Interim Report

September 5, 2011

DigiNotar Certificate Authority breach
"Operation Black Tulip"

Classification **PUBLIC**

Customer DigiNotar B.V.

Subject: Investigation DigiNotar Certificate Authority Environment

Date 5 September 2011
Version 1.0
Author J.R. Prins (CEO Fox-IT)
Business Unit Cybercrime
Pages 13

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

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

1 Introduction

1.1 Background

The company DigiNotar B.V. provides digital certificate services; it hosts a number of Certificate Authorities (CA's). Certificates issued include default SSL certificates, Qualified Certificates and 'PKIoverheid' (Government accredited) certificates.

On the evening of Monday August 29th it became public knowledge that a rogue *.google.com certificate was presented to a number of Internet users in Iran. This false certificate had been issued by DigiNotar B.V. and was revoked[1] that same evening.

On the morning of the following Tuesday, Fox-IT was contacted and asked to investigate the breach and report its findings before the end of the week.

Fox-IT assembled a team and started the investigation immediately. The investigation team includes forensic IT experts, cybercrime investigators, malware analysts and a security expert with PKI experience. The team was headed by CEO J.R. Prins directly.

It was communicated and understood from the outset, that Fox-IT wouldn't be able to complete an in-depth investigation of the incident within this limited timeframe. This is due to the complexity of the PKI environment and the uncommon nature of the breach.

Rather, due to the urgency of this matter, Fox-IT agreed to prepare an interim report at the end of the week with its preliminary findings, which would be published.

1.2 Investigation questions

The investigation predominately focused on following questions:

1. How did the perpetrators access the network?

2. What is the scope and status of the breach?
   - *Have other DigiNotar CA environments been breached?*
   - *Do we still see hacker activity on the network of DigiNotar?*
   - *Are rogue certificates actively being used by hackers?*

3. Can we discover anything about the impact of the incident?
   - *What certificates were issued without knowledge of DigiNotar?*
   - *What other (rogue) certificates might have been generated?*
   - *How many rogue connections were made using rogue certificates?*
   - *What was the nature of these connections?*

In order to address these questions we (basically) (i) implemented specialized monitoring to be able to detect, analyse and follow up on active misuse, and (ii) analysed digital traces on hard disks, and in databases and log files to investigate the origin and impact of the breach.

[1] Revoked: A certificate is irreversibly revoked if, for example, it is discovered that the certificate authority (CA) had improperly issued a certificate, or if a private-key is thought to have been compromised. Certificates may also be revoked for failure of the identified entity to adhere to policy requirements such as publication of false documents, mis-representation of software behavior, or violation of any other policy specified by the CA operator or its customer. The most common reason for revocation is the user no longer being in sole possession of the private key (*e.g.*, the token containing the private key has been lost or stolen).

1.3 This report

The goal of this report is to share relevant information with DigiNotar stakeholders (such as the Dutch Government and the Internet community), based on which they can make their own risk analysis. Because this is a public report, some investigation results and details cannot be included for privacy and/ or security reasons.

Since the investigation has been more of a fact finding mission thus far, we will not draw any conclusions with regards to the network-setup and the security management system. In this report we will not give any advice to improve the technical infrastructure for the long term. Our role is to investigate the incident and give a summary of our findings until now. We leave it to the reader in general and other responsible parties in the PKI- and internet community to draw conclusions, based on these findings. We make a general reservation, as our investigations are still on going.

2 Investigations

2.1 Prior investigations

Some investigations were conducted before we started.

Fox-IT was given access to a report produced by another IT-security firm which performs the regular penetration testing and auditing for DigiNotar. The main conclusions from this report dated July 27th were:

> A number of servers were compromised. The hackers have obtained administrative rights to the outside webservers, the CA server "Relaties-CA" and also to "Public-CA". Traces of hacker activity started on June 17th and ended on July 22nd.

Furthermore, staff from DigiNotar and the parent company Vasco performed their own security investigation. E-mail communication and memos with further information were handed over to us.

This information gave us a rough overview of what happened:

- The signing of 128 rogue certificates was detected on July 19th during the daily routine security check. These certificates were revoked immediately;
- During analysis on July 20th the generation of another 129 certificates was detected. These were also revoked on July 21th;
- Various security measures on infrastructure, system monitoring and OCSP validation have been taken immediately to prevent further attacks.
- More fraudulent issued certificates were discovered during the investigation and 75 more certificates were revoked on July 27th.
- On July 29th a *.google.com certificate issued was discovered that was not revoked before. This certificate was revoked on July 29th.
- DigiNotar found evidence on July 28th that rogue certificates were verified by internet addresses originating from Iran.

