) Daniël Niggebrugge Danny Heppener Frank Groenewegen Janna Wettinck Kevin Strooy Pascal Arends Paul Pols Robbert Kouprie Steffen Moorrees Xander van Pelt Yun Zheng Hu
Business Unit	Cybercrime
Pages	101

Fox-IT BV
Olof Palmestraat 6, Delft
P.O. box 638, 2600 AP Delft
The Netherlands

Tel.: +31 (0)15 284 79 99
Fax: +31 (0)15 284 79 90
Email: fox@fox-it.com
Web: www.fox-it.com

ABN-AMRO
no. 55.46.97.041
Chamber of Commerce
Haaglanden no. 27301624

WARNING
Misuse of this document or any of its information is prohibited and will be prosecuted to the maximum penalty possible. Fox-IT cannot be held responsible for any misconduct or malicious use of this document by a third party or damage caused by any information this document contains.

Fox-IT BV

Olof Palmestraat 6
2616 LM Delft

P.O. box 638
2600 AP Delft

The Netherlands

Phone: +31 (0)15 284 7999
Fax: +31 (0)15 284 7990
Email: fox@fox-it.com
Internet: www.fox-it.com

Management summary

DigiNotar B.V. was founded as a privately-owned notarial collaboration in 1998. DigiNotar provided digital certificate services as a Trusted Third Party and hosted a number of Certificate Authorities (CAs). The certificates issued by DigiNotar were trusted worldwide to secure digital communication on the basis of a Public Key Infrastructure (PKI). The services that DigiNotar provided included issuing Secure Sockets Layer (SSL) certificates to secure websites, issuing accredited qualified certificates that could be used as the legal equivalent of a handwritten signature and issuing PKIoverheid certificates for various Dutch eGovernment purposes. In June and July of 2011 DigiNotar suffered a breach, which resulted in rogue certificates being issued that were subsequently abused in a large scale attack in August of 2011.

Following the detection of the breach on July 19 of 2011, DigiNotar took several measures to control the incident, including the revocation of known rogue certificates and the hiring of a third party specialized in IT security to investigate the intrusion. At the end of July 2011, DigiNotar was under the impression that the intrusion of its network and services had been contained. On August 28, 2011, the content of a rogue wildcard certificate for the `google.com` domain was posted publicly, which had been issued by DigiNotar but which had not yet been revoked. For weeks the rogue certificate had been abused in a large scale Man-In-The-Middle (MITM) attack on approximately 300,000 users that were almost exclusively located in the Islamic Republic of Iran. Traffic that was intended for Google subdomains is likely to have been intercepted or redirected during the MITM-attack, potentially exposing the contents of the intercepted traffic as well as the Google credentials of the affected users.

On August 30, 2011, Fox-IT was asked to investigate the breach at DigiNotar. In the ensuing investigation traces were recovered that indicated that the outer limits of DigiNotar's network were first breached on June 17, 2011. The network that was used by DigiNotar was segmented and the Secure-net network segment that contained all the CA servers could not directly be reached from the Internet. By tunneling connections through other compromised systems in DigiNotar's network, the intruder gained access to the Secure-net network segment on July 1, 2011. The first attempts to create rogue certificates were made on July 2 and the first rogue certificate was successfully issued on July 10, 2011.

The investigation by Fox-IT showed that all eight servers that managed Certificate Authorities had been compromised by the intruder. The log files were generally stored on the same servers that had been compromised and evidence was found that they had been tampered with. Consequently, while these log files could be used to make inconclusive observations regarding unauthorized actions that took place, the absence of suspicious entries could not be used to conclude that no unauthorized actions took place. Serial numbers for certificates that did not match the official records of DigiNotar were recovered on multiple CA servers, including the Qualified-CA server which was used to issue both accredited qualified and government certificates, indicating that these servers may have been used to issue additional and currently unknown rogue certificates.

A fingerprint that was left by the intruder was recovered on a Certificate Authority server, which was also identified after the breach of the Certificate Service Provider Comodo in March of 2011. Over the course of the intrusion at DigiNotar, the intruder used multiple systems as proxies in order to obscure his true identity. However, several traces were recovered during the investigation by Fox-IT that independently point to a perpetrator located in the Islamic Republic of Iran. A complete list of all the IP-addresses that were identified during the investigation that are suspected to have been abused by the intruder were handed over to the Dutch police (KLPD).

The intruder at DigiNotar appears to have had the specific intention of abusing certificates that had been issued by a trusted party in order to spy on a large number of users in the Islamic Republic of Iran. The intrusion at DigiNotar and the ensuing MITM-attack resulted in an erosion of trust of the general public in the existing Public Key Infrastructure, which is central to its operation. Given the impact of a breach at a Certificate Authority on the Public Key Infrastructure as a whole, ensuring the security of every Certificate Authority is paramount to the trust in a Public Key Infrastructure and its role in providing security for a diverse range of activities on the Internet. While the approach to protecting the potential targets from this type of intrusion does not differ significantly from other threats, the range of scenarios that need to be taken into account is rapidly expanding.

Investigative summary

Commissioning of Fox-IT and subsequent measures

On August 30, 2011, Fox-IT was asked by DigiNotar to investigate the intrusion of its network. One of the first measures taken by Fox-IT was to place an incident monitoring service on DigiNotar's network, to determine if unauthorized activity was still taking place. A sensor captures and monitors all traffic between the internal network and the Internet. For the Fox-IT monitoring service, at least one person is on standby at all times to analyze suspicious traffic in real time. Additionally, the behavior of the Online Certificate Status Protocol (OCSP) responder[1] at DigiNotar was changed on September 1, 2011 as a precautionary measure, which effectively revoked all remaining rogue certificates that had been issued by the intruder.

On September 3, 2011, an operational director that acted on behalf of the Dutch state was appointed by the board of DigiNotar under Power of Attorney and the Dutch state. An interim report with preliminary findings was provided to DigiNotar and was published on September 5, 2011 by the Dutch state. At the instruction of the Dutch National Police Services Agency (KLPD) and the public prosecutor's office (OM), identifying evidence regarding the intruder was specifically included in the continued investigation. This definitive report is the outcome of that fact finding investigation performed by Fox-IT into the intrusion of DigiNotar's network and the subsequent MITM attack.

The primary aims of the combined investigation that Fox-IT performed at the request of DigiNotar and the Dutch Ministry of the Interior and Kingdom Relations (BZK) were to determine how DigiNotar's network had been breached, to what extent it had been breached, if the various Certificate Authorities that DigiNotar operated had been compromised and if evidence that could lead to a potential criminal indictment of the intruder could be safeguarded. For these purposes, various sources of information were gathered and examined, including the log files from the web servers, firewalls and the various CA servers. Additionally, the images of relevant systems in DigiNotar's network were analyzed. Approximately 400 forensically sound disk images were created during the course of the investigation of 265 systems, amounting to a total of seven terabytes of compressed data.

The investigation of DigiNotar's network and the intrusion

The DigiNotar network was divided into 24 different internal network segments. An internal and external Demilitarized Zone (DMZ) separated most segments of the internal network from the Internet. The zones were not strictly described or enforced and the firewall contained many rules that specified exceptions for network traffic between the various segments. The main production servers of DigiNotar, including the CA servers and the accompanying hardware security module (netHSM), were located in a physically highly-secured room and in the Secure-net network segment. The Certificate Authorities that were hosted by DigiNotar were managed by software running on eight different CA servers.

The investigation showed that web servers in DigiNotar's external Demilitarized Zone (DMZ-ext-net) were the first point of entry for the intruder on June 17, 2011. During the intrusion, these servers were used to exchange files between internal and external systems, with scripts that were placed on these systems serving as rudimentary file managers. The (recovered) log files from the Main-web server from the period of the intrusion showed a list of 12 internal and 21 suspicious external systems that connected to these scripts and a list of more than 100 unique filenames that were exchanged. Internal systems that requested these scripts were most likely to have been compromised[2], while external systems that requested these scripts were most likely used by the intruder to access DigiNotar's network.

From the web servers in DMZ-ext-net, the intruder first compromised systems in the Office-net network segment between the 17th and 29th of June 2011. Subsequently, the Secure-net network segment that contained the CA servers was compromised on July 1, 2011. Specialized tools were recovered on systems in these segments, which were used to create tunnels that allowed the intruder to make an Internet connection to DigiNotar's systems that were not directly connected to the Internet. The intruder was able

[1] A responder that informs the inquirer of the validity of a certificate using the Online Certificate Status Protocol (OCSP); further details are included in paragraph 10.2.
[2] In information security, a system is regarded as being compromised if its confidentiality, integrity and/or availability can no longer be guaranteed.

to tunnel Remote Desktop Protocol connections in this way, which provided a graphical user interface on the compromised systems, including the compromised CA servers.

Recovered log files showed that the first extraordinary certificate signing attempts on a CA server occurred on July 2, 2011 on the Relation-CA server. The first rogue certificate was successfully issued on July 10, 2011. The investigation by Fox-IT showed that all servers that managed Certificate Authorities had been compromised by the intruder, including the Qualified-CA server, which was used to issue both accredited qualified and government certificates. In total, a non-exhaustive list of 531 rogue certificates with 140 unique distinguished names (DNs) and 53 unique common names (CNs) could be identified. The last known date for traffic that was initiated from within DigiNotar's network to an IP address that was presumably (ab)used by the intruder was on July 22, 2011. Traces of activity by the intruder in DMZ-ext-net were found up to July 24, 2011.

Investigation of compromised CA servers and Certificate Authorities

The logging service for the CA management application ran on the same CA servers that were compromised by the intruder. The investigation also showed that the intruder had full administrative rights and that database records on these CA servers were deleted or otherwise manipulated. Consequently, suspicious entries in the log files of the CA servers can only be used to make inconclusive observations regarding unauthorized actions that took place, but the absence of suspicious entries cannot be used to infer that no unauthorized actions took place.

In order to successfully issue rogue certificates, compromising a server that hosted a Certificate Authority was not enough, as it also required the abuse of an active corresponding private key in the netHSM. This means that the unauthorized actions that might have taken place could not have included the issuing of rogue certificates if the corresponding private key had not been active during the intrusion period. The private keys were activated in the netHSM using smartcards. No records could be provided by DigiNotar regarding if and when smartcards were used to activate private keys, except that the smartcard for the Certificate Authorities managed on the CCV-CA server, which is used to issue certificates used for electronic payment in the retail business, had reportedly been in a vault for the entire intrusion period.

In the log files of some CA servers, log entries were found that indicated the automatic generation of a Certificate Revocation List (CRL). Certificate Authorities usually issue CRLs at regular intervals according to their policies. These CRLs are signed by the issuing Certificate Authorities, which can only occur if a private key was active on the netHSM. The log entries referring to such an automatic process thus indicated that the private keys in the netHSM were activated and that there was potentially an opportunity for the intruder to abuse these private keys.

It is possible that the CA software that was used was able to produce certificates that have identical certificate attributes as previously issued certificates. This includes the serial number and the validity dates, with the exception of the public key and its key identifier. The intruder could have issued certificates that would be seemingly identical to formally issued and trusted ones. Since the possibility could not be excluded that the compromised CA servers had been abused to issue additional rogue certificates and since the rogue certificates may not be distinguishable from legitimate certificates in aspects that are relevant for the purpose of verification within a PKI, it was no longer possible to rely on the authenticity of any certificates that had been issued by the affected Certificate Authorities.

Given the inevitable uncertainty if the Certificate Authorities had been abused to issue rogue certificates, PKI standards required all certificates that were issued by these Certificate Authorities to be revoked and the Certificate Authorities themselves to be removed from trust lists in the software products that contained them. The impact of revoking the certificates that were issued by DigiNotar varied depending on their usage and had to be assessed on a case by case basis.

Investigation into the intruder

In one of the scripts that were found on a CA server, the intruder left a signature that was also identified after the breach of the certificate service provider Comodo. The vast majority of the external IP addresses that were identified during the investigation were probably used as proxies to obscure the identity of the intruder. The true IP address of the intruder may have been revealed by error however, when the intruder erroneously connected to the Main-web server without using one of the proxies that

was regularly used. The error occurred only once and was corrected within seconds. This IP address was also identified in other parts of the investigation.

More specifically, during the investigation a tool was identified that connected back to an external IP that was used as a proxy by the intruder. When this external system was examined, after an official request for assistance by the proper authorities, its log files also showed connections from the IP address that had erroneously been revealed. Furthermore, eight requests were made by this IP-address for a rogue Yahoo certificate, presumably to test DigiNotar's OCSP responses. The first three OCSP requests for the `*.google.com` certificate used for the MITM attack came from an IP address that also connected to the Main-web server once. These two IP addresses and three other IP addresses that were used by the attacker are within close range of one another, located in the Islamic Republic of Iran. A complete list of all the identified IP addresses that are suspected to have been abused by the intruder was shared with the proper authorities.

Investigation of the MITM attack

The fact that the chain of trust of PKI had been broken due to the intrusion at DigiNotar did not just result in a hypothetical threat, as at least one rogue certificate was subsequently abused in practice. A rogue certificate for `*.google.com` was abused to perform a massive man-in-the-middle (MITM) attack. In such an attack, the attacker places himself between two parties to intercept or modify the traffic between them. The investigated MITM attack was compounded with a form of redirection, where users who tried to reach legitimate websites that were hosted by Google were redirected to fraudulent versions of these websites. The traffic which was meant for Google and that was intercepted was not necessarily forwarded to Google, as users may have been presented with a page specifically intended to phish for their credentials.

The requests made to the OCSP responder for the rogue `*.google.com` certificate indicated that a total number of 298,140 unique IP addresses could be identified as having been victimized by the MITM attack. The number of unique IP addresses can only be regarded as a very rough approximation of the number of users affected. Multiple users can be masqueraded behind a single external IP address, while a single user can also make requests from multiple IP addresses. Moreover, relatively old software such as Internet Explorer 6 does not support OCSP requests and these users are therefore not included in the aforementioned approximation.

The IP addresses in the OCSP log files were enriched with GeoIP information, which showed that 95% of these IP addresses originated from the Islamic Republic of Iran. These IP addresses originated from 143 different autonomous systems (often Internet Service Providers), while 60% of the requests originated from only 4 Iranian autonomous systems. A sample of the remaining 5% of the affected IP addresses was inspected, which mainly showed exit nodes for The Onion Router (Tor), proxies and Virtual Private Network (VPN) servers. On this basis it can be concluded that the MITM attacks almost exclusively targeted at users who were located in the Islamic Republic of Iran.

The most likely modus operandi used during the MITM attack, based on the accumulated OCSP data, is that of Domain Name System (DNS) cache poisoning. A DNS cache poisoning attack relies on the fact that DNS servers cache the responses of DNS servers at a higher level in the infrastructure. By flooding a DNS server with forged responses for a particular domain, as if it had received the response from a higher DNS server, it is possible to "poison" the entries in the DNS server and thus its responses to clients at a lower level in the infrastructure. The poisoned entries are valid for as long as the Time To Live (TTL) allows, after which these entries expire and another DNS request would be made to a higher DNS server for the domain if requested by a client. This modus operandi would explain why traffic that went through proxies, Tor exit nodes and VPNs was also affected by the MITM attack and would also correspond with the peak-like behavior and the occurrence of repeated and sudden declines in OCSP requests that were made for rogue certificates.

Table of Contents

Management summary 3

Investigative summary 4

Table of Contents 7

1 Introduction 10

1.1 Background 10
1.2 Events leading up to the report 10
1.3 Involved parties 11
1.4 Timeline of events 12
1.5 Structure of the report 13

2 Incident response investigation 14

2.1 Preliminary research and actions 14
2.2 Investigational approach 14
2.2.1 Incident response monitoring 14
2.2.2 Safeguarding evidence 15

3 State of affairs 16

3.1 Organization 16
3.2 Services 16
3.3 Network infrastructure 16
3.3.1 Network segments 17
3.3.2 Network operation 19
3.3.3 Internet connectivity 19

4 Investigation of web server log files 23

4.1 Sources 23
4.2 Web server log file analysis 23
4.3 Results 24
4.3.1 Internal systems 24
4.3.2 External IP addresses 25
4.3.3 Suspicious files 25
4.3.4 Noteworthy log entries 26
4.4 Conclusion 26

5 Investigation of firewall log files 27

5.1 Sources 27
5.2 Log file analysis 27
5.2.1 Connections from internal IPs to AttIPs 27
5.2.2 Tunnels from DMZ-ext-net to AttIP1 28
5.2.3 Access to Office-net 29
5.2.4 Tunnels from Office-net 29
5.2.5 Access to Secure-net 30
5.2.6 Tunnels from Secure-net 31
5.2.7 Access to stepping stone from Secure-net 31
5.2.8 Other noteworthy traffic 32
5.3 Conclusion 35

6 Investigation of CA servers 37

6.1 Sources 37
6.2 CA software log files 38
6.2.1 Sources 38
6.2.2 CA software log analysis 39
6.3 CA databases 41

6.3.1 Certificates 41
6.3.2 Private keys 42
6.3.3 Serial numbers 43
6.4 Conclusion 43
6.4.1 Rogue certificates 44
6.4.2 Trust in the Certificate Authorities 45
7 System access and tools 47
7.1 Previous investigation 47
7.2 Connection tools 47
7.2.1 Stepping stones 47
7.2.2 Accessing the stepping stones 47
7.2.3 Network tunnels 48
7.3 Gaining a foothold 49
7.3.1 Password cracking tools 49
7.4 Issuing certificates 50
7.4.1 CA management interface 50
7.4.2 XUDA scripts 51
7.4.3 nCipher DLLs 52
7.5 Conclusion 52
8 Remaining investigation 54
8.1 netHSM 54
8.2 Load balancer 54
8.3 External server at AttIP2 54
9 Summary of findings 55
9.1 First point of entry and stepping stones 56
9.2 Compromised systems and Certificate Authorities 56
9.3 Information about the intrusion and the intruder 57
9.4 Timeline of the intrusion 58
10 MITM attack 59
10.1 Identified rogue certificates 59
10.2 Investigation of OCSP responder log files 60
10.2.1 Sources 61
10.2.2 Yahoo certificate 61
10.2.3 Google certificate 62
10.2.4 Unknown serials for verified certificates 62
10.2.5 Targets of the MITM attack 63
10.2.6 Modus operandi for the MITM attack 64
10.3 Conclusion 66
10.3.1 Consequences 66
10.3.2 Timeline of the MITM attack 66
11 Lessons learned 68
12 Potential follow-up investigation 70
12.1 Intruder's steps 70
12.2 Network infrastructure 70
12.3 Investigation of CA servers 70
12.4 Systems 71
12.5 Aftermath 71
13 Terminology 72
Appendix I: References to equipment 74
Appendix II: List of suspected intruders IP-addresses 77
Appendix III: Timeline of noteworthy traffic 79
Appendix IV: Certificate Authorities generating CRLs 82

Appendix V: Certificate Authorities 84
Appendix VI: References to private keys 91
Appendix VII: Unknown serial numbers 93
Appendix VIII: Rogue certificates 95
Appendix IX: Suspicious files 96

1 Introduction

1.1 Background

The confidentiality and security of the communication that occurs over the Internet in large part relies on the use of the cryptographic protocols Transport Layer Security (TLS) and its predecessor Secure Sockets Layer (SSL). An essential element of these protocols is the use of public key certificates, which use a digital signature to bind a public key with the identity of a specific system or a website. These public key certificates are issued by Certificate Authorities (CAs). A certificate authority is a third party that is trusted by both the holder of the certificate and the party that relies on the certificate to identify the holder. Together with the necessary hardware, software and corresponding procedures, the Certificate Authorities form the basis of a Public Key Infrastructure (PKI).

DigiNotar B.V. [3] was a Certificate Authority that provided digital certificate services. The digital certificates were used to secure Internet traffic, to issue (qualified) electronic signatures and to provide data encryption. DigiNotar also issued government accredited PKIoverheid certificates. During the months of June and July of 2011, the security of DigiNotar was breached and rogue certificates were issued. One of these certificates, a rogue Google certificate, was abused on a large scale in August of 2011 targeting primarily Iranian Internet users. At the end of August the intrusion became public knowledge and set into motion a chain of events that eventually led to the removal of all the Certificate Authorities that were hosted by DigiNotar from trust lists and ultimately the bankruptcy of the company.

On September 3 of 2011 the Dutch state publicly expressed the intention to take over the operational control of DigiNotar, including the responsibility for the commissioned investigation into the intrusion of DigiNotar's network by Fox-IT. On this date an operational director that acted on behalf of the Dutch state was appointed by the board of DigiNotar under Power of Attorney. The interim report with the preliminary findings of Fox-IT was provided to DigiNotar and was published on September 5, 2011 by the Dutch state. At the instruction of the Dutch police (KLPD) and the public prosecutor's office (OM), identifying evidence that could lead to the intruder was specifically included in the continued investigation. This report is the outcome of the technical fact finding investigation by Fox-IT into the intrusion of DigiNotar's network and the subsequent man-in-the-middle (MITM) attack. Former employees of Diginotar B.V. were given the chance to respond to a draft version of this report for the purpose of verification and their relevant input was incorporated where appropriate.

This report provides an overview of the results of the investigation by Fox-IT and evidence that was left by the intruder in the internal network of DigiNotar. More detailed information that was uncovered in regard to the identity and/or location of the intruder has been excluded from this report and was made available only to the proper authorities. Once this information was obtained, the focus shifted from tracing the intruder's steps in detail to concluding the investigation and this report.

Questions that lie outside the scope of the investigation will not be answered in this report, but may be answered after further research. The findings in this report are reported in such a way that they can be continued or repeated by other parties if they are provided access to the source material. Potential follow-up questions for further research are included in Chapter 12.

References to servers are made using descriptive names. A comprehensive list of the referenced servers including their IP addresses and exhibit numbers can be found in Appendix I. All dates and timestamps are in Central European (Summer) Time (CEST; UTC+2), unless explicitly stated otherwise.

1.2 Events leading up to the report

The rogue certificates that had been generated on July 10, 2011 were first discovered when an automated routine test that had failed to work was restored on July 19, 2011. The test signaled that there was a mismatch between the certificates that had been issued and the administrative records in the back office of DigiNotar. The staff of DigiNotar proceeded to examine the CA management applications and found that rogue certificates had been issued. In response DigiNotar took several measures to control the incident, including the immediate revocation of serial numbers that corresponded with the

[3] A B.V. (*Besloten Vennootschap*) is a limited liability company, a commonly used legal entity for corporations in the Netherlands.

known rogue certificates, and its employees were under the impression that the incident had been contained at the end of July of 2011.

On August 28, 2011, a concerned Gmail user posted a warning that his web browser had displayed on a Google support forum. The Google Chrome web browser that he used blocked access to the Google website because Chrome detected the usage of an invalid certificate[4]. This certificate had been issued by one of the Certificate Authorities that were controlled by DigiNotar. Subsequently, similar reports were posted on the Internet by others. The Dutch Government Computer Emergency Response Team (GOVCERT.NL) contacted DigiNotar on August 29, after being notified by Cert-Bund and the rogue wildcard Google certificate was revoked. Various other stakeholders were notified in the morning of August 30.

Fox-IT was asked to start an investigation into the breach of DigiNotar's network on August 30, 2011 with the purpose to help DigiNotar to identify if unauthorized activity was still taking place, to reveal to what extent DigiNotar's systems in general and PKIoverheid specifically had been compromised, to identify the path of the intruder through the network, if remarkable OCSP requests were taking place and to ascertain the impact of the rogue certificate that was being abused in the Islamic Republic of Iran. An incident response team was assembled by Fox-IT that started the investigation immediately. The team included forensic IT experts, cybercrime investigators, malware analysts and a security expert with PKI experience.

In the days that followed several actions were taken by DigiNotar with the help of Fox-IT to further control the incident and to limit the damage to its business. On September 2, 2011 an interim report with preliminary findings was drafted for DigiNotar stakeholders in consultation with DigiNotar. These results were shared verbally with GOVCERT.NL by DigiNotar. Once the full impact of the intrusion became clear to the Dutch Ministry of the Interior and Kingdom Relations (BZK) it took over the lead role in Fox-IT's ongoing investigation.

The focus of the investigation shifted as a result of the involvement of the ministry BZK. The focus of the continued investigation was primarily to determine the extent of the breach and its impact on PKIoverheid, to assist the KLPD by investigating the infrastructure to produce evidence against the intruder and to describe the lessons that could be learned from such an incident. As a result, questions regarding the path of the intruder through DigiNotar's network became less relevant and the level of certainty of statements that are made in regard to the attacker's path will reflect this shift in focus. Once it became clear to what extent the CA servers had been compromised and all the IP addresses that could be connected to the intruder were collected, the investigative stage was concluded. This report is the culmination of the incident response investigation that was performed at the request of both DigiNotar and the ministry BZK.

In this report, the term "intruder" should not be read to convey any information in regard to whether one or more persons were involved in the various stages of the intrusion or if these acts were perpetrated by a male or a female. The term "attacker" is used similarly to describe the person or persons who perpetrated the man-in-the-middle (MITM) attack on primarily Iranian users of Google services.

1.3 Involved parties

Multiple parties were involved in the DigiNotar incident response and the subsequent investigation. The parties were as follows:

Party	Role
BZK	The Dutch Ministry of the Interior and Kingdom Relations is responsible for national affairs, including the Dutch PKI infrastructure (PKIoverheid) in which DigiNotar took part.
Cert-Bund	Computer Emergency Response Team der Bundesverwaltung is the German equivalent of GOVCERT.NL.
DigiNotar B.V.	Former notarial collaboration that provided various certificate services including issuing digital certificates.

[4] Google Chrome performs additional certificate verification on Google certificates (certificate pinning) in addition to the standard in PKI prescribed verification.

Party	Role
Fox-IT B.V.	Security company that provides solutions for the protection of state secrets, the investigation of digital crimes, audits, managed security services and consultancy.
GOVCERT.NL	Cyber security and emergency response team of the Dutch government.
KLPD	The Dutch National Police Services Agency and its Team High Tech Crime Unit.
Manufacturers	Manufacturers of software that uses certificates, such as Mozilla, Microsoft, Adobe and the Tor Project.
OM	The Dutch Public Prosecutor.
OPTA	The Independent Post and Telecommunications Authority of the Netherlands is responsible for the registration of Certificate Service Providers (CSPs) that issue qualified electronic signatures.
Parties relying on DigiNotar B.V.	Enterprise customers of DigiNotar who used certificates issued by DigiNotar, such as lawyers, notaries, judicial officers and ministries (and their customers).

1.4 Timeline of events

The timeline below shows the most relevant events that occurred after the public disclosure of the existence of a rogue certificate that had been issued by DigiNotar. An overview of the events that took place before this public disclosure is detailed in paragraph 2.1.

Date	Description
28-Aug-2011	On a Google support forum, a customer of the Iranian ISP ParsOnline posted details about a certificate warning that was presented to him by Google Chrome for a rogue `*.google.com` certificate[5].
29-Aug-2011	Google received multiple reports about an attempted SSL MITM attack. Articles about a rogue `*.google.com` certificate appeared on the blogs of Mozilla, Google, Microsoft and other manufacturers. The rogue `*.google.com` certificate was revoked by DigiNotar.
30-Aug-2011	Fox-IT was asked by DigiNotar to initiate an investigation into the intrusion at DigiNotar to detect whether the intruder was still active.
01-Sep-2011	At the advice of Fox-IT, the behavior of the OCSP responder was changed so its responses were based on a white list of known valid certificates, effectively revoking all unknown certificates (see paragraph 2.2.1).
02-Sep-2011	The preliminary investigation by Fox-IT indicated that the integrity of the CA server that was used for managing qualified certificates and PKIoverheid was breached (Qualified-CA). DigiNotar informed GOVCERT.NL about the details of this finding.
03-Sep-2011	The Dutch government publicly revoked trust in DigiNotar and the certificates that had been issued by the company. Following this announcement, most browser manufacturers also revoked their trust in DigiNotar, if they had not done so already.
05-Sep-2011	The interim report on the breach of the DigiNotar Certificate Authority was published[6]. DigiNotar formally reports the intrusion to the police.
14-Sep-2011	OPTA ended the registration of DigiNotar B.V. as a certificate authority for qualified signatures on the basis of the Dutch Telecommunicatiewet (the Dutch law on telecommunication).
19-Sep-2011	DigiNotar filed a bankruptcy petition under Article 4 of the Dutch Bankruptcy Act.
20-Sep-2011	The Court of Haarlem declared DigiNotar B.V. to be bankrupt.
28-Sep-2011	All qualified and PKIoverheid certificates issued by DigiNotar were revoked.
01-Nov-2011	Most of the remaining active public certificates were revoked. BAPI (used for the Dutch Tax administration) and two private DigiNotar Certificate Authorities were excluded from this revocation[7].

[5] Google Groups, "Is This MITM Attack to Gmail's SSL?" at http://groups.google.com/a/googleproductforums.com/d/topic/gmail/3J3r2JqFNTw/discussion

[6] Rijksoverheid, "Interim Report DigiNotar Certificate Authority breach" at http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1/rapport-fox-it-operation-black-tulip-v1-0.pdf

[7] The Dutch tax administration took additional security measures and accepted the minimal risks that remained. This also applies to the operation of the internally used private CAs.

1.5 Structure of the report

In this introductory chapter, the background of the events against which the incident occurred is described. The overview includes a summary of how DigiNotar's internal network was set up and operated. Chapter 2 provides insight into the incident response investigation that was performed by Fox-IT at the request of DigiNotar and the ministry BZK. More specifically, it details how the investigation was approached and what actions were taken. Chapter 3 provides a general overview of the state of affairs that Fox-IT encountered at DigiNotar when its incident response investigation was initiated.

Chapters 4 through 8 describe the relevant results of the investigation that was performed by Fox-IT. More specifically, Chapter 4 details the investigation into the web servers that were used as stepping stones by the intruder; Chapter 5 details the investigation into the firewall logs; Chapter 6 details the investigation into the CA servers. Chapter 7 contains an overview of the investigation that was performed on safeguarded hard disks. Assorted smaller sources of information for the investigation are discussed in Chapter 8. Chapter 9 contains the investigative conclusions on the basis of the preceding chapters, which includes an image of the referenced systems and network segments.

The large-scale MITM attack that took place in the aftermath of the intrusion of DigiNotar's network is the subject of Chapter 10. In this chapter the results of scrutinized OCSP log files provide more details about this attack.

Lessons that can be learned from the intrusion of DigiNotar's network are discussed in Chapter 11. In Chapter 12 a number of questions are formulated that could serve as the basis for further investigation on the source material. References and a description of some of the commonly used terms in this report are included in Chapter 13.

There are nine appendices to this report that are referenced throughout the report. Appendix I includes the detailed references to the equipment that was present in DigiNotar's internal network. Appendix II provides details about IP addresses that are suspected to be linked to the attacker. Due to the ongoing investigation, the actual IP addresses have been removed. Appendix III provides a timeline of notable traffic that was found when investigating the firewall logs. Appendix IV contains a list of Certificate Authorities that were automatically generating CRLs. Appendix V includes the Certificate Authorities that were hosted at DigiNotar. Appendix VI lists references to private keys that were present in the databases of the CA servers. Appendix VII lists serial numbers encountered in the `serial_no.dbh` database on servers managing Certificate Authorities that could not be related to any found certificates. Appendix VIII provides a list of the unique Common Names of the rogue certificates. Appendix IX lists a number of suspicious files that were encountered on various DigiNotar systems.

While every reasonable precaution was taken to ensure that all the data, facts and conclusions in this report are correct, the information in this report may include errors and facts may have been omitted. The limited degree of inevitable uncertainty is because the results are in part based on information that had to be extracted from systems that had been compromised and thus on data that had or may have been tampered with. Fox-IT performed a time boxed investigation into the intrusion of DigiNotar and the subsequent MITM attack for the ministry BZK. While the time provided allowed Fox-IT to perform the necessary research to support the conclusions in this report, further investigation could still be performed, which may yield new information, given the size of the breach described in this report and the amount of available data.

2 Incident response investigation

2.1 Preliminary research and actions

Prior to the involvement of Fox-IT on August 30, 2011, DigiNotar took several actions during their preliminary research. The timeline below is intended to provide the necessary context and should not be regarded as exhaustive. Based on DigiNotar's incident reports and interviews with the persons involved, the following timeline could be reconstructed:

Date	Description
19-Jul-2011	A daily routine check revealed that rogue certificates had been issued. An incident response team was formed and the identified rogue certificates were revoked.
20-Jul-2011	A script with a message of the Iranian intruder was found. More rogue certificates were discovered.
21-Jul-2011	The rogue certificates that were discovered on July 20, 2011 were revoked. CA servers were shut down at night.
25-Jul-2011	An external firm specialized in IT security was consulted to investigate the incident.
27-Jul-2011	More rogue certificates were discovered and revoked. The external security firm delivered their report. The report showed that a server in the DMZ-ext-net (Docproof2) was compromised by utilizing a known vulnerability in the DotNetNuke software and that a CA server (Relation-CA) was compromised.
28-Jul-2011	It was discovered that a rogue certificate was verified by an IP-address originating from the Islamic Republic of Iran.
29-Aug-2011	The rogue wildcard Google.com certificate that was used in the large-scale MITM attack was revoked.

2.2 Investigational approach

On August 30, 2011, Fox-IT was hired by DigiNotar. Fox-IT assisted DigiNotar by:

- Mitigating the intrusion of the network and systems within it. This included monitoring the network traffic to determine if unauthorized activity was still taking place and giving advice in regard to firewall changes, changes in the infrastructure (disconnecting network segments), rebuilding servers in the DMZ, shutting down services, et cetera.
- Managing the trust of the certificate authority:
    - Initiating a change of the behavior of the OCSP responder to be based on a white list, effectively revoking any unknown certificate serial numbers;
    - Monitoring all OCSP requests for irregularities such as unknown certificate serial numbers, unusual senders or unusual volumes;
    - Investigating which and how many rogue certificates had been issued;
    - Determining the chance that the PKIoverheid environment had been breached.

From September 3,2011 onwards, after the ministry BZK had intervened, Fox-IT additionally assisted by:

- Determining the extent of the breach in DigiNotar's security and specifically if the CA servers that were used to issue qualified certificates and/or certificates for PKIoverheid had been compromised.
- Identifying evidence that could lead to the location and identity of the intruder. This was done by investigating the relevant servers, workstations and network equipment and by assisting the High Tech Crime team of the KLPD.
- Describing the lessons that can be learned from an incident such as the intrusion at DigiNotar.

The main strategy to accomplish the aims was to determine the extent to which servers within the DigiNotar network had been compromised and to identify IP addresses and other evidence that could provide more information about the intruder.

2.2.1 Incident response monitoring

One of the first measures taken by Fox-IT was to place an incident monitoring service in the form of a network sensor on the boundary of the DigiNotar network, to determine if unauthorized activity was still taking place. The sensor captures and monitors all traffic between the internal network and the Internet. Suspicious traffic is detected by the sensor using Intrusion Detection System (IDS) functionality. All

network traffic and flow data is stored on disk so that it can be evaluated afterwards if necessary. The Fox-IT monitoring service has a person on standby at all times to analyze all suspicious traffic in real time. Detected incidents can be escalated to administrators so that further actions can be taken, such as blocking an IP address or IP range, or changing the rules on the firewall for specific ports.

In this particular case, a tailored OCSP responder monitoring service was added to the incident response sensor on August 30, 2011. This addition included a custom sniffing service for logging OCSP requests and scripts that were written to check the OCSP logs against all valid certificates, to check if OCSP requests persisted for known rogue certificates and to detect serial numbers that were unknown and could correspond with rogue certificates. Also irregularities in volumes or originating IP addresses were checked for possible other MITM attacks. As a precautionary measure, any serial number presented to the OCSP responder that did not exist in the back office records was presumed to be invalid and the OCSP responder was set to answer that the serial had been revoked.

2.2.2 Safeguarding evidence

Forensically-sound disk images were created by Fox-IT of the systems that were prone to be compromised. Initially this process was restricted to the servers that hosted the CA software and the firewall management system that contained the firewall logs. At the request of the KLPD, the process was extended to include the creation of images of additional computer systems within DigiNotar's premises.

The disk images that were produced as evidence were numbered with the prefix SVO, which refers to "Stuk Van Overtuiging" (and translates to "evidentiary item"). References within this report to (images of) machines that can also serve as evidence will be made using the function of the server. Approximately 400 disk images were created of 265 systems amounting to a total of seven terabytes of compressed data.

In addition to manually safeguarding servers, an investigational infrastructure was set up using Encase Enterprise. This method provided the means to safeguard servers and workstations without shutting them down thus limiting the impact on the operation of the business. Encase Enterprise provided the means to do a live examination on the connected servers and workstations within DigiNotar's infrastructure. The live investigation was done in an iterative and forensically-sound manner. The infrastructure aided the researchers by allowing them to instantly follow up on their results and to perform further research. Most of the computer systems were still in use during the investigation, which had a negative effect on the overall progress of the investigation, as it slowed down the process of imaging the systems and resulted in the possibility that traces could be overwritten by a running process.

During the investigation, several servers were needed for the purpose of rebuilding a new production infrastructure. If these systems were not already secured they were secured manually before they were used in the new setup. The impact of this was that the systems that were reinstalled were not a part of the network anymore and therefore could not be investigated live. Two systems could not be shut down because of the critical function that they performed for the Dutch tax and customs administration and therefore were not safeguarded or investigated. Conforming to the wishes of the ministry BZK, the following systems were not safeguarded: all but one system in the co-location, approximately 40 workstations, the backup tapes and an unknown number of laptops[8].

[8] Since no complete administration could be presented of the equipment that was in use by DigiNotar.

3 State of affairs

3.1 Organization

DigiNotar B.V. was founded as a privately-owned notarial collaboration in 1998. The customer base of DigiNotar consisted of government institutions, profit and non-profit organizations and individual citizens. The company provided digital certificate services as a Trusted Third Party (TTP) and hosted a number of Certificate Authorities (CAs). Certificates that were issued by DigiNotar included SSL certificates used to secure websites, qualified certificates used to make legal digital signatures and government accredited certificates used by the Dutch government and its citizens. The government accredited 'PKIoverheid'-certificates were used for a wide range of critical eGovernment services in The Netherlands, such as a citizen authentication service, vehicle registration and real-estate registration. The bankruptcy of DigiNotar B.V. was declared by the court of Haarlem on September 20, 2011.

