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
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 revoked¹ 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 21st;
- 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 requests were monitored.

Current browsers perform an OCSP check as soon as the browser connects to an SSL protected website through the https-protocol. 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’. 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. 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 as the famous Cain & Abel tool 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. The same text was found in the Comodo hack in March of this year. This breach also resulted in the generation of rogue certificates.

---

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 it 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 Notarieke 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](image)

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=e1bNWUyJWQ](http://www.youtube.com/watch?v=e1bNWUyJWQ) 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" certificate or are just bogus OCSP requests, for instance done by security researchers. It's still possible other unknown\(^\text{10}\) 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 rogueQualified 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\(^\text{11}\). 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):

<table>
<thead>
<tr>
<th>Common Name</th>
<th>Number of certs issued</th>
</tr>
</thead>
<tbody>
<tr>
<td>CN=<em>.</em>.com</td>
<td>1</td>
</tr>
<tr>
<td>CN=<em>.</em>.org</td>
<td>1</td>
</tr>
<tr>
<td>CN=<em>.</em>.10million.org</td>
<td>2</td>
</tr>
<tr>
<td>CN=<em>.</em>.JanamFadayehRahbar.com</td>
<td>1</td>
</tr>
<tr>
<td>CN=<em>.</em>.RamzShekanShezorg.com</td>
<td>1</td>
</tr>
<tr>
<td>CN=<em>.</em>.SahebeDonyayeDigital.com</td>
<td>1</td>
</tr>
<tr>
<td>CN=<em>.</em>.android.com</td>
<td>1</td>
</tr>
<tr>
<td>CN=<em>.</em>.azadegi.com</td>
<td>1</td>
</tr>
<tr>
<td>CN=<em>.</em>.balatarin.com</td>
<td>3</td>
</tr>
<tr>
<td>CN=<em>.</em>.comodo.com</td>
<td>3</td>
</tr>
<tr>
<td>CN=<em>.</em>.digicert.com</td>
<td>2</td>
</tr>
<tr>
<td>CN=<em>.</em>.globalsign.com</td>
<td>7</td>
</tr>
<tr>
<td>CN=<em>.</em>.google.com</td>
<td>26</td>
</tr>
<tr>
<td>CN=<em>.</em>.logmein.com</td>
<td>1</td>
</tr>
<tr>
<td>CN=<em>.</em>.microsoft.com</td>
<td>3</td>
</tr>
<tr>
<td>CN=<em>.</em>.mossad.gov.il</td>
<td>2</td>
</tr>
<tr>
<td>CN=<em>.</em>.mozilla.org</td>
<td>1</td>
</tr>
<tr>
<td>CN=<em>.</em>.skype.com</td>
<td>22</td>
</tr>
<tr>
<td>CN=<em>.</em>.startssl.com</td>
<td>1</td>
</tr>
<tr>
<td>CN=<em>.</em>.thawte.com</td>
<td>6</td>
</tr>
<tr>
<td>CN=<em>.</em>.torproject.org</td>
<td>14</td>
</tr>
<tr>
<td>CN=<em>.</em>.walla.co.il</td>
<td>2</td>
</tr>
<tr>
<td>CN=<em>.</em>.windowsupdate.com</td>
<td>3</td>
</tr>
<tr>
<td>CN=<em>.</em>.wordpress.com</td>
<td>14</td>
</tr>
<tr>
<td>CN=Comodo Root CA</td>
<td>20</td>
</tr>
<tr>
<td>CN=CyberTrust Root CA</td>
<td>20</td>
</tr>
<tr>
<td>CN=DigiCert Root CA</td>
<td>21</td>
</tr>
<tr>
<td>CN=Equifax Root CA</td>
<td>40</td>
</tr>
<tr>
<td>CN=GlobalSign Root CA</td>
<td>20</td>
</tr>
<tr>
<td>CN=Thawte Root CA</td>
<td>45</td>
</tr>
<tr>
<td>CN=VeriSign Root CA</td>
<td>21</td>
</tr>
<tr>
<td>CN=addons.mozilla.org</td>
<td>17</td>
</tr>
<tr>
<td>CN=azadegi.com</td>
<td>16</td>
</tr>
<tr>
<td>CN=friends.walla.co.il</td>
<td>8</td>
</tr>
<tr>
<td>CN=login.live.com</td>
<td>17</td>
</tr>
<tr>
<td>CN=login.yahoo.com</td>
<td>19</td>
</tr>
<tr>
<td>CN=mspy.logmein.com</td>
<td>17</td>
</tr>
<tr>
<td>CN=twitter.com</td>
<td>19</td>
</tr>
<tr>
<td>CN=wordpress.com</td>
<td>12</td>
</tr>
<tr>
<td>CN=www.10million.org</td>
<td>8</td>
</tr>
<tr>
<td>CN=www.Equifax.com</td>
<td>1</td>
</tr>
<tr>
<td>CN=www.balatarin.com</td>
<td>25</td>
</tr>
<tr>
<td>CN=www.cia.gov</td>
<td>4</td>
</tr>
<tr>
<td>CN=www.cybertrust.com</td>
<td>14</td>
</tr>
<tr>
<td>CN=www.facebook.com</td>
<td>1</td>
</tr>
<tr>
<td>CN=www.globalsign.com</td>
<td>12</td>
</tr>
<tr>
<td>CN=www.google.com</td>
<td>1</td>
</tr>
<tr>
<td>CN=www.hamdam.com</td>
<td>1</td>
</tr>
<tr>
<td>CN=www.mossad.gov.il</td>
<td>5</td>
</tr>
<tr>
<td>CN=www.sis.gov.uk</td>
<td>10</td>
</tr>
<tr>
<td>CN=www.update.microsoft.com</td>
<td>4</td>
</tr>
</tbody>
</table>
5.2 Unknown serial numbers