On August 30th Fox-IT was asked investigate the incident and recommend and implement new security measures. Fox-IT installed a specialized incident response network sensor to assist in the investigation. Furthermore we created images of several other servers.

2.2 Monitoring

The rogue certificate found by Google was issued by the DigiNotar Public CA 2025. The serial number of the certificate was, however, not found in the CA system's records. This leads to the conclusion that it is unknown how many certificates were issued without any record present. In order to identify these unknown certificates and to prevent them from being used by victims, the OCSP responder[2] requests were monitored.

Current browsers perform an OCSP check as soon as the browser connects to an SSL protected website through the https-protocol[3]. The serial number of the certificate presented by the website a user visits is send to the issuing CA OCSP-responder. The OCSP-responder can only answer either with 'good', 'revoked' or 'unknown'. If a certificate serial number is presented to the OCSP-responder and no record of this serial is found, the normal OCSP-responder answer would be 'good'[4]. The OCSP-responder answer 'revoked' is only returned when the serial is revoked by the CA. In order to prevent misuse of the unknown issued serials the OCSP-responder of DigiNotar has been set to answer 'revoked' when presented any unknown certificate serial it has authority over. This was done on September 1st.

The incident response sensor immediately informs if a serial number of a known fraudulently issued certificate is being misused. Also, all unknown serial number requests can be analysed and used in the investigation. All large number of requests to a single serial number is suspicious and will be detected.

---

[2] The **Online Certificate Status Protocol** (**OCSP**) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate.
[3] Other applications using certificates can also use the OCSP verification method.
[4] According to the RFC2560

Note that advanced methods for misusing the rogue certificates are possible by which a thorough attacker can circumvent our detection method.

The incident response sensor logged all network traffic since August 30th. Current analyses still show hacking attempts on the web server originating from Iran. During monitoring, we also saw unusual traffic after the company F-Secure announced its findings of a possible earlier breach of the website.[5] We haven't investigated this breach yet in detail. In August, DigiNotar installed a new web server. It's fair to assume these hacker traces where copied from the previous web server install.

2.3 CA servers investigation

DigiNotar hosts several CA services on different servers. Earlier reports indicated two of these servers where compromised and misused by the attacker(s). It was essential to verify the status of the other CA systems and investigate if they were compromised or misused. Forensic disk images were made of all the CA servers for investigation.

Because of security implications, the details of these results are not shared in this public report. More generally, we found traces of hacker activity with administrator rights on the Qualified and PKIoverheid CA server as well as on other CA servers. Furthermore, we can share that on September 3rd more rogue certificates were discovered. The list of certificates is in the Annex 5.1.

The log files on the Qualified & PKI Overheid CA server do not show traces of deleted entries. These traces are present on other CA servers, where rogue certificates were produced. During further investigation however, we encountered several serial numbers of certificates that cannot be related to trusted certificates. Two of these were found on the Qualified & PKI Overheid CA server. It might be possible that these serial numbers have been temporarily generated by the CA software without being used. Alternatively, these serials were generated as a result of a bug of the software. However, we cannot rule out the possibility that these serial numbers relate to rogue certificates. Further investigation needs to be done to confirm or contradict this. The list of serials is in the Annex 5.2; this list has been communicated with the web browser vendors.

2.4 Firewall investigation

The firewall log files have not been analysed yet.

2.5 Malicious software analyses

A number of malicious/hacker software tools was found. These vary from commonly used tools such a the famous Cain & Abel tool[6] to tailor made software.

Specifically developed software probably enabled the hackers to upload the generated certificates to a dropbox. Both the IP-addresses of an internal DigiNotar server and the IP-address of the dropbox were hardcoded in the software. Possibilities are being explored to investigate this server, as (parts of) the uploaded rogue certificates might be still available there.

A script was found on CA server public 2025. The script was written in a special scripting language only used to develop PKI software. The purpose of the script was to generate signatures by the CA for certificates which have been requested before. The script also contains English language which you can find in Annex 5.3. In the text the hacker left his fingerprint: *Janam Fadaye Rahbar*[7]*.* The same text was found in the Comodo hack in March of this year[8]. This breach also resulted in the generation of rogue certificates.

