DigiNotar - Untrusted CA

Marco Colognese - VR423791

Università degli Studi di Verona

Progetto per il corso di *"Sicurezza delle Reti"*

Dicembre 2018

Introduzione

- *DigiNotar*
  - La *root CA* olandese
- L'attacco al *certificate authority*
  - La scoperta dell'attacco
  - Concretizzazione e conseguenze
  - Le motivazioni
- Le reazioni sul web
  - Le principali compagnie
  - Il governo olandese
- Il report di *Fox-IT*
  - La pubblicazione del rapporto
  - L'analisi e la ricostruzione
- Comodohacker
  - La rivendicazione dell'attacco
  - Il collegamento con l'attacco a *Comodo Group*
- Conclusione

DigiNotar

DigiNotar fu una root certificate authority olandese, istituita nel 1998 dal notaio D. Batenburg e dall'ente nazionale dei notai.

- Offriva consulenze per implementare servizi elettronici nella propria attività; offriva anche certificati sicuri.
- È stata una CA *general-purpose* per diversi anni, prendendo però di mira il mercato di notai e altri professionisti.
- Forniva certificati al governo olandese per i servizi online.
- Venne acquisita dalla compagnia *Vasco Data Security International* nel gennaio 2011.
- Nonostante il primo incidente nei loro sistemi (giugno 2011), i certificati di DigiNotar vennero dichiarati tra i più affidabili.

Poiché i CA sono i primi obiettivi di un attaccante, *DigiNotar* era dotata di importanti sistemi per la sicurezza interna:

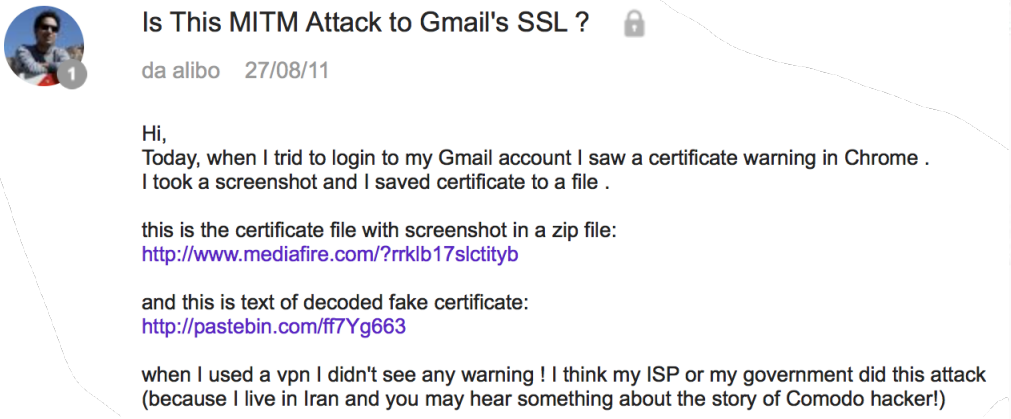
- reti di computer segmentate per limitare i tentativi di accesso;
- *intrusion prevention system* per monitorare il traffico entrante;
- ogni richiesta per un nuovo certificato doveva essere approvata da due dipendenti *DigiNotar*;
- per pubblicare il certificato era necessario inserire una card in un computer tenuto in una stanza altamente sorvegliata;

Ciò dimostra che *DigiNotar* aveva investito molto nei propri sistemi di sicurezza interna per mantenere una buona reputazione in rete.

L'attacco al *certificate authority*

Il 27 agosto 2011, un uomo iraniano (*alibo*), non riuscendo ad accedere all'email, segnala il problema al *Gmail Help Forum*.

- Il browser *Chrome* mostrava: Invalid Server Certificate.
- Il problema sembrava scomparire utilizzando una *VPN* che ne mascherava la posizione.
- Tutto ciò poteva ricondurre ad eventuali azioni prese dal governo iraniano o dall'ISP del paese.
- Il rischio era quello di un *MitM attack*.



