The DigiNotar crisis

from incident response
to crisis coordination

Aart Jochem
NCSC-NL
FIRST Conference
Malta - 18 June 2012
Wave 1
Early nineties: Phil Zimmerman releases PGP
Early nineties: Whitfield Diffie works on public policy aspects of cryptography
Wave 2
Memorandum Vulnerabilities on the Internet
July 2001
Wave 3
Large scale incidents triggers also military respons

Was it Hillar or John?
Chain of trust
Video

2011-08-04 04:00:00
Factsheet: Fraudulently issued security certificate discovered

Last modification: 05-09-2011
First publication: 31-08-2011
Version: 2.2

On 29 August 2011 it became known that a fraudulent DigiNotar security certificate was issued for Google.com, as a result of an intrusion. DigiNotar is a Dutch company that issues, amongst others, SSL certificates. These certificates are used for the identification of websites and protection of internet communication. The discovery of this fraudulent certificate has caused various browser-vendors to stop trusting the DigiNotar Root Certificate Authority and DigiNotar sub-root in their browsers. On September 2, the results of an investigation by Fox-IT have been shared with the government, after which the government has denounced its trust in the DigiNotar certificates.

The main facts at a glance

- The Dutch government denounces trust in certificates issued by DigiNotar.
- After an intrusion in DigiNotar systems, probably several hundred fraudulent certificates were issued.
- A fraudulent certificate for google.com is actually used by attackers.
- There are no Dutch government certificates among the known fraudulent certificates.
DigiNotar
Public CA

DigiNotar
PKIOverheid CA

Sub CA

Sub CA

Sub CA

Sub CA

Hacked
From: Erik de Jong (GOVCERT.NL)
Sent: vrijdag 2 september 2011 23:59
To: Alle medewerkers GOVCERT.NL
Subject: De middernachtscrisishaiku

Het is tijd voor de traditionele middernachtscrisishaiku.

**Trust builds up slowly**
**SSL certificates**
*Poooof* trust gone like that

[1] Elke traditie kent een begin.

From: Aart Jochem (GOVCERT.NL)
Sent: zaterdag 3 september 2011 23:51
To: Alle medewerkers GOVCERT.NL
Subject: RE: De middernachtscrisishaiku

**When trust revoked**
Computers silenced in rack
You and me remain

Aart

From: Bob (GOVCERT.NL)
Sent: Maandag 5 september 2011 23:58
To: Alle medewerkers GOVCERT.NL
Subject: RE: De middernachtscrisishaiku

**Bits, elements of trust**
Gateways to precious freedom
Sorry, revoked

Bob
Building up a crisis

- June
- July
- August
- Sept
- Oct

Hack

*.google.com

Crisis

Parliament, fact finding, etc

No role yet

Coörd

Expert
What’s next?
A PKI is a critical infrastructure

• Treat it like one

• Create awareness

• Monitor the RA’s and CA’s

• Strengthen oversight
Manage certificate as assets

• Have an inventory

• Add to asset management system

• Provide for backups
Support secure techniques

• Look into the new IETF draft RFC for Dane

• Adopt DNSSEC
Summary

• PKI is a critical infrastructure, treat it like one
• Manage individual certificates as assets
• Support development and implementation of secure techniques
• Go through scenarios where your CA becomes untrusted
The DigiNotar Crisis

from incident response
to crisis coordination

Aart.Jochem @ ncsc.nl

FIRST Conference
Malta - 18 June 2012