[5] The IT-Security company F-Secure blogs about a breach of the webserver of DigiNotar in May 2009. http://www.f-secure.com/weblog/archives/00002228.html
[6] Cain&Abel is a very powerful hackers toolkit. It's capable of sniffing and breaking passwords. Most anti-virus software will detect C&A and flag is as malicious.
[7] Supposedly meaning: "I will sacrifice my soul for my leader"
[8] http://www.wired.com/threatlevel/2011/03/comodo_hack/

3 Provisional results

3.1 Fraudulent issued certificates

In total 531 fraudulent certificates have been issued. We have no indication that more certificate were issued by the attacker(s). 344 Of these contain a domain name in the common name. 187 Certificates have in the common name 'Root CA'. We have reason to believe these certificates are not real CA certificates but normal end user certificates.

3.2 Compromised CAs

The attacker(s) had acquired the domain administrator rights. Because all CA servers were members of the same Windows domain, the attacker had administrative access to all of them. Due to the limited time of the ongoing investigation we were unable to determine whether all CA servers were used by the attacker(s). Evidence was found that the following CAs *were* misused by the attacker(s):

- DigiNotar Cyber CA
- DigiNotar Extended Validation CA
- DigiNotar Public CA - G2
- DigiNotar Public CA 2025
- Koninklijke Notariele Beroepsorganisatie CA
- Stichting TTP Infos CA

The security of the following CAs was compromised, but no evidence of misuse was found (this list is incomplete):

- Algemene Relatie Services System CA
- CCV CA
- DigiNotar PKIoverheid CA Organisatie - G2
- DigiNotar PKIoverheid CA Overheid en Bedrijven
- DigiNotar Qualified CA
- DigiNotar Root CA
- DigiNotar Root CA Administrative CA
- DigiNotar Root CA G2
- DigiNotar Root CA System CA
- DigiNotar Services 1024 CA
- DigiNotar Services CA
- EASEE-gas CA
- Hypotrust CA
- MinIenM Autonome Apparaten CA - G2
- MinIenM Organisatie CA - G2
- Ministerie van Justitie JEP1 CA
- Nederlandse Orde van Advocaten - Dutch Bar Association
- Orde van Advocaten SubCA Administrative CA
- Orde van Advocaten SubCA System CA
- Renault Nissan Nederland CA
- SNG CA
- TenneT CA 2011
- TRIAL DigiNotar PKIoverheid Organisatie TEST CA - G2
- TU Delft CA

For some of these CAs extra security measures were in place (like the CCV CA). This makes it more unlikely they were misused.

3.3 Misuse

We investigated the OCSP responder log files around the time of the *.google.com incident. That incident was detected on August 27th. The first known public mention was a posting in a google forum. The user (from Iran) was warned by the Google Chrome browser that there was something wrong with the certificate. The corresponding rogue certificate was created on July 10th.

Based on the logging mentioned above from the OCSP responder, we were able to extract the following information. On August 4th the number of request rose quickly until the certificate was revoked on August 29th at 19:09. Around 300.000 unique requesting IPs to google.com have been identified. Of these IPs >99% originated from Iran, as illustrated in figure 1.[9]