**Root-CA server**

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

813102A2D3016CEB1A95C7D46619617
66E23BEFED7DE849C951CCB3F522A57
71CE18C02421824510EFS51513B78
B7A6FECB1E84420B7747C82E5358B3
65E08BD1F01E499C8E0E94D32A0F6B
80C969D3F177CA9FDC285105882A8
7F73ECA14CB0A8DB52CF6D693C56A1D

**Qualified-CA server**

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

CE62E63E7CA99B6A136124F7245493C
B6DE06F30C5C4B98F3J53503883C4

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:

2586CA3115C2FBE4F7GA1BD53735BEB3
A0CF459D0E281A3022DBF8143B27E40223
FCCF53CB3D041A9F6666690CFC84
3B1B8A1962F479979EBH3577D6AD92B7
C53B5B8F74799E9EB5277D6AD92B7
B59D542671CB3F9143F3CD9D88
D5A65747D709C01863F5890FE1876
4DDA28D281D6419B872D82064086DC
OB1A8EEF6166D3C9A2082BBDC50
32D8DO6D64110275926A549087F87BD7
C93965326171C7842F34C4731A1F6E
F04A31843695D2CD6527A2321F121
87C0416123051F9C8916C8350225BB6
8F751D8C2A07417B1A10D91D40E684
6C363529C43147B20C54FC6690F3FF
9916C35325B860737775A20BD4C72
5F484A41123051F9C8916C8350225BB6
DB63E2CE611075075FCCBE98AE8A601
C641E8B7F11863C4F1EA0D333C55E78
7B891F1F0C08BD133C23C13E24FCF1C

**Public-CA server**

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

79C03DCEC8A130D2022BFF143B2E40223
FCCF53CB3D041A9F6666690CFC84
BB0EEAF922D4C696117FCB3D56D4A
4F2C72D6427CABBE383545865F43B
3B1B8A1962F479979EBH3577D6AD92B7
EPPDFDA4927DF64232C5D0F28DCE14
5D4532671CB3F9143F3CD9D88
ABB21F4353552693051A053507F1C
6FAC8733B28695F131A8C9DB8C
5563ED5F2CD2C652A1C32995B5A086
CTAFBFE4955D5FAP759F62BD40178C9
555A679F7C01863F5890FE1876
4AA28D281D6419B872D82064086DC
CAB767F1E72DCB47ED2F8842888E7
OB1A8EEF6166D3C9A2082BBDC50
9C799F216772BAC047A21A1535A4
13548FC19C5C9F51A52ECD808E36
20711C9B78E154547748E3F8B3C2F
8779175633874768E239E86
5D08D04613275926A549087F87BD7
572AD20325A33D49F519B2FC5292A6C
C88A0E4D72976A8F0A7456CB309763
39396336286F43756FC48296D7A8E0
82332FD2F656CD06CB47185F5321
4DA9D061A5CA6797C68C036CC4F8
954E1AB914EDBE8664044451
171A85996E71A3318C7D964C5EBC66
2859C31D8C2C08DA5EDE4F4
E9BE80BF75F6E3B41552CD942CB8
3BC81524053DF42240626665026
E69B95466448B6A3B3F7B40D3
7GDFE3CA22D4C56BD56587855
C3D16C6C2BDF353F5315CB42F2ED0
39B5DO6CE5C36F2A2791D55F561
1166178EC9DC33C7EBEB1630F9A3A
DF3D6A9FEDDFEC8C5DC808B8EA20D2
A6833B26A9F11116203B9137C3C8
327B5A443C69180D7B9A796B2C25488
7A1ajes17784E2502291166C547448
F6EB154AC815BCD298SDA01871456F

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

6 I know you are shocked of my skills, how i got access to your network
7 to your internal network from outside
8 how i got full control on your domain controller
9 how i logged in into this computer
10 Now I learned XPUA programming
11 Now I got this IDEA to write such XPUA code
12 How i was sure it's going to work?
13 How i bypassed your expensive firewall, routers, NetSSH, unbreakable hardware keys
14 How i did all XPUA programming without 1 line of resource, got this idea, owned your
15 network accessed your domain controller, got all your passwords, signed my certificates
16 and received them shortly
17 There is no any hardware or software in this world exists which could stop my heavy
18 attacks
19 My brain or my skills or my will or my expertise
20 That's all ok! Everything I do is out of imagination of people in world
21 I know you'll see this message when it is too late, sorry for that
22 I know it's not something you or any one in this world have thought about.
23 But everything is not what you see in material world, when God wants something to happen
24
25
26 My signature as always: Jamam Fadaye Fadbar
27
28 Rakhare action male hamishe moodeh bash, te vaghfi ke man va amalle man baraye in marzo
29 boom
30 va baraye barafshite negah dahamane parazhaye faghih bar mikonanad
31 dafe har dostmane mowaddi ghat kheshbed boud
32 Rakhareen, Tanomeh vojoosam zadeye ke han joni o hox jamami

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 OCSP 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  OCSP based on white list