3.2 Services

DigiNotar hosted multiple Certificate Authorities and provided various services based on certificates. The most important Certificate Authorities that were hosted by DigiNotar were:

- *DigiNotar PKIoverheid CA Organisatie - G2*. This is one of the sub-CAs of the root "Staat der Nederlanden Root CA" (translates to "State of the Netherlands"), which was part of the PKIoverheid infrastructure. These certificates are used for organizations in their communication with the Dutch government.
- *DigiNotar Root CA*. The root certificate was in the trust list of several web browsers, operating systems and document readers.
- *DigiNotar Qualified CA*. This sub-CA of the DigiNotar Root CA was a registered authority and the qualified certificates that it issued could be used to legally sign documents on the basis of directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures.
- *DigiNotar Extended Validation CA*. This sub-CA of the DigiNotar Root CA could issue generally accepted EV-SSL certificates that are used to protect websites.

Several other sub-Certificate Authorities of the DigiNotar Root CA existed in the infrastructure of DigiNotar. Also, various other root certificates existed for various services. During the investigation a complete list of Certificate Authorities that were hosted by DigiNotar was created, which is included in Appendix VI.

3.3 Network infrastructure

In order to clarify the investigative results in chapters 4 through 8, a general overview of the network infrastructure is provided in this chapter. The overview of the network infrastructure and its normal operation is based on information that was provided by DigiNotar.

The DigiNotar network had two connections to the Internet that were provided by two different Internet Service Providers, one at the main location and one at the co-location. Behind the router that is responsible for Internet connectivity at the main location, a TippingPoint 50 Intrusion Prevention System (IPS) was present. The IPS was running a default configuration and was not used optimally, as it was placed in front of the firewall and consequently gave a lot of false positives. The IPS was planned to be placed behind the firewall. Behind the IPS the traffic was routed to a redundant Nokia firewall appliance, which was running Check Point Firewall-1 / VPN-1 (Check Point SecurePlatform NGX R65 HFA 50) with a separate management server. A third party assisted DigiNotar in operating the firewalls with support and technical fallback. A load balancer routed the traffic to the web servers.

A number of co-located servers were part of the network for the purpose of disaster recovery and business continuity. The co-located servers were not located in the same building or in a building near the main location.

Most of the systems in the DigiNotar network were running a Microsoft Windows operating system.

3.3.1 Network segments

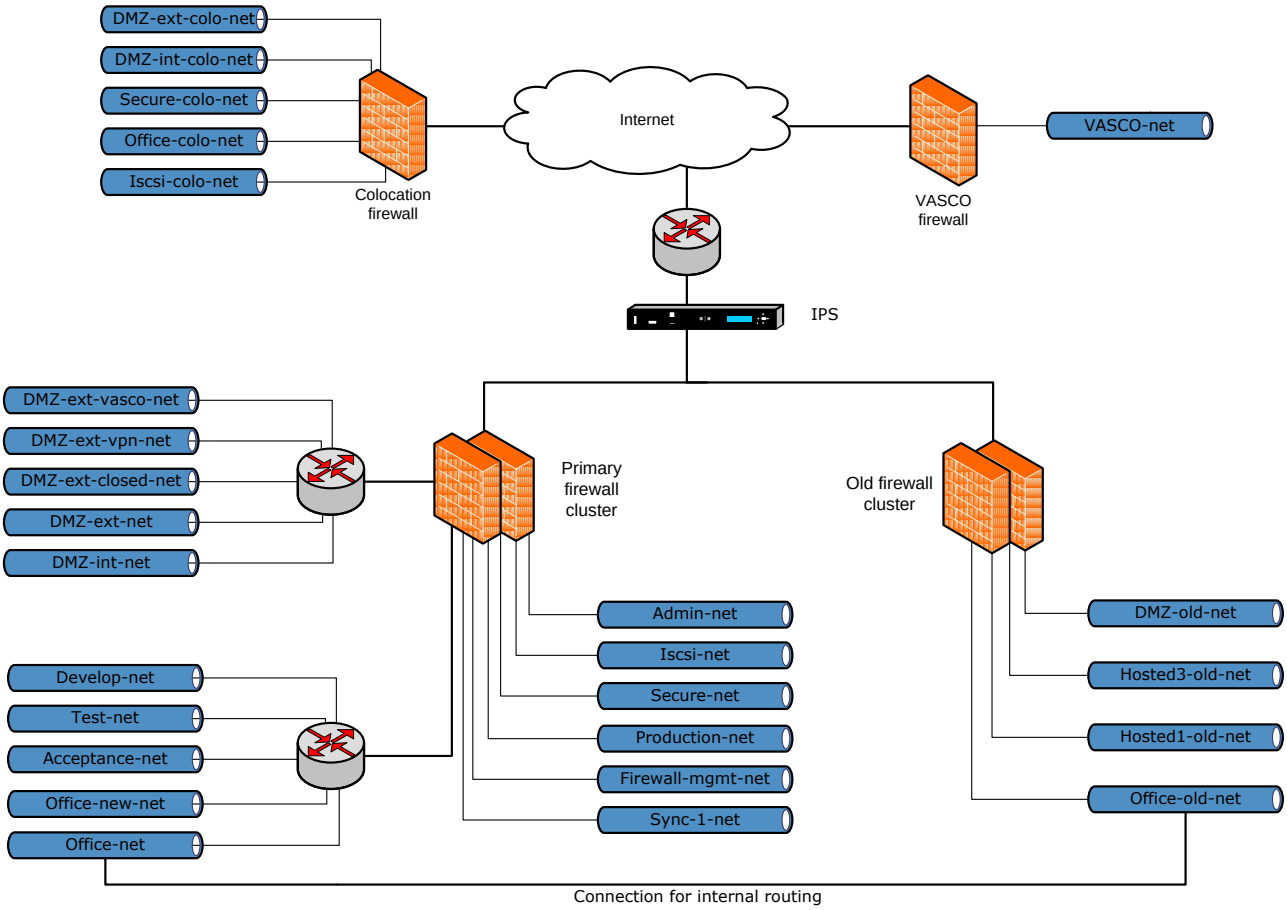


Figure 1 A sketch of the DigiNotar network[9]

The DigiNotar network was divided into 24 different internal network segments. The following list of segments was enforced, as extracted from the firewall settings on August 30.

Net name[10]	IP range	Description
DMZ-old-net	10.10.0.0/24	Old DMZ network
DMZ-ext-net	10.10.20.0/24	External DMZ network
DMZ-ext-closed-net	10.10.30.0/24	Closed external DMZ network
DMZ-ext-vpn-net	10.10.40.0/24	VPN network
DMZ-ext-vasco-net	10.10.50.0/24	Vasco external DMZ network
Production-net	10.10.110.0/24	Secure production network
DMZ-int-net	10.10.200.0/24	Internal DMZ network
Admin-net	10.10.210.0/24	Management network
Acceptance-net	10.10.230.0/24	Acceptance network
Test-net	10.10.240.0/24	Test network
Develop-net	10.10.250.0/24	Development network
Office-new-net	10.31.32.0/23	New office network
Vasco-net	10.32.0.0/16	Connection to the Vasco network
Iscsi-net	10.200.200.0/23	Internal ISCSI network
Iscsi-colo-net	10.200.202.0/23	Co-location - ISCSI DMZ network
Office-net	172.17.20.0/25	Office network and temporary network
Hosted1-old-net	172.17.20.128/28	Old ”hosted1” network

[9] Based on a drawing provided by DigiNotar. The exact lay-out of the layer-2 network (switches) in this sketch was not verified.
[10] Network segment name as it is used in this report.

Net name[10]	IP range	Description
Hosted3-old-net	172.17.20.160/28	Old "hosted3" network
Secure-net	172.18.20.0/24	Secure network locating the CAs and netHSMs
DMZ-ext-colo-net	172.25.20.0/24	Co-location – external DMZ network
DMZ-int-colo-net	172.26.20.0/24	Co-location – internal DMZ network
Secure-colo-net	172.27.20.0/24	Co-location – Secure network
Office-colo-net	172.28.20.0/24	Co-location – office network
Sync-1-net	192.168.1.0/29	First FireWall-1 synchronization network
Ext-net	62.58.35.96/28	External network addresses
Firewall-mgmt-net	62.58.74.128/27	Remote access for the management of the firewall

The construction of the network security zones corresponded with best practices as the following sketch depicts. A more detailed figure of the systems and network segments that are mentioned in this report is included in chapter 9.

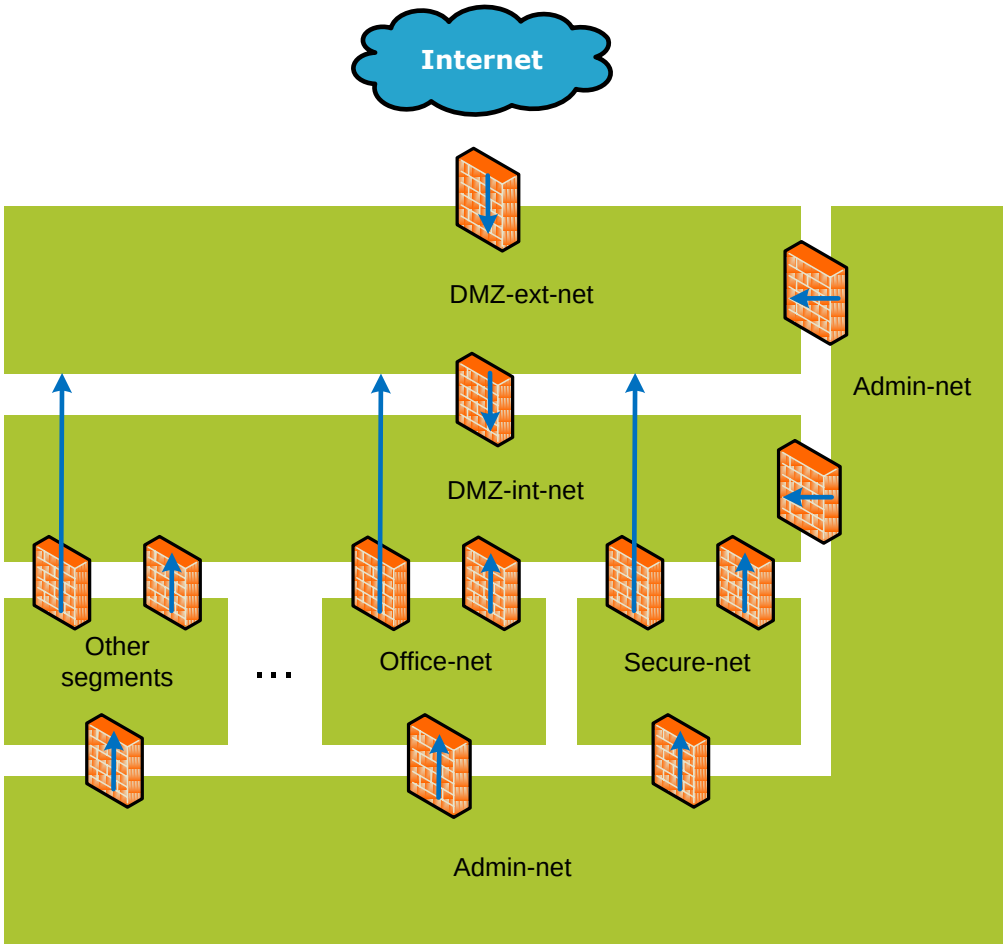


Figure 2 Network security zones

An internal and external DeMilitarized Zone (DMZ) prohibited direct connections between the Internet and the internal network. The firewall prohibited any connections initiated from DMZ-int-net to DMZ-ext-net as well as connections that were initiated from DMZ-int to Secure-net[11]. The administrators could access all the systems through remote desktop connections from their workstations, which were located in a room that was physically only accessible to administrators. Several exceptions existed in the firewall configuration for network traffic between the various segments[12].

[11] The description of the operation of the firewall is based on interviews with the administrators of DigiNotar.
[12] A total number of 156 rules existed in the firewall. Firewall rules influence the interconnections that are allowed and disallowed between zones.

3.3.2 Network operation

During normal operation, a customer requested a certificate on one of the websites running on a web server in the external DMZ (DMZ-ext-net). The request was then stored by the web server on a server in the internal DMZ (DMZ-int-net). These requests were periodically collected by a service in Secure-net. In the CAP (Control Application) administrative application, the request was stored and administrative procedures such as vetting were initiated.

When a request was approved using the four-eye principle, the request was marked as such in the database. Subsequently, an administrative employee logged onto a workstation running a DARPI client (*DigiNotar Abonnementen Registratie Production Interface*[13]) in a separate room and processed the request. Depending on the procedure, a private key was generated if it was not generated by the customer and a certificate request was sent to one of the CA servers. The CA software automatically signed the request and returned the certificate.

In order for the CA software to automatically sign the certificate request, the appropriate private key needed to be activated in the netHSM. This was done by authorized employees by entering a smartcard into the netHSM combined with a PIN code.

It was also possible for the CA operator to manually create certificates, for certificate requests that could not be processed by the DARPI application. In order to issue these certificates the CA operator had to log into the CA application with its smartcard, provided someone else had given the operator physical access to the secured room. After verification by another person the certificate was created.

The main servers and network devices of DigiNotar, including the CA servers and netHSM, were located in a physically highly-secured room at the main location. This room could be entered only if authorized personnel used a biometric hand recognition device and entered the correct PIN code. This inner room was protected by an outer room connected by a set of doors that opened dependent on each other creating a sluice. These sluice doors had to be separately opened with an electronic door card that was operated using a separate system than for any other door. To gain access to the outer room from a publicly accessible zone, another electronic door had to be opened with an electronic card.

Systems that needed the most protection were located in the Secure-net network segment. These systems included the servers that ran the CA management software, the "production" servers and the hardware security module that was accessible over the network (netHSM). The workstations and servers in this production network were used, among others, to initialize and personalize smartcards or other PKI tokens, issue certificates and create PIN letters. These production workstations could access the back-end records in Office-net as well as the CA servers in Secure-net. The custom applications used for production are called CAP, DARPI and BAPI (*Belastingdienst*[14] *Advanced Program Integration*) and were all developed in-house.

The CA management software that ran on the CA servers connected over the network to the netHSMs, where the private keys of the Certificate Authorities were stored in encrypted form. At the main location, at least eight CA servers were present, including one test CA server and one root CA server. At the co-location, seven redundant (virtual) CA servers were located for the purpose of business continuity[15]. In total DigiNotar used four netHSMs, one of which was in the secure segment for the CAs, a second in the internal DMZ (DMZ-int) for the "Parelsnoer" service, a third in the test environment and the fourth in the co-located secure network segment (Secure-colo-net).

3.3.3 Internet connectivity

For the purpose of the investigation, it was helpful to know how DigiNotar was connected to the Internet. Although no exhaustive inventory was made, it became clear during the investigation that many websites were hosted by DigiNotar. A survey was made of the connection to the Internet.

[13] Translates to "Subscription Registration Production Interface".
[14] The Dutch tax and customs administration.
[15] The systems were on 'warm' standby; the servers were switched on and backups were stored there on a regular basis.

3.3.3.1 Registered Internet IP addresses

The following IP address ranges were identified to be used by DigiNotar:

IP start	IP end	net name
62.58.35.96	62.58.35.111	TELE2-CUST-DIGINOTAR-BV
62.58.36.112	62.58.36.127	VERSATEL-CUST-Diginotar-B-Vx
62.58.44.96	62.58.44.127	VERSATEL-CUST-Diginotar-B-Vx
81.58.241.160	81.58.241.175	VERSATEL-CUST-Diginotar-B-Vx
87.213.105.80	87.213.105.95	TELE2-CUST-Diginotar
87.213.114.0	87.213.114.15	VERSATEL-CUST-Diginotar-B-Vx
87.213.114.160	87.213.114.191	VERSATEL-CUST-Diginotar-B-Vx
143.177.3.40	143.177.3.47	-
143.177.11.0	143.177.11.15	-
193.173.36.32	193.173.36.47	OTS25849

3.3.3.2 Web service scan

During a service scan performed by Fox-IT on September 14, 2011, a long list of servers were identified as accessible from the Internet.

IP address	Port 80 HTTP	Port 443 HTTPS
62.58.35.107	X	X
62.58.36.113	X	X
62.58.36.116	X	X
62.58.36.117	X	X
62.58.36.118	X	X
62.58.36.119	X	X
62.58.36.121	X	X
62.58.36.122	X	X
62.58.36.123		X
62.58.36.124		X
62.58.36.125	X	X
62.58.36.126	X	X
62.58.36.127	X	X
62.58.44.96	X	X
62.58.44.97	X	X
62.58.44.98	X	X
62.58.44.99	X	X
62.58.44.100		X
62.58.44.102	X	X
62.58.44.103	X	X
62.58.44.104	X	X
62.58.44.105	X	
62.58.44.107	X	X
62.58.44.109	X	X
62.58.44.110		X
62.58.44.112	X	X
62.58.44.113	X	X
62.58.44.114	X	X
62.58.44.118	X	X

IP address	Port 80 HTTP	Port 443 HTTPS
62.58.44.119	X	X
62.58.44.121	X	X
62.58.44.123	X	X
62.58.44.125	X	X
62.58.44.126	X	X
62.58.44.127	X	X
81.58.241.160	X	X
81.58.241.161	X	X
81.58.241.162	X	
81.58.241.163	X	X
81.58.241.164	X	
81.58.241.165	X	X
81.58.241.167	X	X
81.58.241.168	X	X
81.58.241.171	X	X
81.58.241.172	X	X
81.58.241.173	X	X
81.58.241.174	X	X
81.58.241.175	X	
87.213.105.80	X	
87.213.105.81	X	X
87.213.105.82	X	
87.213.105.83	X	
87.213.105.84	X	
87.213.105.85	X	
87.213.105.87	X	X
87.213.105.89	X	
87.213.105.90	X	X
87.213.105.91	X	X

IP address	Port 80 HTTP	Port 443 HTTPS
87.213.105.92		
87.213.105.93	X	
87.213.105.94	X	X
87.213.105.95	X	X
87.213.114.3	X	X
87.213.114.4	X	X
87.213.114.5	X	X
143.177.3.40	X	X
143.177.3.41		X
143.177.3.44	X	X
143.177.3.45	X	
143.177.3.46	X	
143.177.3.47	X	X
143.177.11.1	X	X
143.177.11.2	X	
143.177.11.3	X	X
143.177.11.4	X	
143.177.11.5	X	X
143.177.11.6	X	X
143.177.11.7	X	X
143.177.11.8	X	X
143.177.11.9	X	
143.177.11.10	X	X
143.177.11.11	X	X
143.177.11.12	X	
143.177.11.14	X	X
143.177.11.15	X	X

A DNS query of the IP addresses that were used (among others) showed the following entries:

IP address	DNS lookup
62.58.36.114	mailhost.diginotar.nl
62.58.36.116	mail.diginea.nl
62.58.36.118	www.diginotar.nl
62.58.36.120	authenticatie.pass.nl
62.58.36.121	belastingdienst.diginotar.nl
62.58.36.125	service.diginotar.nl

IP address	DNS lookup
62.58.36.126	Registratie.diginotar.nl
62.58.44.107	digi01.mailwitness.net
62.58.44.108	digibackup.mailwitness.net evssl.diginotar.nl
62.58.44.109	sha2.diginotar.nl
62.58.44.111	ftp.diginotar.nl
62.58.44.113	www.evssl.nl
62.58.44.116	genghini.mailwitness.net
62.58.44.121	danka.mailwitness.net
62.58.44.122	bgg.mailwitness.net
62.58.44.123	diginotar.mailwitness.net
62.58.44.124	test.pass.nl
62.58.44.125	*.diginotar.com diginotar.com diginotar.net
143.177.3.41	mailhost1.diginotar.nl mail.digifactuur.nl mail.diginotar.com
143.177.3.42	directory.diginotar.nl
143.177.3.43	www.servicecentrum.diginotar.nl
143.177.3.45	validation.diginotar.nl
143.177.11.2	servicecenter.diginotar.nl
143.177.11.4	demonstratie.pass.nl
143.177.11.10	onlineaanvraag.diginotar.nl
143.177.11.11	www.pass.nl
193.173.36.36	ns1.diginotar.nl
193.173.36.39	mailhostuw.diginotar.nl

Additionally, a service scan showed a number of noteworthy services:

IP address	Service
62.58.44.111 (ftp.diginotar.nl)	FTP server
87.213.105.92 (port 8888)	Web server
62.58.35.108, 62.58.35.109 & 62.58.35.110	VPN server
62.58.36.114	Mail server
87.213.114.2	DNS server

3.3.3.3 Web server configuration

From some of the web servers that were present in DMZ-ext-net, the following internal IP addresses were extracted from their configuration.

Server	Internal IP	Site name
Main-web server	10.10.20.11	Notarisgombert.nl
	10.10.20.14	Darwizard
	10.10.20.28	evssl.diginotar.nl
	10.10.20.41	DigiNotar.nl
	10.10.20.46	www.evssl.nl
	10.10.20.58	DigiNotar.com
	10.10.20.61	OCSPclient
	10.10.20.69	sha2.diginotar.nl
	10.10.20.73	BapiOphalen
	10.10.20.97	Bapiviewer
Docproof1 server	10.10.20.37	Docproof
Docproof2 server	10.10.20.65	Docproof
Pass-web server	10.10.20.16	PassWeb - PASS15
	10.10.20.40	NTP
	10.10.20.35	TIM_tim.diginotar.nl

Server	Internal IP	Site name
Soap-signing web server	10.10.20.98	SS_Provincie-Utrecht.signing.diginotar.nl
	10.10.20.129	SS_Gelderland.signing.diginotar.nl
	10.10.20.42	TimeStampServer
	10.10.20.92	SoapSigning
	10.10.20.84	SS_Lelystad.Signing.diginotar.nl
	10.10.20.85	SS_Waterschapdedommel.signing.diginotar.nl
	10.10.20.86	SS_Signing.diginotar.nl
	10.10.20.137	DigiDownload
	10.10.20.87	SS_Teylingen.signing.diginotar.nl
	10.10.20.88	SS_PZH.signing.diginotar.nl
	10.10.20.89	SS_sintanthonis.signing.diginotar.nl
	10.10.20.130	SS_Leeuwarden.Signing.diginotar.nl
	10.10.20.90	SS_PNB.signing.diginotar.nl
	10.10.20.91	SS_Leiderdorp.Signing.diginotar.nl
	10.10.20.99	SS_Drenthe.Signing.diginotar.nl
	10.10.20.93	SS_Overijssel.Signing.diginotar.nl
Main-web-new[16]	10.10.20.172	evssl.diginotar.nl
	10.10.20.164	BapiViewer
	10.10.20.165	DarWizard
	10.10.20.182	bct.csp.minienm.nl
	10.10.20.173	www.diginotar.com
	10.10.20.167	OCSPClient
	10.10.20.174	service.diginotar.nl
	10.10.20.169	BapiOphalenCert
	10.10.20.183	test.bct.csp.minienm.nl
	10.10.20.175	www.evssl.nl
	10.10.20.158	www.diginotar.nl www.diginotar.com diginotar.com diginotar.nl www.evssl.nl evssl.diginotar.nl
	10.10.20.184	test.csp.minienm.nl
	10.10.20.181	csp.minienm.nl
	10.10.20.176	sha2.diginotar.nl

[16] Main-web server was replaced by Main-web-new: the first firewall entries of 10.10.20.158 from the main-web-new server appeared on July 18, 2011. Logs of the old Main-web server showed activity up until August 1, 2011. More details are included in Chapter 4.

4 Investigation of web server log files

During the initial incident response investigation that was performed before the involvement of Fox-IT, it was identified that at least two web servers were running outdated versions of the DotNetNuke software. There are known security vulnerabilities in these outdated versions of the DotNetNuke software and the initial incident response investigation concluded that these vulnerabilities had been exploited to gain first entry into DigiNotar's network.

These compromised web servers were used by the intruder as stepping stones to transfer data and tools between DigiNotar's internal network and the Internet. Both the Main-web and Docproof2 web servers were investigated in order to examine what files and tools were transferred and what internal and external systems had connected to these compromised systems in DMZ-ext-net.

4.1 Sources

After a crash of the main web server of DigiNotar, an employee of DigiNotar found evidence that the Main-web server had been compromised. A new web server was installed on other hardware using an old backup, which left the data of the compromised web server, including the log files up to August 1, 2011, intact for further investigation.

During the incident response investigation by Fox-IT on the Taxi-CA and Qualified-CA servers, evidence was found indicating that these systems had connected to a specific file (`settings.aspx`) on the Main-web server that acted as a rudimentary file manager, among other things. With this file manager the directory `/beurs` could be used to store and exchange hacking tools and other unauthorized files. Other investigated systems within the network later showed cached web pages originating from this directory, as detailed in Chapter 7. A sample of a cached version of `settings.aspx` is shown below.

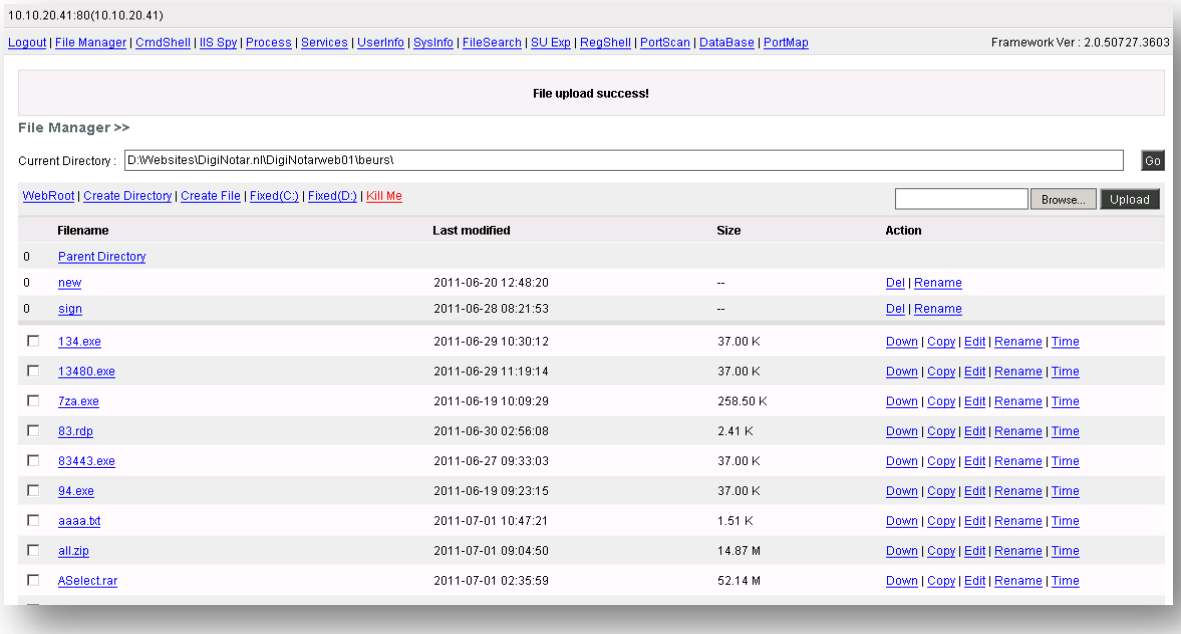


Figure 3 A sample of a cached version of `settings.aspx`

4.2 Web server log file analysis

The directory `/beurs` was located on the Main-web server at `D:\Websites\DigiNotar.nl\DigiNotarweb01\beurs` and was available internally at `http://10.10.20.41/beurs` and publicly at `http://www.diginotar.nl/beurs`. When the directory `/beurs` was examined, no files were present in the disk image, but the evidence on Taxi-CA and Qualified-CA servers indicated that files had indeed been present in this directory (see paragraph 7.2.2).

The Microsoft IIS log files of the Main-web server were subsequently examined in order to determine which internal and external systems had made a connection to the directory `/beurs` including all files in that directory. The log files were stored in `C:\WINDOWS\system32\LogFiles\W3SVC1062701327\` and `C:\Data\Websites\Logging\W3SVC1062701327\` and were named `EX<YYMMDD>.log`. The timestamps in the logs are based on Coordinated Universal Time (UTC) and the time deviation of the server was minimal. The log files have the following format:[17]

```
2011-07-11 00:30:48 W3SVC1062701327 10.10.20.41 GET /beurs/settings.aspx - 80 -
aaa.bbb.ccc.ddd Mozilla/5.0+(Windows+NT+6.1;+rv:2.0.1)
+Gecko/20100101+Firefox/4.0.1 200 0 0
```

In a log entry such as the one above, one can distinguish when a system identifiable by its IP address (`aaa.bbb.ccc.ddd`) made a connection to the Main-web server (10.10.20.41) and which operating system and browser were most likely used to do so (`Mozilla/5.0+(Windows+NT+6.1;+rv:2.0.1`). Furthermore, one can distinguish the request that was performed (`GET /beurs/settings.aspx`) and the web server's response to this request (status OK: `200`).

During the incident response investigation, it became clear that a number of log files were missing, which included log files from the period around the intrusion. More specifically, access log files for the period up to July 11, 2011 had been removed from the Main-web server. However, the error logs in the `HTTPERR` directory were still present on the Main-web server and contained entries prior to July 11, 2011. According to DigiNotar, the log files were most likely deleted by an administrator of DigiNotar during an incident where the available space on the hard disk was filled by large log files. According to DigiNotar, the files were deleted after a brief inspection that showed no remarkable entries.

The files `Default.aspx` and `old_Default.aspx` that had originally been located in the `/beurs` directory were recovered in a backup that was made on August 27, 2009 and which was located at `D:\Websites\BackUp\Diginotar01.old`. This could mean that the `/beurs` directory had been inactive for a while, which may have been a reason to use this directory, as well as that it may have been emptied by the intruder.

4.3 Results

Since the removed log files had partially been overwritten, recovery software could not be used. Therefore a pattern matching text search was performed on the entire disk image searching for log entries that contained `/beurs`. This method recovered 1,583 log entries. It showed that uploading a file to the web server was done with a post-request to the `aspx` script, and downloading a file could be done by connecting to the `/beurs` directory. The scripts `settings.aspx` and `up.aspx` were used to upload files. The recovered logs revealed a list of internal and external IP addresses that had connected to the `/beurs` directory, which was used as a stepping stone.

4.3.1 Internal systems

Based on entries in the log files, the following 13 internal systems could be identified as having connected to the `/beurs` directory on the compromised Main-web server.

Network	Server
DMZ-int-net	Docproof-db
Office-net	BAPI-db
	Production121
	Squid-proxy server
	Office-file
Secure-net	CAP-app-web
	CAP-app-db
	Relation-CA

[17] More details can be found at Microsoft Technet, "W3C Extended Log File Format (IIS 6.0)" at http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/iis/676400bc-8969-4aa7-851a-9319490a9bbb.mspx

Network	Server
	Public-CA
	CCV-CA
	Root-CA
	Qualified-CA
	Taxi-CA

All the internal systems that had connected to the `/beurs` directory, which was used as a stepping stone by the intruder during the intrusion, should be regarded as compromised unless specific evidence would indicate otherwise. This was the case for Squid-proxy, which was probably not compromised but used as a proxy by other machines in the Office-net.

It was noticed that the connections from the Public-CA server to the script `up.asxp` showed a regular pattern of connections.

4.3.2 External IP addresses

The IP addresses of external systems that had accessed the directory `/beurs` were likely to have been utilized by the intruder and are included in Appendix II (referenced as AttIPxx). This list of IP addresses is not exhaustive, as a number of log files had been removed, were overwritten, and were beyond recovery. In total, 26 unique external IP addresses were identified during the investigation of the web server log files.

Some of these IP addresses were probably not related to the intruder. For example, requests from four different IP addresses originating from the Netherlands and Belgium were only seen during the internal incident response investigation that started on July 19, 2011. Another IP address resolved to a Googlebot web crawler and was therefore excluded. The remaining 21 IP addresses were suspicious and were probably utilized by the attacker, because files were up or downloaded and the `aspx`-scripts were used by these IPs. Results from other parts of the investigation also point to seven of these IP addresses that are referenced as AttIP3, AttIP4, AttIP5, AttIP6, AttIP13, AttIP19 and AttIP22.

4.3.3 Suspicious files

From the results of pattern matching text searches, a list of files was composed that had been present in the directory `/beurs` of the Main-web server over time. The following list of 125 files is not exhaustive, as a number of log files appear to have been removed and overwritten and were beyond recovery.

File name	File name	File name	File name
aaaa.txt	darv28.exe	ids.zip	saerts.zip.part3.txt
all.zip	darv28.zip	jobdone.zip	saerts.zip.part4.txt
asdasd.zip	darv29.zip	keo.zip	settings
aselect.rar	darv3.zip	last.zip	Settings.aspx
bapi.zip	darv30.zip	lastdb.zip	settings.aspx
beurs.aspx	darv31.zip	lb.msi	settings.zip
bin.zip	darv33.zip	ldap.msi	sms.msi
c.zip	darv34.exe	ldap.msi	SQLServer2005_SSMSEE.msi
cachedump.exe	darv34.zip	md5s.txt	ssl.zip
certcontainer.dll	darv35.zip	mimi.zip mohem.zip	tijdstempel.pfx
code.zip	darv36.zip	mswinsck.ocx	Troj25.exe
csign.zip	darv37.zip	msxml6.msi	twitter.zip
dar.rar	darv38.zip	nc.exe	up.aspx
dar.zip	darv4.zip	newjob.zip	USBDeview.exe
darpi.zip	darv5.zip	nfast.zip	validate.zip
darv11.zip	darv6.zip	nssl.zip	vcredist_x86.exe
darv12.zip	darv7.zip	origrsa.zip	webapp.zip
darv13.zip	darv8.zip	passadmin.rar	websign.rar
darv15.zip	darv9.zip	pki.zip	win.exe
darv16.zip	data.zip	PortQry.exe	win2.exe
darv17.zip	dbpub.zip	psexec.exe	win3.exe
darv18.zip	Default.aspx	putty.exe	z3.exe
darv19.zip	Depends.exe	PwDump.exe	z4.exe
darv20.zip	depends.exe	qualifieddata.zip	z5.exe
darv21.zip	DigiNotar_Services_CA.cer	Read1.exe	Zip2.exe
darv22.zip	direct.exe	Read2.exe	zip3.exe
darv23.zip	direct.zip	Read3.exe	zipped.zip
darv24.exe	direct83.exe	Repositories.zip	Zipper.exe
darv24.zip	elm.zip	rsa_cm_68.zip	
darv25.zip	ev-add.zip	rsaservice.rar	
darv26.zip	f1.cer	saerts.zip.part1.txt	
darv27.zip	final.zip	saerts.zip.part2.txt	

Some of these names are related to internally used names. For example:

- A-select is a service provided by DigiNotar
- BAPI is an administration application for the Dutch tax administration
- DAR is the administration application hosting all customers information (*DigiNotar Abonnementen Registratie*)
- Qualified is the name of one of the CA servers (Qualified-CA)
- Public (pub) is the name of another CA server (Public-CA)
- rsa_cm_68 is the directory where the CA management software is installed on the CA servers

4.3.4 Noteworthy log entries

In the access logs of the Main-web server a remarkable piece of evidence was found.

```
2011-07-24 13:16:48 10.10.20.41 GET /settings.aspx - 80 – AttIP3
      Mozilla/5.0+(Windows+NT+5.1;+rv:5.0)+Gecko/20100101+Firefox/5.0
2011-07-24 13:16:53 10.10.20.41 POST /settings.aspx - 80 – AttIP4
      Mozilla/5.0+(Windows+NT+5.1;+rv:5.0)+Gecko/20100101+Firefox/5.0
```

The entries in the log files indicate that the intruder regularly used the proxy on AttIP4 to connect to the stepping stone in order to obscure his identity. It appears that the intruder erroneously connected to the stepping stone without using the proxy on AttIP4 (possibly in a proxy chain) which revealed AttIP3. Five seconds later the error was corrected and the request was repeated using the proxy on AttIP4. AttIP3 had previously been used to test the OCSP response for a rogue Yahoo certificate that had been issued by DigiNotar. AttIP3 resolved to a DSL user in the Islamic Republic of Iran (see also paragraph 10.2.2).

4.4 Conclusion

Some of the incriminating files and logs were deleted from the Main-web server by DigiNotar, by the intruder or by an automated process. However, by searching through the images of the entire disk the remains of deleted web server access log entries were found. Additionally, error log files were present on the Main-web server and log files were present on the Docproof2 server. From these log entries, a list of IP addresses that had connected to the directory `/beurs`, which was used as a stepping stone, was generated. Of the internal systems that were found to have connected to this directory and the corresponding script, 12 were most likely compromised by the intruder. A total of 125 file names were extracted, which were copied to or from the stepping stones.

Moreover, the log entries that were recovered produced a list of 26 external IP addresses that had been used to connect to the Main-web server stepping stone. On this basis of this part of the investigation, Fox-IT deems it very likely that 21 of these IP addresses were (ab)used by the intruder. The vast majority of these IP addresses were most likely used as a proxy to obscure the identity of the intruder, but the true IP address of the intruder may have been revealed by error. All these IP addresses were handed over to the KLPD.

5 Investigation of firewall log files

Within DigiNotar's infrastructure there was a central position for the firewall. The firewall was configured so that all violations of firewall rules as well as all the accepted traffic connections were logged, which resulted in up to 2 million log entries per day. The large amount of log data that was generated has great potential for tracing the intruder's steps, even though data mining on such a large amount of data is time intensive.

The firewall was only able to log connections between the network segments that it segregated. Traffic within a segment was not logged by the firewall, with the exception of traffic that had the firewall as its destination.

5.1 Sources

A Check Point appliance on a redundant Nokia IP390 platform with a separate management server was used as the firewall within the main infrastructure. A previously-used redundant Sun firewall platform was also present in the network. At the co-location, another Check Point firewall based on a Nokia appliance platform was present.

Fox-IT created a forensic image of the disk of the firewall management server located at the main location. In our forensic lab, a copy of the disk image was virtualized and the management station was accessed using the Check Point SmartConsole software. The log files were exported for further processing and examination.

For the purpose of this investigation, the traffic logs were of primary interest. The traffic logs contain the following fields:

- Timestamp
- Action (accept / drop / reject / encrypt / decrypt / keyinst)
- Firewall interface name and traffic direction
- Firewall rule (name, ID and number)
- Source and destination IP and port
- Protocol
- ICMP (code and type)
- NAT (rule number, translated IP / port)
- DNS query
- VPN (scheme, method, peer gateway)
- TCP out of state, flags
- IPSec specification
- Attack details

The timestamps of the firewall logs are based on Central European (Summer) Time (CEST).

5.2 Log file analysis

Not all the fields in the log files were relevant for the investigation. Only the source and destination IP addresses, port numbers and the "accept" and "drop" actions were used. The investigated log files date from May 31, 2011 at 23:51:57 up to July 31, 2011 at 23:51:36 and contain a total of 112,840,345 records. Logs that date back further were also available but were irrelevant for the purpose of this investigation.