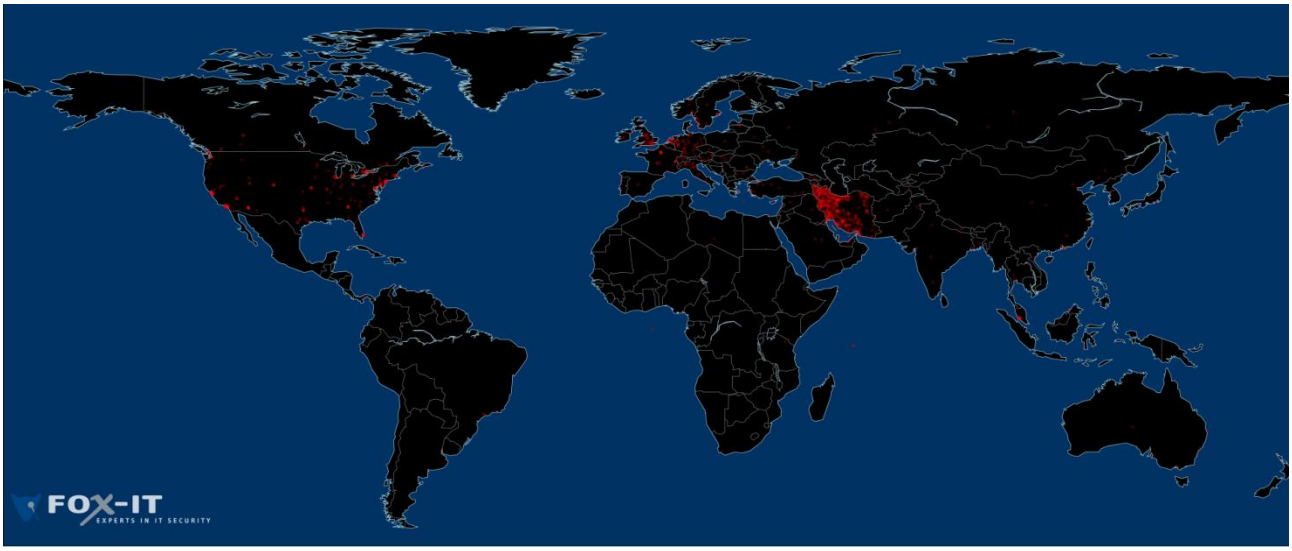

Figure 1: OCSP requests for the rogue *.google.com certificate

A sample of the IP's outside of Iran showed mainly to be TOR-exit nodes, proxies and other (VPN) servers, and almost no direct subscribers.

The list of IP-addresses will be handed over to Google. Google can inform their users that during this period their e-mail might have been intercepted. Not only the e-mail itself but also a login cookie could have been intercepted. Using this cookie the hacker is able to log in directly to the Gmail mailbox of the victim and also read the stored e-mails. Besides that, he is able to log in all other services Google offers to users like stored location information from Latitude or documents in GoogleDocs. Once the hacker is able to receive his targets' e-mail he is also able to reset passwords of others services like Facebook and Twitter using the lost password button. The login cookie stays valid for a longer period. It would be wise for all users in Iran to at least logout and login but even better change passwords.

Other OSCP request logs show some activity on August the 30th with a misused *.torproject.org certificate. None of these originated from Iran. However this does not prove that rogue certificates weren't abused between the issue date and revocation date of the certificates based on the OCSP logs because some applications might not use the OCSP protocol for revocation checking.

[9] This static image shows all IP-addresses detected. On http://www.youtube.com/watch?v=_eIbNWUyJWQ you can see the interception of Google users taking place in a timeline.

4 Discussion

4.1 Skills and goal of the hackers

We found that the hackers were active for a longer period of time. They used both known hacker tools as well as software and scripts developed specifically for this task. Some of the software gives an amateurish impression, while some scripts, on the other hand, are very advanced. In at least one script, fingerprints from the hacker are left on purpose, which were also found in the Comodo breach investigation of March 2011. Parts of the log files, which would reveal more about the creation of the signatures, have been deleted.

The list of domains and the fact that 99% of the users are in Iran suggest that the objective of the hackers is to intercept private communications in Iran.

4.2 Other possible rogue certificates

Using the OCSP responder requests we verify if the requested serial belongs to a known certificate. We have seen requests for unknown serials that cannot be matched against a known certificate. It's possible that these serials belong to a "rogue" certiticate or are just bogus OCSP requests, for instance done by security researchers. It's still possible other unknown[10] rogue certificates have been produced.

OCSP logging could still catch other possible rogue certificates based on the number of requests for an unknown serial, although it's difficult to match the common name with that serial if the certificate in question is not known.

4.3 Trust in the PKIoverheid and Qualified environment

Although all CA-servers have been accessed by a hacker with full administrative access rights and attempts have been made to use the running PKI-software we have no proof of generated rogue Qualified or PKIoverheid certificates. The log files of these CA-Servers validate as correct and no deleted log files have been found on these CA-servers. This is in contrast to our findings on the other breached CA servers.

Investigators encountered two (2) serial numbers of certificates on the Qualified or PKIoverheid server that cannot be related to trusted certificates[11]. Based on this, we cannot rule out the possibility that these relate to rogue certificates.

4.4 Current network infrastructure at DigiNotar

The successful hack implies that the current network setup and / or procedures at DigiNotar are not sufficiently secure to prevent this kind of attack.

The most critical servers contain malicious software that can normally be detected by anti-virus software. The separation of critical components was not functioning or was not in place. We have strong indications that the CA-servers, although physically very securely placed in a tempest proof environment, were accessible over the network from the management LAN.

