Research report

Date	:	July 27, 2011
Company	:	ITsec Security Services BV
Classification	:	confidential
To	:	[redacted]
From	:	
Copy	:	-
Project	:	SS-REL-NOTAR-1102
About	:	Security Incident 2011
Enclosures	:	-
Document no.	:	SS-REL-NOTAR-1102-10.TN01
File	:	ss-rel-notar-1102.tn01 research report security incident 2011.docx

Introduction

In July 2011 Diginotar discovered that several systems were compromised and that an attacker was able to generate and sign certificates.

This document documents the result of the security analysis that has been performed. Furthermore, the actions that have been taken to prevent further security incidents are documented.

Cause of the security breach

- The attacker compromised a webserver of Diginotar due to a security vulnerability that is present within the DotNetNuke software.

DotNetNuke version 4.8.2.0 is installed on host winsrv119. This version is affected by a file upload vulnerability. For details, see:
http://www.dotnetnuke.com/News/Security-Policy/Security-Bulletin-no.16.aspx

Evidence found

The attacker compromised the host winsrv119. Tools have been found on this host that are used to obtain the password hashes of local system users, such as the administrator user. A file containing these hashes has been found. Due to the weak security of Windows passwords, it must be assumed that the attacker was able to compromise the passwords (for example with rainbow tables) of the accounts found on the system. On the system, the Administrator account and the domain administrator account of one of the system administrators is present.

According to one of the system administrators, the local administrator account password is used on most other systems. Spot checks confirm this.

- The attacker was able to traverse the infrastructure and obtain access to at least two CA's that were used to generate certificates. After investigating the firewall rule set and several systems, it is still unclear how the attacker was able to obtain access to the CAs from the external DMZ as the firewall rule set does not permit direct access to the CAs. Several systems that may act as a stepping stone have been investigated but no evidence has been found that indicates compromittation.
- It has been verified that CAs could communicate through HTTP(S) with systems present within the external DMZ, such as the compromised hosts. In turn, the compromised hosts could communicate with other hosts on the internet through HTTP(S).

Forensic analysis of the disk image of Winsrv055 (Relatsies CA) shows that the domain administrator account of the secure network was compromised. This is concluded from the fact that on Saturday 2 July 2011 in the evening, a file called dnpub.zip was created on this host containing several files, such as LDAP dump files. This file was deleted afterwards.

Firewall log analysis showed that the attacker was using the systems up to 22 July 2011.

Known compromised systems

- Winsrv101 (Webserver)
- Winsrv118 (Docproof)
- Winsrv119 (Docproof)
- Winsrv108 (TIM)
- Winsrv055 (Relaties CA)
- Winsrv056 (Public CA)

Actions taken

1. The docproof servers have been taken offline to prevent further access.
2. Docproof servers are no longer accessible from the internet but are active to keep some production processes online.
3. Extra firewall rules have been enabled to restrict access to the 'secure' network containing the CAs. Also, outgoing traffic is restricted. Please note that some hosts in the secure network can connect to DMZ systems for production purposes (http(s)).

4. A disk image has been created from the following systems:

   Winsrv119 (Docproof)

   Winsrv055 (Relaties CA)

   Winsrv056 (Public CA)

   These images can be used for further analysis.
5. A script has been created to scan all server systems and workstations for known malicious files. Files created by the attacker has been the primary input.
6. All compromised systems have been virus scanned and anti-rootkit software has been used to determine the presence of rootkits. Please note that it can never be said with certainty that compromised systems are rootkit free unless forensic analysis is performed.
7. Due to the large number of systems present within the infrastructure and the limited time frame that was available, not all systems have been investigated in detail.

Timeline

Date	Event
17 June 2011 04:20	Winsrv119 compromised (Docproof)
17 June 2011 07:26	Winsrv118 compromised (Docproof)
17 June 2011 10:50	Winsrv101 compromised (Website)
17 June 2011 19:26	Winsrv108 compromised (TIM)
20 June 2011 05:52	Winsrv017 compromised (Signing server)
02 July 2011 05:07	Winsrv055 compromised (CA Relaties)
04 July 2011 00:59	Winsrv055 x-select-settings.xuda on system
10 July 2011 11.05	Roque certificates are generated on two CAs
22 July 2011 13:11	Last outbound traffic to attacker IP address according to the firewall log