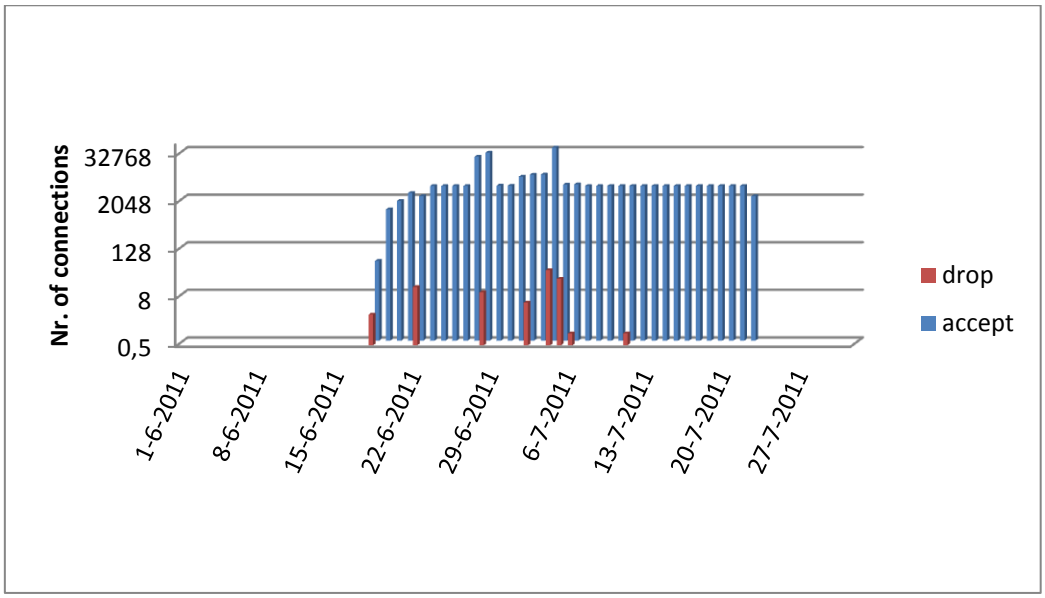
The approach for the analysis of the firewall logs was based on the results of the investigation performed on other exhibits. The search for anomalies was guided by the expertise of the investigators and the situation at hand. The degree of certainty in which the identified anomalies can be linked to the intruder on the basis of the firewall log files alone varies. Anomalies that cannot conclusively be connected to the intruder are included in paragraph 5.2.8.

5.2.1 Connections from internal IPs to AttIPs

During the investigation, a list of external IP addresses that were suspected to have been used by the intruder was created. This list was based on the web server log files that the intruder used as a stepping stone (as described in paragraph 4.3.2) and the IP addresses that were found in the tools that were left

by the intruder (as described in Chapter 7). The complete list of these IP addresses is included in Appendix II.

On June 18, 2011 connections started to appear that were initiated from systems with internal IP addresses of DigiNotar to the suspected intruder's IP addresses. The log entries with source IP addresses in the ranges 10.0.0.0/8 and 172.16.0.0/12 to the intruders IP addresses in the firewall log files are visualized in the following graph.[18]



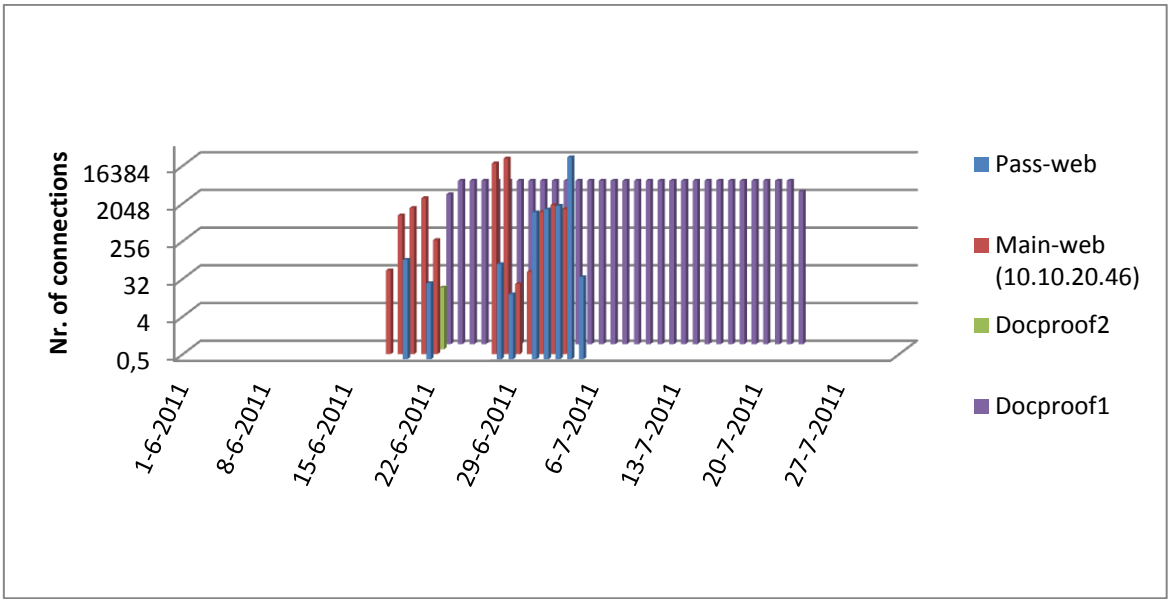
Internal IPs → suspicious intruder IPs

The data indicates that the first connections back to the intruder were established from two machines in the external DMZ network (DMZ-ext-net), namely the Main-web and Docproof1 web servers. The last connection back to the suspicious intruder IP addresses occurred on July 22, 2011. This part of the investigation also showed that successful connections only took place from internal IP address to AttIP1, AttIP2, AttIP19 and AttIP22. Additionally, unsuccessful connections (dropped by the firewall) were attempted to AttIP13.

5.2.2 Tunnels from DMZ-ext-net to AttIP1

Early on in the investigation, a tool was identified that had been created by the intruder which contained an external IP address used by the intruder (AttIP1). It was then discovered that connections from the ext-DMZ-net to this IP address had taken place. Based on entries in the log files, it was examined if other connections from DMZ-ext-net to this specific IP address could be found.

[18] Please note the use of a logarithmic scale. This scale is used to emphasize the occurrence of the connections rather than the number of connections. One bar indicates the connections of one day.

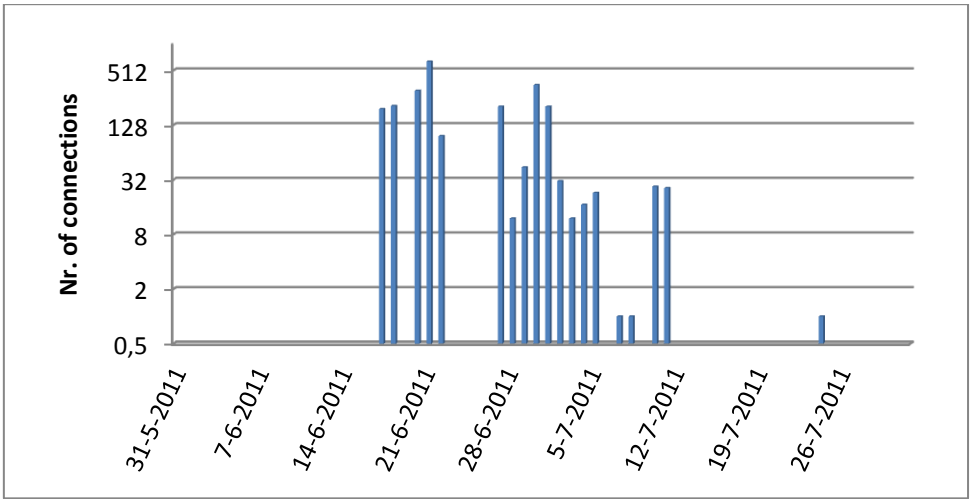


Web servers → AttIP1 port 443

This showed that at least 4 servers in DMZ-ext-net had connected back to the intruder since June 18, 2011. It also showed a regular pattern for the connections between the Docproof1 server and AttIP1.

5.2.3 Access to Office-net

As of June 17, 2011 at 11:28, accepted connections started to appear between the Main-web server and the BAPI-db server on port 1433, which is used for the Microsoft SQL service.



Main-web (10.10.20.46) → BAPI-db on port 1433

This indicated that the firewall accepted connections on this port between DMZ-ext-net and Office-net, but that no such connection had taken place between June 1, 2011 and June 16, 2011. The identified traffic from June 17, 2011 onwards indicated that the MSSQL database server on BAPI-db was probed from Main-web. This activity matched with a file that was identified on the Main-web server which contained a string with credentials to access the database on BAPI-db (see paragraph 7.3).

5.2.4 Tunnels from Office-net

A number of tools that were left by the intruder were used to create network tunnels (see also paragraph 7.2.3). These tunnels were setup between an internal server (TCP port 3389) and a server in the DMZ-ext segment (TCP port 443). Port 3389 indicates that the tunnels were used to tunnel Terminal Services or Remote Desktop Protocol (RDP) traffic. Port 443, which is generally used for HTTPS, was utilized so

that the traffic could pass through the firewall. Analysis of the traffic log files of the firewall showed that these tunnels had been used.

File name	troj134.exe
Connect from	BAPI-db server
Connect to	eHerkenning-AD server
Connections	

Date	Nr. of log entries
2011-06-30	74522
2011-07-01	124510
2011-07-02	26351
2011-07-03	49021
2011-07-04	530
2011-07-05	11

File name	troj172.exe
Connect from	BAPI-db server
Connect to	Pass-web server
Connections	

Date	Nr. of log entries
2011-06-29	1

File name	troj25.exe
Connect from	Source-build server
Connect to	eHerkenning-AD server
Connections	None were found

Although a tool was found to tunnel remote desktop traffic, no conclusions can be drawn that the Source-build was compromised. Also, the investigation of the firewall logs showed no connections of this tunnel.

The tunnels allowed the intruder to connect to a remote desktop service on systems in the Office-net segment. The data showed that the intruder had created tunnels to access systems in the Office-net on and after June 29, 2011.

5.2.5 Access to Secure-net

The earliest suspicious traffic identified from the Secure-net was encountered when traffic from Secure-net with destination port 80 was examined. The following extraordinary log entries were identified:

```
2011-07-01 01:16:36 - drop - [tcp] 172.18.20.230:2404 -> 172.18.20.2:80
2011-07-01 01:16:39 - drop - [tcp] 172.18.20.230:2404 -> 172.18.20.2:80
2011-07-01 01:16:45 - drop - [tcp] 172.18.20.230:2404 -> 172.18.20.2:80
2011-07-01 01:17:07 - drop - [tcp] 172.18.20.230:2408 -> 172.18.20.2:80
2011-07-01 01:17:10 - drop - [tcp] 172.18.20.230:2408 -> 172.18.20.2:80
2011-07-01 01:17:16 - drop - [tcp] 172.18.20.230:2408 -> 172.18.20.2:80
2011-07-01 01:18:04 - drop - [tcp] 172.18.20.230:2422 -> 172.18.20.2:80
2011-07-01 01:18:07 - drop - [tcp] 172.18.20.230:2422 -> 172.18.20.2:80
2011-07-01 01:18:13 - drop - [tcp] 172.18.20.230:2422 -> 172.18.20.2:80
2011-07-01 01:19:28 - drop - [tcp] 172.18.20.230:2436 -> 172.18.20.2:80
2011-07-01 01:19:31 - drop - [tcp] 172.18.20.230:2436 -> 172.18.20.2:80
2011-07-01 01:19:37 - drop - [tcp] 172.18.20.230:2436 -> 172.18.20.2:80
2011-07-01 01:20:10 - drop - [tcp] 172.18.20.230:2446 -> 172.18.20.2:80
2011-07-01 01:20:13 - drop - [tcp] 172.18.20.230:2446 -> 172.18.20.2:80
2011-07-01 01:20:19 - drop - [tcp] 172.18.20.230:2446 -> 172.18.20.2:80
```

The entries concern traffic within the Secure-net segment, but which was still logged by the firewall. The reason for this is that the destination IP (172.18.20.2) is the firewall itself. The earliest suspicious log entry from the secure network segment occurred on July 1, 2011 at 01:16 CEST. About an hour later, more dropped traffic to ports 139, 443 and 445 on the firewall IP was logged originating from 172.18.20.230 (the BAPI-production workstation).

This led to the presumption that the intruder first entered the Secure-net segment on the BAPI-production workstation and then conducted a port scan on ports 80, 139, 443 and 445 within the subnet, which included the firewall and thus resulted in the aforementioned log entries.

5.2.6 Tunnels from Secure-net

Servers located in DMZ-ext-net acted as an intermediate hop or stepping stone between the internal network of DigiNotar and the Internet. For this purpose the intruder used tunnels through port 443 that allowed him to connect to servers that were not directly connected to the Internet.

All traffic originating from Secure-net to other network segments on port 443 was examined. This resulted in 3,062 logged traffic connections. The majority of these connections (2,970) originated from CAP-app-web and CAP-web server to the cluster address Cluster-prodpass in DMZ-ext-net. This traffic occurred before and after the intrusion and was probably ordinary traffic.

When this traffic is ignored, it leaves 92 traffic connections out of the original 3,062 that were further investigated. Out of these 92 connections, 54 relate to blocked traffic that originated from Public-CA server on July 4, 2011 between 03:25 and 04:42. The blocked traffic was intended for the following IPs:

- AttIP1:443 (see Appendix II);
- Pass-web server;
- Docproof1 web server;
- 10.10.2.139:443 (not in the server list - presumably a typing error made by the intruder).

Due to the unusual time that these attempts occurred, it was safe to assume that the intruder had access to the Public-CA server at this time.

The remaining 38 of the 92 connections that were further investigated relate to accepted traffic. These log entries show that direct connections were made from the Secure-net segment to the DMZ-ext-net segment:

From	To	Nr. of conn.
CAP-app-db server	Main-web server	5
Relations-CA server	Main-web server	2
Public-CA server	eHerkenning-AD	15
Public-CA server	eHerkenning-HM	7
Public-CA server	Pass-web	3
Public-CA server	Main-web server	2
CCV-CA server	Main-web server	2
Taxi-CA server	Main-web server	2

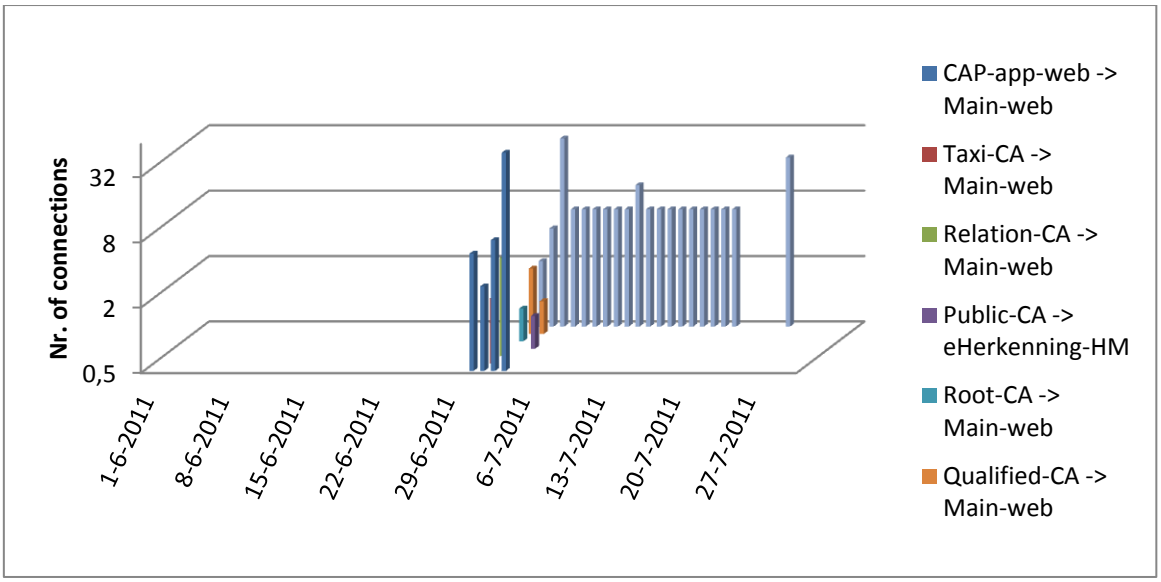
This confirmed that suspicious connections from Secure-net to DMZ-ext-net took place as of on July 2, 2011 at 06:40:44. Further investigation could conclusively establish if this traffic is related to the intruder.

5.2.7 Access to stepping stone from Secure-net

When all traffic originating from Secure-net to DMZ-ext-net was examined it was noticed that connections over port 80 were accepted by the firewall. When ordinary traffic that also occurred before the intrusion was eliminated, the following suspicious traffic remained:

From	To	Nr. Of conn.
CAP-app-web server	Main-web server port 80	68
Relation-CA server	Main-web server port 80	4
Public-CA server	eHerkenning-HM server port 80	1
Public-CA server	Main-web server port 80	151
Root-CA server	Main-web server port 80	1
Qualified-CA server	Main-web server port 80	3
Taxi-CA server	Main-web server port 80	2

Over time this could be visualized as follows:



Abnormal connections Secure-net → DMZ-ext-net port 80

The investigation showed that on July 1, 2011 at 22:52, the first successful connection was made from the Secure-net (the CAP-app-web server) to one of the compromised stepping stone servers. The investigation also showed that on July 2, 2011 at 00:14:14, the first connection from a CA server (Taxi-CA) to the Main-web took place.

Another noticeable anomaly consisted of a regular connection pattern between Public-CA server and the Main-web stepping stone server. From July 4, 2011 to July 7, 2011, daily connections took place at 15:09:36, 18:09:36 and 21:09:36. From July 8, 2011 to July 20, 2011, these connections occurred daily at 01:09:38, 04:09:36 and 07:09:35. This indicated that some form of traffic generated by a scheduled process took place.

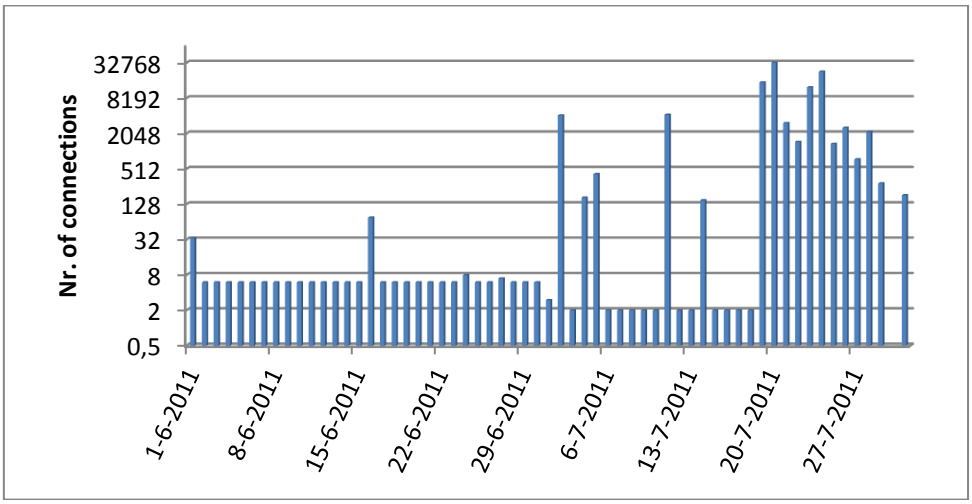
If we exclude the traffic peak on July 25, 2011, as this peak was probably due to incident response activities, the last traffic between the Secure-net and the stepping stone took place on July 20, 2011 at 07:09:35 from the Public-CA server.

5.2.8 Other noteworthy traffic

The previous paragraphs of the firewall log investigations show results based on the firewall logs that can be correlated with other exhibits to draw conclusions in regard to the attacker. The conclusions are mostly in regard to the exit path that was used to exfiltrate data and/or to create easy access for future visits. The following paragraphs detail the remaining results of the investigation that was performed on the firewall logs. Although the following anomalies cannot be unambiguously connected to activity of the intruder, they are noteworthy and provide sufficient reason for further investigation. An extensive list of the identified noteworthy traffic, complemented with investigation notes, is included in a timeline in Appendix III. In the following paragraphs, only the most remarkable anomalies are noted.

5.2.8.1 E-mail traffic

The firewall logs show unusual traffic with destination port 25 (SMTP) between the CAP-app-web server in the Secure-net segment and the Exchange-mail server in the Office-net segment. As port 25 is generally used for the purpose of e-mail, this could indicate intensive e-mail traffic that normally does not occur in these quantities. The figure below illustrates the anomaly.

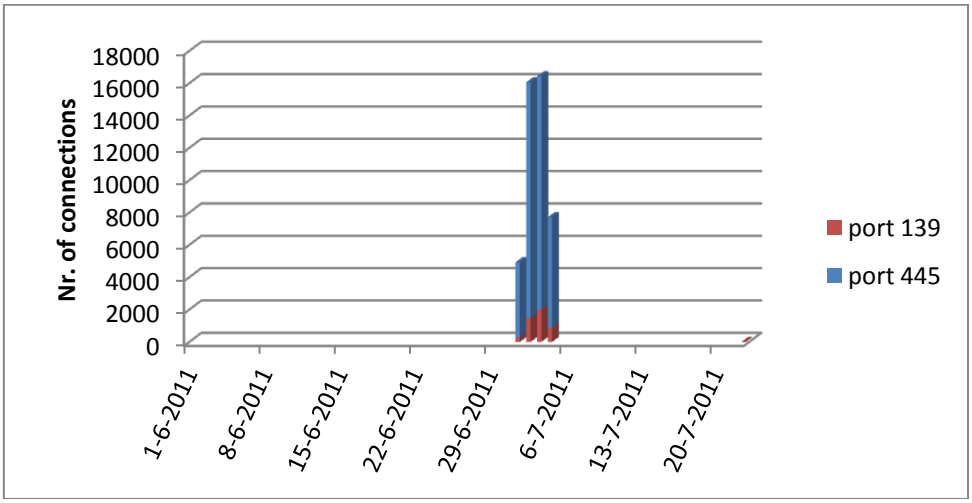


Anomaly CAP-app-web → Exchange-mail

The normal traffic on port 25 consists of six regular SMTP-connections each day at given intervals (four at 9:00 and two at 00:30), probably the result of a scheduled task. After June 30, 2011, the regular connections at 09:00 cease to take place. Then, suddenly, in the night of July 2, 2011, approximately 4,100 connections occurred. Then, additional spikes of traffic occurred on the 4th, 5th, 11th and 14th of July, 2011. Between July 19 and July 29, very large numbers of connections on port 25 took place. The last mentioned anomalous traffic coincides with the incident response actions that were initiated on July 19, 2011. According to DigiNotar, anomalous SMTP traffic may also have been caused by intensive testing of Taxi CA, which used SMTP as mode of transport.

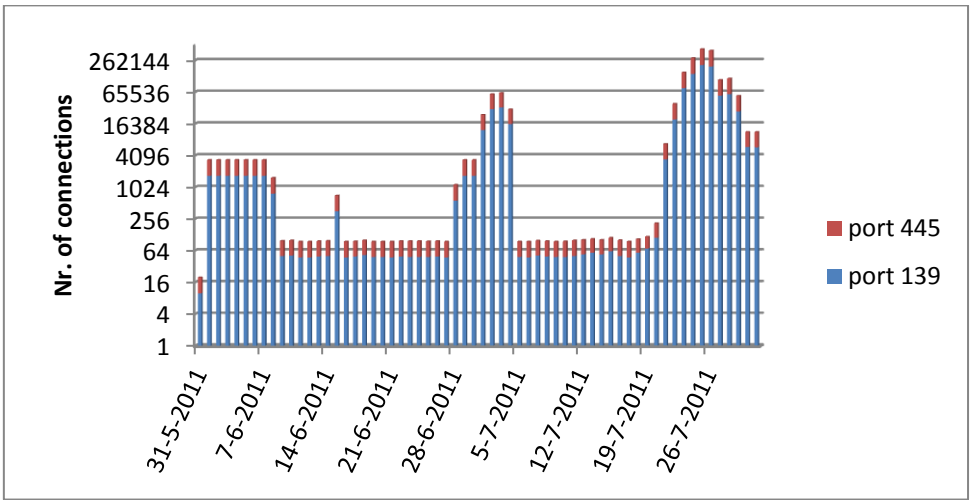
5.2.8.2 Co-location

At the co-location, suspicious (dropped) traffic was detected originating from the co-located secure network segment (Secure-colo-net) to the main secure network (Secure-net). The traffic occurred between the Admin-DNS server and the CAP-app-web server on ports 139 and 445.



Anomaly connections Admin-DNS → CAP-app-web on port 139 and 445

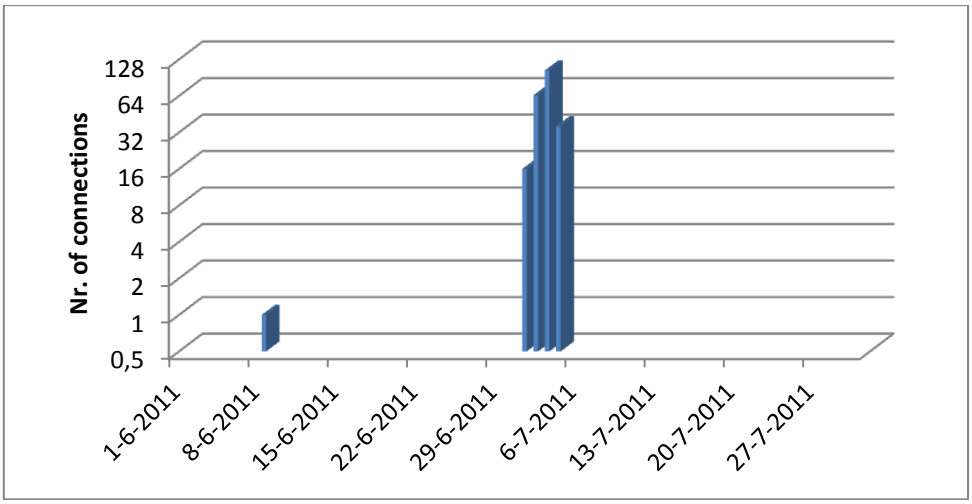
This could indicate that the intruder had gained a foothold in Secure-colo-net as of July 1, 2011. The reverse connection from Secure-net to Secure-colo-net showed the following pattern:



CAP-app-web → Admin-DNS port 139 and 445

This indicates some regular traffic (approximately 50 packets per day) and some monthly traffic. The spikes during the first four days of July are anomalous (the scale is logarithmic). The traffic after July 19 is extreme when compared to the ordinary traffic, but could be explained by incident response activity.

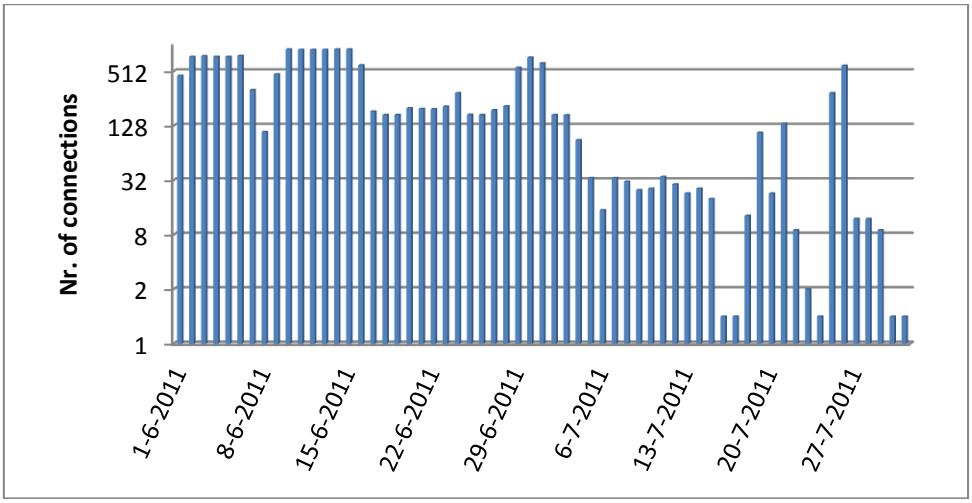
Other noticeable traffic was discovered on port 137 during the first four days of July (in addition to a connection on June 8, 2011):



Anomaly connections CAP-app-web port 137 → Admin-DNS on port 137

5.2.8.3 Internal DMZ-net

A noticeable change in the normal traffic between Secure-net and DMZ-int-net was found between the CAP-app-web and the Production-Notification server. Normal traffic between these segments depends on the amount of requests, which may vary significantly.



CAP-app-web server → Production-notification server port 80

The traffic shows a steep decrease in connections from July 4, 2011 onwards. From July 16, 2011 to the last-examined logs, a very erratic pattern occurs.

5.3 Conclusion

The examination and analysis of the firewall traffic logs provided some insight into the steps and foothold of the intruder. Connections initiated from internal IP addresses to external IP addresses that were suspected to have been used by the intruder were found. This indicated that from June 18, 2011 the intruder had a foothold on a server in the DMZ-ext-net. In total, four servers in the DMZ-ext-net were found to have been used to connect back to suspicious external IP addresses on the basis of the firewall log files. Other evidence confirmed that some of these servers were used as a stepping stone. During this part of the investigation four of the IP addresses suspected to have been used by the attacker were found to have been accessed from within the DigiNotar network.

From June 17, 2011, connections were initiated to a database server in the Office-net from the DMZ-ext-net. This indicates that the Microsoft SQL database running on that server was probed or used. From June 29, 2011, traffic initiated from the server in the Office-net started to appear, indicating tunneled remote desktop connections from servers in the DMZ-ext-net. This indicates that the foothold of the intruder was extended to the Office-net.

First signs of suspicious traffic from the Secure-net were found on July 1, 2011, possibly a network scan. This traffic originated from the BAPI-production workstation. Due to limitations on the investigation this workstation was not examined. Later on July 2, 2011, traffic from CA server and other servers in the Secure-net was initiated towards the stepping stones in the DMZ-ext-net.

Based on the firewall logs the following servers were identified as likely to have been compromised:

Network	Server
DMZ-ext-net	Main-web server
	eHerkenning-AD server
	eHerkenning-HM server
	Pass-web server
	Docproof1
	Docproof2
Office-net	BAPI-db server
	Source-build

Network	Server
Secure-net	BAPI-production (workstation)
	CAP-app-db server
	Relations-CA server
	Public-CA server
	CCV-CA server
	Taxi-CA server
	CAP-app-web server
	Root-CA server
	Qualified-CA server

Based on investigation of the firewall logs, the following external AttIP addresses are likely to been utilized by the attacker (see also Appendix II):

Intruder IP	Remark
AttIP1	Successful connections initiated from DMZ-ext-net and specifically tunnels from DMZ-ext-net. Blocked attempts from Secure-net.
AttIP2	Successful connections initiated from DMZ-ext-net.
AttIP13	Dropped connections initiated from DMZ-ext-net.
AttIP19	Successful connections initiated from DMZ-ext-net.
AttIP22	Successful connections initiated from DMZ-ext-net.

6 Investigation of CA servers

The rogue certificates that had first been generated on July 10, 2011 were first discovered when an automated routine test that had failed to work was restored on July 19, 2011. The test verified certificates that had been issued with the records in the back office and showed that a number of these certificates lacked any records in the back office of DigiNotar. The staff of DigiNotar proceeded to examine the CA managing applications and found that rogue certificates had been issued. The serial numbers that corresponded with these rogue certificates were revoked immediately[19]. An initial incident response team was formed and a further investigation was launched. As a result, more rogue certificates were found and revoked on July 21, 2011 and on July 27, 2011. At the end of July, DigiNotar was convinced that the breach of its infrastructure was under control and that the damage had been repaired.

On August 28, 2011, another rogue certificate issued for all services on the Google.com domain and its sub domains, which had not been revoked, was found by a Gmail user[20]. A search through the management software did not reveal the serial number that belonged to this certificate. In order to revoke the rogue `*.google.com` certificate, another certificate was created with the same serial number and revoked effectively on August 29, 2011 at 19:09:05 (CEST).

Fox-IT investigated the CA management software to determine if any additional certificates were falsely issued. Fox-IT also investigated if other Certificate Authorities had been compromised.

It is important to note that the CA servers did not log to a separate secure log server. All the investigated log files originated from servers that had been compromised. As a result, all the identified log files may have been tampered with, log files may have been replaced by earlier versions or the log service may have been shut down intentionally. Consequently, suspicious entries in the log files can only be used to make inconclusive observations regarding unauthorized actions that took place, but the absence of suspicious entries cannot be used to infer that no unauthorized actions took place.

6.1 Sources

Eight systems that operated as CA servers were investigated:[21]

- **CCV-CA server.** This server managed the certificates that were used for electronic payment in the retail business. The name CCV refers to the company that used these certificates (www.ccv.eu).
- **Nova-CA server.** Also called Orde-CA, which managed certificates of the Nederlandse Orde van Advocaten (Dutch Bar Association) (www.advocatenorde.nl).
- **Public-CA server.** This server managed the certificates that were used for public services, including the DigiNotar Extended Validation Certificate Authority, which was used for protecting websites with SSL.
- **Qualified-CA server.** Managed the certificates that DigiNotar issued on behalf of the Staat der Nederlanden (the Dutch state). This was a sub-Certificate Authority in the PKI hierarchy called PKIoverheid (PKI government). This server also managed the DigiNotar Qualified Certificate Authority, allowing documents that had been signed with these certificates to be used as the legal equivalent of a handwritten signature as determined in the European Union Directive 1999/93/EC. DigiNotar was registered to issue these qualified signatures.[22]
- **Relation-CA server.** On this server the Certificate Authorities of other important clients of DigiNotar were hosted such as:[23]

[19] Initially the invalidity date of the revoked certificates was set to the date when the revocation took place. Later this was corrected to the date when the rogue certificates had been issued, ensuring that the certificates would be considered invalid for any possible date.
[20] Google Groups, "Is This MITM Attack to Gmail's SSL?" at http://groups.google.com/a/googleproductforums.com/d/topic/gmail/3J3r2JqFNTw/discussion and Pastebin, "Gmail.com SSL MITM ATTACK BY Iranian Government – 27/8/2011" at http://pastebin.com/ff7Yg663
[21] Other systems found running CA managing software were WINVM012 and WINVM032. No exhaustive search was undertaken to identify all the systems running CA management software because these eight systems managed the most important Certificate Authorities.
[22] This registration was ended on September 14, 2011.
[23] A complete list is included in Appendix VI.

    - TenneT, a large Dutch electricity supplier (www.tennet.org)
    - Koninklijke Notariële Beroepsorganisatie (Royal Netherlands Notarial Organisation at `www.knb.nl`)
- **Root-CA.** Managed the root Certificate Authority certificates of DigiNotar and all the certificates of the Ministerie van Infrastructuur en Milieu (Dutch ministry of Infrastructure and the Environment).
- **Taxi-CA.** Hosted the Certificate Authorities that were used for a project for the registration of taxi drivers in The Netherlands for the Ministerie van Infrastructuur en Milieu. The test CA environment of the Ministerie van Infrastructuur en Milieu was also hosted on this server.
- **Test-CA.** Different kinds of test Certificate Authorities were managed on this server. They all had "test" in the common name of their certificates with the exception of three CA certificates (appendix VI).

The CA servers had access to the nCipher netHSM that was also located in Secure-net. The netHSM devices store private key material in a secure way, so that the key material cannot leave the device unencrypted. The private keys can only be used if a smartcard, which is secured with a PIN code, is present in the netHSM.

On the CA servers, software from RSA was installed in order to manage certificates. The product used was the RSA Certificate Manager (RSA CM).[24] The CA software consists of several services. One of the services provides a web interface for users and administrators. Another service logs the activity of the software into log files. The CA software also provides an application programming interface (API) that enables programmers to develop PKI applications. These applications can be developed using a scripting language called XUDA (Xcert Universal Database API). Since no information that could be used for a public report could be exchanged with RSA, Fox-IT used reverse engineering techniques to perform the investigation.

For the purpose of the investigation, Fox-IT used a list that was provided by DigiNotar, which contained all the certificates that had been issued by DigiNotar. This list `allcerts.csv` was created by exporting the CA databases and contained the following information regarding the certificates:

Value	Meaning
md5	The MD5 checksum of the certificate as calculated by the CA software
CA md5	The MD5 checksum of the issuing CA certificate
Serial nr.	The serial number of the certificate
Cert dn	The distinguished name field of the certificate
Valid from & valid until	The date fields of the certificate
Revocation date	The date of revocation (if applicable)

6.2 CA software log files

6.2.1 Sources

All CA servers were outfitted with software that logged relevant information for the ongoing processes. The information was stored in log files that were in the format `xslog_{yyyyMMdd}.xml`. It appears that the log files were not being rotated or removed automatically. A new log file was created whenever the machine was rebooted or when the logging service was restarted. The following log files from the period within which the intruder was active were investigated:

Server	Log files
CCV-CA	`xslog_20110616.xml`
Nova-CA	`xslog_20110401.xml`

Public-CA	`xslog_20110325.xml`
	`xslog_20110711.xml`
	`xslog_20110711_1.xml`

Qualified-CA	`xslog_20110224.xml`
	`xslog_20110702.xml`
	`xslog_20110704.xml`
	`xslog_20110723.xml`

[24] Older versions of this software are known as RSA Keon.

Server	Log files
Relation-CA	xslog_20110407.xml
Root-CA	xslog_20110616.xml
Taxi-CA	xslog_20110517.xml xslog_20110711.xml
Test-CA	xslog_20110224.xml

The integrity of blocks of data within the log files can be verified using a signature. The CA software can be used to verify the integrity of the log files, which was done for all CA management application instances by an employee of DigiNotar. Two log files failed the verification by the CA software, which originated from Public-CA server:

- xslog_20110711_1.xml
- xslog_20110720.xml

The integrity of other log files was verified by the CA software without failure. The breached integrity of xslog_20110711_1.xml corresponds with descriptions that were found in the incident log book. The log book contains log entries showing that when the console on the Public-CA machine was started on July 20, 2011, rogue certificates were being issued and that the machine was shut down. The corresponding customary entries "Log Server Stopped" and "Final Entry" are missing from this log file.