The network has been severely breached. All CA servers were members of one Windows domain, which made it possible to access them all using one obtained user/password combination. The password was not very strong and could easily be brute-forced.

The software installed on the public web servers was outdated and not patched.

No antivirus protection was present on the investigated servers.

An intrusion prevention system is operational. It is not clear at the moment why it didn't block some of the outside web server attacks. No secure central network logging is in place.

[10] Unknown as in, that we haven't been able to revoke them yet because we don't know their existence.
[11] OCSP requests to these serial numbers will result in a 'revoke' reply.

5 Appendix

5.1 Fraudulent issued certificates

The following list of Common Names in certificates are presumed to be generated by the attacker(s):

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

5.2 Unknown serial numbers

Root-CA server

On the 'Root-CA' server the following serials were encountered:

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

Qualified-CA server

On the 'Qualified-CA' server the following serials were encountered:

```
C6E2E63E7CA99BBA1361E4FB7245493C
863DE266FB30C5C489BF53F6553088C4
```

These serials might have been issued by the following CAs:

- DigiNotar PKIoverheid CA Organisatie - G2
- DigiNotar Qualified CA System CA
- DigiNotar Root CA
- DigiNotar Qualified CA Administrative CA
- DigiNotar Qualified CA
- TRIAL DigiNotar PKIoverheid Organisatie TEST CA G2
- TRIAL DigiNotar PKIoverheid Organisatie TEST CA - G2
- DigiNotar PKIoverheid CA Overheid en Bedrijven

'Taxi-CA

On the 'Taxi-CA' server the following serials were encountered:

```
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 server

On the 'Public-CA' server the following serials were encountered:

```
79C03FE0C81A3022DBF8143B27E40223    8B0EABAF922D4C6E6917FCBE365DD64A    82C42F0EDC18BD751727BE5C54413EF7
FCCF53CB3D0A71494AF9664690FFCF84    4FC2D72D6427CABBE3E859453865F43B    03124C25849D9E49BC2A2FAD3E10C8A4
82BC18B1AA5D59C61D0EFDBEA7664C08    53B53BF2F74997EBEB2577D63DA692B7    EFF0DD4B4927DF64232C5D2FF280C1E4
5D4352671C39616670B2F34C173A1F63    ABB21F43553F2695031A1C85355D7F1C    9EDCB5E1FE1255A2F1D7FC52C4AFA3B1
6FA3C48173B3B289943F113A8CD9DB8C    5563605FDC2DC865E2A1C32995B5A086    3A32AAA9DFE2CA7F9E003885E316944B
CFAF9BE4E5BD0F5A75F628E45E0178C9    5DD6A72747D90C018B63F959DFE7C976    4455B43B9173CBAE4E247272EE2573D5
4ADA28D281D3D14D19FB782D64086D0C    CAB736FFE7DCB2C47ED2FF88842888E7    B95F62E86194734C9F68D4BF8B200C49
0B41ABEE6F4168D3CDE5A7D223B58BC1    9C79C9FE16727BAC407B4AA21B153A54    FE873B742B230B22AE540E840490A2F4
13548FC160BC5C9F315AE28CDB490E36    2D711C9CB79EC15445747BFE3F8BC92F    8779917563EC38B7746B8ECAFE239BE6
5D8D0D43611275982E6A5490E7F87BD7    752A2D0325A3D34D9F5198C2F5C92A6C    72CBC4824C6215B139FDE6BA10DAC6AD
C880AE4D7927E6A8FA7D456CB03E9763    39936336286F843756FC4BC296D7A8E0    8D09D4B98DE67C9E9C7C18CB72AD2418
82072FC8F8DD7E6C0ECE9B47185F0521    4A6D90618A5CA6797C768C03C860C4F8    07BC72A463D4DE33B2BE733D6FAC991D
90DB656E273476CC8367782555582FA8B   0954E1AB9141ED7E8B640FE681046451    D3E2205C3B899FC99D77FE802985283F
171A8599EDE711A3315BC7D694CEBEC6    8259C3E1DB6C2C9B7FCD6A305EADEFE4    A5029D6A057D50D20ECFE0E528EDA067
E9EB8075F7FE3683B431552C2D962CB0    BC01852405D3F4E22C48600266655026    C8B2487ADFAF969E34306029AC934406
E6F9E095464F64448840A832FB3443DB    9F7DDFE3CAAD224EC6BD68B60DE78550    5F3C1BDC7A2BCD47ABAF0C8E62D9F757
C83D16E9CB29DCF35F3B351CB942FE0D    A67C22A6E1F9D87799548EBFC7D5527E    601315BB085FECF29538DA3F9B7BA1CE
39B5DD0ECC85C3F62A72391DC055F561    11661878CCE9DC337CEEBB16E30F9A3A    30170F15A240446E6B482E0A364E3CCA
DF3FD6AFBBFBC30C9AD80BF764A102DB    6BF3BEB26AFF31116200B14F4378C33B    0590B310AEFC7A3EDC03ECA2A6F6624F
327B9A443C49018D7B0A97B6EC2254B8    7A61A7778842E502E2291166C4574485    FDEB145AAC81B8CD29B8DA018E71456F
```

```
C3F9F45F19E334C8303F44288856D843
028CF7556F8BE27026800448FA6AA527
E93B28B47C34B243EBA62E58FE2FF46F
F89F5DE575755A3B4C0DECC6EDA7C804
5D8F8D78B0C19EF4479F744DECBD84BC
EAACDC2F46D4A86F39B035B793F4A94F
9D06313F21A4EDF734C324FFBCB9E2B5
35C54E845AE855F818504C8C189F52C7
E3E120935934CBD77E1DA7F00431F745
0A6DFACFDEAE74A816031534BE90B75A
9AD82BE2FED538B10BDFBD229A8A5AEA
C0F216CA8197AD00F0D98927EAE29E64
DE76B17BFB1B6D6D6634C8C104A6E59F
A90F1BB43E9DB5EDFC60C15FB897C593
8625B32398C2722D96E7B972580A0238
D1FDE3A78C9D2E80C2303CC4E3E92A4C
B355E909FD55C5E9EF1A6E67E9C18203
ADB59A303C6260DBE466F0149AB11A4A
5CEBD524469A075FB6B42D06C9BF27AD
0E0886EEAA119CF14F1C54387060929A
B4F9299F05A327E60543C4CDE3277FC0
E4B2F09505726306314DF05B734FD9D0
4DD0497CBAABBA058574A611B26151BA
7073C6C01DEE4E158F554555F697F7D9
EB72415ECD0B4AACBDEEA3734F4349BF
BED90D98FA3A1E0A5BD78AD54E55774D
3CDCD81930F91AC0B990664931E5412E
763B0C2A7B83066A9D995C8C4FD9E35E
720DF591261D710ADC73127C1BC4303D
C06C12DBBC7055FE40950803238EC104
62BF5A170CC779ADE7EF0090F395D5E6
61BF9A0FF2CE9D55D86BC063839F72F4
B5D7A148CA6C1F9693A2C16ACDD66226
35FBDCDF923F99B5E1C5FF4423B715B8
F1EBE73557546DC8B21E0A2DE5E3A33E
EBE7561CA573DA5DBB8EFAA250A40FD3
6BACB6C5B74FA747A3CF375EC3095035
6C1950AA83F4663F1BA063B5275C25EC
56EF1EE54D65EF7B39AF541E95BB45A9
2B1EA767EC59E46364BC2DF9B1F30B97
3913B1E1C35BDDF02CE03C916E8AA638
AFA2F7E964280B36DB0D714B86256F54
022E35B1ACD40F040C444DF32A7B8DE6
170370B60D515F164119BE54FD55E1ED
CBFE437C9B62805C4353516699E44649
5FFA79AB76CE359089A2F729A1D44B31
5298BCBD11B3952E3FDDC6FDD6711F5C
1836289F75F74A0BA5E769561DE3E7CD
DEB427AC9F1E8A0D0237049C80DF7E7F
FD8FE350325318C893AFE03F9DFC7096
A8031D608F6549941879981764674DD7
DDAD29B8B1215191E7EB5AAEE0219338
3F8A5EA1756DDF4A6B6F2645B4911486
30DF96D87EEC8CA77A135ECCAB1AD25E
7DD8E0E1906C1754E11E901927CCABBD
DAC51C3D23B163601305AF99DF129689
D77EC92400AE0D9FA57DEF4DD8CFA4D4
09369288E36D7AFFEE94EA81998FA316
EEBE1885532234328919191 3F6D769EB
C00132DA154BDEE361EDEE727226D0F5
6580BE22A0566352B9622777BFCB7164
7352C61297D6B04E874EDAD12480F78E
F658C0D52B3EEF71DDE6C284E7E1B337
E1253D04A17AB8E47F4A5916B9BF9D23
8922A9A23BE960FFE9707A0B3F4D75BD
EAE97F465015E49A14F3B23403ACFA11
13A757022817C0514A5C142FE9BF143A
5132F0FCB3F8DCAA501C620575D33FEE
39953BF6383A00D29BEB377568E3DE7A
67887932934DFF086153CA905E7DE9EE
DCD1072719692871126E4159D80EFDA8
C6741E3D08C0FFD4617B94E654DD89F1
D0BA58BA609CC1A001F612987A822BEF
6B339433956F1505104BB231314A153E
C1366C7246041A3089E1C244C5DC42E7
61D11B35765ECB85890D5349786D9FCA
44C287C1C3697367B0E6CB78A78C1DF5
DAACF72BC91FB6DA90A804933CB72E23
2ACBA14BB6F65F7BD0A485BFCB6D023F
84BE5D762F37E9018D623C8E91F4D924
1A89324D6D3E6DE6726C688BFF225DDD
F5FA42A5B421705E4803DA93C4F7E099
A869B96BCDF1D474C0714763AA34A8C9
3EA0F90DE57187FC7E1AC45AE44D16C6
F7DE638B76C3958AA3413A9785A19900
3F8C9CDAACBB533AE94F47456819FA0E
209920C169512D3EB4A1ED7CAD17D033
B2F57BD01BAAF7AF01EF442910CEBBA0
C0766829AA4D2E1A5D97213A4E4A654E
FC9993EA7A4E761B6CB79ABE2BD3CDE1