The entries in the log files contain the following information:

- LOG_NUMBER: a sequential unique log entry number
- LOG_SOURCE: the source of the log entry (either from the Certificate Administration management, Secure Directory or Logging Server)
- EVENT_CONDITION: either ATTEMPT or COMPLETION of an action
- DATE,TIME: the date and time of the entry (in CEST time zone)
- ID: a hexadecimal value consisting of 32 characters (29 unique IDs have been encountered - 6 of these were encountered more than 100,000 times)
- IP_ADDR: the IP address associated with the action
- LOG_DATA: the structure of this field varies depending on the data that it contains. A "Certificate signing" entry has the following fields:
  - Succeeded or failed
  - Certificate presented: an MD5 value of 32 characters of the certificate presented to the CA software with the request
  - certDN with distinguished name fields
  - MD5-value of the certificate
  - Issuing CA MD5

Note that no serial number was logged for the issued certificates. Therefore, no link could be established between a certificate and an entry in the log files on the basis of a serial number. The relation between a certificate and a log entry may have been established using the MD5 value of the certificate that was in the log file; however, the data that was used to calculate the MD5 was not known.[25] The certificates that were stored in the databases also contained the MD5 value of the certificate. Therefore, it was attempted to make a definitive link between entries in the log files and the certificates on the basis of the MD5 value in these databases.

6.2.2 CA software log analysis

In the log files of some CA servers, log entries were found indicating the automatic generation of a Certificate Revocation List (CRL). Certificate Authorities usually issue CRLs at regular intervals according to their policies. These CRLs are signed by the issuing Certificate Authorities, which can only occur if a private key was active on the netHSM. The log entries referring to such an automatic process thus indicated that the private keys in the netHSM were activated and that there was potentially an opportunity for the intruder to abuse these private keys.

[25] The MD5 value did not correspond with the MD5 fingerprint or the MD5 sum of the certificate in PEM or DER format.

In the examined log files, a large number of automatically generated CRLs were found. The complete list is included in Appendix IV.

Server	Number of Certificate Authorities
Nova-CA	3
Public-CA	10
Root-CA	6
Qualified-CA	8
Test-CA	27
Relation-CA	8

CCV-CA server
The logs of the CCV-CA server showed no activity between June 17, 2011 and July 22, 2011. No automated CRL generation process was found.

Public-CA server
The log entries of Public-CA server showed the automated generation of CRLs for (among others) the Certificate Authorities of *Cyber CA*, *Extended Validation CA*, *Public CA - G2*, *Public CA 2025* and *Services 1024 CA*.

The analysis of the log file `xslog_20110325.xml` on the Public-CA server showed that the first signs of abnormal activity and certificate signing attempts occurred on Sunday July 3, 2011 at 12:15:44. Between Thursday July 7, 2011 at 23:19:33 and Sunday July 9, 2011 at 12:53:16, it appears that experiments took place by the intruder outside of office hours. During this timeframe old certificate requests appear to have been reissued. For example, `beveiligd.gemeentesudwestfryslan.nl` was issued twice with different CA keys. On July 10, 2011 at 19:55:56, the log files showed that the first rogue certificate was successfully issued on the Public-CA server (a `*.google.com` certificate). Between 19:55:56 and 23:55:57 on July 10, 2011, a total of 198 rogue certificates were issued on the Public-CA server. The log server was stopped on 11-Jul-2011 at 01:41:19.

The log file `xslog_20110711.xml` started on July 11, 2011 at 08:18:42, leaving a gap in the logs of about six and a half hours. The next log file (`xslog_20110711_1.xml`) contained only a few entries, most of them logging failed certificate signing attempts.

The next log file (`xslog_20110711_1.xml`) started on July 11, 2011 at 11:24:49, most likely after a reboot of the system or the logging service. On July 18, 2011 at 16:19:27, a burst of 124 rogue certificates were created. Another burst of 124 rogue certificates were issued on July 20, 2011 at 08:56:41. According to DigiNotar, this burst was an isolated incident that produced a copy of generated rogue certificates in the previous burst and prior measures had been taken to prevent the certificates from being published. No other rogue certificates were found in the logs of the Public-CA server after this point in time. The log file was not properly terminated. The last log entry dated from July 20, 2011 at 08:57:11.

The following log file (`xslog_20110720.xml`) started on July 20, 2011 at 12:19:37, has no entries and was terminated at 12:21:41. The next log file (`xslog_20110720_1.xml`) started on July 20, 2011 at 12:34:52. No obvious suspicious activity was found in this file. The final entry was on July 20, 2011 at 18:20:14. After that all entries in the log files appeared to relate to normal activity. The servers were shut down daily.

Based on logs of the Public-CA server, 446 certificates were issued between July 10, 2011 at 19:55:56 and July 20, 2011 at 08:57:11 on the Public-CA server that were evidently rogue based on the common name that was used.

Relation-CA server
The log entries of Relation-CA server showed the automated generation of CRLs for (among others) the Certificate Authorities of *KNB CA 2*, *Ministerie van Justitie CA* and *Stichting TTP Infos CA*.

The analysis of the log file `xslog_20110407.xml` on Relation-CA server showed that the first signs of extraordinary activity and certificate signing attempts occurred on July 2, 2011 at 19:59:34. The first

successful rogue certificate was created on the Relation-CA server on July 10, 2011 at 13:05:10 with the common name `*.google.com`. The log file ended normally on July 20, 2011 at 18:20:29.

The logs of the Relation-CA server showed that a total of 85 rogue certificates were successfully created on the Relation-CA server between 13:05:10 and 23:35:54 on July 10, 2011.

Root-CA, Nova-CA and Test-CA servers
The examination of the log files showed an automated CRL generation process on all three CA servers, including the Certificate Authorities of *DigiNotar Root CA*, *Root CA G2* and *MinIenM Organisatie CA - G2* on the Root-CA server, and the Certificate Authority *Nederlandse Orde van Advocaten* on the Nova-CA server. Very few certificates were issued by these Certificate Authorities during the intrusion, according to the log files. No unusual or remarkable log entries were found.

Taxi-CA server
The logs of the Taxi-CA server showed no activity between June 16, 2011 and July 11, 2011. No unusual or remarkable log entries were found. No automated CRL generation process was found.

Qualified-CA server
The log entries of the Qualified-CA server showed automated backup processes and generation of CRLs, which included the Certificate Authorities *DigiNotar PKIoverheid CA*, *PKIoverheid CA Organisatie - G2*, *Overheid en Bedrijven*, *DigiNotar Qualified CA* and *DigiNotar Qualified CA - G2*.

When the log files of the Qualified-CA server were examined, the two successive log files, `xslog_20110224.xml` and `xslog_20110702.xml`, showed that the log server was turned off on July 2, 2011 at 02:13:40 presumably by the intruder and turned on again at 10:12:43. This leaves a gap of approximately eight hours during which no activity was logged. No other unusual or remarkable log entries were found.

6.3 CA databases

The CA management software used databases to store various application data. Several database files were stored in the directory `{install directory}\Xudad\db\`. The main database file was named `id2entry.dbh`. The main database file contained records of the certificates that had been issued, including several characteristics for the issued certificates.

During its investigation, Fox-IT encountered database files named `serial_no.dbh` that contained serial numbers plausibly identifying the certificates issued by the software. All the found `id2entry.dbh` and `serial_no.dbh` database files were examined, including recoverable deleted files. All these database files were in the Berkeley DB format.

6.3.1 Certificates

The certificates stored in the main database file were extracted and converted into the PEM (Privacy Enhanced Mail) format. The following methodology was used in order to do this:

- Perform a case insensitive search for the string `pem_x509::` in the `id2entry.dbh` files
- Extract the trailing data block
- Decode the text from its base64 format
- Encapsulate the text with `-----BEGIN PUBLIC KEY-----` and `-----END PUBLIC KEY-----`.

When the certificates were extracted in this way, some extracted data blocks were invalid. An attempt to read them with, for instance, OpenSSL would result in an error. A check revealed that complete versions of these data blocks were also present in the database. This led Fox-IT to conclude that no certificates were missed using this method.

Additionally, some certificates were stored more than once in the database or were found in a backup database. Comparing the fingerprints[26] of the certificates identified the duplicates. The incomplete and duplicate certificates were excluded from further analysis.

[26] In public key cryptography, a public key fingerprint is a short sequence of bytes used to authenticate or look up a longer public key.

The following numbers of certificates were identified. The validity period has not been taken into account. Details of these certificates are provided in Appendix V.

	Root-CA server	Qualified-CA server	CCV-CA server	Nova-CA server
Total number of certificates	73	23621	36	37868
Unique subject name	45	22483	26	35742
Different issuers	10	13	9	5
Basic constraints = TRUE	29	7	20	2
Self signed	5	4	8	4

	Public-CA server	Taxi-CA server	Test-CA server	Relation-CA server
Total number of certificates	46101	1348	3111	11671
Unique subject name	44161	601	2088	11168
Different issuers	13	17	32	16
Basic constraints = TRUE	9	15	42	12
Self signed	4	5	11	6

6.3.2 Private keys

The `id2entry.dbh` database files contained entries labeled `privatekey::`. After decoding the base64 data, these entries showed the following ASN.1 structure (Root-CA server is used for this example):

```
 0:d=0  hl=2 l= 111 cons: SEQUENCE
 2:d=1  hl=2 l=   1 prim: INTEGER    :02
 5:d=1  hl=2 l=  19 prim: IA5STRING  :XCSP nCipher Native
26:d=1  hl=2 l=   1 prim: INTEGER    :53
29:d=1  hl=2 l=  64 prim: cont [ 0 ] :30 3E 16 0E 72 73 61 2D 6B 65 6F 6E 2D 63 61 2D  0>..rsa-keon-ca-
                                      36 38 16 10 31 33 30 38 32 32 33 37 36 30 33 32  68..130822376032
                                      37 30 30 30 16 11 53 45 43 55 52 45 20 4F 50 45  7000..SECURE OPE
                                      52 41 54 49 4F 4E 53 01 01 FF 02 01 02 02 01 04  RATIONS.........
95:d=1  hl=2 l=  16 prim: cont [ 1 ] :30 0E 80 01 01 81 01 00 04 06 02 04 84 8D A7 10  0.?.............
```

The decoded ASN.1 structure led investigators to believe that these are references to private keys in the netHSM. If this is the case, then investigators can conclude that the software installed on the server could use these keys and could show what Certificate Authorities were used on what server.

In the records surrounding the private key entries, there was no indication of the certificate or common name linked to these keys. However, a data block labeled `publickey::` was present. For the example mentioned above, investigators extracted the public key and matched it with the public keys of the extracted certificates. This resulted in the Certificate Authority certificate with the common name '`CN=MinIenM Autonome Apparaten CA - G2`'. Using this method, investigators were able to determine what CA servers could use which private keys in the netHSM, lookup the corresponding certificate and thus identify the Certificate Authority.

In some instances, different keys were used for the same distinguished name (DN). This occurred, for example, if a certificate expired and a new key was generated. A complete list of the references to private keys and the matching distinguished name is provided in Appendix VI. The validity period has not been taken into account.

Server	Total number of keys	Unique subject Name	Unknown key
Root-CA	11	11	None
Qualified-CA	8	8	None
CCV-CA	10	8	2
Nova-CA	3	3	None
Taxi-CA	17	15	2
Test-CA	43	34	4
Relation-CA	15	14	1
Public-CA	10	10	None

Also note that for some keys no matching certificate was found. This means that a reference to a private key in the netHSM could not be matched with a corresponding certificate.

6.3.3 Serial numbers

Removed database files were discovered on multiple CA servers, raising the suspicion that the intruder had manipulated database and log files. For example, the serial number of the rogue `*.google.com` certificate that was abused in the MITM attack was only present in a `serial_no.dbh` database that had been removed from the server and was recovered during the investigation.

The assumption was made that the `serial_no.dbh` database contained all serial numbers for certificates, including rogue certificates that had been issued by the CA software. To establish if serial numbers corresponding with rogue certificates were indeed present, all `id2entry.dbh` and `serial_no.dbh` files were collected for each CA server, including all recoverable files that had been removed. It was investigated whether every serial number in `serial_no.dbh` could be matched with an issued certificate.

In order to determine this, two sets of serial numbers were created. Set A included serial numbers from all `serial_no.dbh` files. Set B included serial numbers from all `id2entry.dbh` files. The difference between these lists resulted in set C, containing the unknown serial numbers. As an extra check, these serial numbers were matched against the `allcerts.csv` list of issued certificates that was provided by DigiNotar.

This method was applied for all the CA servers. The results showed unknown serial numbers originating from four of the eight CA servers. A complete list of unknown serial numbers for the CA servers can be found in Appendix VII. It was impossible to match a serial number to a specific common name or to match it to a specific issuing Certificate Authority since this information was not present in the database.

CA server	Number of unknown serial numbers
Root-CA	7
Qualified-CA	2
Taxi-CA	24
Public-CA	203

In the time available for the investigation, it could not be established conclusively for all instances why the discrepancy between the `serial_no.dbh` and `id2entry.dbh` databases existed. The examination of the OCSP responder logs showed that five of these unknown serial numbers were validated, including the `*.google.com` certificate used for the large-scale MITM attack (see paragraph 10.2). Given the fact that a number of unknown serial numbers were known to correspond with rogue certificates, it is plausible that most or even all unknown serial numbers are the result of rogue certificates that had been issued. However, unknown serial numbers may also have been caused by software errors or as a result of aborting the issuing process. As a precautionary measure, all the unknown serial numbers were revoked.

6.4 Conclusion

The CA management software of eight CA servers at DigiNotar was investigated by Fox-IT. After a thorough search, it was found that the number of issued rogue certificates in the log files exceeded the number of rogue certificates in the CA management application. This led to the conclusion that the CA software had been manipulated and records in the database had been deleted.

An important goal of this part of the investigation was to determine what Certificate Authorities had issued rogue certificates and thus could no longer be trusted. Since the logging service was running on the same systems that had been compromised and that records had been manipulated, the log files could only be used to make inconclusive observations regarding unauthorized actions. The absence of suspicious entries in the log files could not be used to infer that no unauthorized actions took place.

However, in order to issue certificates by a Certificate Authority on a CA server, the corresponding private key of the Certificate Authority in the netHSM needed to be active. This meant that the unauthorized actions that might have taken place could not have included the issuing of rogue certificates if the corresponding private key had not been active during the period in which the intrusion took place.

The log files recorded the distinguished name of a certificate but not its serial number. To revoke a certificate, however, the serial number of the certificate was essential. The revocation process was therefore changed to be based on the known valid certificates (a white list method) at the advice of Fox-IT (see also paragraph 2.2.1).

6.4.1 Rogue certificates

Based on the investigation of the log files, a total number of 531 rogue certificates were identified (446 on the Public-CA server and 85 on the Relation-CA server). These were identified as rogue because of the highly irregular common names of the certificates. Other certificates that were issued during the time the intruder was active on the CA servers may also have been fraudulent. Further investigation could determine if this is indeed the case.

Of the 531 rogue certificates found in the logs, 332 certificates were recovered in the databases and their serial numbers were known. One previously unknown certificate was posted by the Google.com user. For the remaining 198 log entries, no certificate was found and therefore the serial was marked as unknown.

The number of rogue certificates that could be connected to the issuing Certificate Authorities was:

Certificate Authority Common Name (Issuer)	Total	Unknown serial[27]	Cert.[28]	CA server
DigiNotar Cyber CA	108	1	107	Public-CA
DigiNotar Extended Validation CA	98	14	84	Public-CA
DigiNotar Public CA - G2	56	0	56	Public-CA
DigiNotar Public CA 2025	184	183	1 (29)	Public-CA
Koninklijke Notariele Beroepsorganisatie CA	67	0	67	Relation-CA
Stichting TTP Infos CA	18	0	18	Relation-CA
Total	**531**	**198**	**333**	

The investigation identified 236 serial numbers in the `serial_no.dbh` databases that have no obvious relation to log entries or recovered certificates. The following table compares the earlier list of serial numbers originating from CA servers with log entries without matching serial numbers.

CA server	Serials without matching certificate	Logs without matching serial
Root-CA	7	0
Qualified-CA	2	0
Taxi-CA	24	0
Public-CA	203	198
Relation-CA	0	0

Because it remains unknown when serial numbers were stored in the `serial_no.dbh` database, the total number of rogue certificates was unverifiable.

Of these rogue certificates, 344 have domain names as their common name. The remaining 187 have "Root CA" in their common name. This does not necessarily mean that they could have been used as an issuing certificate. Of the 333 rogue certificates that were found, none had the basic constraint attribute set, meaning that they could not be used for issuing certificates. Also in the logs of the CA management software, no logs were present of rogue-issued Certificate Authority certificates. However, no contraindication was found that it was impossible to issue rogue issuing certificates or that these were not created by the intruder either. Depending on the way the software verifies certificates, the basic constraint attribute can be ignored.

[27] Traces of these certificates were found in the logs and not in the databases, therefore the serial number is not known.
[28] The certificate is found in the database.
[29] The rogue wildcard Google.com certificate that was abused in the MITM attack.

The key usage of the 333 found certificates were all set as a critical attribute and were meant for the purpose of digital signature, key encipherment and data encipherment or a combination thereof. No code or certificate signing key usage was found.[30]

The 531 encountered rogue certificates contain 140 unique distinguished names and 53 unique common names. A list of the common names is included in Appendix VIII.

6.4.2 Trust in the Certificate Authorities

The situation that Fox-IT encountered was that the CA management software had clearly been manipulated. It was evident that the issuing Certificate Authorities of the rogue certificates, as identified on the basis of their Common Name, had to be revoked according to PKI standards[31]. Additionally, untraceable serial numbers on some of the CA servers raised suspicions in regard to the security of the Certificate Authorities that were managed on those machines. Gaps in log files of these CA servers added to the suspicions in regard to their security.

Some uncertainties in the operation of the CA management software still exist[32]. These uncertainties include if deleted log files could be detected, if the log settings had been manipulated, if the log service was stopped while the issuing software kept running, how the untraceable serial numbers were issued, et cetera. A scenario that may have been possible is that the intruder could have created a backup of the database and log files, then issued several certificates and restored the original backup thus removing all evidence.

The investigation of the suspicious files and, specifically, the presence of cached versions of the `/beurs` directory on the stepping stone showed that the operating systems of all CA servers had been compromised and were used at some point by the intruder (see Chapter 4).

Having compromised the CA servers, the only additional barrier for issuing rogue certificates that remained was the activation of the Certificate Authorities' private keys, which are activated with a smartcard on the netHSM. Some Certificate Authorities were continuously operational as evidenced by the automatic generation of CRLs, meaning that the corresponding private keys in the netHSM were always activated. If, for example, an offline record had been kept of when these smartcards were present or removed, a contraindication could have been given that a Certificate Authority could not have been abused to issue rogue certificates. However, no evidence could be produced by DigiNotar that private keys were not activated during the time of the intrusion. According to DigiNotar, the smartcard for CCV-Certificate Authority had been in a vault for the entire period of the intrusion and its private key was not activated during this period.

It is possible that the CA software that was used was able to produce certificates that have identical certificate attributes as previously issued certificates. This includes the serial number and the validity dates, with the exception of the public key and its key identifier. The intruder could have issued certificates that would be seemingly identical to formally issued and trusted ones. Since the possibility could not be excluded that the compromised CA servers had been abused to issue additional rogue certificates and since the rogue certificates may not be distinguishable from legitimate certificates in aspects that are relevant for the purpose of verification within a PKI, it was no longer possible to rely on the authenticity of any certificates that had been issued by the affected Certificate Authorities. It may also have been possible that the intruder used other CA management software to have certificates signed directly by the netHSM (bypassing even the XUDA interface). This was not investigated further.

---

[30] A user on Pastebin named 'ComodoHacker' created a binary (`calc.exe`) and signed it with the `*.google.com` certificate used in the MITM attack. Although this certificate had no explicit code signing key usage the Microsoft Windows operating system accepts the signature.

[31] RFC 5280 for instance stipulates that the "Existence of bogus certificates and CRLs will undermine confidence in the system. If such a compromise is detected, all certificates issued to the compromised CA MUST be revoked, preventing services between its users and users of other CAs". According to this RFC, certificates also need to be revoked if a CA and the corresponding private key are merely suspected to be compromised.

[32] RSA was contacted concerning the operation of the software, but no information that could be used by Fox-IT for a public report could be exchanged. Our efforts in this regard were abandoned after while due to the increasing irrelevancy of the specific issue for the overall investigation.

The overall conclusion was that the possibility could not be excluded that all Certificate Authority keys managed by DigiNotar, with the exception of the private keys for the CCV-Certificate Authority, could have been abused to issue rogue certificates. Even certificates that would appear to have been issued before the intrusion took place could not be verified by the public key infrastructure and therefore could not be trusted. According to standards and best practices in the industry, the certificates had to be revoked, as the intruder could have issued seemingly identical certificates (including issuing dates in the past). All DigiNotar certificates originating from the compromised CA servers therefore could no longer be trusted and the Certificate Authorities had to be removed from trust lists with the exception of the CCV certificates. The impact of the revocation of the certificates that had been issued by DigiNotar varied depending on their usage and had to be assessed on a case by case basis.

7 System access and tools

The goal of this part of the investigation was to identify tools that had been used during the intrusion and the purpose for which they were used. For this purpose, the images of systems were probed for anomalies and for files that could be connected to other parts of the investigation. In order to identify suspicious files, the timestamps of the files on disk images were examined, including recoverable files. Timestamps indicated when a file was created, copied, accessed or modified. In combination with the file location and file name, a file could be marked as suspicious for further examination.

This examination of the following servers is detailed in this chapter:

Network	Server
Secure-net	Qualified-CA
	Taxi-CA
	Relation-CA
	Public-CA
	Root-CA
	CCV-CA
Office-net	Office-file server
	BAPI-db
DMZ-ext-net	Main-web
	Docproof2

All the timestamps in this chapter are based on Coordinated Universal Time (UTC). A non-exhaustive list of the suspicious files that were found is included in Appendix IX.

7.1 Previous investigation

The initial internal investigation by DigiNotar was done on the file `svchost.exe` which was found on the Public-CA server. This investigation concluded that the file created a file `jobsdone.zip` and uploaded this file to the stepping stone Main-web in DMZ-ext-net using the `/beurs/up.aspx` script. The investigation also stated that the file `svchost.exe` created a connection to that same server on port 53. The file `svchost.exe` was created on the Public-CA server on July 3, 2011 at 23:56. These results indicated that an automated process might have been in place. This could mean that certificates were automatically issued and transferred via the stepping stone to the intruder.

7.2 Connection tools

7.2.1 Stepping stones

The intruder placed `aspx`-scripts on at least two compromised web servers in DMZ-ext-net. These scripts were used amongst others as a file manager in order to up- and download files between internal and external systems.

Timestamp	File name	Server
17-Jun-2011 02:33:35	b.aspx	Docproof2
17-Jun-2011 05:26:36	settings.aspx	Main-web

The results of the investigation show that as of June 17, 2011 the web servers had been compromised and files could be up- and downloaded to DMZ-ext-net. From that point onwards, the web servers could be used as stepping stones to exchange files between systems on the Internet and compromised systems inside of DigiNotar's network. The scripts also contained other functionality such as port scanning, port mapping and restarting services. No evidence was found that these functions were used however.

7.2.2 Accessing the stepping stones

The temporary Internet files of the investigated Windows systems hosting the CA management software showed cached copies of a file exchange location on the Main-web server in DMZ-ext-net. These cached copies showed a directory listing of the file manager on the web server with files sizes and modification

dates. This was discovered early on in the investigation and it therefore quickly became clear that the intruder had used the web servers in the external DMZ network as stepping stones to transfer files between arbitrary systems on the Internet and crucial systems in DigiNotar's network.

In addition to cached HTML pages, the temporary Internet files also showed other cached files from the web servers that were used as stepping stones. These locally cached files were the result of a file that was downloaded from a stepping stone. A number of files that were uploaded to the stepping stone could also be identified due to an upload notification in the cached HTML pages of the file manager. The path of the temporary Internet files on the hard disk also showed which Windows user accessed the web page or downloaded the file.

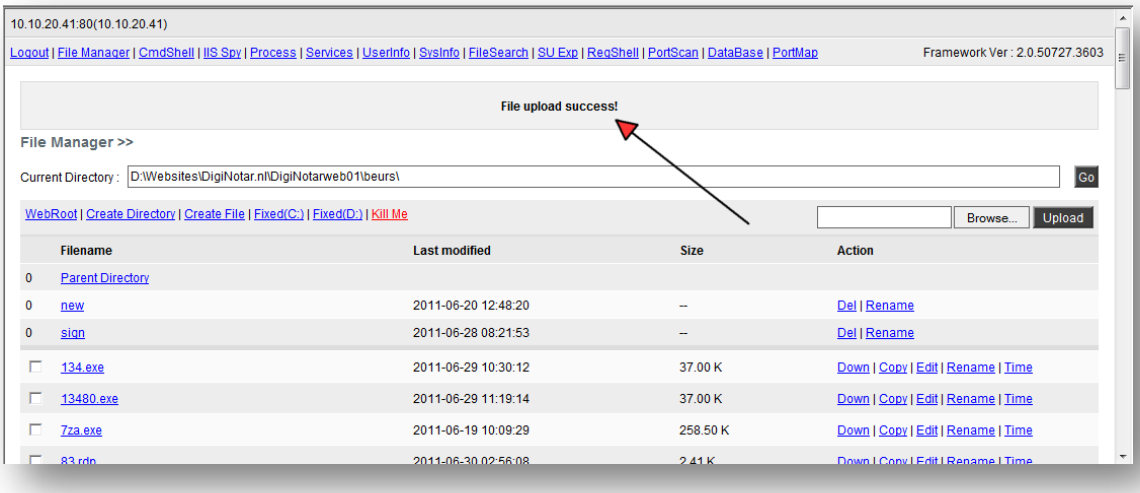


Figure 4 Example of a cached file upload page

If traces of a (recoverable) cached copy of the file exchange scripts from the stepping stones were identified on a system, the system could be marked as compromised by the intruder as only the intruder was aware of the existence of these scripts at that point in time. For this reason, the systems were probed for existing or recoverable `settings[*].htm` files (with * representing a number) and their content was inspected. The following systems showed traces of this cached page.

Server	File name	Size	First file create timestamp
BAPI-db	Settings[1].htm	3097	1-Jul-2011 14:33:59
Taxi-CA	Settings[1].htm	104502	1-Jul-2011 22:14:31
Qualified-CA	settings[1].htm	102048	1-Jul-2011 23:48:43
Root-CA	Settings[1].htm	3097	2-Jul-2011 2:40:06
Relation-CA	SETtings[1].htm	3097	2-Jul-2011 20:35:21
Public-CA	SETtings[1].htm	103156	3-Jul-2011 11:03:16

This led to the conclusion that the CA servers cited above were compromised by the intruder and that files may have been transferred to or from the stepping stone in the DMZ-ext-net. The fact that these files originated from Microsoft Internet Explorer also meant that a graphical user interface was available on these systems to the intruder using a tunneled remote desktop connection.

7.2.3 Network tunnels

A number of identified files that produced a tunnel between two IP addresses were examined more closely. The IP addresses were "hard coded" in the executable. Combined with the fact that the date and time of creation time was fairly recent led the investigators to believe that the files were specifically created (or modified) to run in the DigiNotar network.

The port numbers used suggested that a remote desktop connection (port 3389) was tunneled through port 443 (generally used for HTTPS).

File name	Source host	Destination host
troj134.exe	BAPI-db server	eHerkenning-AD server
troj172.exe	BAPI-db server	Pass-web server
troj25.exe	Source-build server	eHerkenning-AD server
troj65.exe	Docproof2 server	AttIP1

The earliest evidence of these tools in the examined servers was on June 29, 2011 at 22:13 on the BAPI-db server in Office-net.

Other created tools were partially investigated, specifically:

File name	Results
94.exe	Found on Docproof2. Created a connection to AttIP2.
134.exe	Created a connection to the server eHerkenning-AD on Port 443
13480.exe	Found on BAPI-db. Created a connection to the server eHerkenning-AD on Port 443

7.3 Gaining a foothold

Several tools found were used to scan for vulnerabilities and to increase the intruder's level of access in the network, such as scanning tools, port redirectors and remote process executor tools. Also, several files were found that indicated that the intruder had attempted to "brute force" terminal service or remote desktop credentials. These tools appeared on the stepping stone file exchange on June 18, 2011.

Traces in the "Documents and settings" directory on the BAPI-db server indicated that the intruder utilized the user account `MSSQLusr` starting on June 17, 2011 at 16:15:49. This user account was used by the Microsoft SQL service that was running on the BAPI-db server. Additionally, on the Main-web server the file `web.config` was identified that contained a string with credentials to access the database on BAPI-db:

```
<add key="connstring" value="Server=172.17.20.4;_Database=BAPI01;
uid=Bapi01usr;pwd=Bapi01usr12345!" />
```

This led to the conclusion that the intruder connected to the Microsoft SQL service running on the BAPI-db server from the Main-web using a found password and executed programs on the BAPI-db. The connections were not prohibited by the firewall as the investigation on the firewall log has shown in paragraph 5.2.3.

When the rights of the MSSQLusr account were examined it showed that MSSQLusr was part of the local administrators group, but the `LastWrite` date for the group was 18 June, 2011 at 02:18:48. The administrator rights could have been obtained after an effort by the intruder to escalate his rights or because the `MSSQLuser` had local administrator in the first place and that no further efforts were necessary. Event logs were not available to determine when MSSQLusr was first added to the local administrators group. On 1 July, 2011 at 14:33:59, the intruder used the local administrator account on the BAPI-db server.

The data shows that the intruder had used the administrator rights on the Qualified-CA server for the domain `DNPRODUCTIE` on July 1, 2011 at 23:48:43. Although this date is the first date seen in the investigation using a domain administrator account, it does not mean that the rights were not utilized earlier.

7.3.1 Password cracking tools

On the CCV-CA server, the well known `Cain & Abel` tool with `winpcap` had been installed. This tool can be used to extract and to crack password hashes. `Cain & Abel` can also be used to extract password hashes and to "brute force" the hashes to reveal the original passwords. Also the `pwdump` and `cachedump.exe` tools were found on the BAPI-db server and a stepping stone server.

On the desktop of the CCV-CA server, deleted files were found containing the output from the tool `pwdump`:

- `winsvr022.txt` (winsvr022 is the Qualified-CA server)
- `winsvr056.txt` (winsvr056 is the Public-CA server)
- `winsvr167.txt` (winsvr167 is the Root-CA server)

Evidence was found that `Cain & Abel` was used to capture credentials using a man-in-the-middle attack. More specifically, deleted Kerberos tickets and NTLM challenge-responses were found in the files `K5.LST`, `KRB5.LST`, `SMB.LST` and `HOSTS.LST`.

On the Docproof2 stepping stone, a file `test.txt` was found with the output of `cachedump.exe`. The file contained the `mscache` hash of one of the administrators. The administrator password could easily be brute forced on the basis of the hash, which indicated that the password that was used was relatively weak.

The earliest traces of a similar tool `PwDump.exe` in the examined servers in Office-net date from June 17, 2011 at 16:19 on the BAPI-db server. The earliest traces of the tool `cachedump.exe` in the examined servers in Office-net date from June 21, 2011 at 12:50 on the BAPI-db server.

Also the files `mimi.zip`, `mimikatz.exe`, `demineur.dll`, `klock.dll` and `sekurlsa.dll` were found in the cached web pages of the file exchange on the stepping stone. These files are part of the `mimikatz` security auditing tool. The earliest time of these tools in the examined servers in Office-net are from June 20, 2011 at 11:14 on the BAPI-db server. The traces on the Taxi-CA server showed that the intruder had logged in as administrator and downloaded the file `mimi.zip`.

7.4 Issuing certificates

7.4.1 CA management interface

The temporary Internet files also showed activity on the local CA software web service (by the user `Administrator.DNPRODUCTIE`):

Server	File name	Size	Create date	Create Time
Qualified-CA	domain-main[3].htm	4162	1-Jul-2011	23:22:03
Root-CA	domain-main[1].htm	4162	2-Jul-2011	1:01:41
Root-CA	request-cacert[1].htm	27449	2-Jul-2011	1:05:47
Root-CA	cert-search-results[1].htm	26718	2-Jul-2011	1:06:36
Root-CA	view-cert[1].htm	13557	2-Jul-2011	1:07:17
Root-CA	domain-main[1].htm	4166	2-Jul-2011	1:08:38
Root-CA	request-msie[1].htm	233043	2-Jul-2011	1:08:45
Root-CA	add-msie-request[1].htm	7332	2-Jul-2011	1:10:03
Root-CA	cert-search-results[1].htm	2309	2-Jul-2011	1:11:23
Root-CA	view-cert[1].htm	15164	2-Jul-2011	1:11:52
Root-CA	MinIenM Organisatie CA - G2[1].p7b	5239	2-Jul-2011	1:12:42
Root-CA	cert-search-results[1].htm	3711	2-Jul-2011	1:15:56
Relation-CA	cert-search-script[1]	20027	2-Jul-2011	20:42:08
Relation-CA	cert-search-results[5].htm	58415	2-Jul-2011	20:43:29
Relation-CA	view-cert[1].htm	13654	2-Jul-2011	20:43:43
Relation-CA	index[2].htm	5291	2-Jul-2011	21:20:20
Relation-CA	cert-search[1].htm	11192	2-Jul-2011	21:20:30
Relation-CA	cert-search-script[1].htm	19411	2-Jul-2011	21:20:30
Relation-CA	cert-search-results[4].htm	340	2-Jul-2011	21:22:25
Relation-CA	cert-search-results[6].htm	9966	2-Jul-2011	21:37:08
Relation-CA	get-ca-list[3].htm	3071717	2-Jul-2011	21:51:22
Relation-CA	get-ca-list[2].htm	3071717	2-Jul-2011	21:54:12
Relation-CA	index[1].htm	2525	2-Jul-2011	21:55:49
Relation-CA	get-ca-list[5].htm	332	2-Jul-2011	21:55:57

These traces showed that the intruder was experimenting with the CA management software. On the Relation-CA server, many `pkcs10` requests were made using the local CA software web interface. Also many Certificate Signing Requests (CSRs) were manually made with this interface.

7.4.2 XUDA scripts

The CA management software has an interface that can be used to execute custom applications. These applications can be developed using a scripting language called XUDA (Xcert Universal Database API).

On July 2, 2011 at 02:18:56, the Root-CA server created a Dr. Watson error dump of `Xuda.exe`. This means that `xuda.exe` had crashed, which was probably due to experimentation by the intruder given the time of occurrence (Saturday night local time).

On the Relation-CA server, the XUDA script `get.xuda` was recovered, which was created on July 2, 2011 at 16:58. This script was accessed by the local Internet Explorer on the Relation-CA server, as evidenced by a cached page showing a XUDA error.

Another XUDA script was found on the Public-CA server. This file `x-select-settings.xuda` was found with a modification timestamp of July 3, 2011 at 22:59:18. The script contained XUDA-code that uses the Xcert Universal Database API in order to utilize the CA software. In this script, two lists of 113 signing requests were included. The investigation on the CA management software as described in Chapter 6 shows more rogue certificates were issued than the amount of signing requests included in the XUDA script.

In this script, a personal message from the intruder was enclosed:

```
 3 I know you are shocked of my skills, how i got access to your network
 4 to your internal network from outside
 5 how I got full control on your domain controller
 6 how I got logged in into this computer
 7 HoW I LEARNED XUDA PROGRAMMING
 8 HOW I got this IDEA to write such XUDA code
 9 How I was sure it's going to work?
10 How i bypassed your expensive firewall, routers, NetHSM, unbreakable hardware keys
11 How I did all xUDA programming without 1 line of resource, got this idea, owned your
 . network accesses your domain controlled, got all your passwords, signed my certificates
 . and received them shortly
12 THERE IS NO ANY HARDWARE OR SOFTWARE IN THIS WORLD EXISTS WHICH COULD STOP MY HEAVY
 . ATTACKS
13 MY BRAIN OR MY SKILLS OR MY WILL OR MY EXPERTISE
14 That's all ok! EVerything I do is out of imagination of people in world
15 I know you'll see this message when it is too late, sorry for that
16 I know it's not something you or any one in this world have thought about
17 But everything is not what you see in material world, when God wants something to happen
18
19
20 My signature as always: Janam Fadaye Rahbar
21
22
23 Rahbare azizam mesle hamishe asoode bash, ta vaghti ke man va amsale man baraye in marzo
 . boom
24 va baraye barafrashte negah dashtane parchame velayate faghih kar mikonand
25 daste har doshmano mozdouri ghat khahad bood
26 Rahbaram, Tamame vojoodam fadaye to ke ham jani o ham janani
```

The intruder left his fingerprint in the text: *Janam Fadaye Rahbar*[33]*.* The same text was found after the security breach at the Comodo certificate authority in March of 2011,[34] which also resulted in the issuing of rogue certificates.

[33] Supposedly translates to: "I will sacrifice my soul for my leader"
[34] Wired, "Independent Iranian Hacker Claims Responsibility for Comodo Hack" at http://www.wired.com/threatlevel/2011/03/comodo_hack/

7.4.3 nCipher DLLs

During the investigation on the Qualified-CA server, it appeared that some of the DLLs that were used to access the netHSM had been modified. These files were located in the `WINDOWS\system32` directory:

- `nfmodexp.dll`
- `ncspmess.dll`
- `ncsp.dll`
- `ncspdd.dll`
- `ncspsigdd.dll`

The unusual creation, modification and access times for these files were all around July 2, 2011 at 00:24:03, which was sufficient reason to mark these files as suspicious.

The manufacturer of the nCipher netHSM (Thales e-Security) provided us with the hash digest of the original DLLs. These hashes matched exactly with the hashes of the encountered DLLs. This led to the conclusion that the encountered DLLs had not been tampered with. It remains possible however that the DLLs had been modified but were later replaced by the original DLLs, which would explain the unusual creation date.

Related to this, nCipher logs were encountered with unusual timestamps. The following nCipher logs from the Root-CA server were created on July 2, 2011 at 01:28:19:

- `Application Data\nCipher\Log Files\keysafe.log`
- `Application Data\nCipher\Log Files\cmdadp.log`
- `Application Data\nCipher\Log Files\cmdadp-debug.log`

These traces on the DLLs and logs could indicate that the intruder had tried to use the netHSM and its stored private keys directly.

7.5 Conclusion

By examining the browser history and temporary Internet files of the compromised CA servers, it quickly became clear that the intruder used the Main-web and Docproof2 servers in DMZ-ext-net as stepping stones to transfer files. Scripts that provided the file exchange functionality were first placed on these servers in the early hours of June 17, 2011.

After compromising the web servers in DMZ-ext-net, the intruder used the Microsoft SQL service running on the BAPI-db server to execute files utilizing the BAPI-db server in the Office-net.