4D556B338FAA020979A740B4C3AEE28C
8ED896B9A622FF24559A3429E5888E0A
8CF1F45323EC5AB449451E7A9476CFDC
D1718E9BD91257D2169C81197D508A67
E4A691D602667849 68DF971D6BF473AF
B3B64F1925F759A2E145190333D1D6D2
ED4C2EBC14B85F46A9A75F159DF8BEB3
CDBC0441C10DB5ABA43120E63A048425
DC1665266A0198728861AC99ED368928
706BBC770C62D41DD799721ABD1868AB
B2205D8CBDDFE49D7C5F0F95D506718F
901F30DB86EEB1666F5A8CAE1C7BD08B
9A3A951BE27E0729726FD8B80060E7E1
6410577C738133297472F6C22C2BB397
C8C06B0C6B7FE7CA66BCFE617AB6C4E6
58C18B290620E18B8C78AC1912E5DCD7
2F5ABFDCCAB1A2927E54283296F19FB8
A07CB7881E35C91FD9C5D20F6102572C
05E2E6A4CD09EA54D665B075FE22A256
8BA800DDDD865B6BF3A85ADEC4C29730
07B546E8E002FC5854651BE31802F96D
DF2AD7F766E2EEFAF0FD1FB5C6883AB4
1C6EA2DA6ECED5C5C761BCA9CA4C5308
A640A29E706AF38557B86619EAF45E7A
F88885670C3D55EBA52096A65310DACA
B85E7BB83667097F15D8A3DEAAA1B198
A5F6F149B468683318DC178F4208E237
04841B82A9D81E44CB4F2D98CFE7C374
A81686CEFDEFFCE82B8DBF100E1395F1
9952073595776A3D7A8101664A56AB96
A076DA72A8C8E2137F05FE3FA59870EB
121378A6DE0A13DDB295106E912A4E14
65A925E578098658FADA30E9FB67B5E4
5B8E5202EC6769F2389605D33DC245B2
EA71F746BD17D1B05450329818572F2E
DD8C315D2CA61870CBCF9D56ED7474E2
F346A1E62FED476F472560C6DDE0CADC
CBBCB9E06F9FC92C533B2F2A5284BA22
79DCFDA2700E06F8EAA640BA9B827810
17CF5474D5A8B4E735E69E017CEC2F37
7034FBF641CEB257FC109A6819D19DA0
6E6D052B5ABC015C779EA3500FA11A28
FAB79682C8EAE556F11ECF6DAD7121BA
0370390E48A7F26AA62188A79E612DC3
59F8BDDA3F56D8026FAB6E3130F5D843
C731140FAA7690918BABF17BECB7938D
8C605DFAA0EC88CDB7D12F7250C9F53A
68F252CD36F2798A2182F6406A31A5A2
BD7CB0D124DFDE784CD5B9EF288C304E
3D2BC95A85EF539A68DAC84542A1AE7A
8CC74931E64061491652CC169C8BAAB3
4157D99E46A3E45E6130A95645410DAC
E34C4FC7488C4DFEF0EA475A17AF2C7B
```

These serials might have been issued by the following CAs (list incomplete):

- Algemene Relatie Services System CA
- CCV CA
- DigiNotar Cyber CA
- DigiNotar Extended Validation CA
- DigiNotar PKIoverheid CA Organisatie - G2
- DigiNotar PKIoverheid CA Overheid en Bedrijven
- DigiNotar Public CA - G2
- DigiNotar Public CA 2025
- DigiNotar Qualified CA
- DigiNotar Qualified CA Administrative CA
- DigiNotar Qualified CA System CA
- DigiNotar Root CA
- DigiNotar Root CA Administrative CA
- DigiNotar Root CA G2
- DigiNotar Root CA System CA
- DigiNotar Services 1024 CA
- DigiNotar Services CA
- EASEE-gas CA
- Hypotrust CA
- Koninklijke Notariele Beroepsorganisatie CA
- MinIenM Autonome Apparaten CA - G2
- MinIenM Organisatie CA - G2
- Ministerie van Justitie JEP1 CA
- Nederlandse Orde van Advocaten - Dutch Bar Association

- Orde van Advocaten SubCA Administrative CA
- Orde van Advocaten SubCA System CA
- Renault Nissan Nederland CA
- SNG CA
- Stichting TTP Infos CA
- TenneT CA 2011
- TRIAL DigiNotar PKIoverheid Organisatie TEST CA - G2
- TRIAL DigiNotar PKIoverheid Organisatie TEST CA G2
- TU Delft CA

5.3 Plain text left in script to generate signatures on rogue certificates