Tools were found that had been created by the intruder to provide network tunnels. Most of the investigated tunnels were used to set up a remote desktop connection with systems that were not directly connected to the Internet using the stepping stones. The IP addresses in these tools were used to tunnel traffic between the intruder (AttIP1 and AttIP2) and servers in the DMZ-ext-net (Docproof2) and subsequently between the DMZ-ext-net (eHerkenning-AD and Pass-web) and servers in the Office-net (BAPI-db and Source-build).

The investigation showed that the first found activity by the intruder in Secure-net took place on July 1, 2011 at 22:14:31 on the Taxi-CA server. The intruder first used the administrator rights for the domain `DNPRODUCTIE` on July 1, 2011 at 23:48:43 (on the Qualified-CA server). Although this date was the first date seen in the investigation, it does not mean that the rights were not utilized earlier. All CA servers in Secure-net were included in this domain.

Traces of tools and attempts to brute force password hashes were found. Furthermore, traces of attempts were found to create certificates with the user interface of the CA management software. Moreover, XUDA scripts and other traces were found that indicated that the programming interface of the CA software was abused.

Results of the initial investigation by DigiNotar indicated that an automatic process was in place to transfer files to the stepping stone.

The presence of cached pages of the file exchange HTML-pages from the stepping stone indicated that the servers containing these cached pages had been compromised by the intruder. Additionally, found

tools, logs and other traces marked or confirmed all the investigated servers as having been compromised on the basis of the results of this part of the investigation:

Network	Server
Secure-net	Qualified-CA
	Taxi-CA
	Relation-CA
	Public-CA
	Root-CA
	CCV-CA
Office-net	Office-file server
	BAPI-db
DMZ-ext-net	Main-web
	Docproof2

Based on the investigation of tools found, the following external AttIP addresses are likely to been utilized by the attacker (see also Appendix II):

Intruder IP	Remark
AttIP1	Malware found on Docproof2 (troj65.exe)
AttIP2	Malware found on Docproof2 (95.exe)

8 Remaining investigation

During the investigation, a limited number of assorted sources were examined. The results of these examinations are combined in this chapter.

8.1 netHSM

DigiNotar used nCipher netHSM 500s. The systems have limited logging facilities. It is recommended by the vendor to store the logs on a separate log server, but this was not done at DigiNotar. The logs were stored on the netHSM for a short period of time and were deleted every time the system was turned off. This had already occurred when the investigation was started by Fox-IT. No useful log files could be retrieved.

8.2 Load balancer

The network traffic was load balanced by a Coyotepoint Equalizer e550SL appliance. The logs from this appliance were stored on a central syslog server. An investigation of the logs from the load balancer and those that were present in the appliance itself showed no information that was relevant for the investigation.

8.3 External server at AttIP2

During the investigation a tool was found that connected back to the external IP address AttIP2 (see paragraph 7.2.3). On September 13, 2011, an official request for assistance to the authorities in the country where the server was located was issued. A copy of this server was investigated.

The web server log files from the server on AttIP2 showed interesting entries of GET requests from AttIP3. These log entries showed that the file `mails.rar` was downloaded several times on July 19, 2011 between 16:35:51 and 19:42:17. This file was only downloaded by AttIP3, except for the first occurrence when it was downloaded by AttIP5.

9 Summary of findings

The primary aims of the investigation that Fox-IT performed at the request of the ministry BZK were to determine how DigiNotar's network had been breached, to what extent it had been breached, which Certificate Authorities had been compromised and if evidence could be safeguarded that could lead to a potential criminal indictment of the intruder. For these purposes, various sources of information were gathered and examined, including the log files from the web servers, firewall and the various CA servers. Additionally, the images of relevant systems in DigiNotar's network were analyzed.

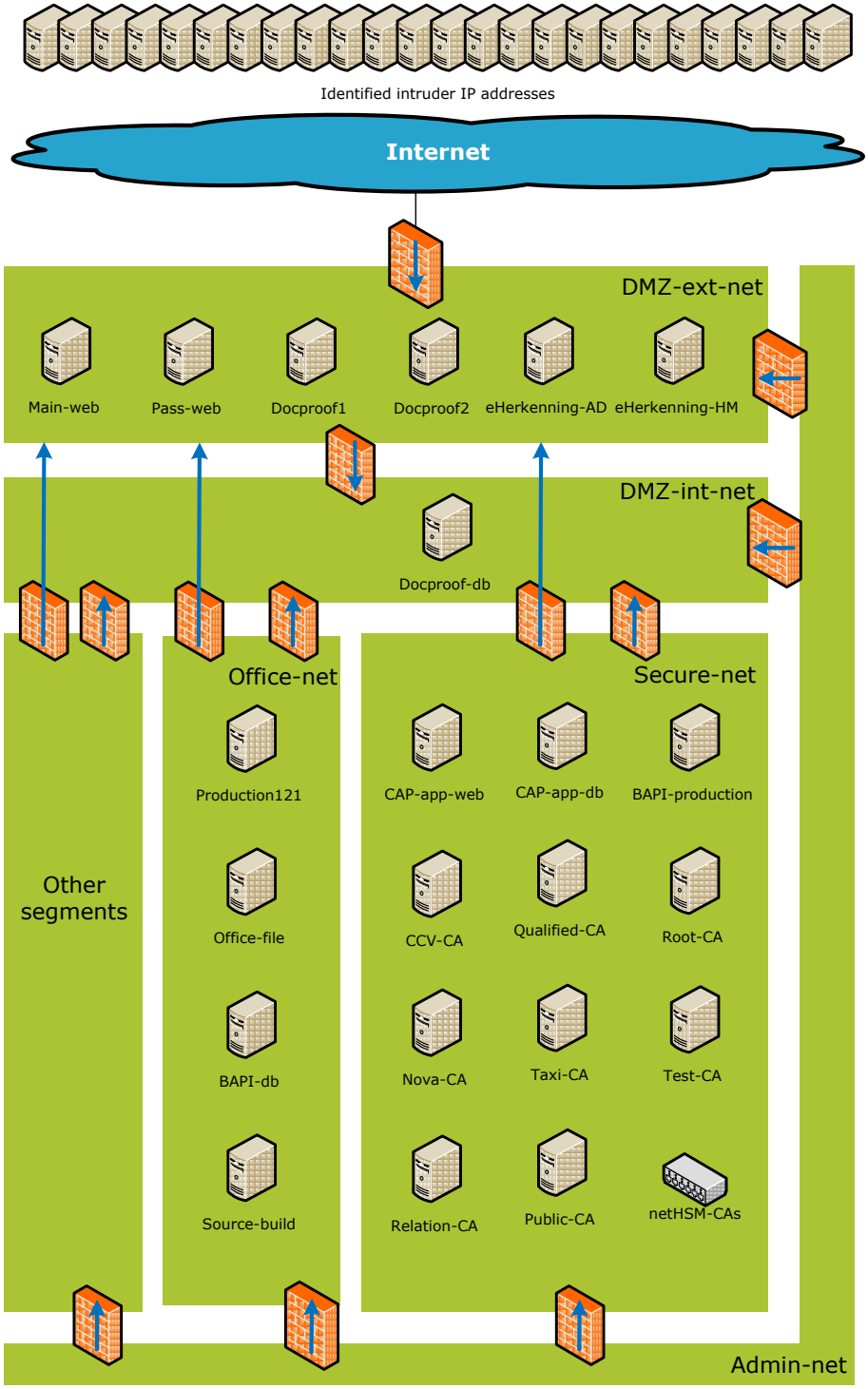


Figure 5 Referenced systems

9.1 First point of entry and stepping stones

The web servers on the outskirts of DigiNotar's network (DMZ-ext-net) served as the first point of entry for the intruder. Both the Main-web and the Docproof2 web servers were running an outdated version of DotNetNuke that suffered from known security vulnerabilities and were compromised on June 17, 2011. Log files that had been deleted on Main-web server were recovered and showed that scripts named `settings.aspx` and `up.aspx` in the directory `/beurs` had been used as rudimentary file managers and that the server acted as a stepping stone to other systems in the network. A similar script was identified on the Docproof2 server, but was used less frequently.

The log entries from the web servers that referenced the `/beurs` directory could be used to generate a list of both internal and external systems that had connected to these systems in order to use them as stepping stones. Internal systems that had connected to the `/beurs` directory could be flagged as having been compromised, while external systems that had connected to these scripts had been abused by the intruder. In total, 12 internal and 21 external suspicious IP addresses connected to the `/beurs` directory during the period that the security of DigiNotar's network was breached and 125 unique file names could be identified as having been copied to or from these stepping stones.

9.2 Compromised systems and Certificate Authorities

Based on the investigations of web server log files and the hard disks, the following internal systems could be identified as having been compromised:

Network Segment	Server
DMZ-ext-net	Main-web
	Pass-web
	Docproof1
	Docproof2
	eHerkenning-AD
	eHerkenning-HM
DMZ-int-net	Docproof-db
Office-net	BAPI-db
	Office-file
	Production121
	Source-build
Secure-net	CAP-app-db
	CAP-app-web
	Public-CA
	Qualified-CA
	Relation-CA
	Root-CA
	CCV-CA
	Taxi-CA
	BAPI-production

In addition to these systems, the attacker had the opportunity to compromise many more systems. No complete survey has been made to identify all the compromised systems due to limited time of the investigation.

The investigation showed that database records of the software managing the Certificate Authorities had been deleted or otherwise manipulated. The log files of the CA management software were stored on the same CA servers that had been compromised. Consequently, suspicious entries in the log files can only be used to make inconclusive observations regarding unauthorized actions that took place, but the absence of suspicious entries cannot be used to infer that no unauthorized actions took place.

However, in order to successfully issue rogue certificates, compromising a system that managed a Certificate Authority was not sufficient, as it also required the use of an active private key in a netHSM. This meant that the unauthorized actions that might have taken place could not have included the issuing of rogue certificates if the corresponding private key had not been active during the period in which the

intrusion took place. No records could be provided by DigiNotar if and when smartcards had been used to activate private keys in the netHSM, except that the smartcard for the CCV Certificate Authority had reportedly been in a vault for the entire period of the intrusion.

A Certificate Revocation List (CRL) generation process was identified for many Certificate Authorities on several CA servers. The identification of the regular automatic generation of CRLs showed that private keys in the netHSM for a number of Certificate Authorities were active and potentially provided an opportunity for the intruder to abuse these private keys. The combination of a compromised server, the automatic CRL generation, and the fact that logs had been or could have been tampered with, meant that the possibility could not be excluded that Certificate Authorities had been abused to issue rogue certificates. Even if no CRL generation process was active, the possibility could not be excluded that a compromised CA server had been instructed to issue rogue certificates once the corresponding private key was activated for its intended purpose.

Furthermore, it was found that the number of issued rogue certificates in the log files exceeded the number of rogue certificates in the CA management application. Additionally, serial numbers of certificates were identified that could not be matched with any certificate that DigiNotar had intentionally or unintentionally issued. These unknown serial numbers included the rogue wildcard Google.com certificate that was abused in the massive MITM attack primarily on Iranian users. The identification of unknown serials on a CA server therefore meant that the possibility could not be excluded that the Certificate Authority may have issued rogue certificates. Unknown serial numbers were identified to have been issued by certificate authorities hosted on the Public-CA, Qualified-CA, Root-CA and Taxi-CA servers.

Recovered log files from the Relation-CA server showed that the first extraordinary activity on the server occurred on July 2, 2011 and that the first rogue certificate was issued on the server on July 10, 2011. Recovered traces showed that the Remote Desktop Protocol had been used to gain access using a graphical user interface to at least seven servers: BAPI-db, Taxi-CA, Qualified-CA, Root-CA, Relation-CA, Public-CA and Qualified-CA. These connections were made through network tunnels bypassing the firewall.

It was evident that rogue certificates had been issued by Certificate Authorities managed on the Public-CA and Relation-CA servers, identifiable on the basis of their Common Name, that had to be revoked. Additionally, all unknown serial numbers had to be revoked as a number of these serials were known to correspond with rogue certificates. Given the fact that all DigiNotar's servers managing Certificate Authorities had been compromised and that relevant logging occurred on the same systems, all Certificate Authorities may have been abused in ways that are not reflected in (recoverable) log files. The way in which the Certificate Authorities may have been abused could not have included the issuing of rogue certificates, unless the corresponding private key was active in the netHSM at some point during the intrusion. Only the CCV Certificate Authority could be excluded from the list of Certificate Authorities that may have issued rogue certificates on this basis.

9.3 Information about the intrusion and the intruder

The intruder first gained unauthorized access to DigiNotar's network on June 17, 2011 and connections to AttIPs that were abused by the intruder were initiated from internal systems up to July 22, 2011. From the DMZ-ext-net, the intruder gained access to servers in the Office-net using a MSSQL server in that network. The first unauthorized connection that was identified from Office-net to DMZ-ext-net occurred on June 29, 2011. The first suspicious activity found in the Secure-net was on July 1, 2011 and connections appeared from Secure-net to DMZ-ext-net starting on July 2, 2011. Traces from the intruder were found in DMZ-ext-net up to Jul 24, 2011.

Unauthorized customized tools were used by the intruder to tunnel traffic intended for port 3389 (generally used for Remote Desktop Protocol) through port 443 (generally used for HTTPS). These tunnels allowed the intruder to connect to systems in the Office-net and Secure-net network segments, using the Remote Desktop Protocol in order to operate using a graphical user interface. This finding was confirmed by the presence of cached versions of the rudimentary file manager `settings.aspx` in the Temporary Internet Files on the hard disks of systems in these segments. These traces proved that Internet Explorer had been used in a graphical environment by the intruder.

The vast majority of the external IP addresses that were identified during the investigation were probably used as proxies to obscure the identity of the intruder. The true IP address of the intruder may have been revealed by error however, when the intruder erroneously connected to the Main-web server without using the proxy on AttIP4. This IP address AttIP3 was also identified in other parts of the investigation. More specifically, during the investigation a tool was identified that connected back to AttIP2. When this external system was examined, after an official request for assistance to the proper foreign authorities, its log files also showed connections from AttIP3. Furthermore, eight requests were made by AttIP3 when the DigiNotar's OCSP responses were tested for a rogue Yahoo certificate. AttIP3 resolved to a DSL user in the Islamic Republic of Iran. The first three OCSP requests of the wildcard Google.com certificate used for the MITM attack came from AttIP6 that also connected to the stepping stone on the Main-web server. The IP addresses AttIP6 and AttIP3 are from the same class-a network together with AttIP12, AttIP13 and AttIP14. A complete list of all the identified AttIPs has been handed over to the Dutch police (KLPD).

9.4 Timeline of the intrusion

Date	Notes
17-Jun-2011	Both the Main-web and the Docproof2 web server were compromised. File exchange functionality in DMZ-ext-net was in place. The first attempts to connect to the MSSQL server (BAPI-db) occurred from DMX-ext-net to Office-net. Later that day the first suspicious activity on the BAPI-db server in the Office-net occurred using the `MSSQLusr` user account.
18-Jun-2011	The first traffic was initiated by internal servers to IP addresses known to have been abused by the intruder (connect back functionality).
29-Jun-2011	Various scanning attempts were made to increase the foothold in other network segments (see Appendix III). The fact that scanning attempts were apparently necessary indicated that the intruder was still restricted to Office-net. The first tunneled connections over port 443 occurred from Office-net to DMZ-ext.
1-Jul-2011	The first scanning activity occurred in Secure-net. The stepping stone web page was accessed on CA servers in the Secure-net.
2-Jul-2011	The first successful connection was made from Secure-net to the stepping stone in DMZ-ext. Date of the first traces of experiments with the CA management software web interface and XUDA scripts on the Root-CA and Relation-CA servers.
3-Jul-2011	Modification time of a XUDA script with a personal message from the intruder on the Public-CA server and the first extraordinary activity in the CA software logs on the Public-CA server.
4-Jul-2011	Tools were setup to automatically transfer files from the Public-CA server to the stepping stone.
10-Jul-2011	The first rogue certificate was successfully created on the Relation-CA server. Subsequently, another 85 rogue certificates were created on the Relation-CA server. Another 198 rogue certificates were created on the Public-CA server. OCSP requests for rogue certificates started arriving at DigiNotar's OCSP responder from an DSL subscriber in Iran.
18-Jul-2011	Log files showed a burst of 124 rogue certificates that were created on the Public-CA server.
20-Jul-2011	Log files showed another burst of 124 rogue certificates were created on the Public-CA server. This is the last known date of the creation of rogue certificates.
22-Jul-2011	The last traffic was initiated from within DigiNotar's network to known intruders' IP addresses based on the investigation of the firewall logs.
24-Jul-2011	Last known date for traces of the intruder in DMZ-ext-net.

10 MITM attack

The investigation that was performed on the servers of DigiNotar as described in the previous chapters clearly showed that a large number of rogue certificates were issued by the intruder. The goal of the intrusion at DigiNotar appeared to have been to get a Certificate Authority to sign certificates. Most of the Certificate Authorities that were managed by DigiNotar were on trust lists of popular software products. Consequently, most operating systems, web browsers and document viewers instantly trusted the certificates that had been issued by DigiNotar.

The investigation showed that even though a large number of rogue certificates were identified, it could not be excluded that many more existed nor could it be excluded that these certificates could have had any content. This resulted in a situation where the intruder created certificates that could contain whatever content he desired and that these certificates would be trusted by all the most commonly used software products. Since most users trust their software, the chain of trust effectively meant that users trusted an unknown and malicious party.

The fact that the chain of trust of PKI had been broken by the intrusion at DigiNotar did not just result in a hypothetical threat, but a rogue certificate was abused in practice to mislead users on a large scale. The following paragraphs detail insights that resulted from Fox-IT's investigation of the breach of DigiNotar as well as of the MITM attack that subsequently took place using the issued rogue certificates.

10.1 Identified rogue certificates

The investigation identified certificates that were issued during the intrusion of DigiNotar's CA servers. Some of these certificates that were issued during this timeframe were intentionally created by DigiNotar and matched the administration in DigiNotar's back office. Certificates that were issued but that were unknown to the back office records generally used very noticeable common names within the certificates. Based on these noticeable names, other certificates were identified and accumulated to a list of 531 rogue certificates. It cannot be ruled out that the rogue certificates that were created during the period within which the intruder was active may also have contained ordinary common names. However, only the certificates with unusual common names could be flagged as rogue and further examined, since the serial numbers of certificates were not logged when they were issued.

When examining the distinguished names (DN) of the 531 certificates that were marked as rogue, only 140 unique distinguished names were encountered. Part of the distinguished names is a common name (CN). Most applications that use certificates only take note of the common name. Of the 531 certificates, only 53 unique common names were found. For example, when looking at the following distinguished names one unique common name can be identified, that is `*.google.com`.

```
CN=*.google.com, SN=google, OU=Knowledge Department, L=US, O=Google Inc, C=US
CN=*.google.com, TITLE=Google, SN=PK0002292001, L=Mountain View, O=Google Inc, C=US
```

The list below shows the common names of the identified certificates that were flagged as rogue, including the number of certificates that were issued using the common name. Of these common names, 46 contained a DNS domain name and the other 7 CNs contained names of Certificates Authorities.

Common name	Number Issued
..com	1
..org	1
*.10million.org	2
*.android.com	1
*.aol.com	1
*.azadegi.com	2
*.balatarin.com	3
*.comodo.com	3
*.digicert.com	2
*.globalsign.com	7
*.google.com	26
*.JanamFadayeRahbar.com	1
*.logmein.com	1

Common name	Number Issued
*.microsoft.com	3
*.mossad.gov.il	2
*.mozilla.org	1
*.RamzShekaneBozorg.com	1
*.SahebeDonyayeDigital.com	1
*.skype.com	22
*.startssl.com	1
*.thawte.com	6
*.torproject.org	14
*.walla.co.il	2
*.windowsupdate.com	3
*.wordpress.com	14
addons.mozilla.org	17

Common name	Number Issued
azadegi.com	16
friends.walla.co.il	8
GlobalSign Root CA	20
login.live.com	17
login.yahoo.com	19
my.screenname.aol.com	1
secure.logmein.com	17
twitter.com	18
wordpress.com	12
www.10million.org	8
www.balatarin.com	16
www.cia.gov	25
www.cybertrust.com	1
www.Equifax.com	1

Common name	Number Issued
www.facebook.com	14
www.globalsign.com	1
www.google.com	12
www.hamdami.com	1
www.mossad.gov.il	5
www.sis.gov.uk	10
www.update.microsoft.com	4
Comodo Root CA	20
CyberTrust Root CA	20
DigiCert Root CA	21
Equifax Root CA	40
Thawte Root CA	45
VeriSign Root CA	21

Some of these common names can be considered a signature from the intruder:

- CN=*.SahebeDonyayeDigital.com, SN=PK000229200006592, OU=Elme Bikaran, L=Tehran, O=Daneshmande Bi nazir, C=IR
- CN=*.RamzShekaneBozorg.com, SN=PK000229200006593, OU=Sare Toro Ham Mishkanam, L=Tehran, O=Hameye Ramzaro Mishkanam, C=IR
- CN=*.JanamFadayeRahbar.com, SN=PK000229200006594, OU=Sarbaze Gomnam, L=Tehran, O=Ke Jano Janan Toyi, C=IR

Reportedly, RamzShekaneBozorg (.com) translates to "great cracker" in Farsi, "Hameyeh Ramzaro Mishkanam" translates to "I will crack all encryption" and "Sare Toro Ham Mishkanam" translates to "I hate/break your head."

Anyone in possession of these rogue certificates could host a website that corresponded with the common name of a rogue certificate and mislead people to trust the website as the original site. By hosting a fraudulent website and redirecting the requests that are made by users to the original website, an attacker can monitor the interaction between the original website and the user without the knowledge of the user. This kind of attack is called a man-in-the-middle (MITM) attack. During the large-scale MITM attack that was perpetrated against primarily Iranian Internet users, the attack was compounded with a form of redirection, where users who tried to reach legitimate websites that were hosted by Google were redirected to fraudulent websites that used a certificate with `*.google.com` as its common name. The traffic which was meant for Google and that was intercepted was not necessarily forwarded to Google, as users may have been presented with a page specifically intended to phish for their credentials.

10.2 Investigation of OCSP responder log files

There are standards that prescribe how certificates should be created, be formatted, how they can be used, et cetera. All the systems involved in the creation and maintenance of certificates together form a Public Key Infrastructure (PKI). The standards also prescribe that software using certificates must verify the status of the certificate. It must be verified if the certificate that is presented has not been revoked. The most commonly used way to do this is by verifying the status online in real time at the issuing Certificate Authority. This is done using the Online Certificate Status Protocol (OCSP). An OCSP responder was present at DigiNotar.

The log files of the OCSP responder were an interesting source for information because, when a rogue certificate was used to mislead users, the software that was utilized by the users verified the validity of the certificate at the OCSP responder. This provided a possibility to detect what rogue certificates were being abused and what IP addresses were affected. Profiling the OCSP responder logs could provide further insight into the MITM attack that was perpetrated using rogue certificates originating from DigiNotar. The question was posed what the greatest common divisors were in the abuse of the rogue certificates in the MITM attack.

A difficulty with this investigation was that an OCSP request that is made to the OCSP responder only consists of a serial number. Additionally, more rogue certificates could have been issued by DigiNotar than that could be identified on the basis of the evidence that could be recovered. These rogue

certificates could have any content and serial number. Therefore, it would not always be possible to determine what the common name or URL of the certificate was for the serial that the user was verifying.

Before August 29, 2011, all the OSCP verification requests of unknown serials resulted in the response of GOOD or UNKNOWN, as this is the standard prescribed response in such a case.

The content of a rogue certificate that was issued by DigiNotar, but which could only be identified as an unknown serial number in a deleted file on the CA server at DigiNotar, became public when a `*.google.com` certificate was posted by a concerned user on a forum.[35] Once the news reached DigiNotar, the serial number was revoked effectively on August 29, 2011 at 19:09:05 (CEST). This certificate became known because of an additional check on the validity of the used certificate that was performed by Google Chrome.

Between August 29, 2011 and September 1, 2011, unknown serials were manually revoked by DigiNotar. On the advice of Fox-IT, a precautionary measure was taken, namely that any serial number query that was presented to the OCSP responder which did not match with the records in the back office of DigiNotar was presumed to be rogue. In such a case, the OCSP responder was set to answer that the serial number had been revoked. This white-list based OCSP response was fully functional on September 1, 2011.

10.2.1 Sources

Log files of the OCSP verification requests from May 1, 2011 at 0:00 to August 30, 2011 at 1:56 were examined. During this period, approximately 27 million requests were made averaging at 300,000 requests per day. This log was enriched with localization fields using GeoIP from MaxMind, making it possible to determine where IP addresses are located.[36] The log files contained the following information:

- Timestamp of the request (in CEST)
- The identifier for the certificate authority receiving the request
- Serial number of the certificate that is being verified (additionally marked normal or rogue)
- IP address of the requesting client, including
    - Its country name and code
    - Its registered Autonomous System (AS) name and number[37]

10.2.2 Yahoo certificate

Fox-IT's investigation showed that remarkable OCSP requests were made for a rogue certificate with the common name `login.yahoo.com`. The first request for this rogue certificate occurred only one hour and 50 minutes after the certificate was presumably generated. Furthermore, the request originated from an IP address that was identified during the investigation of the DigiNotar intrusion (namely AttIP3).

OCSP requests Yahoo certificate	
Serial	`3612f911f611984191fc310e74645d16`
Issuer	Koninklijke Notariele Beroepsorganisatie CA
Common Name	`login.yahoo.com`
Validity	Not before 10-Jul-2011 16:22:26 (UTC) Not after 9-Jul-2013 16:22:26 (UTC)
Revoked	27-Jul-2011 12:01:41 (UTC)
Total usage	10-Jul-2011 20:12:11 to 29-Jul-2011 11:52:40 (CEST) 8 requests from AttIP3 0 status GOOD responses

This led to the assumption that the DigiNotar intruder created the rogue certificate for `login.yahoo.com` and later attempted to verify the status of the certificate.

[35] Google Groups, "Is This MITM Attack to Gmail's SSL?" at http://groups.google.com/a/googleproductforums.com/d/topic/gmail/3J3r2JqFNTw/discussion
[36] Within an reasonable margin of error.
[37] Identifying the registered network operator, usually an Internet Service Provider (ISP).

10.2.3 Google certificate

The serial number of the Google.com certificate that was found by a Gmail user was encountered many times in the OCSP logs. Between the first request and the moment that the certificate was revoked, the OCSP responder had responded to approximately 300,000 unique IP addresses that it was valid.

OCSP requests Google certificate	
Serial	05e2e6a4cd09ea54d665b075fe22a256
Issuer	DigiNotar Public CA 2025
Common Name	*.google.com
Validity	Not before 10-Jul-2011 19:06:30 (UTC) Not after 9-Jul-2013 19:06:30 (UTC)
Revoked	29-Aug-2011 16:58:47 (UTC)
OCSP requests	654.313 status GOOD responses from 298.140 unique IP addresses between 30-Jul-2011 09:11:47 and 2011-08-29 19:09:05 (CEST)

The amount of unique IP addresses that made OCSP requests can only be regarded as a very rough approximation of the amount of users who were affected. Multiple users can be masqueraded behind a single external IP address, while a single user can also make requests from multiple IP addresses. Moreover, relatively old software such as Internet Explorer 6 does not support OCSP requests and these users are not included in the aforementioned number. In conclusion, it can be said that users behind these IP addresses that made OCSP requests were the victims of a MITM attack and were redirected to a fraudulent version of a Google website.

When examining OCSP requests, it was noticed that the first three requests were made within one hour on July 30, 2011 from an IP address that was also discovered in the examination of the DigiNotar intrusion (AttIP6). The next requests were made starting August 4, 2011 at 03:05:40 (CEST) and showed a sudden increase and diversity. The other IP addresses found in the DigiNotar intrusion were not observed attempting to validate the *.google.com certificate.

10.2.4 Unknown serials for verified certificates

While the investigation focused on the rogue wildcard Google certificate, a limited number of OCSP requests for other serial numbers were also identified. Below is a list of OCSP requests for unknown serial numbers for which the OCSP responder answered with "GOOD," indicating that the certificate was valid. The amount of requests for the *.google.com certificate clearly outnumber all other requests. The next table shows the OCSP responses to verification requests of unknown serial numbers.

Serial number[38]	Response	Number of reqs.	First request (CEST)	Last request (CEST)
0B41ABEE6F4168D3CDE5A7D223B58BC1*	GOOD	214	10-Jul-2011 20:34:16	30-Jul-2011 06:28:33
009D06313F21A4EDF734C324FFBCB9E2B5*	GOOD	2	13-Jul-2011 13:19:52	16-Jul-2011 10:11:51
44231633DEE9C328362FADC029C33B	GOOD	63	17-Jul-2011 10:32:45	26-Aug-2011 09:04:51
7C7529653431664F443A3F6C74EB9996	GOOD	231	17-Jul-2011 10:30:16	31-Aug-2011 13:54:17
417EA223198A83712618F185387463	GOOD	16	18-Jul-2011 12:21:48	27-Aug-2011 11:07:15
6AD8A1F4EBD649345320AEC182CFC2	GOOD	10	18-Jul-2011 07:57:34	25-Aug-2011 11:51:04
00E1253D04A17AB8E47F4A5916B9BF9D23*	GOOD	8	23-Jul-2011 10:21:08	30-Jul-2011 09:51:08
7A61A7778842E502E2291166C4574485*	GOOD	1	23-Jul-2011 11:32:03	23-Jul-2011 11:32:03

[38] The serial numbers marked with an asterisk were present in a serial_no.dbh database (see Chapter 6).

Serial number[38]	Response	Number of reqs.	First request (CEST)	Last request (CEST)
05E2E6A4CD09EA54D665B075FE22A256* (*.google.com)	GOOD	654313	30-Jul-2011 09:11:47	29-Aug-2011 19:09:04

For the other serial numbers in this list, no matching certificate could be found. These unknown serials may have been used for small scale MITM attacks or for testing by the attacker.

10.2.5 Targets of the MITM attack

The accumulated affected IP addresses were plotted to provide an insight into how the MITM attack developed over time. It was noted that the number of affected IP addresses seemed to have grown fast from August 4, 2011 onwards.

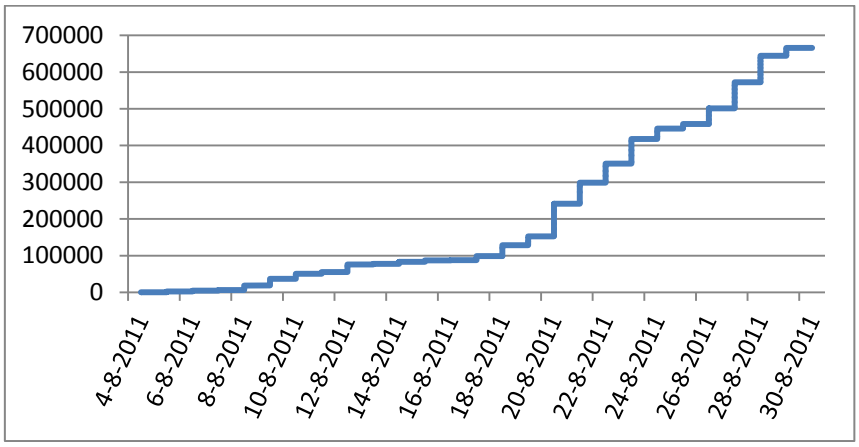


Figure 6 Cumulative number of originating IP addresses

The location information showed that 95% of the OCSP requests for the `*.google.com` certificate originated from Iran (634,665 out of the 665,974 OCSP requests). A1 in the figure below refers to 'Anonymous Proxy' according to the GeoIP results.

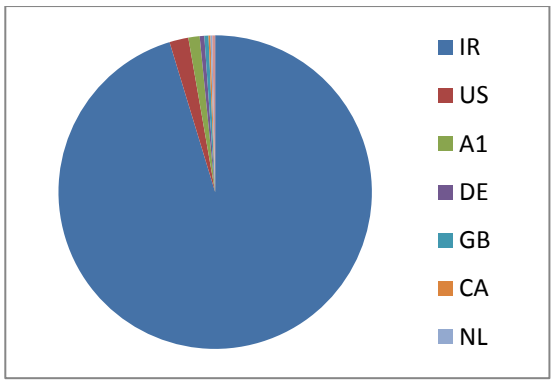


Figure 7 Originating country OCSP requests for the Google.com certificate

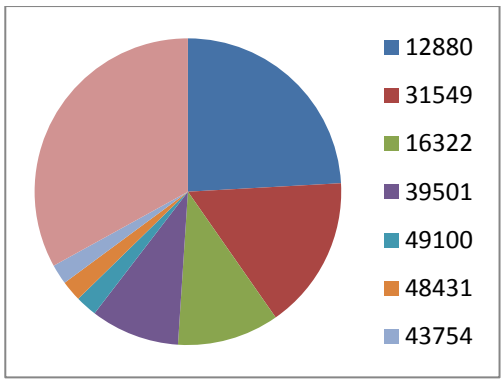


Figure 8 Originating Autonomous System Number (ASN) of the requests

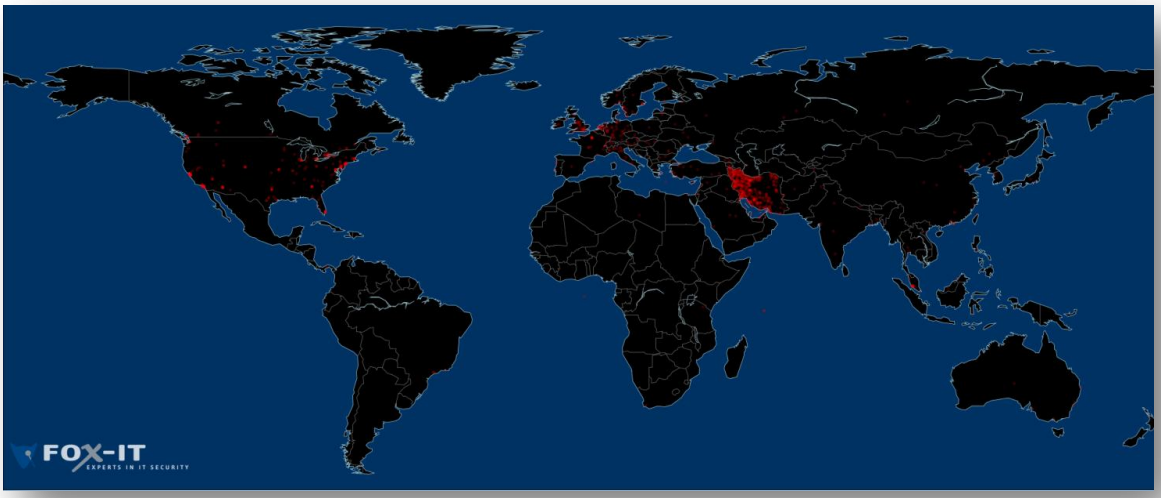


Figure 9 OCSP requests for the rogue `*.google.com` certificate[39]

In total the requests originated from 143 different ASes, while 60% of the requests originated from only 4 Iranian ASes. The spread amongst the other ASes was very broad. The top 7 of rogue requests per Iranian AS are listed below.

ASN	AS name		Number of requests
AS12880	DCI-AS	Information Technology Company (ITC)	160633
AS31549	RASANA	Aria Rasana Tadbir	107761
AS16322	PARSONLINE	PARSONLINE Autonomous System	71520
AS39501	NGSAS	Neda Gostar Saba Data Transfer Company Private Joint	62492
AS49100	IR-THR-PTE	Pishgaman Tose Ertebatat	15110
AS48431	MAXNET-AS	Bozorg Net-e Aria	14652
AS43754	ASIATECH-AS	AsiaTech Inc.	13998

The identification of 5% of the IP addresses outside of the Islamic Republic of Iran could partially have been caused by the inaccuracies of the GeoIP location information that was used. A sample of the IPs located outside of the Islamic Republic of Iran was inspected. Mainly Tor-exit nodes, proxies and VPN servers were identified. On this basis, it can be concluded that the MITM attacks were specifically and almost exclusively targeted at users that were located in the Islamic Republic of Iran.

10.2.6 Modus operandi for the MITM attack

In order to perpetrate a MITM attack in which SSL is used, traffic must be rerouted from the browser of the legitimate website to a fraudulent website, in addition to presenting a certificate that can be validated. Three modi operandi can be identified that could plausibly have been used to redirect users from the legitimate to the fraudulent version of a specific website.

[39] This static image shows all the IP addresses that were detected. A video at http://www.youtube.com/watch?v=wZsWoSxxwVY shows a timeline of the MITM attack on Google users taking place.

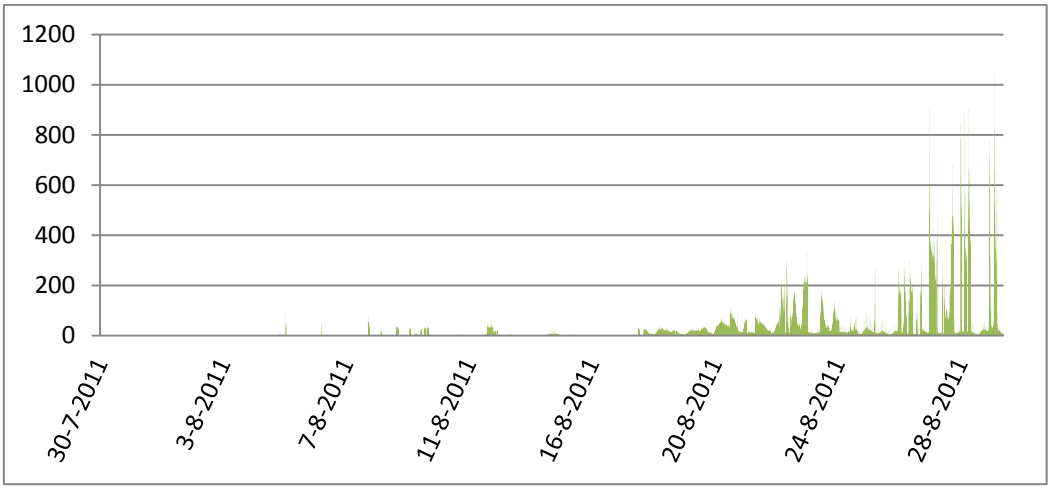


Figure 10 Number of requests per minute

One way in which users can be redirected to a fraudulent website is using a "transparent" MITM attack. Such an attack relies on the fact that one has access to a system that handles the traffic upstream, where specialized hardware can be used to distinguish between traffic or to perform a MITM attack on SSL for a specific domain. A press statement regarding Tor[40] suggests that Deep Packet Inspection (DPI) Intrusion Prevention Systems (IPS) are used for censorship purposes and implies that specialized hardware may be in place within the Iranian Internet infrastructure, that could provide such functionality.

However, approximately 6000 IP addresses were identified that originated outside of the Islamic Republic of Iran that correspond mainly with dedicated proxies, Tor and VPN exit nodes. Connections to these servers occur over secured lines and should remain unaffected by a "transparent" MITM attack. While rogue certificates were issued for Tor during the intrusion in DigiNotar's network, it is highly unlikely that rogue certificates could have been used to reroute traffic that went through all the identified foreign VPNs. Furthermore, the peak-like behavior that could be identified in the OCSP requests for rogue certificates does not correspond with a "transparent" MITM attack.

Another way in which traffic may be redirected is by making changes directly in a DNS server that is operated at a high level of the infrastructure. Even if services such as Tor or VPN are used, DNS queries will by default be made to the local DNS server. Therefore, a modus operandi where DNS was abused to redirect traffic could accommodate for the fact that traffic that went through proxies, Tor or VPN was also redirected. However, the hypothesis that changes were made directly to a DNS server that operated at a high level in the infrastructure does not correspond with the peak-like behavior that was identified in the amount of OCSP requests for rogue certificates. If traffic had been redirected in this way, one would expect that the amount of OCSP requests would have grown during the attack without the occurrence of repeated and sudden declines.

The most likely modus operandi to have been used during the MITM attack, based on the accumulated OCSP data, is that of DNS cache poisoning. A DNS cache poisoning attack relies on the fact that DNS servers cache the response of DNS servers at a higher level in the infrastructure. By flooding a DNS server with forged responses for a particular domain, as if it had received the response from a higher DNS server, it is possible to "poison" the entries in the DNS server and thus its responses to clients at a lower level in the infrastructure. The poisoned entries are valid for as long as the Time To Live (TTL) allows, after which these entries expire and another DNS request would be made to a higher DNS server for the domain if it is requested by a client. This methodology would explain why traffic that went through proxies, Tor and VPN was also affected by the MITM attack and also corresponds with the peak-like behavior and the occurrence of repeated and sudden declines in OCSP requests for rogue certificates.

[40] Tor project blog, "Iran blocks Tor; Tor releases same-day fix" at http://blog.torproject.org/blog/iran-blocks-tor-tor-releases-same-day-fix

10.3 Conclusion

Most of the identified rogue certificates contain a DNS domain name in the common name, indicating that they were intended to be used for a website. From 1 September 2011 onwards, all OCSP requests for unknown certificate serial numbers were answered as if they had been revoked. Before this date, all requests for unknown serial numbers were answered by the OCSP responder as if the corresponding certificates were valid. This was the prescribed standard response for an OCSP responder to unknown serial numbers.

The OCSP request logs showed that one serial that was used in a certificate for the URL `*.google.com` was abused on a massive scale in a MITM attack on the people of the Islamic Republic of Iran. This conclusion was supported by the fact that 95% of OCSP requests for the abused certificate originated from the Islamic Republic of Iran and that the remaining 5% of the requests originated from systems that were generally used as a proxy, VPN or Tor exit node.

The number of unique IP addresses that made OCSP requests for the rogue certificate was still growing when the certificate was revoked. The attack had covered 143 Iranian ASes (often ISPs) and 298,140 unique IP addresses. The amount of IP addresses was only a very rough approximation for the amount of affected users, as users may share an IP address, use multiple IP addresses or use software that does not support OCSP requests.

The broad scope of 143 ASNs and 298,140 unique IP addresses does not reveal a well-defined, narrow target. The maximum coverage of the attack's unique IP addresses may have been intentional. Without detailed knowledge about the Iranian infrastructure, it is impossible to conclusively determine how the MITM attack was perpetrated, but the OCSP data implies that DNS cache poisoning is the most likely modus operandi to have been used.

In addition to the rogue `*.google.com` certificate, validation requests were made for serial numbers that correspond with known rogue certificates as well as for unknown serial numbers. Initially these requests were answered by the OCSP responder as if they were valid. This makes it plausible that other rogue and unknown certificates may have been used for other MITM attacks on a much smaller scale. An attempt was made to verify a certificate with the common name `login.yahoo.com` by AttIP3, an IP address that had previously been identified in the context of the investigation of the DigiNotar intrusion.

10.3.1 Consequences

A large number of citizens of the Islamic Republic of Iran became victims of a MITM attack. All services of Google.com could have been the object of attack. Most likely the confidentiality of Gmail accounts was compromised and their credentials, the login cookie and the contents of their e-mails could have been intercepted. Using the credentials or the login cookie, an attacker may be able to log in directly to the Gmail mailbox of the victim and read their stored e-mails. Additionally, the MITM attacker may have been able to log into all other services that Google offers to users, such as stored location information from Latitude or documents in GoogleDocs. Once an attacker is able to receive his targets' e-mails, he is also able to reset passwords of others services such as Facebook and Twitter using the lost password functionality.

10.3.2 Timeline of the MITM attack

Date	Notes
27-Jul-2011	First OCSP request at DigiNotar for the rogue wildcard Google certificate.
28-Jul-2011	DigiNotar found evidence that attempts were made to verify the rogue `login.yahoo.com` certificate by IP addresses originating from the Islamic Republic of Iran.
04-Aug-2011	The beginning of massive activity on the OCSP responder for a rogue `*.google.com` certificate originating from the Islamic Republic of Iran.
28-Aug-2011	On the Google support forums, a customer of the Iranian ISP ParsOnline posted details about a certificate warning that was presented to him by Google Chrome for a rogue `*.google.com` certificate.

Date	Notes
29-Aug-2011	Google received multiple reports in regard to an attempted SSL MITM attack and articles about a rogue `*.google.com` certificate appeared on the blogs of, among others, Mozilla, Google and Microsoft. On the same day, the rogue `*.google.com` certificate was revoked. Additionally, GOVCERT.NL was notified by Cert-Bund.
30-Aug-2011	Fox-IT was asked by DigiNotar to initiate an investigation into the intrusion of DigiNotar and placed an incident response sensor in the network of DigiNotar.
31-Aug-2011	Google Chrome blacklisted a list of known rogue serial numbers.
01-Sep-2011	The behavior of the OCSP responder was changed to function based on a white list, effectively revoking all unknown serial numbers and therefore all remaining rogue certificates.

11 Lessons learned

Fox-IT was specifically asked by the ministry BZK to address the lessons that can be learned from an incident such as the intrusion of DigiNotar's network. The described lessons that can be learned from such an incident do not necessarily imply that DigiNotar failed to implement the following measures.

Average users and businesses will have a very limited capacity to protect themselves properly against attacks such as those against Trusted Third Parties in the Public Key Infrastructure. In general, the best way for average users to protect themselves on public networks is to keep their software up to date, to use an antivirus product and to be wary of content from untrusted sources. The MITM attack on users that was perpetrated in the aftermath of the intrusion of DigiNotar's network was only detected by Google when users of the Google Chrome browser reported abnormal behaviour while using Google services.

Since users have a very limited ability to protect themselves from attacks that abuse the Public Key Infrastructure, they need to be able to trust the security of all the parties that make up the Public Key Infrastructure in order for the system as a whole to operate securely. Given the impact that a breach in the security of a Certificate Authority has on the Public Key Infrastructure as a whole and the Internet in general, ensuring the security of every Certificate Authority is paramount to the trust in PKI and its role in providing security for a diverse range of activities on the Internet. While the approach to protecting the potential targets from this type of intrusion does not differ significantly from other threats, the range of scenarios that need to be taken into account is rapidly expanding.

More generally users and businesses including Certificate Service Providers (CSPs) can protect themselves against a wide range of security threats. Various security books, articles, courses and standards can provide detailed information about taking appropriate security measures. In addition to implementing a formal information security management system (such as ISO-27001), we would like to note a number of basic practical requirements for critical environments such as those on which CSPs rely.

As with any organization, it is important for CSPs to complement prevention with detection. There is no such thing as an absolute guarantee that preventive measures will be sufficient to prevent an attack. When complemented with measures aimed at the detection of attempts to intrude a secured infrastructure however, it is possible minimize the chances of a successful intrusion. Furthermore, detection can prevent that critical parts of the infrastructure can be targeted, even in the case of a breach of a specific segment.

It is also important to enforce a strict separation in the tasks with competing aims that employees perform, insofar as these tasks may affect the security of the organization or its infrastructure. For example, a person that is responsible for system administration should not be the same person that sets up and maintains the firewall or other security components of the infrastructure. A system administrator may aim to provide users with a pleasant working environment, while the operator of a firewall will aim to create an optimally secure setup of the firewall and the interaction between the segments that it segregates and regulates. The framework within which the operator of the firewall performs his tasks should be defined by a security officer, who is specifically tasked with defining and enforcing a security policy tailored to your organization.

Additional measures, point by point:

- Air gap vital systems as much as possible, to make sure that they are physically separated on a network level from untrusted networks such as the Internet.
- Update all software products on all systems with the latest patches as often as possible. Subscribe to relevant mailing lists or use dedicated patch management software to support this process.
- Harden all systems. Do not rely on default settings. Make sure that the most critical systems are only being used for the critical processes that they are intended for. By limiting the amount of services on any given system, the attack surface for an attacker is limited.
- Regularly have the security of your infrastructure and systems therein tested by penetration testers. Do not always use the same team to perform penetration tests.
- Monitor your systems and network and make sure that anomalies trigger notifications to the appropriate employee(s).

- Use data that can be accumulated by the OCSP responder to check if unknown serials are being validated.
- Separate vital logging services from the systems that perform other vital functions. In an infrastructure where secure logging is vital, a logging server can be placed behind a unidirectional security gateway.
- Ensure forensic readiness so that, for example, all events that are relevant for an incident response team are logged, that events from multiple systems can be correlated, that a balance is found in advance between business continuity and potential evidence gathering, that roles and reporting structures are defined for and communicated to all employees and external parties that take part in incident response before an incident takes place and that a feedback loop is created to learn from incidents in the past.

12 Potential follow-up investigation

The scope and goal of the investigation regarding the intrusion at DigiNotar that was performed by Fox-IT changed over time. At first, the focus was on controlling the incident by mitigating the intrusion and regaining trust in the systems. Later the focus changed to identifying evidence that could lead to the location and identity of the intruder and safeguarding evidence. As time progressed, the need for detailed information about the intrusion and its aftermath lessened for the ministry BZK, who commissioned the continued investigation, as the primary investigative questions could be answered. Therefore, not all questions were answered and a number of traces were not fully investigated. Consequently, the information that was uncovered during the investigation can be used as the basis for further research in regard to several additional questions.

12.1 Intruder's steps

As the results of the investigation presented in the previous chapters show, some steps made by the intruder in his path through the network were not detailed. More specifically, some questions remain unanswered, such as:

- Were the database credentials on the BAPI-db discovered by the intruder in the `web.config`?
- How did the intruder gain access to the Secure-net? Examination of the BAPI production workstation may provide a conclusive answer to this.
- What was the exact behavior of the CA management software?
    - How were log and database files of the CA management software normally created, were log files manipulated and if so in what way?
    - Are vulnerabilities present in the software and were they abused by the intruder?
- What information was stored in the CAP database? Were private keys or passwords stored in this database?

12.2 Network infrastructure

Paragraph 3.3 describes the normal operation of the network segments and firewall based on interviews with the administrators. The exact firewall rules have not been examined to confirm their statements in this regard.

12.3 Investigation of CA servers

Chapter 6 contains the results of the investigations of the CA servers. Additionally, more research is possible into the following questions:

- The exact behavior of the used CA management software could be analyzed.
    - Did the intruder use the option in the CA software to perform a complete backup of the databases? What traces did this leave on the system?
    - What extensions were installed that provided functionality that could have aided the intruder in issuing rogue certificates?
    - Further investigation could be performed to explain the duplicate certificates that were found in the database files.
    - Was the CA software and netHSM setup able to startup unattended? Was it possible to restart CA servers or services and activate private keys on the netHSM? What configuration options are there for an unattended setup? Were attempts made by the intruder to change these settings?
    - Can the CA management software detect deleted log files? Is it possible to establish with absolute certainty if log files may have been tampered with?
    - Why could private keys found in `id2entry.dbh` not be matched with the certificates extracted from the databases?
- The CA web server log files (`enrol-cipher.log`) of the Public-CA server could contain interesting entries outside office hours that could be examined further.
- The CA servers could be searched for any further remains of deleted (log) files.
- How were the private keys in the netHSM activated exactly? Was it possible to activate more than one key with a smartcard?
- Were the certificates of the keys used in the netHSM in the internal DMZ for the *Parelsnoer* service on the trust lists of operating systems? The servers that hosted the *Parelsnoer* service

were not investigated. If their certificates or root certificates were also on trust lists, it would be interesting to determine if these servers were utilized by the intruder.

12.4 Systems

Chapter 7 contains the results of the investigations of systems access and tools. Additionally, the following questions could be researched:

- The CA servers, netHSM, firewall and other equipment at the co-location were not investigated thoroughly, which could provide additional results. Some suspicious connections have been identified as originating from one of the co-located servers.
- The system event logs of most of the servers were exported and retained. This was done in August 2011. The log files of some of these systems have not been examined.
- Further research is possible on the extensive firewall logs including their integrity.
- The backup tapes could be investigated for traces of the intrusion and may contain deleted tools.
- Some of the servers in the DMZ-ext-net were not investigated, namely those that were used for various services that DigiNotar provided. Investigating these servers might provide insights regarding potential misuse of these DigiNotar services.
- Examination of all executables that were transported through the stepping stones might reveal additional insights on the methods used by the intruder.

12.5 Aftermath

Chapter 10 contains the results of the investigation of the large-scale MITM attack where one of the rogue certificates was abused. Additionally, the following questions could be researched:

- The OCSP data could be used to examine the limited set of IP addresses outside of the Islamic Republic of Iran that were targeted in the MITM attack further, to determine if they can all be identified as proxies, Tor-exit nodes and VPN providers.
- If additional data from Google could be obtained, it would be possible to determine if login data that could have been obtained during the MITM attack was abused in practice.
- Data regarding OCSP requests for valid certificates from other Certificate Authorities could be used to determine if a "round robin" algorithm was used and thus provide more information about the capabilities of the attacker and the infrastructure that was used.
- Zooming in on the targets and the underlying infrastructure in the Islamic Republic of Iran could reveal information about the identity and aim of the MITM attacker.
- The CRL requests could be examined to reveal additional abuse of rogue certificates.

13 Terminology

Term	Meaning
AS	Autonomous System
ASN	Within the Internet, an Autonomous System (AS) is a collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators that presents a common, clearly defined routing policy to the Internet. A unique AS Number (ASN) is allocated to each AS for use in (Border Gateway Patrol) routing.
ASN.1	Abstract System Notation One is a standard for the notation of data in networking.
ASPX	Web pages that are based on the ASP.NET web application framework by Microsoft.
BAPI	Belastingdienst Advanced Program Integration (Dutch tax administration)
CA	Certificate Authority, an issuer of certificates.
CAP	Control Application for the back office administration.
Certificate	A digital file used among others to authenticate a website and to encrypt network traffic. The validity of a certificate is generally verified with the issuer (CA).
CEST	Central European Summer Time (UTC+2).
CN	Common Name of a certificate.
CRL	Certificate Revocation List.
CSP	Certificate Service Provider.
CSR	Certificate Signing Request.
DARPI	DigiNotar "Abonnementen Registratie" (Subscription Registration) Production Interface.
DER	Distinguished Encoding Rules is a standard that is used to encode an ASN.1 value.
DMZ	Demilitarized Zone. Its purpose it to add an additional layer of security to an organization's local area network.
DN	Distinguished Name of a certificate.
DNS	Domain Name System is a hierarchical distributed naming system for systems connected to a network that translates domain names to IP addresses.
GET	A GET request is a HTTP request to receive a file that is specified using an URL.
HTM/HTML	HyperText Markup Language is a standard and file format that is used for web pages.
HTTPS	HyperText Transfer Protocol Secure is a combination of HTTP with SSL/TLS.
ISP	Internet Service Provider.
IPS	Intrusion Prevention System.
IP	Internet Protocol. An IP address is used to identify a specific system within a network.
MD5	Message Digest algorithm is a cryptographic hash function that can be used to check data integrity.
MITM	Man-in-the-Middle. In this type of attack an attacker places himself between two parties in order to intercept the traffic that occurs between these parties.
Mscache	A hash for cached credentials for user on a Windows domain.
MSSQL	Microsoft SQL Server is a database management system that was developed by Microsoft.
netHSM	Hardware security module that is accessible over the network that contains private keys.
OCSP	Online Certificate Status Protocol, a protocol that is used to obtain the revocation status of certificates as described in RFC 2560.
PEM	Privacy Enhanced Mail is a proposed standard for securing e-mail using public key cryptography.
PIN mailer	Sends a Personal Identification Number.
PKI	Public Key Infrastructure.
Port	A 16 bit number that is used to refer to a communications endpoint.
RDP	Remote Desktop Protocol is a proprietary protocol by Microsoft to provide a user with a graphical interface to another computer.
RFC	Request For Comments describe the specifications, protocols, procedures and events that are related to the Internet and Internet-connected systems.
SMTP	Simple Mail Transfer Protocol is used to send e-mail across IP networks.
SSL	Secure Sockets Layer and the subsequent Transport Layer Security are cryptographic protocols to provide secure communication of a public telecommunication network.
SVO	Evidentiary item ("Stuk Van Overtuiging").
Tor	The onion router. Initiative of the Tor project. Intended to enable online anonymity.
TTP	Trusted Third Party.
Tunnel	An Internet Protocol communications channel between systems.

Term	Meaning
UTC	Coordinated Universal Time.
VPN	Virtual Private Networks are used to secure data that is transferred over a public telecommunication infrastructure.
XUDA	Xcert Universal Database API.

Appendix I: References to equipment

The servers, workstations and network equipment referenced in this report are listed in the following table. The names used in this report are characteristic of each item's usage. For cross reference, the server ID used by DigiNotar and the related exhibit number are included in table. Also, the IP address and network segment are shown.

When a server is referenced in the report and it has more than one IP address assigned to it, the specific IP address is included in the reference. If no IP address is included in the reference, the bold-marked IP address at the top of the line entry applies.

Name[41]	Server Id[42]	SVO number[43]	IP-address	Network segment	Remarks
CA servers					
Root-CA	winsvr167	SVO1	172.18.20.247	Secure-net	
Qualified-CA	winsvr022	SVO2	172.18.20.249	Secure-net	
CCV-CA	winsvr057	SVO3	172.18.20.246	Secure-net	
Nova-CA	winsvr021	SVO4	172.18.20.252	Secure-net	Also called 'Orde-CA'.
Taxi-CA	winsvr053	SVO5	172.18.20.251	Secure-net	
Test-CA	winsvr054	SVO7	172.18.20.250	Secure-net	
Relation-CA	winsvr055	SVO12 DD.055	172.18.20.244	Secure-net	
Public-CA	winsvr056	SVO13 DD.056	172.18.20.245	Secure-net	
DNTest-CA	winvm012	SVO149	10.10.240.39	Test-net	
DNAcceptance-CA	winvm032	SVO114	10.10.230.39	Acceptance-net	
Public-CA-Colo	winsvruw07	SVO342	172.27.20.19	Secure-colo-net	
Qualified-CA-Colo	winsvruw08	n/a	172.27.20.20	Secure-colo-net	
Relation-CA-Colo	winsvruw09	SVO325	172.27.20.17	Secure-colo-net	
Root-CA-Colo	winsvruw10	n/a	172.27.20.15	Secure-colo-net	
Nova-CA-Colo	winsvruw11	n/a	172.27.20.16	Secure-colo-net	Also called 'Orde-CA'.
CCV-CA-Colo	winsvruw18	n/a	172.27.20.23	Secure-colo-net	
Taxi-CA-Colo	winsvruw19	n/a	172.27.20.26	Secure-colo-net	
netHSMs					
NetHSM-CAs	dnhsm01	n/a	172.18.20.254	Secure-net	
NetHSM-web	dnhsm02	n/a	10.10.200.254	DMZ-int-net	
NetHSM-test	dnhsm04	n/a	10.10.240.254	Test-net	Also called "Stichting continuïteit hsm"
NetHSM-CAs-Colo	dnhsmuw01	n/a	172.27.20.254	Secure-colo-net	
HSM-connector	winvm024	SVO179 SVO180	10.10.240.35	Test-net	
Web servers					
Main-web	winsvr101	SVO8	**10.10.20.41** 10.10.20.11 10.10.20.14 10.10.20.28 10.10.20.46 10.10.20.58 10.10.20.61 10.10.20.69 10.10.20.73 10.10.20.97	DMZ-ext-net	
Docproof2	winsvr119	DD.119 SVO328	10.10.20.65	DMZ-ext-net	
Docproof1	winsvr118	SVO11	10.10.20.37	DMZ-ext-net	

[41] Server name as it is used in this report.
[42] Server Id as it is used by DigiNotar.
[43] This is an internal code for a piece of evidence (such as a disk image).

Name[41]	Server Id[42]	SVO number[43]	IP-address	Network segment	Remarks
Pass-web	winsvr108	SVO35 SVO36	**10.10.20.16** 10.10.20.40 10.10.20.35 143.177.11.3 143.177.11.12	DMZ-ext-net	Hosting the website auth.pass.nl
Soap-signing	Winsvr109	SVO46	10.10.20.98 10.10.20.129 10.10.20.42 10.10.20.92 10.10.20.84 10.10.20.85 10.10.20.86 10.10.20.137 10.10.20.87 10.10.20.88 10.10.20.89 10.10.20.130 10.10.20.90 10.10.20.91 10.10.20.99 10.10.20.93	DMZ-ext-net	
Main-web-new	winvm045	SVO55 SVO56 SVO57	**10.10.20.158** 10.10.20.172 10.10.20.164 10.10.20.165 10.10.20.182 10.10.20.173 10.10.20.167 10.10.20.174 10.10.20.169 10.10.20.183 10.10.20.175 10.10.20.184 10.10.20.181 10.10.20.176	DMZ-ext-net	Main-web was replaced by WINVM045. The first firewall entries of 10.10.20.158 from WINVM045 appeared on 18-Jul-2011. See also chapter 4.
Other in DMZ					
eHerkenning-AD	winsvr155	SVO51	**10.10.20.134** 62.58.44.101	DMZ-ext-net	
eHerkenning-HM	winsvr157	SVO28 SVO29 SVO31	**10.10.20.139** 143.177.3.40	DMZ-ext-net	
Docproof-db	Winsvr066	SVO312 SVO313 SVO314	10.10.200.20	DMZ-int-net	
Production-notification	winsvr009	SVO34	**10.10.200.18** 62.58.44.120	DMZ-int-net	
Workstations					
Production121	digiws121	SVO371	172.17.20.59	Office-net	
BAPI-production	digiws146	n/a	172.18.20.230	Secure-net	
Develop182	digiws182	n/a	172.17.20.114	Office-net	
AdminWS164	digiws164	SVO10	10.10.210.32	Admin-net	
Other					
BAPI-db	winsvr007	SVO75 SVO76	172.17.20.4	Office-net	Internally called Bapi Database New.
Source-build	winsvr003	SVO374	172.17.20.25	Office-net	
Source-build-new	winsvr010	SVO100	172.17.20.21	Office-net	
Office-file	winsvr065	SVO77 SVO78	172.17.20.8	Office-net	
Exchange-mail	winsvr126	SVO21 SVO22 SVO95	172.17.20.5	Office-net	Exchange mail server.

Name[41]	Server Id[42]	SVO number[43]	IP-address	Network segment	Remarks
CAP-app-web	winsvr130	SVO317	172.18.20.10	Secure-net	Part of the CAP application (Control Application)
CAP-app-db	winsvr131	SVO321 SVO322 SVO323	172.18.20.11	Secure-net	Part of the CAP application (Control Application)
CAP-web	winsvr125	SVO340 SVO341	172.18.20.12	Secure-net	Part of the CAP application (Control Application)
CAP-CCDB	winvm048	SVO225 SVO226	10.10.240.25	Test-net	
Admin-DNS	winsvruw05	n/a	**172.27.20.21** 193.173.36.37	Secure-colo-net	
AntiVirus	winsvr008	SVO14 SVO26	10.10.210.14	Admin-net	
Network equipment					
Load-balancer-1	dnlb01	n/a	10.10.20.8	DMZ-ext-net	
Load-balancer-2	dnlb02	n/a	10.10.20.9	DMZ-ext-net	
Squid-proxy	dlx001	SVO283	172.17.20.7	Office-net	
Syslog	dlx131	SVO288 SVO289	10.10.210.35	Admin-net	
Cluster addresses					
Cluster-prodpass		n/a	**10.10.20.18** 62.58.44.107	DMZ-ext-net	Cluster production Pass

Appendix II: List of suspected intruders IP-addresses

The IP addresses that were found leading to the location or identification of the intruder are not included in this report due to the ongoing investigation. These IP addresses are referred to as *AttIP* in this report.

Reference	Country	Source	Remark
AttIP1	United Kingdom	Malware on Docproof2	`troj65.exe` was probably used for tunneling RDP.
		Firewall logs	Successful connections initiated from DMZ-ext-net (tunnels). Blocked attempts from Secure-net.
AttIP2	United Kingdom	Malware on Docproof2	`95.exe`
		Other	Server was confiscated by the Dutch police (KLPD).
		Firewall logs	Successful connections initiated from DMZ-ext-net.
AttIP3	Islamic Republic of Iran	Access to /beurs on Main-web	Probably revealed by error in proxy chain (see paragraph 4.3.4).
		OCSP log	OCSP request test run for a rogue `login.yahoo.com` certificate. Resolved to an DSL user in Iran.
		Other	Made connections to server running at AttIP2.
AttIP4	Netherlands	Access to /beurs on Main-web	Suspicious. Much activity.
AttIP5	Russian Federation	Access to /beurs on Main-web	Suspicious. Much activity.
		Other	Server was confiscated by the Dutch police (KLPD).
		Other	Made connections to server running at AttIP2.
AttIP6	Islamic Republic of Iran	Access to /beurs on Main-web	Suspicious. One log entry for a post to `settings.aspx`.
		OCSP log	First 3 requests of the `*.google.com` certificate used in the MITM attack.
AttIP7	United States	Access to /beurs on Main-web	Suspicious. One log entry for a post to `settings.aspx`.
AttIP8	United States	Access to /beurs on Main-web	Suspicious. Many file downloads.
AttIP9	Germany	Access to /beurs on Main-web	Suspicious. Downloaded some files.
AttIP10	United States	IIS logs on Docproof2	Unknown.
AttIP11	United States	Access to /beurs on Main-web	Suspicious. One file downloaded.
AttIP12	Islamic Republic of Iran	Access to /beurs on Main-web	Suspicious. Many file downloads.
AttIP13	Islamic Republic of Iran	Access to /beurs on Main-web	Suspicious. Many file downloads.
		Firewall logs	Dropped connections initiated from DMZ-ext-net.
AttIP14	Islamic Republic of Iran	Access to /beurs on Main-web	Suspicious. Downloaded files.
AttIP15	Germany	Access to /beurs on Main-web	Suspicious.
AttIP16	United States	Access to /beurs on Main-web	Suspicious. Downloaded a file.

Reference	Country	Source	Remark
AttIP17	Islamic Republic of Iran	Access to /beurs on Main-web	Suspicious. Downloaded the file `jobsdone.zip`.
AttIP18	Australia	Access to /beurs on Main-web	Suspicious. Posts and gets to `settings.aspx`. Downloaded the file `jobsdone.zip`.
AttIP19	United States	Access to /beurs on Main-web	Suspicious. Downloaded files.
		Firewall logs	Successful connections initiated from DMZ-ext-net.
AttIP20	Israel	Access to /beurs on Main-web	Suspicious. Uses `settings.aspx` very often.
AttIP21	United States	Access to /beurs on Main-web	Suspicious. Downloaded files.
AttIP22	United Kingdom	Access to /beurs on Main-web	Suspicious. Downloaded files.
		Firewall logs	Successful connections initiated from internal IPs.
AttIP23	Finland	Access to /beurs on Main-web	Suspicious. Posts and gets to `settings.aspx`.
N/A	United States	Access to /beurs on Main-web	Not suspicious. Gets `default.aspx`. IP resolves to Googlebot web crawler.
N/A	Netherlands	Access to /beurs on Main-web	Not suspicious. Probably used for internal incident response activities, since it was only seen on July 27, 2011.
N/A	Belgium	Access to /beurs on Main-web	Not suspicious. Probably used for internal incident response activities, since it was only seen on July 24, 2011.
N/A	Belgium	Access to /beurs on Main-web	Not suspicious. Probably used for internal incident response activities, since it was only seen on July 23, 2011.
N/A	Netherlands	Access to /beurs on Main-web	Not suspicious. Probably used for internal incident response activities, since it was only seen on July 28, 2011.

The IP addresses AttIP3, AttIP6, AttIP12, AttIP13 and AttIP14 are in a close range together and share the same class A network (/24).

Appendix III: Timeline of noteworthy traffic

This appendix shows the timeline of noticeable traffic as it was found when examining the firewall logs.

Time start	Time end	Notes	Source server	Destination server	Destination port
2011-06-17					
13:06:57	13:07:00	RDP attempts[44] from office net to admin net	Develop182	AntiVirus	3389
2011-06-28					
14:24:42	14:24:51	Port 139/ 445 attempts[45] from secure to colo-secure net	Taxi-CA	Admin-DNS	139/445
2011-06-29					
11:56:15	11:56:24	RDP attempts from DMZ ext to Office net	Main-web	Source-build	3389
13:13:33	13:14:40	Network discovery from DMZ ext to Test net	Main-web	HSM-connector 10.10.240.48	80,137
13:17:42	13:18:45	Network discovery from DMZ ext to DMZ int	Main-web	NetHSM-web	80,137, 443
13:20:52	13:21:05	Network discovery from DMZ ext to secure net	Main-web	NetHSM-CAs	137, 443
13:21:38	13:21:54	Network discovery from DMZ ext to Colo-Secure net	Main-web	NetHSM-CAs-Colo	137, 443
13:22:26	13:22:40	Network discovery from DMZ ext to Test net	Main-web	NetHSM-test	137, 443
13:26:06	13:26:23	Connection attempts from Office to Secure net	BAPI-db	CAP-app-web	80, 3389
13:26:22	13:26:35	Network discovery from DMZ ext to Secure	Main-web	CAP-app-web	80, 137
13:27:14	13:29:25	Connection attempts from Office to Secure net	BAPI-db	CAP-app-web CAP-app-db	21, 1433, 135, 137
13:29:39	13:29:52	Network discovery from DMZ ext to Secure net	Main-web	CAP-app-db	137, 1433
13:29:50	13:30:03	Connection attempts from Office to Secure net	BAPI-db	CAP-app-db	80, 137
13:31:06	13:31:19	Network discovery from DMZ ext to Test net	Main-web	CAP-CCDB	80, 137
13:33:32	13:34:08	Network discovery from DMZ ext to DMZ old	Main-web	10.10.0.12	80, 137, 443
13:40:40	13:40:44	Connection attempts from DMZ ext to Office	Main-web	172.17.20.164	137, 443
15:11:13	15:11:25		Office-file	BAPI-production	139->4461
2011-06-30					
00:08:21	00:08:24	Some more attempts	eHerkenning-AD	BAPI-db	137
00:16:34		Connect back home	eHerkenning-AD	AttIP2	443
00:36:46	00:41:37	Connection attempts from DMZ-ext-net to Office-net	Main-web	BAPI-db	21, 80, 137
02:22:26	02:22:35	Failed RDP attempts	BAPI-db	CAP-app-web	3389
02:22:56	02:23:38	Successful HTTP/HTTPS connections	BAPI-db Squid-proxy	CAP-app-web	80, 443
02:24:18	02:24:19	Connect back from Office db server to drop server @DMZ	BAPI-db	eHerkenning-AD	443
02:25:10	02:26:59	Failed RDP/SQL attempts from the Office net	Source-build BAPI-db	CAP-app-web CAP-app-db	80, 137, 1433, 3389
02:28:31	02:28:40		eHerkenning-AD	CAP-CCDB	443
10:39:59	10:40:29	Failed attempts	Pass-web	BAPI-db	139, 445, 1433
13:22:05	13:22:15	FTP from the DMZ (could be legal activity)	Main-web (10.10.20.46)	Source-build-new	21
23:54:04	23:56:36	Unknown dropped activity.	Office-file:139	BAPI-production	
2011-07-01					

[44] Probably not relevant for this attack.
[45] Probably not relevant for this attack since no traces on Taxi-CA server were found before 01-Jul-2011.

Time start	Time end	Notes	Source server	Destination server	Destination port
01:15:30	01:15:38[46]	Dropped activity from another host.	172.17.20.22:139	BAPI-production	2400
01:16:15	01:17:16	Port scan on local segment.[47]	BAPI-production	Firewall (172.18.20.2)	
01:17:22	01:19:49	Connect back attempts to the admin-net.	172.17.20.59 BAPI-production	AntiVirus	80, 139, 445
01:23:52	01:24:46		BAPI-db:139	BAPI-production	
18:00:56	18:02:26	Failed attempts.	BAPI-db	172.18.20.239	135, 319, 389
20:23:52	20:24:05	And again sometime later.	BAPI-db	Taxi-CA	80,137
21:21:54	21:22:24		BAPI-db:139	BAPI-production	
22:52:47	23:40:45	Successful connections to DMZ stepping stone.	CAP-app-web	Main-web	80
2011-07-02					
00:14:14	00:47:07	Successful connections to DMZ stepping stone.	CAP-app-web	Main-web	80
01:48:42	01:48:42	Successful connections to DMZ stepping stone.	CAP-app-web	Main-web	80
02:10:01	02:10:01	Successful connections to DMZ stepping stone.	CAP-app-web	Main-web	80
02:10:01		First occurrence of many SMTP connections.	CAP-app-web	172.17.20.5	25
02:18:36	02:18:36	Successful connections to DMZ stepping stone.	CAP-app-web	Main-web	80
02:26:54	02:27:02	Strange port combinations	Admin-DNS:445	CAP-app-web:1433	
03:36:15	03:44:19	Unsuccessful connections to public stepping stone.	Root-CA [ICMP]	AttIP1	8/0
04:40:06	04:40:06	Successful connections to DMZ stepping stone.	Root-CA	Main-web	80
05:37:05	05:48:56	Successful connections to DMZ stepping stone.	Root-CA	Main-web	80
21:57:55	22:35:20	Successful connections to DMZ stepping stone.	Root-CA	Main-web	80
23:33:40	23:34:56	Admin possibly working late.	AdminWS164	CAP-app-db	1056, 1433
23:35:57	23:35:57	Admin possibly working late.	AdminWS164	CAP-app-db	1433, 3389
2011-07-03					
00:14:48	00:14:48	Successful connections to DMZ stepping stone.	Qualified-CA	Main-web	80
13:03:02	13:15:51	Successful connections to DMZ stepping stone.	Public-CA	Main-web	80
16:51:36	16:54:06	Successful connections to DMZ stepping stone.	Public-CA	Main-web	80
2011-07-04					
00:48:43	21:09:36	Successful connections to DMZ stepping stone.	Public-CA	Main-web	80
2011-07-05					
00:15:40	00:18:26	Admin possibly working late.	AdminWS164	CAP-app-web	3389
15:09:35	21:09:36	Successful connections to DMZ stepping stone at regular intervals. Automation could be in place.	Public-CA	Main-web	80
2011-07-06					
15:09:36	21:09:36	Successful connections to DMZ stepping stone at regular intervals. Automation could be in place.	Public-CA	Main-web	80
2011-07-07					

[46] From here on outgoing traffic exists originating from Secure-net.
[47] Only the IP-address of firewall itself is logged.

Time start	Time end	Notes	Source server	Destination server	Destination port
15:09:36	21:09:36	Successful connections to DMZ stepping stone at regular intervals. Automation could be in place.	Public-CA	Main-web	80
22:58:18	22:58:27		BAPI-production	NetHSM-web	80
2011-07-08					
01:09:36	07:09:36	Successful connections to DMZ stepping stone. Other interval.	Public-CA	Main-web	80
2011-07-09					
01:09:36	07:09:36	Successful connections to DMZ stepping stone.	Public-CA CAP-app-web	Main-web	80
10:05:32	10:06:03		CAP-app-web	Main-web	80
10:06:07	23:34:59	Successful connections to DMZ stepping stone.	CAP-app-web	Main-web	80
2011-07-10					
00:00:14	00:26:24	Continued.	CAP-app-web	Main-web	80
01:09:36	01:09:37	Successful connections to DMZ stepping stone.	Public-CA	Main-web	80
01:24:36	01:24:36	Switching host.	CAP-app-web	Main-web	80
04:09:36	04:11:36	Successful connections to DMZ stepping stone.	Public-CA CAP-app-web	Main-web	80
07:09:36	07:09:36	Successful connections to DMZ stepping stone.	Public-CA	Main-web	80
10:01:04	23:57:55	Successful connections to DMZ stepping stone.	CAP-app-web	Main-web	80
2011-07-11					
00:46:58	00:51:43	Successful connections to DMZ stepping stone.	Public-CA	Main-web	80

From here on there are connections from Public-CA port 1385 to Main-web port 80 at regular intervals at 01:09:36, 01:33:33, 04:09:36, 04:09:37, 07:09:43 and 07:09:44 each day from 11-07-2011 up until 20-07-2011.

Time start	Time end	Notes	Source server	Destination server	Destination port
2011-07-20					
16:46:50	16:47:30	Dropped connections. May be caused by incident response actions.	BAPI-production	Office-file	80
16:57:33	16:57:33	Successful connections to DMZ drop. May be caused by incident response actions.	BAPI-production	Office-file	80
2011-07-25					
18:50:52	19:10:08	Few days later. Successful connections to DMZ drop. May be caused by incident response actions.	Public-CA	Main-web	80
19:10:37	19:13:05	Dropped connections to DMZ drop. Firewall adjusted.	Public-CA	Main-web	80
2011-07-26					
09:09:14	09:09:23	Dropped connection. May be caused by incident response actions.	CAP-app-web	62.58.36.117	80
09:10:46	09:10:47	Accepted connections. May be caused by incident response actions.	172.18.20.25	62.58.36.117	80

All timestamps are in CEST.

Appendix IV: Certificate Authorities generating CRLs

The Certificate Authorities that automatically generated CRLs based on repetitive log entries in the CA management software.