```
I know you are shocked of my skills, how i got access to your network
to your internal network from outside
how I got full control on your domain controller
how I got logged in into this computer
HoW I LEARNED XUDA PROGRAMMING
HOW I got this IDEA to write such XUDA code
How I was sure it's going to work?
How i bypassed your expensive firewall, routers, NetHSM, unbreakable hardware keys
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
THERE IS NO ANY HARDWARE OR SOFTWARE IN THIS WORLD EXISTS WHICH COULD STOP MY HEAVY
. ATTACKS
MY BRAIN OR MY SKILLS OR MY WILL OR MY EXPERTISE
That's all ok! EVerything I do is out of imagination of people in world
I know you'll see this message when it is too late, sorry for that
I know it's not something you or any one in this world have thought about
But everything is not what you see in material world, when God wants something to happen


My signature as always: Janam Fadaye Rahbar


Rahbare azizam mesle hamishe asoode bash, ta vaghti ke man va amsale man baraye in marzo
. boom
va baraye barafrashte negah dashtane parchame velayate faghih kar mikonand
daste har doshmano mozdouri ghat khahad bood
Rahbaram, Tamame vojoodam fadaye to ke ham jani o ham janani
```

5.4 Timeline

06-Jun-2011	Possibly first exploration by the attacker(s)
17-Jun-2011	Servers in the DMZ in control of the attacker(s)
19-Jun-2011	Incident detected by DigiNotar by daily audit procedure
02-Jul-2011	First attempt creating a rogue certificate
10-Jul-2011	The first succeeded rogue certificate (*.Google.com)
20-Jul-2011	Last known succeeded rogue certificate was created
22-Jul-2011	Last outbound traffic to attacker(s) IP (not confirmed)
22-Jul-2011	Start investigation by IT-security firm (not confirmed)
27-Jul-2011	Delivery of security report of IT-security firm
27-Jul-2011	First rogue *.google.com OSCP request
28-Jul-2011	First seen that rogue certificates were verified from Iran
04-Aug-2011	Start massive activity of *.google.com on OCSP responder
27-Aug-2011	First mention of *.google.com certificate in blog
29-Aug-2011	GOVCERT.NL is notified by CERT-BUND
29-Aug-2011	The *.google.com certificate is revoked
30-Aug-2011	Start investigation by Fox-IT
30-Aug-2011	Incident response sensor active
01-Sep-2011	OSCP based on white list