Server	CA nickname
Nova-CA	Nederlandse Orde van Advocaten
	Orde van Advocaten SubCA Administrative CA
	Orde van Advocaten SubCA System CA
Public-CA	DigiNotar Cyber CA
	DigiNotar Extended Validation CA
	DigiNotar Private CA
	DigiNotar Public CA - G2
	DigiNotar Public CA 2025 Administrative CA
	DigiNotar Public CA 2025 System CA
	DigiNotar Public CA 2025
	DigiNotar Services 1024 CA
	DigiNotar Services CA
	CertiID Enterprise Certificate Authority
Root-CA	DigiNotar Root CA Administrative CA
	DigiNotar Root CA G2
	DigiNotar Root CA System CA
	DigiNotar Root CA
	MinIenM Organisatie CA - G2
	MinIenM SIMULATOR NL Organisatie CA-G2
Qualified-CA	DigiNotar PKIoverheid CA Organisatie - G2
	DigiNotar PKIoverheid CA Overheid en Bedrijven
	DigiNotar Qualified CA - G2
	DigiNotar Qualified CA Administrative CA
	DigiNotar Qualified CA System CA
	DigiNotar Qualified CA
	TRIAL DigiNotar PKIoverheid Organisatie TEST CA G2-1
	TRIAL DigiNotar PKIoverheid Organisatie TEST CA G2
Test-CA	AA Interfinance Test CA
	DigiNotar HSM RSA Test CA Administrative CA
	DigiNotar HSM RSA Test CA System CA
	DigiNotar RSA Test Root 4096 G2
	DigiNotar RSA Test Root 4096
	Hypotrust CA
	TEST Key Recovery CA
	Test DigiNotar Company CA
	Test DigiNotar Extended Validation CA
	Test DigiNotar PKIOverheid CA Overheid en bedrijven
	Test DigiNotar PKIoverheid CA Organisatie - G2
	Test DigiNotar Private CA
	Test DigiNotar Public Subroot G2
	Test DigiNotar Public Subroot
	Test DigiNotar Qualified CA
	Test DigiNotar Services CA
	Test EASEE- gas CA
	Test KNB CA
	Test Ministerie van Justitie CA 2
	Test Nederlandse Orde van Advocaten - Dutch Bar Association
	Test Renault Nissan Nederland CA
	Test SHOCK CA
	Test SNG CA 2048
	Test SSL 3 Client Root CA 2010
	Test SSL 3 Server Root CA 2010

Server	CA nickname
	Test Stichting TTP Infos CA
	Test TU Delft CA
Relation-CA	Algemene Relatie Services Administrative CA
	Algemene Relatie Services System CA
	EASEE-gas CA
	KNB CA 2
	Ministerie van Justitie CA
	SNG CA
	Stichting TTP Infos CA
	TU Delft CA

Appendix V: Certificate Authorities

Based on the investigations of the database files of the CA management software, the issuing CAs were determined. The validity period has not been taken into account.

Root-CA server

Issuers and numbers of occurrences of certificates found in the database files on the Root-CA server.

Root-CA: Issuer	#
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Root CA Administrative CA	2
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Root CA System CA	32
/C=NL/O=DigiNotar B.V./OU=Operations/CN=winsvr020	1
/C=NL/O=DigiNotar/CN=DigiNotar Root CA G2/emailAddress=info@diginotar.nl	6
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl	24
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Autonome Apparaten CA - G2	1
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Organisatie CA - G2	2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Autonome Apparaten CA - G2	1
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Organisatie CA - G2	1
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Root CA - G2	3

Certificates with the basic constraints attribute set found in the database files on the Root-CA server.

Root-CA: Basic constraints = TRUE
/C=FR/O=EASEE-gas/CN=EASEE-gas CA
/C=NL/O=AA Interfinance B.V./CN=AA Interfinance CA
/C=NL/O=Delft University of Technology/CN=TU Delft CA
/C=NL/O=DigiNotar/CN=CertiID Enterprise Certificate Authority/emailAddress=info@diginotar.com
/C=NL/O=DigiNotar/CN=DigiNotar Extended Validation CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Private CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Public CA - G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Public CA 2025/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Qualified CA - G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Qualified CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Root CA G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Services 1024 CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Services CA/emailAddress=info@diginotar.nl
/C=NL/O=Hypotrust/CN=Hypotrust CA
/C=NL/O=Koninklijke Notariele Beroepsorganisatie/CN=Koninklijke Notariele Beroepsorganisatie CA
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Autonome Apparaten CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Organisatie CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Autonome Apparaten CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Organisatie CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Root CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Taxi CA Boordcomputerkaarten - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Taxi CA Systeemkaarten - G2
/C=NL/O=Ministerie van Justitie/CN=Ministerie van Justitie JEP1 CA
/C=NL/O=Nederlandse Orde van Advocaten/CN=Nederlandse Orde van Advocaten - Dutch Bar Association
/C=NL/O=Renault Nissan Nederland N.V./CN=Renault Nissan Nederland CA
/C=NL/O=Stichting Netwerk Gerechtsdeurwaarders/CN=SNG CA
/C=NL/O=Stichting SHOCK/CN=SHOCK CA
/C=NL/O=Stichting TTP Infos/CN=Stichting TTP Infos CA

Self-signed root certificates found in the database files on the Root-CA server.

Root-CA: Self signed
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Root CA System CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=winsvr020
/C=NL/O=DigiNotar/CN=DigiNotar Root CA G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Root CA - G2

Qualified-CA server

Issuers and numbers of occurrences of certificates found in the database files on the Qualified-CA server.

Qualified-CA: Issuer	#
/C=NL/O=DigiNotar B.V. TEST/CN=TRIAL DigiNotar PKIoverheid Organisatie TEST CA - G2	142
/C=NL/O=DigiNotar B.V. TEST/CN=TRIAL DigiNotar PKIoverheid Organisatie TEST CA G2	1
/C=NL/O=DigiNotar B.V./CN=DigiNotar PKIoverheid CA Organisatie - G2	1560
/C=NL/O=DigiNotar B.V./CN=DigiNotar PKIoverheid CA Overheid en Bedrijven	5358
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Qualified CA Administrative CA	5
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Qualified CA System CA	33
/C=NL/O=DigiNotar B.V./OU=Operations/CN=winsvr022	1
/C=NL/O=DigiNotar/CN=DigiNotar Qualified CA/emailAddress=info@diginotar.nl	16515
/C=NL/O=DigiNotar/CN=DigiNotar Root CA G2/emailAddress=info@diginotar.nl	1
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl	2
/C=NL/O=PKIoverheid TEST/CN=TRIAL PKIoverheid Organisatie TEST CA - G2	1
/C=NL/O=Staat der Nederlanden/CN=Staat der Nederlanden Organisatie CA - G2	1
/C=NL/O=Staat der Nederlanden/CN=Staat der Nederlanden Overheid CA	1

Certificates with the basic constraints attribute set found in the database files on the Qualified-CA server.

Qualified-CA: Basic constraints = TRUE
/C=NL/O=DigiNotar B.V. TEST/CN=TRIAL DigiNotar PKIoverheid Organisatie TEST CA - G2
/C=NL/O=DigiNotar B.V. TEST/CN=TRIAL DigiNotar PKIoverheid Organisatie TEST CA G2
/C=NL/O=DigiNotar B.V./CN=DigiNotar PKIoverheid CA Organisatie - G2
/C=NL/O=DigiNotar B.V./CN=DigiNotar PKIoverheid CA Overheid en Bedrijven
/C=NL/O=DigiNotar/CN=DigiNotar Qualified CA - G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Qualified CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl

Self-signed root certificates found in the database files on the Qualified-CA server.

Qualified-CA: Self signed
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Qualified CA Administrative CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Qualified CA System CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=winsvr022
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl

CCV-CA server

Issuers and numbers of occurrences of certificates found in the database files on the CCV-CA server.

CCV-CA: Issuer	#
/C=BE/O=CCV Belgium NV/SA/CN=Prod UpLoad Root CA 2010	1
/C=CH/O=CCV Jeronimo S.A./CN=Prod SSL3 Client Root CA 2010	2
/C=CH/O=CCV Jeronimo S.A./CN=Prod SSL3 Server Root CA 2010	1
/C=CH/O=CCV Jeronimo S.A./CN=Prod UpLoad Root CA 2010	1
/C=DE/O=CCV Deutschland GmbH/CN=Prod UpLoad Root CA 2010	1
/C=NL/O=CCV Services B.V./CN=Prod UpLoad Root CA 2010	14
/C=NL/O=DigiNotar B.V./OU=IT/CN=CCV Group CA Administrative CA	1
/C=NL/O=DigiNotar B.V./OU=IT/CN=CCV Group CA System CA	14
/C=NL/O=DigiNotar B.V./OU=IT/CN=winsvr057.DNproductie	2

Certificates with the basic constraints attribute set found in the database files on the CCV-CA server.

CCV-CA: Basic constraints = TRUE
/C=BE/O=CCV Belgium NV/SA/CN=Prod UpLoad Root CA 2010
/C=CH/O=CCV Jeronimo S.A./CN=CCV-CH-TMS 2010
/C=CH/O=CCV Jeronimo S.A./CN=Prod SSL3 Client Root CA 2010
/C=CH/O=CCV Jeronimo S.A./CN=Prod SSL3 Server Root CA 2010
/C=CH/O=CCV Jeronimo S.A./CN=Prod UpLoad Root CA 2010
/C=DE/O=CCV Deutschland GmbH/CN=Prod UpLoad Root CA 2010
/C=NL/O=CCV Services B.V./CN=Prod UpLoad Root CA 2010
/C=NL/O=CCV Services B.V./CN=USPP-Perso Certificate ST4000 260-110-364
/C=NL/O=CCV Services B.V./CN=USPP-Perso Certificate ST4000 260-160-364
/C=NL/O=CCV Services B.V./CN=USPP-Perso Certificate ST4000 260-179-095
/C=NL/O=CCV Services B.V./CN=USPP-Perso Certificate ST4000 260-237-323
/C=NL/O=CCV Services B.V./CN=USPP-Perso Certificate ST4000 260-300-362
/C=NL/O=CCV Services B.V./CN=USPP-Perso Certificate ST4000 260-310-362

CCV-CA: Basic constraints = TRUE
/C=NL/O=CCV Services B.V./CN=USPP-Perso Certificate ST4000 260-399-095
/C=NL/O=CCV Services B.V./CN=USPP-Perso Certificate ST4000 260-507-524
/C=NL/O=CCV Services B.V./CN=USPP-Perso Certificate ST4000 260-537-524
/C=NL/O=CCV Services B.V./CN=USPP-Perso Certificate ST4000 260-569-094
/C=NL/O=CCV Services B.V./CN=USPP-Perso Certificate ST4000 260-659-094
/C=NL/O=DigiNotar B.V./OU=IT/CN=CCV Group CA Administrative CA
/C=NL/O=DigiNotar B.V./OU=IT/CN=CCV Group CA System CA

Self-signed root certificates found in the database files on the CCV-CA server.

CCV-CA: Self signed
/C=BE/O=CCV Belgium NV/SA/CN=Prod UpLoad Root CA 2010
/C=CH/O=CCV Jeronimo S.A./CN=Prod SSL3 Client Root CA 2010
/C=CH/O=CCV Jeronimo S.A./CN=Prod SSL3 Server Root CA 2010
/C=CH/O=CCV Jeronimo S.A./CN=Prod UpLoad Root CA 2010
/C=DE/O=CCV Deutschland GmbH/CN=Prod UpLoad Root CA 2010
/C=NL/O=CCV Services B.V./CN=Prod UpLoad Root CA 2010
/C=NL/O=DigiNotar B.V./OU=IT/CN=CCV Group CA System CA
/C=NL/O=DigiNotar B.V./OU=IT/CN=winsvr057.DNproductie

Nova-CA server

Issuers and numbers of occurrences of certificates found in the database files on the Nova-CA server.

Nova-CA: Issuer	#
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Orde van Advocaten SubCA Administrative CA	4
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Orde van Advocaten SubCA System CA	31
/C=NL/O=DigiNotar B.V./OU=Operations/CN=winsvr021	1
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl	2
/C=NL/O=Nederlandse Orde van Advocaten/CN=Nederlandse Orde van Advocaten - Dutch Bar Association	37830

Certificates with the basic constraints attribute set found in the database files on the Nova-CA server.

Nova-CA: Basic constraints = TRUE
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl
/C=NL/O=Nederlandse Orde van Advocaten/CN=Nederlandse Orde van Advocaten - Dutch Bar Association

Self-signed root certificates found in the database files on the Nova-CA server.

Nova-CA: Self signed
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Orde van Advocaten SubCA Administrative CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Orde van Advocaten SubCA System CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=winsvr021
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl

Taxi-CA server

Issuers and numbers of occurrences of certificates found in the database files on the Taxi-CA server.

Taxi-CA: Issuer	#
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Taxi CA Administrative CA	4
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Taxi CA System CA	15
/C=NL/O=DigiNotar/OU=IT/CN=Winsvr053.DNproductie	1
/C=NL/O=Inspectie Verkeer en Waterstaat/OU=Test CA/CN=IVW SIMULATOR NL Autonome Apparaten CA - G2	1
/C=NL/O=Inspectie Verkeer en Waterstaat/OU=Test CA/CN=IVW SIMULATOR NL Organisatie CA - G2	1
/C=NL/O=Inspectie Verkeer en Waterstaat/OU=Test CA/CN=IVW SIMULATOR NL Root CA - G2	3
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Productieomgeving/CN=BCT Infrastructuur AP CA	13
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Autonome Apparaten CA - G2	1
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Organisatie CA - G2	1
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Taxi CA Boordcomputerkaarten - G2	639
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Taxi CA Systeemkaarten - G2	230
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Autonome Apparaten CA - G2	2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Organisatie CA - G2	3
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM SIMULATOR NL Root CA - G2	2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Taxi CA Boordcomputerkaarten - G2	420
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Taxi CA Systeemkaarten - G2	7

Taxi-CA: Issuer	#
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Testomgeving/CN=BCT Infrastructuur OT CA	5

Certificates with the basic constraints attribute set found in the database files on the Taxi-CA server.

Taxi-CA: Basic constraints = TRUE
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Taxi CA Administrative CA
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Taxi CA System CA
/C=NL/O=Inspectie Verkeer en Waterstaat/OU=Test CA/CN=IVW SIMULATOR NL Autonome Apparaten CA - G2
/C=NL/O=Inspectie Verkeer en Waterstaat/OU=Test CA/CN=IVW SIMULATOR NL Organisatie CA - G2
/C=NL/O=Inspectie Verkeer en Waterstaat/OU=Test CA/CN=IVW SIMULATOR NL Root CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Productieomgeving/CN=BCT Infrastructuur AP CA
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Taxi CA Boordcomputerkaarten - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Taxi CA Systeemkaarten - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Autonome Apparaten CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Organisatie CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM SIMULATOR NL Autonome Apparaten CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM SIMULATOR NL Organisatie CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Taxi CA Boordcomputerkaarten - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Taxi CA Systeemkaarten - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Testomgeving/CN=BCT Infrastructuur OT CA

Self-signed root certificates found in the database files on the Taxi-CA server.

Taxi-CA: Self signed
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Taxi CA System CA
/C=NL/O=DigiNotar/OU=IT/CN=Winsvr053.DNproductie
/C=NL/O=Inspectie Verkeer en Waterstaat/OU=Test CA/CN=IVW SIMULATOR NL Root CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Productieomgeving/CN=BCT Infrastructuur AP CA
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Testomgeving/CN=BCT Infrastructuur OT CA

Test-CA server

Issuers and numbers of occurrences of certificates found in the database files on the Test-CA server.

Test-CA: Issuer	#
/C=DE/O=CCV Deutschland GmbH/CN=Test UpLoad Root CA 2010	8
/C=FR/O=EASEE-gas/CN=Test EASEE-gas CA	25
/C=NL/O=AA Interfinance B.V./CN=Test AA Interfinance CA/emailAddress=info@diginotar.nl	2
/C=NL/O=CCV Group/CN=Test SSL3 Client Root CA 2010	4
/C=NL/O=CCV Group/CN=Test SSL3 Server Root CA 2010	4
/C=NL/O=CCV Services B.V./CN=Test UpLoad Root CA 2010	1
/C=NL/O=Delft University of Technology/CN=Test TU Delft CA	91
/C=NL/O=DigiNotar B.V./CN=Test DigiNotar PKIoverheid CA Organisatie - G2	1
/C=NL/O=DigiNotar B.V./CN=Test DigiNotar PKIoverheid CA Overheid en bedrijven	562
/C=NL/O=DigiNotar/CN=Test DigiNotar Company CA	3
/C=NL/O=DigiNotar/CN=Test DigiNotar Extended Validation CA	20
/C=NL/O=DigiNotar/CN=Test DigiNotar Extended Validation Services CA/emailAddress=info@diginotar.nl	6
/C=NL/O=DigiNotar/CN=Test DigiNotar Private CA/emailAddress=info@diginotar.nl	5
/C=NL/O=DigiNotar/CN=Test DigiNotar Public CA 2025 G2/emailAddress=info@diginotar.nl	1
/C=NL/O=DigiNotar/CN=Test DigiNotar Public CA 2025/emailAddress=info@diginotar.nl	606
/C=NL/O=DigiNotar/CN=Test DigiNotar Qualified CA/emailAddress=info@diginotar.nl	1134
/C=NL/O=DigiNotar/CN=Test DigiNotar Root CA G2/emailAddress=info@diginotar.nl	2
/C=NL/O=DigiNotar/CN=Test DigiNotar Root CA/emailAddress=info@diginotar.nl	47
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar HSM RSA Test CA Administrative CA	6
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar HSM RSA Test CA System CA	42
/C=NL/O=DigiNotar/OU=IT/CN=RSATESTCA	1
/C=NL/O=Hypotrust/CN=Hypotrust CA	87
/C=NL/O=Interbank N.V./CN=Test Interbank N.V.	1
/C=NL/O=Koninklijk Notariele Beroepsorganisatie/CN=Test Koninklijk Notariele Beroepsorganisatie CA	29
/C=NL/O=Nederlandse Orde van Advocaten/CN=Test Nederlandse Orde van Advocaten - Dutch Bar Association	97
/C=NL/O=Stichting Netwerk Gerechtsdeurwaarders/CN=Test SNG CA	11
/C=NL/O=Stichting SHOCK/CN=Test SHOCK CA	16
/C=NL/O=Stichting TTP Infos/CN=Test Stichting TTP Infos CA	52
/C=NL/O=Test Ministerie van Justitie/CN=Test Ministerie van Justitie CA	174
/CN=Test AA Interfinance CA/O=AA Interfinance B.V./C=NL	30
/CN=Test Renault Nissan Nederland CA/O=Renault Nissan Nederland N.V./C=NL	42
/emailAddress=info@diginotar.nl/C=NL/O=DigiNotar/OU=TEST/CN=TEST Key Recovery CA	1

Certificates with the basic constraints attribute set found in the database files on the Test-CA server.

Test-CA: Basic constraints = TRUE
/C=DE/O=CCV Deutschland GmbH/CN=Test UpLoad Root CA 2010
/C=DE/O=CCV Deutschland GmbH/CN=USPP-Perso Certificate ST4000 260-219-072
/C=DE/O=CCV Deutschland GmbH/CN=USPP-Perso Certificate ST4000 260-269-072
/C=DE/O=CCV Deutschland GmbH/CN=USPP-Perso Certificate ST4000 260-429-072
/C=DE/O=CCV Deutschland GmbH/CN=USPP-Perso Certificate ST4000 260-439-072
/C=FR/O=EASEE-gas/CN=Test EASEE-gas CA
/C=NL/O=AA Interfinance B.V./CN=AA Interfinance CA/emailAddress=info@diginotar.nl
/C=NL/O=AA Interfinance B.V./CN=Test AA Interfinance CA/emailAddress=info@diginotar.nl
/C=NL/O=CCV Group/CN=oltp.ccvpay.nl
/C=NL/O=CCV Group/CN=Test SSL3 Client Root CA 2010
/C=NL/O=CCV Group/CN=Test SSL3 Server Root CA 2010
/C=NL/O=CCV Group/CN=Test.SSL3.certificate.erwin.nl
/C=NL/O=CCV Services B.V./CN=Test UpLoad Root CA 2010
/C=NL/O=Delft University of Technology/CN=Test TU Delft CA
/C=NL/O=DigiNotar B.V./CN=Test DigiNotar PKIoverheid CA Organisatie - G2
/C=NL/O=DigiNotar B.V./CN=Test DigiNotar PKIoverheid CA Overheid en bedrijven
/C=NL/O=DigiNotar/CN=Test DigiNotar Company CA
/C=NL/O=DigiNotar/CN=Test DigiNotar Extended Validation CA
/C=NL/O=DigiNotar/CN=Test DigiNotar Extended Validation Services CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Private CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Public CA 2025 G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Public CA 2025/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Qualified CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Root CA G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Root CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Services CA/emailAddress=info@diginotar.nl
/C=NL/O=Hypotrust/CN=Hypotrust CA
/C=NL/O=Interbank N.V./CN=Test Interbank N.V.
/C=NL/O=Koninklijk Notariele Beroepsorganisatie/CN=Test Koninklijk Notariele Beroepsorganisatie CA
/C=NL/O=Ministerie van Justitie/CN=Ministerie van Justitie CA
/C=NL/O=Nederlandse Orde van Advocaten/CN=Test Nederlandse Orde van Advocaten - Dutch Bar Association
/C=NL/O=Schuberg Philis/CN=Schuberg Philis Class 1 Issuing CA
/C=NL/O=Schuberg Philis/CN=Schuberg Philis Class 2 Issuing CA
/C=NL/O=Schuberg Philis/CN=Test Schuberg Philis Class 1 Issuing CA
/C=NL/O=Stichting Netwerk Gerechtsdeurwaarders/CN=Test SNG CA
/C=NL/O=Stichting SHOCK/CN=Test SHOCK CA
/C=NL/O=Stichting TTP Infos/CN=Test Stichting TTP Infos CA
/C=NL/O=Test Ministerie van Justitie/CN=Test Ministerie van Justitie CA
/CN=oltp.ccvpay.nl/OU=DMT/O=CCV Group/L=Arnhem/ST=Gelderland/C=NL
/CN=Test AA Interfinance CA/O=AA Interfinance B.V./C=NL
/CN=Test.SSL3.certificate.erwin.nl/OU=Systems/O=CCV Group/L=Arnhem/ST=Gelderland/C=NL
/emailAddress=info@diginotar.nl/C=NL/O=DigiNotar/CN=Test DigiNotar Public CA

Self-signed root certificates found in the database files on the Test-CA server.

Test-CA: Self signed
/C=DE/O=CCV Deutschland GmbH/CN=Test UpLoad Root CA 2010
/C=NL/O=CCV Group/CN=Test SSL3 Client Root CA 2010
/C=NL/O=CCV Group/CN=Test SSL3 Server Root CA 2010
/C=NL/O=CCV Services B.V./CN=Test UpLoad Root CA 2010
/C=NL/O=DigiNotar B.V./CN=Test DigiNotar PKIoverheid CA Organisatie - G2
/C=NL/O=DigiNotar/CN=Test DigiNotar Qualified CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Root CA G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Root CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar HSM RSA Test CA Administrative CA
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar HSM RSA Test CA System CA
/C=NL/O=DigiNotar/OU=IT/CN=RSATESTCA

Relation-CA server

Issuers and numbers of occurrences of certificates found in the database files on the Relation-CA server.

Relation-CA: Issuer	#
/C=FR/O=EASEE-gas/CN=EASEE-gas CA	47
/C=NL/O=AA Interfinance B.V./CN=AA Interfinance CA	5
/C=NL/O=Delft University of Technology/CN=TU Delft CA	274
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Algemene Relatie Services Administrative CA	3
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Algemene Relatie Services System CA	31
/C=NL/O=DigiNotar B.V./OU=Operations/CN=winsvr055	1
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl	11

Relation-CA: Issuer	#
/C=NL/O=Hypotrust/CN=Hypotrust CA	977
/C=NL/O=Koninklijk Notariele Beroepsorganisatie/CN=Koninklijk Notariele Beroepsorganisatie CA	1
/C=NL/O=Koninklijke Notariele Beroepsorganisatie/CN=Koninklijke Notariele Beroepsorganisatie CA	1192
/C=NL/O=Ministerie van Justitie/CN=Ministerie van Justitie JEP1 CA	6139
/C=NL/O=Renault Nissan Nederland N.V./CN=Renault Nissan Nederland CA	155
/C=NL/O=Stichting Netwerk Gerechtsdeurwaarders/CN=SNG CA	379
/C=NL/O=Stichting SHOCK/CN=SHOCK CA	1
/C=NL/O=Stichting TTP Infos/CN=Stichting TTP Infos CA	2320
/C=NL/O=TenneT TSO BV/CN=TenneT CA 2011	135

Certificates with the basic constraints attribute set found in the database files on the Relation-CA server.

Relation-CA: Basic constraints = TRUE
/C=FR/O=EASEE-gas/CN=EASEE-gas CA
/C=NL/O=AA Interfinance B.V./CN=AA Interfinance CA
/C=NL/O=Delft University of Technology/CN=TU Delft CA
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl
/C=NL/O=Hypotrust/CN=Hypotrust CA
/C=NL/O=Koninklijke Notariele Beroepsorganisatie/CN=Koninklijke Notariele Beroepsorganisatie CA
/C=NL/O=Ministerie van Justitie/CN=Ministerie van Justitie JEP1 CA
/C=NL/O=Renault Nissan Nederland N.V./CN=Renault Nissan Nederland CA
/C=NL/O=Stichting Netwerk Gerechtsdeurwaarders/CN=SNG CA
/C=NL/O=Stichting SHOCK/CN=SHOCK CA
/C=NL/O=Stichting TTP Infos/CN=Stichting TTP Infos CA
/C=NL/O=TenneT TSO BV/CN=TenneT CA 2011

Self signed root certificates found in the database files on the Relation-CA server.

Relation-CA: Self signed
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Algemene Relatie Services Administrative CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Algemene Relatie Services System CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=winsvr055
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl
/C=NL/O=Koninklijk Notariele Beroepsorganisatie/CN=Koninklijk Notariele Beroepsorganisatie CA
/C=NL/O=TenneT TSO BV/CN=TenneT CA 2011

Public-CA server

Issuers and numbers of occurrences of certificates found in the database files on the Public-CA server.

Public-CA: Issuer	#
/C=NL/O=DigiNotar/CN=DigiNotar Cyber CA/emailAddress=info@diginotar.nl	124
/C=NL/O=DigiNotar/CN=DigiNotar Extended Validation CA/emailAddress=info@diginotar.nl	226
/C=NL/O=DigiNotar/CN=DigiNotar Private CA/emailAddress=info@diginotar.nl	2
/C=NL/O=DigiNotar/CN=DigiNotar Public CA - G2/emailAddress=info@diginotar.nl	54
/C=NL/O=DigiNotar/CN=DigiNotar Public CA 2025/emailAddress=info@diginotar.nl	45002
/C=NL/O=DigiNotar/CN=DigiNotar Root CA G2/emailAddress=info@diginotar.nl	2
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl	6
/C=NL/O=DigiNotar/CN=DigiNotar Services 1024 CA/emailAddress=info@diginotar.nl	564
/C=NL/O=DigiNotar/CN=DigiNotar Services CA/emailAddress=info@diginotar.nl	86
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Public CA 2025 Administrative CA	4
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Public CA 2025 System CA	29
/C=NL/O=DigiNotar/OU=IT/CN=winsvr056	1
/C=US/O=GTE Corporation/OU=GTE CyberTrust Solutions, Inc./CN=GTE CyberTrust Global Root	1

Certificates with the basic constraints attribute set found in the database files on the Public-CA server.

Public-CA: Basic constraints = TRUE
/C=NL/O=DigiNotar/CN=CertiID Enterprise Certificate Authority/emailAddress=info@diginotar.com
/C=NL/O=DigiNotar/CN=DigiNotar Cyber CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Extended Validation CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Private CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Public CA - G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Public CA 2025/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Services 1024 CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Services CA/emailAddress=info@diginotar.nl

Self-signed root certificates found in the database files on the Public-CA server.

Public-CA: Self signed
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Root CA System CA
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Public CA 2025 Administrative CA
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Public CA 2025 System CA
/C=NL/O=DigiNotar/OU=IT/CN=winsvr056

Appendix VI: References to private keys

This appendix contains lists of private keys that were present in the databases of the CA servers. The validity period has not been taken into account. The entries *No Certificate found* mean that a private key entry was found in the database but that no corresponding certificate or name was found.

Root-CA keys
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Root CA Administrative CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Root CA System CA
/C=NL/O=DigiNotar/CN=DigiNotar Root CA G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Organisatie CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Root CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Autonome Apparaten CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Organisatie CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Autonome Apparaten CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Organisatie CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Root CA - G2

Qualified-CA keys
/C=NL/O=DigiNotar B.V. TEST/CN=TRIAL DigiNotar PKIoverheid Organisatie TEST CA G2
/C=NL/O=DigiNotar B.V. TEST/CN=TRIAL DigiNotar PKIoverheid Organisatie TEST CA - G2
/C=NL/O=DigiNotar B.V./CN=DigiNotar PKIoverheid CA Organisatie - G2
/C=NL/O=DigiNotar B.V./CN=DigiNotar PKIoverheid CA Overheid en Bedrijven
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Qualified CA Administrative CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Qualified CA System CA
/C=NL/O=DigiNotar/CN=DigiNotar Qualified CA - G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Qualified CA/emailAddress=info@diginotar.nl

CCV-CA keys
/C=BE/O=CCV Belgium NV/SA/CN=Prod UpLoad Root CA 2010
/C=CH/O=CCV Jeronimo S.A./CN=Prod SSL3 Client Root CA 2010
/C=CH/O=CCV Jeronimo S.A./CN=Prod SSL3 Server Root CA 2010
/C=CH/O=CCV Jeronimo S.A./CN=Prod UpLoad Root CA 2010
/C=DE/O=CCV Deutschland GmbH/CN=Prod UpLoad Root CA 2010
/C=NL/O=CCV Services B.V./CN=Prod UpLoad Root CA 2010
/C=NL/O=DigiNotar B.V./OU=IT/CN=CCV Group CA Administrative CA
/C=NL/O=DigiNotar B.V./OU=IT/CN=CCV Group CA System CA
No Certificate found
No Certificate found

Nova-CA keys
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Orde van Advocaten SubCA Administrative CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Orde van Advocaten SubCA System CA
/C=NL/O=Nederlandse Orde van Advocaten/CN=Nederlandse Orde van Advocaten - Dutch Bar Association

Taxi-CA keys
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Taxi CA Administrative CA
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Taxi CA System CA
/C=NL/O=Inspectie Verkeer en Waterstaat/OU=Test CA/CN=IVW SIMULATOR NL Root CA - G2
/C=NL/O=Inspectie Verkeer en Waterstaat/OU=Test CA/CN=IVW SIMULATOR NL Organisatie CA - G2
/C=NL/O=Inspectie Verkeer en Waterstaat/OU=Test CA/CN=IVW SIMULATOR NL Autonome Apparaten CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Productieomgeving/CN=BCT Infrastructuur AP CA
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Taxi CA Systeemkaarten - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Taxi CA Boordcomputerkaarten - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM SIMULATOR NL Organisatie CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Organisatie CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Taxi CA Systeemkaarten - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Autonome Apparaten CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Taxi CA Boordcomputerkaarten - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM SIMULATOR NL Autonome Apparaten CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Testomgeving/CN=BCT Infrastructuur OT CA
No certificate found
No certificate found

Test-CA keys
/C=DE/O=CCV Deutschland GmbH/CN=Test UpLoad Root CA 2010
/C=FR/O=EASEE-gas/CN=Test EASEE-gas CA
/C=NL/O=AA Interfinance B.V./CN=AA Interfinance CA/emailAddress=info@diginotar.nl
/C=NL/O=AA Interfinance B.V./CN=Test AA Interfinance CA/emailAddress=info@diginotar.nl
/C=NL/O=CCV Group/CN=Test SSL3 Client Root CA 2010
/C=NL/O=CCV Group/CN=Test SSL3 Client Root CA 2010
/C=NL/O=CCV Group/CN=Test SSL3 Server Root CA 2010
/C=NL/O=CCV Group/CN=Test SSL3 Server Root CA 2010
/C=NL/O=CCV Services B.V./CN=Test UpLoad Root CA 2010
/C=NL/O=Delft University of Technology/CN=Test TU Delft CA
/C=NL/O=DigiNotar B.V./CN=Test DigiNotar PKIoverheid CA Organisatie - G2
/C=NL/O=DigiNotar B.V./CN=Test DigiNotar PKIoverheid CA Overheid en bedrijven
/C=NL/O=DigiNotar/CN=Test DigiNotar Company CA
/C=NL/O=DigiNotar/CN=Test DigiNotar Extended Validation CA
/C=NL/O=DigiNotar/CN=Test DigiNotar Extended Validation Services CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Private CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Public CA 2025 G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Public CA 2025/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Qualified CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Root CA G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Root CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Services CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar HSM RSA Test CA Administrative CA
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar HSM RSA Test CA System CA
/C=NL/O=Hypotrust/CN=Hypotrust CA
/C=NL/O=Interbank N.V./CN=Test Interbank N.V.
/C=NL/O=Koninklijk Notariele Beroepsorganisatie/CN=Test Koninklijk Notariele Beroepsorganisatie CA
/C=NL/O=Ministerie van Justitie/CN=Ministerie van Justitie CA
/C=NL/O=Ministerie van Justitie/CN=Ministerie van Justitie CA
/C=NL/O=Nederlandse Orde van Advocaten/CN=Test Nederlandse Orde van Advocaten - Dutch Bar Association
/C=NL/O=Stichting Netwerk Gerechtsdeurwaarders/CN=Test SNG CA
/C=NL/O=Stichting Netwerk Gerechtsdeurwaarders/CN=Test SNG CA
/C=NL/O=Stichting SHOCK/CN=Test SHOCK CA
/C=NL/O=Stichting TTP Infos/CN=Test Stichting TTP Infos CA
/C=NL/O=Test Ministerie van Justitie/CN=Test Ministerie van Justitie CA
/CN=Test AA Interfinance CA/O=AA Interfinance B.V./C=NL
/emailAddress=info@diginotar.nl/C=NL/O=DigiNotar/CN=Test DigiNotar Public CA
/emailAddress=info@diginotar.nl/C=NL/O=DigiNotar/OU=TEST/CN=TEST Key Recovery CA
No certificate found
No certificate found
No certificate found
No certificate found

Relation-CA keys
/C=FR/O=EASEE-gas/CN=EASEE-gas CA
/C=NL/O=AA Interfinance B.V./CN=AA Interfinance CA
/C=NL/O=Delft University of Technology/CN=TU Delft CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Algemene Relatie Services System CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Algemene Relatie Services Administrative CA
/C=NL/O=Hypotrust/CN=Hypotrust CA
/C=NL/O=Koninklijk Notariele Beroepsorganisatie/CN=Koninklijk Notariele Beroepsorganisatie CA
/C=NL/O=Koninklijke Notariele Beroepsorganisatie/CN=Koninklijke Notariele Beroepsorganisatie CA
/C=NL/O=Ministerie van Justitie/CN=Ministerie van Justitie JEP1 CA
/C=NL/O=Renault Nissan Nederland N.V./CN=Renault Nissan Nederland CA
/C=NL/O=Stichting Netwerk Gerechtsdeurwaarders/CN=SNG CA
/C=NL/O=Stichting SHOCK/CN=SHOCK CA
/C=NL/O=Stichting TTP Infos/CN=Stichting TTP Infos CA
/C=NL/O=TenneT TSO BV/CN=TenneT CA 2011
No certificate found

Public-CA keys
/C=NL/O=DigiNotar/CN=CertiID Enterprise Certificate Authority/emailAddress=info@diginotar.com
/C=NL/O=DigiNotar/CN=DigiNotar Cyber CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Extended Validation CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Private CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Public CA - G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Public CA 2025/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Services 1024 CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Services CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Public CA 2025 Administrative CA
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Public CA 2025 System CA

Appendix VII: Unknown serial numbers

The following serial numbers were encountered in the `serial_no.dbh` database on servers managing the Certificate Authorities, but could not be related to any identified certificates.

Root-CA

```
83120A023016C9E1A59CC7D146619617
68E32B2FE117DFE89C905B1CCBE22AB7
711CE18C0423218425510EF51513B7B8
B7ABEFC8A1F844207B774C782E5385B3
6E0088D11C7E4E98CC9E0694D32A0F6B
80C990D339F177CA9FDAC258105882AB
7F73EC0A14C4BA065BECFAD69DC5A61D
```

Qualified-CA

```
C6E2E63E7CA99BBA1361E4FB7245493C
863DE266FB30C5C489BF53F6553088C4
```

Taxi-CA

```
25B6CA311C52F0E4F72A1BD53774B5B3
A0CF459D0D1EA9A946861A0A02783D88
71A10FA4C491D3A72D18D33E3CCF576C
FE456B099700A6C428A193FE5968C9FD
E7E2B46B8C9AA64679E03841F88CA5A0
AEC9F2324D80020B6E2B2A1103D6A4E8
CB20C25F14583AFC86465F14E621FBC1
947FF1DB66A41D809A9BC7E7344E342A
90BCA541B4DF5E77FB1349684F84A930
AB4967CE8B94FCF8DA7691922E6FD59C
BA479991C9103C005726FAB83088A8D6
363E9AAF4DAC7085F31B89B2AC49059A
8A63042B8A8FA256035773BC9417435A
963CCB2601B15C73DCA821F4BC4C7458
6B7057D5DE0170842C372821D3F17DB2
C391438C15FF31BD89544A7F68DDF3B3
7278CB2A8270A3E66A021A7CD75F1211
F401D4C50FCA9161A70ED9D91D40E684
6C396359C423417E20C54CFC6690F3FF
9916C8350225BB607857375A02B6DC72
0F48A14121370B5CF4828EF826749FBC
DB43E2CE6110750785FCBBE9A8EAE061
C641E4B7F19B63C4FF1EA6D3833FC874
D8B771F90BC01C9ED1333C23EF24CFC1
```

Public-CA

```
79C03FE0C81A3022DBF8143B27E40223  BC01852405D3F4E22C48600266655026  E3E120935934CBD77E1DA7F00431F745
FCCF53CB3D0A71494AF9664690FFCF84  9F7DDFE3CAAD224EC6BD68B60DE78550  0A6DFACFDEAE74A816031534BE90B75A
82BC18B1AA5D59C61D0EFDBEA7664C08  A67C22A6E1F9D87799548EBFC7D5527E  9AD82BE2FED538B10BDFBD229A8A5AEA
5D4352671C39616670B2F34C173A1F63  11661878CCE9DC337CEEBB16E30F9A3A  C0F216CA8197AD00F0D98927EAE29E64
6FA3C48173B3B289943F113A8CD9DB8C  6BF3BEB26AFF31116200B14F4378C33B  DE76B17BFB1B6D6D6634C8C104A6E59F
CFAF9BE4E5BD0F5A75F628E45E0178C9  7A61A7778842E502E2291166C4574485  A90F1BB43E9DB5EDFC60C15FB897C593
4ADA28D281D3D14D19FB782D64086D0C  82C42F0EDC18BD751727BE5C54413EF7  8625B32398C2722D96E7B972580A0238
0B41ABEE6F4168D3CDE5A7D223B58BC1  03124C25849D9E49BC2A2FAD3E10C8A4  D1FDE3A78C9D2E80C2303CC4E3E92A4C
13548FC160BC5C9F315AE28CDB490E36  EFF0DD4B4927DF64232C5D2FF280C1E4  B355E909FD55C5E9EF1A6E67E9C18203
5D8D0D43611275982E6A5490E7F87BD7  9EDCB5E1FE1255A2F1D7FC52C4AFA3B1  ADB59A303C6260DBE466F0149AB11A4A
C880AE4D7927E6A8FA7D456CB03E9763  3A32AAA9DFE2CA7F9E003885E316944B  5CEBD524469A075FB6B42D06C9BF27AD
82072FC8F8DD7E6C0ECE9B47185F0521  4455B43B9173CBAE4E247272EE2573D5  0E0886EEAA119CF14F1C54387060929A
90DB656E273476CC836778255582FA8B  B95F62E86194734C9F68D4BF8B200C49  B4F9299F05A327E60543C4CDE3277FC0
171A8599EDE711A3315BC7D694CEBEC6  FE873B742B230B22AE540E840490A2F4  E4B2F09505726306314DF05B734FD9D0
E9EB8075F7FE3683B431552C2D962CB0  8779917563EC38B7746B8ECAFE239BE6  4DD0497CBAABBA058574A611B26151BA
E6F9E095464F64448840A832FB3443DB  72CBC4824C6215B139FDE6BA10DAC6AD  7073C6C01DEE4E158F554555F697F7D9
C83D16E9CB29DCF35F3B351CB942FE0D  8D09D4B98DE67C9E9C7C18CB72AD2418  EB72415ECD0B4AACBDEEA3734F4349BF
39B5DD0ECC85C3F62A72391DC055F561  07BC72A463D4DE33B2BE733D6FAC991D  BED90D98FA3A1E0A5BD78AD54E55774D
DF3FD6AFBBFBC30C9AD80BF764A102DB  D3E2205C3B899FC99D77FE802985283F  3CDCD81930F91AC0B990664931E5412E
327B9A443C49018D7B0A97B6EC2254B8  A5029D6A057D50D20ECFE0E528EDA067  763B0C2A7B83066A9D995C8C4FD9E35E
8B0EABAF922D4C6E6917FCBE365DD64A  C8B2487ADFAF969E34306029AC934406  720DF591261D710ADC73127C1BC4303D
4FC2D72D6427CABBE3E859453865F43B  5F3C1BDC7A2BCD47ABAF0C8E62D9F757  C06C12DBBC7055FE40950803238EC104
53B53BF2F74997EBEB2577D63DA692B7  601315BB085FECF29538DA3F9B7BA1CE  62BF5A170CC779ADE7EF0090F395D5E6
ABB21F43553F2695031A1C85355D7F1C  30170F15A240446E6B482E0A364E3CCA  61BF9A0FF2CE9D55D86BC063839F72F4
5563605FDC2DC865E2A1C32995B5A086  0590B310AEFC7A3EDC03ECA2A6F6624F  B5D7A148CA6C1F9693A2C16ACDD66226
5DD6A72747D90C018B63F959DFE7C976  FDEB145AAC81B8CD29B8DA018E71456F  35FBDCDF923F99B5E1C5FF4423B715B8
CAB736FFE7DCB2C47ED2FF88842888E7  C3F9F45F19E334C8303F44288856D843  F1EBE73557546DC8B21E0A2DE5E3A33E
9C79C9FE16727BAC407B4AA21B153A54  028CF7556F8BE27026800448FA6AA527  EBE7561CA573DA5DBB8EFAA250A40FD3
2D711C9CB79EC15445747BFE3F8BC92F  E93B28B47C34B243EBA62E58FE2FF46F  6BACB6C5B74FA747A3CF375EC3095035
752A2D0325A3D34D9F5198C2F5C92A6C  F89F5DE575755A3B4C0DECC6EDA7C804  6C1950AA83F4663F1BA063B5275C25EC
39936336286F843756FC4BC296D7A8E0  5D8F8D78B0C19EF4479F744DECBD84BC  56EF1EE54D65EF7B39AF541E95BB45A9
4A6D90618A5CA6797C768C03C860C4F8  EAACDC2F46D4A86F39B035B793F4A94F  2B1EA767EC59E46364BC2DF9B1F30B97
0954E1AB9141ED7E8B640FE681046451  9D06313F21A4EDF734C324FFBCB9E2B5  3913B1E1C35BDDF02CE03C916E8AA638
8259C3E1DB6C2C9B7FCD6A305EADEFE4  35C54E845AE855F818504C8C189F52C7  AFA2F7E964280B36DB0D714B86256F54
```

Public-CA		
022E35B1ACD40F040C444DF32A7B8DE6	D0BA58BA609CC1A001F612987A822BEF	9A3A951BE27E0729726FD8B80060E7E1
170370B60D515F164119BE54FD55E1ED	6B339433956F1505104BB231314A153E	6410577C738133297472F6C22C2BB397
CBFE437C9B62805C4353516699E44649	C1366C7246041A3089E1C244C5DC42E7	C8C06B0C6B7FE7CA66BCFE617AB6C4E6
5FFA79AB76CE359089A2F729A1D44B31	61D11B35765ECB85890D5349786D9FCA	58C18B290620E18B8C78AC1912E5DCD7
5298BCBD11B3952E3FDDC6FDD6711F5C	44C287C1C3697367B0E6CB78A78C1DF5	2F5ABFDCCAB1A2927E54283296F19FB8
1836289F75F74A0BA5E769561DE3E7CD	DAACF72BC91FB6DA90A804933CB72E23	A07CB7881E35C91FD9C5D20F6102572C
DEB427AC9F1E8A0D0237049C80DF7E7F	2ACBA14BB6F65F7BD0A485BFCB6D023F	05E2E6A4CD09EA54D665B075FE22A256
FD8FE350325318C893AFE03F9DFC7096	84BE5D762F37E9018D623C8E91F4D924	8BA800DDDD865B6BF3A85ADEC4C29730
A8031D608F6549941879981764674DD7	1A89324D6D3E6DE6726C688BFF225DDD	07B546E8E002FC5854651BE31802F96D
DDAD29B8B1215191E7EB5AAEE0219338	F5FA42A5B421705E4803DA93C4F7E099	DF2AD7F766E2EEFAF0FD1FB5C6883AB4
3F8A5EA1756DDF4A6B6F2645B4911486	A869B96BCDF1D474C0714763AA34A8C9	1C6EA2DA6ECED5C5C761BCA9CA4C5308
30DF96D87EEC8CA77A135ECCAB1AD25E	3EA0F90DE57187FC7E1AC45AE44D16C6	A640A29E706AF38557B86619EAF45E7A
7DD8E0E1906C1754E11E901927CCABBD	F7DE638B76C3958AA3413A9785A19900	F88885670C3D55EBA52096A65310DACA
DAC51C3D23B163601305AF99DF129689	3F8C9CDAACBB533AE94F47456819FA0E	B85E7BB83667097F15D8A3DEAAA1B198
D77EC92400AE0D9FA57DEF4DD8CFA4D4	209920C169512D3EB4A1ED7CAD17D033	A5F6F149B468683318DC178F4208E237
09369288E36D7AFFEE94EA81998FA316	B2F57BD01BAAF7AF01EF442910CEBBA0	04841B82A9D81E44CB4F2D98CFE7C374
EEBE188553223432891919 13F6D769EB	C0766829AA4D2E1A5D97213A4E4A654E	A81686CEFDEFFCE82B8DBF100E1395F1
C00132DA154BDEE361EDEE727226D0F5	FC9993EA7A4E761B6CB79ABE2BD3CDE1	9952073595776A3D7A8101664A56AB96
6580BE22A0566352B9622777BFCB7164	4D556B338FAA020979A740B4C3AEE28C	A076DA72A8C8E2137F05FE3FA59870EB
7352C61297D6B04E874EDAD12480F78E	8ED896B9A622FF24559A3429E5888E0A	121378A6DE0A13DDB295106E912A4E14
F658C0D52B3EEF71DDE6C284E7E1B337	8CF1F45323EC5AB449451E7A9476CFDC	65A925E578098658FADA30E9FB67B5E4
E1253D04A17AB8E47F4A5916B9BF9D23	D1718E9BD91257D2169C81197D508A67	5B8E5202EC6769F2389605D33DC245B2
8922A9A23BE960FFE9707A0B3F4D75BD	E4A691D60266784968DF971D6BF473AF	EA71F746BD17D1B05450329818572F2E
EAE97F465015E49A14F3B23403ACFA11	B3B64F1925F759A2E145190333D1D6D2	DD8C315D2CA61870CBCF9D56ED7474E2
13A757022817C0514A5C142FE9BF143A	ED4C2EBC14B85F46A9A75F159DF8BEB3	F346A1E62FED476F472560C6DDE0CADC
5132F0FCB3F8DCAA501C620575D33FEE	CDBC0441C10DB5ABA43120E63A048425	CBBCB9E06F9FC92C533B2F2A5284BA22
39953BF6383A00D29BEB377568E3DE7A	DC1665266A0198728861AC99ED368928	79DCFDA2700E06F8EAA640BA9B827810
67887932934DFF086153CA905E7DE9EE	706BBC770C62D41DD799721ABD1868AB	17CF5474D5A8B4E735E69E017CEC2F37
DCD1072719692871126E4159D80EFDA8	B2205D8CBDDFE49D7C5F0F95D506718F	7034FBF641CEB257FC109A6819D19DA0
C6741E3D08C0FFD4617B94E654DD89F1	901F30DB86EEB1666F5A8CAE1C7BD08B	6E6D052B5ABC015C779EA3500FA11A28
8CC74931E64061491652CC169C8BAAB3	C731140FAA7690918BABF17BECB7938D	0370390E48A7F26AA62188A79E612DC3
4157D99E46A3E45E6130A95645410DAC	8C605DFAA0EC88CDB7D12F7250C9F53A	
E34C4FC7488C4DFEF0EA475A17AF2C7B	68F252CD36F2798A2182F6406A31A5A2	
59F8BDDA3F56D8026FAB6E3130F5D843	BD7CB0D124DFDE784CD5B9EF288C304E	
FAB79682C8EAE556F11ECF6DAD7121BA	3D2BC95A85EF539A68DAC84542A1AE7A	

Appendix VIII: Rogue certificates

Of the 531 encountered rogue certificates, 140 unique distinguished names and 53 unique common names were identified.

Common Name	Number issued
..com	1
..org	1
*.10million.org	2
*.android.com	1
*.aol.com	1
*.azadegi.com	2
*.balatarin.com	3
*.comodo.com	3
*.digicert.com	2
*.globalsign.com	7
*.google.com	26
*.JanamFadayeRahbar.com	1
*.logmein.com	1
*.microsoft.com	3
*.mossad.gov.il	2
*.mozilla.org	1
*.RamzShekaneBozorg.com	1
*.SahebeDonyayeDigital.com	1
*.skype.com	22
*.startssl.com	1
*.thawte.com	6
*.torproject.org	14
*.walla.co.il	2
*.windowsupdate.com	3
*.wordpress.com	14
addons.mozilla.org	17
azadegi.com	16
Comodo Root CA	20
CyberTrust Root CA	20
DigiCert Root CA	21
Equifax Root CA	40
friends.walla.co.il	8
GlobalSign Root CA	20
login.live.com	17
login.yahoo.com	19
my.screenname.aol.com	1
secure.logmein.com	17
Thawte Root CA	45
twitter.com	18
VeriSign Root CA	21
wordpress.com	12
www.10million.org	8
www.balatarin.com	16
www.cia.gov	25
www.cybertrust.com	1
www.Equifax.com	1
www.facebook.com	14
www.globalsign.com	1
www.google.com	12
www.hamdami.com	1
www.mossad.gov.il	5
www.sis.gov.uk	10
www.update.microsoft.com	4

Appendix IX: Suspicious files

Suspicious files were encountered on the following servers:

Network	Server
Secure-net	Qualified-CA
	Taxi-CA
	Relation-CA
	Public-CA
	Root-CA
	BAPI-db
	CCV-CA
Office-net	Office-file server
	BAPI-db
DMZ-ext-net	Main-web
	Docproof2

Temporary Internet files

A non-exhaustive list of suspicious files found in the temporary Internet files directory:

Server	File name	User	Size	Create Date	Create time
BAPI-db	kir[1].txt	MSSQLusr	9	17-Jun-2011	16:15:49
BAPI-db	libeay32[1].dll	MSSQLusr	1017344	17-Jun-2011	16:18:44
BAPI-db	PwDump7[1].exe	MSSQLusr	77824	17-Jun-2011	16:19:21
BAPI-db	PwDump[1].exe	MSSQLusr	393216	17-Jun-2011	18:56:01
BAPI-db	7za[1].exe	MSSQLusr	264704	17-Jun-2011	19:33:55
BAPI-db	mswinsck[1].ocx	MSSQLusr	127808	17-Jun-2011	19:41:31
BAPI-db	base64[1].exe	MSSQLusr	45056	18-Jun-2011	0:34:05
BAPI-db	test[1].zip	MSSQLusr	2666	18-Jun-2011	5:11:53
BAPI-db	mstsc[1].exe	MSSQLusr	407552	18-Jun-2011	14:46:46
BAPI-db	mstscax[1].dll	MSSQLusr	655360	18-Jun-2011	14:47:28
BAPI-db	clxtshar[1].dll	MSSQLusr	69632	18-Jun-2011	14:47:51
BAPI-db	tclient[1].dll	MSSQLusr	68096	18-Jun-2011	14:48:29
BAPI-db	test2[1].zip	MSSQLusr	2666	18-Jun-2011	14:53:55
BAPI-db	nc[1].exe	MSSQLusr	65028	20-Jun-2011	10:34:15
BAPI-db	demineur[1].dll	MSSQLusr	151552	20-Jun-2011	11:14:09
BAPI-db	klock[1].dll	MSSQLusr	153600	20-Jun-2011	11:14:27
BAPI-db	mimikatz[1].exe	MSSQLusr	368128	20-Jun-2011	11:15:40
BAPI-db	sekurlsa[1].dll	MSSQLusr	200704	20-Jun-2011	11:15:51
BAPI-db	cachedump[1].exe	MSSQLusr	45056	21-Jun-2011	12:50:00
BAPI-db	PwDump[1].exe	MSSQLusr	393216	21-Jun-2011	13:09:47
BAPI-db	mswinsck[2].ocx	MSSQLusr	127808	21-Jun-2011	13:46:33
BAPI-db	uploader[2].exe	MSSQLusr	28672	21-Jun-2011	14:18:15
BAPI-db	uploader[1].exe	MSSQLusr	28672	21-Jun-2011	15:07:23
BAPI-db	up3[1].exe	MSSQLusr	28672	21-Jun-2011	15:21:03
BAPI-db	sfk[1].exe	MSSQLusr	1155072	21-Jun-2011	19:53:15
BAPI-db	ReadF[1].exe	MSSQLusr	8192	22-Jun-2011	8:41:06
BAPI-db	Read1[1].exe	MSSQLusr	9728	22-Jun-2011	10:26:02
BAPI-db	Read2[1].exe	MSSQLusr	9728	22-Jun-2011	10:46:20
BAPI-db	Read3[1].exe	MSSQLusr	9728	22-Jun-2011	12:17:29
BAPI-db	Read4[1].exe	MSSQLusr	9728	22-Jun-2011	12:20:09
BAPI-db	Read5[1].exe	MSSQLusr	10240	22-Jun-2011	12:34:28
BAPI-db	PortQry[1].exe	MSSQLusr	143360	29-Jun-2011	9:44:53
BAPI-db	troj172[1].exe	MSSQLusr	61440	29-Jun-2011	22:13:34
BAPI-db	troj172[1].exe	MSSQLusr	61440	29-Jun-2011	22:13:34
BAPI-db	troj134[1].exe	MSSQLusr	61440	29-Jun-2011	22:18:17
BAPI-db	troj134[1].exe	MSSQLusr	61440	29-Jun-2011	22:18:17
BAPI-db	134[1].exe	MSSQLusr	37888	29-Jun-2011	22:30:33
BAPI-db	RunAs[1].exe	MSSQLusr	24576	29-Jun-2011	22:52:25
BAPI-db	RDP[1].exe	MSSQLusr	553472	29-Jun-2011	23:01:49
BAPI-db	13480[1].exe	MSSQLusr	37888	29-Jun-2011	23:19:32

Server	File name	User	Size	Create Date	Create time
BAPI-db	Troj25[1].exe	MSSQLusr	61440	1-Jul-2011	13:45:18
BAPI-db	psexec[1].exe	MSSQLusr	381816	1-Jul-2011	19:12:25
BAPI-db	mimi[1].zip	MSSQLusr	477545	1-Jul-2011	22:15:25
Taxi-CA	mimi[1].zip	Administrator	477545	1-Jul-2011	22:15:49
Qualified-CA	172.18.20[1].htm	Administrator.DNPRODUCTIE	4867	1-Jul-2011	23:20:51
Taxi-CA	winsvr130[1].htm	Administrator.DNPRODUCTIE	476	2-Jul-2011	0:53:44
Root-CA	corner[2].gif	administrator.DNPRODUCTIE	3196	2-Jul-2011	1:00:58
Root-CA	enrollbg[4].gif	administrator.DNPRODUCTIE	558	2-Jul-2011	1:00:58
Root-CA	icontrol[1].vbs	administrator.DNPRODUCTIE	35007	2-Jul-2011	1:08:45
Root-CA	up[1]	administrator.DNPRODUCTIE	3415	2-Jul-2011	1:24:31
Root-CA	favicon[1].ico	administrator.DNPRODUCTIE	3878	2-Jul-2011	2:40:06
BAPI-db	ldap[1].msi	MSSQLusr	14297088	2-Jul-2011	18:41:27
Relation-CA	get[1].htm	Administrator.DNPRODUCTIE	323	2-Jul-2011	20:57:35
Relation-CA	banner[1].htm	Administrator.DNPRODUCTIE	6143	2-Jul-2011	21:55:49
Relation-CA	172.18.20[1].htm	Administrator.DNPRODUCTIE	5291	2-Jul-2011	21:59:01
Relation-CA	172.18.20[1]	Administrator.DNPRODUCTIE	5692	2-Jul-2011	21:59:34
BAPI-db	direct[1].exe	MSSQLusr	37888	3-Jul-2011	23:40:23
BAPI-db	direct[1].zip	MSSQLusr	19702	4-Jul-2011	1:06:00
Taxi-CA	direct[1].zip	Administrator.DNPRODUCTIE	19702	4-Jul-2011	4:18:39

Recent files

A non-exhaustive list of suspicious files and other unspecified pages found in the recent files directory:

Server	File name	User	Create date	Create time
Main-web	Nieuw - Tekstdocument.txt.lnk	Administrator	20-Jun-2011	2:15:43
BAPI-db	pki.zip.lnk	Administrator	1-Jul-2011	14:58:07
BAPI-db	DARPI.lnk	Administrator	1-Jul-2011	16:13:07
Taxi-CA	Desktop.ini	Administrator	1-Jul-2011	22:32:39
Taxi-CA	Recent	Administrator	1-Jul-2011	22:32:39
Qualified-CA	certs.lnk	Administrator.DNPRODUCTIE	1-Jul-2011	23:29:57
Qualified-CA	ssl.crt.lnk	Administrator.DNPRODUCTIE	1-Jul-2011	23:29:57
Qualified-CA	root.crt.lnk	Administrator.DNPRODUCTIE	1-Jul-2011	23:31:45
Qualified-CA	cas.crt.lnk	Administrator.DNPRODUCTIE	1-Jul-2011	23:32:06
Qualified-CA	a.crt.lnk	Administrator.DNPRODUCTIE	1-Jul-2011	23:35:35
Qualified-CA	qualifiedData.zip.lnk	Administrator.DNPRODUCTIE	2-Jul-2011	0:09:57
Qualified-CA	qualifiedData.zip.lnk	Administrator.DNPRODUCTIE	2-Jul-2011	0:09:57
Root-CA	MinIenM Organisatie CA - G2.p7b.lnk	administrator.DNPRODUCTIE	2-Jul-2011	1:12:54
Root-CA	httpd.conf.lnk	administrator.DNPRODUCTIE	2-Jul-2011	2:13:05
Root-CA	dist.lnk	administrator.DNPRODUCTIE	2-Jul-2011	2:27:17
Root-CA	schema.conf.lnk	administrator.DNPRODUCTIE	2-Jul-2011	2:27:49
Root-CA	iXudad.conf.lnk	administrator.DNPRODUCTIE	2-Jul-2011	2:29:19
Root-CA	xudad.oc.conf.lnk	administrator.DNPRODUCTIE	2-Jul-2011	2:30:43
Root-CA	origrsa.zip.lnk	administrator.DNPRODUCTIE	2-Jul-2011	2:40:26
Root-CA	CertiID Enterprise Certificate Authority.crt.lnk	administrator.DNPRODUCTIE	2-Jul-2011	2:48:45
Root-CA	muh.lnk	administrator.DNPRODUCTIE	2-Jul-2011	2:48:45
Root-CA	USPP-Perso Certificate ST4000 260-160-364.crt.lnk	administrator.DNPRODUCTIE	2-Jul-2011	2:50:20
Root-CA	certs.lnk	administrator.DNPRODUCTIE	2-Jul-2011	2:50:20
Relation-CA	dbpub.zip.lnk	Administrator.DNPRODUCTIE	2-Jul-2011	20:35:41
Qualified-CA	m.zip.lnk	Administrator.DNPRODUCTIE	2-Jul-2011	22:15:28
Public-CA	Desktop.ini	Admin1[48]	4-Jul-2011	0:05:17

[48] The real username is replaced by a pseudonym to protect the privacy of the personnel of DigiNotar.

Other local settings files

A non-exhaustive list of other suspicious files found in the local settings directory:

Server	Full path	Size	Create date	Create time
BAPI-db	Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Credentials\S-1-5-21-2196791791-1123517030-1950105499-500\	256	30-Jan-2006	11:44:01
Public-CA	Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\$I30	4096	20-Jul-2010	12:55:21
Public-CA	Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\	56	20-Jul-2010	12:55:21
Public-CA	Documents and Settings\Admin1\Local Settings\Application Data\	472	17-Jun-2011	14:05:22
BAPI-db	Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Credentials\S-1-5-21-2196791791-1123517030-1950105499-500\Credentials	346	1-Jul-2011	14:46:46
Taxi-CA	Documents and Settings\Administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011061320110620\index.dat	49152	2-Jul-2011	0:53:44
Taxi-CA	Documents and Settings\Administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011061320110620\	152	2-Jul-2011	0:53:44
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011061320110620\index.dat	32768	2-Jul-2011	1:00:58
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011070220110703\index.dat	32768	2-Jul-2011	1:00:58
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011061320110620\	152	2-Jul-2011	1:00:58
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011070220110703\	152	2-Jul-2011	1:00:58
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\Dr Watson\	264	2-Jul-2011	2:18:56
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\Dr Watson\	264	2-Jul-2011	2:18:56
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\Dr Watson\drwtsn32.log	203258	2-Jul-2011	2:18:56
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\Dr Watson\drwtsn32.log	203258	2-Jul-2011	2:18:56
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\Dr Watson\user.dmp	90852	2-Jul-2011	2:18:56
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\Dr Watson\user.dmp	90852	2-Jul-2011	2:18:56
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\Internet Explorer\Recovery\Last Active\{51503BD7-A456-11E0-941C-D48564505644}.dat	70144	2-Jul-2011	2:52:26
Relation-CA	Documents and Settings\Administrator.DNPRODUCTIE\Local Settings\Application Data\Softerra\LDAP Browser 4\UserImages.bmp	9014	2-Jul-2011	21:46:30
Public-CA	Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\Terminal Server Client\	144	4-Jul-2011	4:11:29
Taxi-CA	Documents and Settings\Administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011062720110704\index.dat	32768	4-Jul-2011	4:19:23
Taxi-CA	Documents and Settings\Administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011070420110705\index.dat	32768	4-Jul-2011	4:19:23
Taxi-CA	Documents and Settings\Administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011062720110704\	152	4-Jul-2011	4:19:23
Taxi-CA	Documents and Settings\Administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011070420110705\	152	4-Jul-2011	4:19:23

Other files

A non-exhaustive list of remaining suspicious files:

Server	Full path	Size
BAPI-db	WINDOWS\system32\drivers\etc\hosts	792
BAPI-db	Program Files\Symantec AntiVirus\savrt.dat	3220
BAPI-db	Program Files\Symantec AntiVirus\SRTSEXCL.DAT	76
BAPI-db	WINDOWS\system32\config\default	262144
BAPI-db	WINDOWS\system32\config\SAM	262144
BAPI-db	WINDOWS\system32\config\SECURITY	262144
BAPI-db	WINDOWS\Tasks\SchedLgU.Txt	10364
BAPI-db	WINDOWS\system32\ipconfig.exe	63488
BAPI-db	Program Files\Symantec AntiVirus\$I30	12288
BAPI-db	Program Files\Symantec AntiVirus\	288
BAPI-db	Documents and Settings\All Users\Application Data\Symantec\Common Client\settings.dat	20204
BAPI-db	Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBConfig.log	3676
BAPI-db	Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBDebug.log	64
BAPI-db	Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBDetect.log	64
BAPI-db	Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBNotify.log	64
BAPI-db	Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBRefr.log	64
BAPI-db	Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBSetCfg.log	64
BAPI-db	Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBSetDev.log	64
BAPI-db	Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBSetLoc.log	2108
BAPI-db	Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBSetUsr.log	64
BAPI-db	Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBStHash.log	64
BAPI-db	Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBStMSI.log	7576
BAPI-db	Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBValid.log	64
BAPI-db	Program Files\Common Files\Symantec Shared\SPBBC\LOGS\SPPolicy.log	64
BAPI-db	Program Files\Common Files\Symantec Shared\SPBBC\LOGS\SPStart.log	64
BAPI-db	Program Files\Common Files\Symantec Shared\SPBBC\LOGS\SPStop.log	64
BAPI-db	Partition 5\Log [NTFS]\[root]\MSSQL\Log\finance01_Log.LDF	1048576
BAPI-db	Partition 5\Log [NTFS]\[root]\MSSQL\Log\Applog01_Log.LDF	2359296
BAPI-db	Documents and Settings\Admin3\Bureaublad\WebRAOBeheer02\Web.config	7415
Main-web	Partition 3\Data [NTFS]\[root]\Websites\Bapiviewer\BapiViewer\web.config	5471
Public-CA	WINDOWS\system32\wbem\Logs\mofcomp.log	14664
BAPI-db	Partition 5\Log [NTFS]\[root]\MSSQL\Log\wietse_log.ldf	3145728
Docproof2	Partition 3\Data [NTFS]\[root]\Websites\Docproof\Docproof01\js\b.aspx	72689
Docproof2	Partition 3\Data [NTFS]\[root]\Websites\Docproof\Docproof01\RunAs.exe	24576
BAPI-db	Documents and Settings\All Users\Application Data\Symantec\Symantec AntiVirus Corporate Edition\7.5\Logs\06172011.Log	262
BAPI-db	Documents and Settings\All Users\Application Data\Symantec\Symantec AntiVirus Corporate Edition\7.5\Logs\06172011.Log	262
BAPI-db	WINDOWS\system32\archive.zip	198024801
BAPI-db	WINDOWS\system32\mswinsck.ocx	127808
Main-web	Partition 3\Data [NTFS]\[orphan]\demineur.dll	151552
Main-web	Partition 3\Data [NTFS]\[orphan]\klock.dll	153600
Main-web	Partition 3\Data [NTFS]\[orphan]\mimikatz.exe	368128
Main-web	Partition 3\Data [NTFS]\[orphan]\sekurlsa.dll	200704
Main-web	Documents and Settings\Administrator\Recent\Nieuw - Tekstdocument.txt.lnk	872
BAPI-db	WINDOWS\system32\BAPI-DB_MS IIS DCOM Server.pvk	332
BAPI-db	WINDOWS\system32\BAPI-DB_SELFSIGN_DEFAULT_CONTAINER.pvk	620
BAPI-db	WINDOWS\system32\BAPI-DB_Microsoft Internet Information Server.pvk	332
BAPI-db	WINDOWS\system32\BAPI-DB_tmpHydraLSKeyContainer.pvk	332
BAPI-db	WINDOWS\system32\BAPI-DB_0_BAPI-db.diginotar.nl.pfx	1737
BAPI-db	WINDOWS\system32\Documents.7z	1015873568
BAPI-db	WINDOWS\system32\bsqweyec.dll	65536
BAPI-db	WINDOWS\system32\xjegjvhr.exe	53760
BAPI-db	WINDOWS\system32\uploader\	48
Docproof2	Partition 3\Data [NTFS]\[root]\Websites\Docproof\Docproof01\demo\94.exe	37888
Docproof2	Partition 3\Data [NTFS]\[root]\Websites\Docproof\Docproof01\Troj65.exe	61440
Docproof2	Partition 3\Data [NTFS]\[root]\Websites\Docproof\Docproof01\demo\PwDump.exe	393216
Docproof2	Partition 3\Data [NTFS]\[root]\Websites\Docproof\Docproof01\demo\cachedump.exe	45056
Docproof2	Partition 3\Data [NTFS]\[root]\Websites\Docproof\Docproof01\demo\test.txt	127
BAPI-db	Documents and Settings\Administrator\Desktop\rdp.exe	553472

Server	Full path	Size
BAPI-db	Documents and Settings\Administrator\Desktop\rdp.exe	553472
BAPI-db	Documents and Settings\Administrator\Desktop\Default.rdp	2458
Office-file	Documents and Settings\Administrator\Cookies\administrator@10.10.20[1].txt	141
Office-file	Documents and Settings\Administrator\Desktop\sfk.exe\	1155072
Office-file	WINDOWS\system32\sfk.exe\	1155072
BAPI-db	Documents and Settings\Administrator\Desktop\13480.exe	37888
BAPI-db	Documents and Settings\Administrator\Cookies\administrator@10.10.20[1].txt	141
BAPI-db	Documents and Settings\Administrator\Recent\pki.zip.lnk	424
BAPI-db	Documents and Settings\Administrator\Recent\DARPI.lnk	941
Taxi-CA	Documents and Settings\Administrator\Cookies\administrator@10.10.20[1].txt	139
Taxi-CA	WINDOWS\system32\Microsoft\Crypto\	136
Taxi-CA	WINDOWS\system32\Microsoft\Crypto\RSA\MachineKeys\	48
Taxi-CA	WINDOWS\system32\Microsoft\Crypto\RSA\	256
Taxi-CA	Documents and Settings\Administrator\Recent\Desktop.ini	150
Taxi-CA	Documents and Settings\Administrator\Recent\	152
Qualified-CA	Documents and Settings\Administrator.DNPRODUCTIE\Recent\certs.lnk	598
Qualified-CA	Documents and Settings\Administrator.DNPRODUCTIE\Recent\ssl.crt.lnk	720
Qualified-CA	Documents and Settings\Administrator.DNPRODUCTIE\Recent\root.crt.lnk	725
Qualified-CA	Documents and Settings\Administrator.DNPRODUCTIE\Recent\cas.crt.lnk	720
Qualified-CA	Documents and Settings\Administrator.DNPRODUCTIE\Recent\a.crt.lnk	736
Qualified-CA	Documents and Settings\Administrator.DNPRODUCTIE\Cookies\administrator@10.10.20[1].txt	141
Qualified-CA	Documents and Settings\Administrator.DNPRODUCTIE\Recent\qualifiedData.zip.lnk	448
Qualified-CA	Documents and Settings\Administrator.DNPRODUCTIE\Recent\qualifiedData.zip.lnk	448
Qualified-CA	WINDOWS\system32\Microsoft\Protect\S-1-5-18\User\457718b9-fa34-41e3-8d9d-3ecf7391929c	388
Qualified-CA	WINDOWS\system32\nfmodexp.dll	742680
Qualified-CA	WINDOWS\system32\nfmodexp.dll	742680
Qualified-CA	WINDOWS\system32\ncspmess.dll	357656
Qualified-CA	WINDOWS\system32\ncspmess.dll	357656
Qualified-CA	WINDOWS\system32\ncsp.dll	1041688
Qualified-CA	WINDOWS\system32\ncsp.dll	1041688
Qualified-CA	WINDOWS\system32\ncspdd.dll	1041688
Qualified-CA	WINDOWS\system32\ncspdd.dll	1041688
Qualified-CA	WINDOWS\system32\ncspsigdd.dll	1033496
Qualified-CA	WINDOWS\system32\ncspsigdd.dll	1033496
Root-CA	WINDOWS\SchCache\DNproductie.sch	370536
Root-CA	WINDOWS\SchCache\	272
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Application Data\Microsoft\Crypto\RSA\S-1-5-21-4190788878-266275749-1156481715-500\9cb4f8bdfaa302f85333ef07fa3fb192_60643e52-42b0-4d55-aea2-38a5b64b11ec	2073
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Application Data\Microsoft\SystemCertificates\Request\Certificates\40F1C4C24E802122FBC4DB5061CADF1DDCEB33DD	858
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Application Data\Microsoft\SystemCertificates\Request\Certificates\	320
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Application Data\Microsoft\SystemCertificates\Request\CRLs\	48
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Application Data\Microsoft\SystemCertificates\Request\CTLs\	48
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Application Data\Microsoft\SystemCertificates\Request\	456
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Recent\MinIenM Organisatie CA - G2.p7b.lnk	560
Root-CA	Documents and Settings\All Users\Application Data\nCipher\Log Files\keysafe.log	566
Root-CA	Documents and Settings\All Users\Application Data\nCipher\Log Files\cmdadp.log	388
Root-CA	Documents and Settings\All Users\Application Data\nCipher\Log Files\cmdadp-debug.log	0
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Recent\httpd.conf.lnk	696
Root-CA	WINDOWS\PCHealth\ErrorRep\	256
Root-CA	WINDOWS\PCHealth\ErrorRep\	256
Root-CA	WINDOWS\PCHealth\ErrorRep\UserDumps\	576
Root-CA	WINDOWS\PCHealth\ErrorRep\UserDumps\	576
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Recent\dist.lnk	531
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Recent\schema.conf.lnk	677

Server	Full path	Size
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Recent\iXudad.conf.lnk	677
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Recent\xudad.oc.conf.lnk	683
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Cookies\administrator@10.10.20[1].txt	140
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Cookies\administrator@10.10.20[1].txt	140
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Recent\origrsa.zip.lnk	416
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Recent\CertiID Enterprise Certificate Authority.crt.lnk	804
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\NetHood\d$ on CCV-CA\	256
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\NetHood\d$ on CCV-CA\	256
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\NetHood\d$ on CCV-CA\Desktop.ini	75
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\NetHood\d$ on CCV-CA\Desktop.ini	75
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Recent\muh.lnk	571
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\NetHood\d$ on CCV-CA\target.lnk	463
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\NetHood\d$ on CCV-CA\target.lnk	463
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Recent\USPP-Perso Certificate ST4000 260-160-364.crt.lnk	879
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Recent\certs.lnk	631
CCV-CA	Documents and Settings\administrator.DNPRODUCTIE\Desktop\Qualified-CA.txt	461
CCV-CA	Documents and Settings\administrator.DNPRODUCTIE\Desktop\Root-CA.txt	272
CCV-CA	Documents and Settings\administrator.DNPRODUCTIE\Desktop\kcavkfsc.dll	65536
CCV-CA	Documents and Settings\administrator.DNPRODUCTIE\Desktop\njnypgqa.exe	53760
CCV-CA	Documents and Settings\administrator.DNPRODUCTIE\Desktop\Public-CA.txt	458
Relation-CA	Partition 2\Data [NTFS]\[root]\Progs\rsa_cm_68\Web server\enroll-server\ca\get.xuda	254
Relation-CA	Documents and Settings\Administrator.DNPRODUCTIE\Desktop\dbpub.zip	59545925
Relation-CA	Documents and Settings\Admin2\Desktop\administrator@10.10.20[1].txt	141
Relation-CA	Documents and Settings\Administrator.DNPRODUCTIE\Recent\dbpub.zip.lnk	404
Qualified-CA	Documents and Settings\Administrator.DNPRODUCTIE\Recent\m.zip.lnk	380
Public-CA	Partition 5\NONAME [NTFS]\[orphan]\add-pkcs10-request[16].htm	96617
Public-CA	WINDOWS\system\osvchost.exe	36864
Public-CA	Documents and Settings\Admin1\Recent\Desktop.ini	150
Public-CA	WINDOWS\system32\wbem\AutoRecover\C8463ECBE33BC240263A0B094E46D510.mof	2826402
Public-CA	WINDOWS\system32\wbem\AutoRecover\23BDE61F1F4FACE17E9B0C01F2A1FD9B.mof	36574
Public-CA	Partition 5\NONAME [NTFS]\[orphan]\Settings[2].htm	3097
Public-CA	Partition 5\NONAME [NTFS]\[orphan]\direct83[1].exe	37888
Public-CA	WINDOWS\system32\csrsss.exe\	37888
Public-CA	WINDOWS\system32\csrsss.exe\Zone.Identifier	26
Public-CA	Partition 5\NONAME [NTFS]\[orphan]\139[1].exe	37888
Public-CA	WINDOWS\system32\svhost.exe\	37888
Public-CA	WINDOWS\system32\svhost.exe\Zone.Identifier	26
Taxi-CA	WINDOWS\system\svchost.exe\	19702
Taxi-CA	WINDOWS\system\svchost.exe\Zone.Identifier	26
Relation-CA	Documents and Settings\Administrator.DNPRODUCTIE\My Documents\Default.rdp	1214
Public-CA	Partition 2\NONAME [NTFS]\[orphan]\x-select-settings.xuda	28875