Is This MITM Attack to Gmail's SSL ?

da alibo 27/08/11

Hi,
Today, when I trid to login to my Gmail account I saw a certificate warning in Chrome .
I took a screenshot and I saved certificate to a file .

this is the certificate file with screenshot in a zip file:
http://www.mediafire.com/?rrklb17slctityb

and this is text of decoded fake certificate:
http://pastebin.com/ff7Yg663

when I used a vpn I didn't see any warning ! I think my ISP or my government did this attack
(because I live in Iran and you may hear something about the story of Comodo hacker!)

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- Protects e-mail messages
- Ensures software came from software publisher
- Protects software from alteration after publication
- Allows data to be signed with the current time

* Refer to the certification authority's statement for details.

Issued to: *.google.com

Issued by: DigiNotar Public CA 2025

Valid from 7/10/2011 **to** 7/9/2013

Nell'estate del 2011 l'attacco iniziò a concretizzarsi, portando i primi risultati, fino a diventare qualcosa di irreversibile:

- Nel mese di giugno un attaccante iniziò a scavare all'interno del labirinto di reti partizionate, fino alla svolta.
- Il 10 luglio riesce ad emettere il primo certificato compromesso: **.google.com*;
- Entro la fine dell'estate si scoprì che furono emessi ben 531 certificati fraudolenti firmati da *DigiNotar*.
- Il certificato di **.google.com* venne individuato da Chrome poiché Google, per i propri certificati, riservava controlli extra.

Nonostante *DigiNotar* investisse molto a livello fisico nei propri sistemi di sicurezza, commise importanti errori a livello software.

- Utilizzava *Windows* e ciascun server si trovava sotto un unico dominio Windows; per accedere era sufficiente conoscere la combinazione user/password valida per tutti i server.
- La password scelta non era sufficientemente sicura e poteva essere facilmente violata attraverso un brute-force attack.
- Lasciò in esecuzione nei propri web server alcuni unpached software, creando così delle vulnerabilità nel sistema.
- Non vi era nessuna protezione antivirus all'interno dei server, spianando la strada ad eventuali codici malevoli.
- L'Intrusion Prevention System era operativo ma posizionato male (davanti al firewall), segnalando molti falsi positivi.

Il 19 luglio, un controllo di routine rivela l'esistenza di certificati apparentemente firmati da *DigiNotar* che però non erano presenti all'interno dei registri dell'azienda.

- questi vengono immediatamente revocati e viene avviata un'indagine interna;
- quest'ultima porta alla luce altri certificati compromessi che vennero prontamente revocati;
- prima della fine di luglio la società riteneva che il problema fosse definitivamente stato risolto;
- *DigiNotar* scelse di non comunicare nulla riguardo l'accaduto, violando il *Dutch Telecommunications Act*.
- Fino al 27 agosto, giorno in cui il problema (ancora presente), divenne di dominio pubblico.

Le conseguenze di un attacco di questo genere potevano essere molto gravi. L'emissione di certificati falsi esponeva gli utenti ad attacchi informatici di vario genere:

- Phishing attack: attraverso un certificato falso l'attaccante può spacciare per sicura una pagina che in realtà è stata creata da lui per estorcere informazioni ad un utente;
- dal precedente si può concretizzare un MitM attack, poiché l'attaccante ha il pieno controllo della web page in cui l'utente inserisce i propri dati personali, inconscio del fatto che l'attaccante sta osservando tutto.
- la stessa pagina può essere utilizzata per indurre l'utente a scaricare del codice malevolo che poi l'attaccante sfrutterà per ottenere un punto di accesso o per altri scopi illeciti.

I motivi dell'attacco sono stati ricondotti al governo iraniano di *Ahmadinejād* che intercettava le comunicazioni della popolazione:

- in quel periodo molte persone venivano uccise per aver avuto pareri diversi da chi era al potere;
- il governo voleva controllare le email dei cittadini per individuare i dissidenti policiti;
- questo attacco ha colpito almeno 300 mila persone, di cui il 99% erano cittadini iraniani;
- il sospetto viene quasi confermato dalla "*firma*" lasciata dall'hacker all'interno di uno script in un server;

Le reazioni sul web

Nei giorno 29 e 30 agosto 2011 vengono pubblicati in rete le prime segnalazioni da parte delle compagnie più note:

- Nel *Google Security Blog* appare un post intitolato: *"An update on attempted man-in-the-middle attacks"*.
  - Il 3 settembre vengono ufficialmente respinti tutti i certificati firmati da *DigiNotar*.
- Nel *Mozilla Security Blog* viene pubblicato un avviso intitolato: *"Fraudulent *.google.com Certificate"*.
  - Il 2 settembre viene revocata la fiducia verso *DigiNotar*, non sapendo quanti altri certificati fraudolenti siano ancora in rete.
- *Chrome* annuncia una nuova release in cui viene disabilitata una *certificate authority*.
- Il blog *TechNet* di *Microsoft* annuncia la rimozione automatica di *DigiNotar* dai CA attendibili da *Windows Vista* e precedenti.

Dopo oltre una settimana di silenzio dalla scoperta, anche *Apple* annuncia la rimozione dei certificati di*DigiNotar* da Safari.

- Dopo la scoperta internazionale dell'attacco a *DigiNotar*, il governo olandese decise di prendersi a carico la compagnia.
- Non ritenevano che i certificati dell'azienda fossero compromessi e continuarono ad utilizzarli per i servizi statali.
- Il governo commissionò Fox-IT per le indagini sull'accaduto.
- Il 3 settembre, dopo i primi risultati dell'indagine, anche il governo passò ad un'altra autorità di certificazione.
- Il 20 settembre, *Vasco* annunciò che *DigiNotar* dichiarerà bancarotta, presentando un'istanza di fallimento.

Il report di Fox-IT

Il governo olandese aveva incaricato *Fox-IT* per effettuare le indagini necessarie e stendere un rapporto dettagliato.

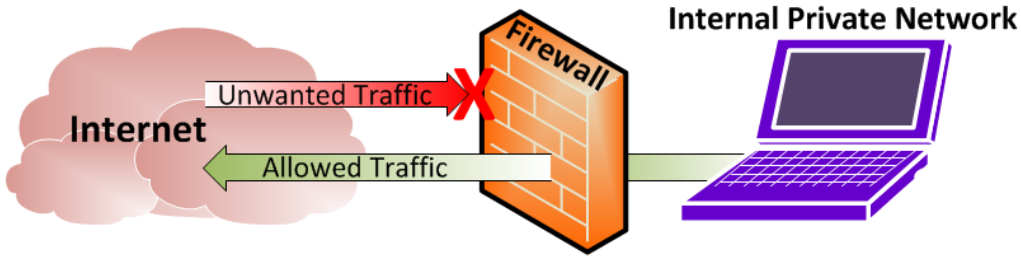
- Inizialmente venne chiesto di non pubblicare il rapporto per evitare ulteriori reclami nei confronti di *DigiNotar*.
- Ottobre 2012: oltre un anno dopo, il report dell'operazione *Black Tulip* viene pubblicato.
- Si parla di una compromissione quasi totale del sistema.
- Identifica la zona con le vittime più colpite (Iran), parlando anche di Comodohacker ed il suo precedente attacco.

Sono stati identificati 531 certificati compromessi pubblicati.

- alcuni certificati non sono stati identificati e potrebbero essere stati utilizzati dallo stato;
- l'attacco ha permesso di eseguire *MitM attack* in larga scala sugli utenti iraniani di Gmail, impersonificando Google in tutti i browser che ritenevano valido il certificato **.google.com* distribuito da *DigiNotar*.
- sono stati prodotti certificati anche per altri domini importanti come Yahoo, Mozilla, Twitter, Microsoft e Android.

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

- L'attaccante aveva il pieno controllo di tutti gli 8 server della compagnia per la distribuzione di certificati;
- I file di log per individuare azioni sospette, salvati all'interno dei server compromessi, sono stati anch'essi manomessi.
- *DigiNotar* possedeva una rete interna altamente segmentata e separata dall'Internet pubblico.
- La società non aveva però applicato regole rigorose ai firewall nella propria rete; ciò avrebbe permesso all'intruso di spostarsi dal web server inizialmente compromesso, al server che ospita le autorità di certificazione.

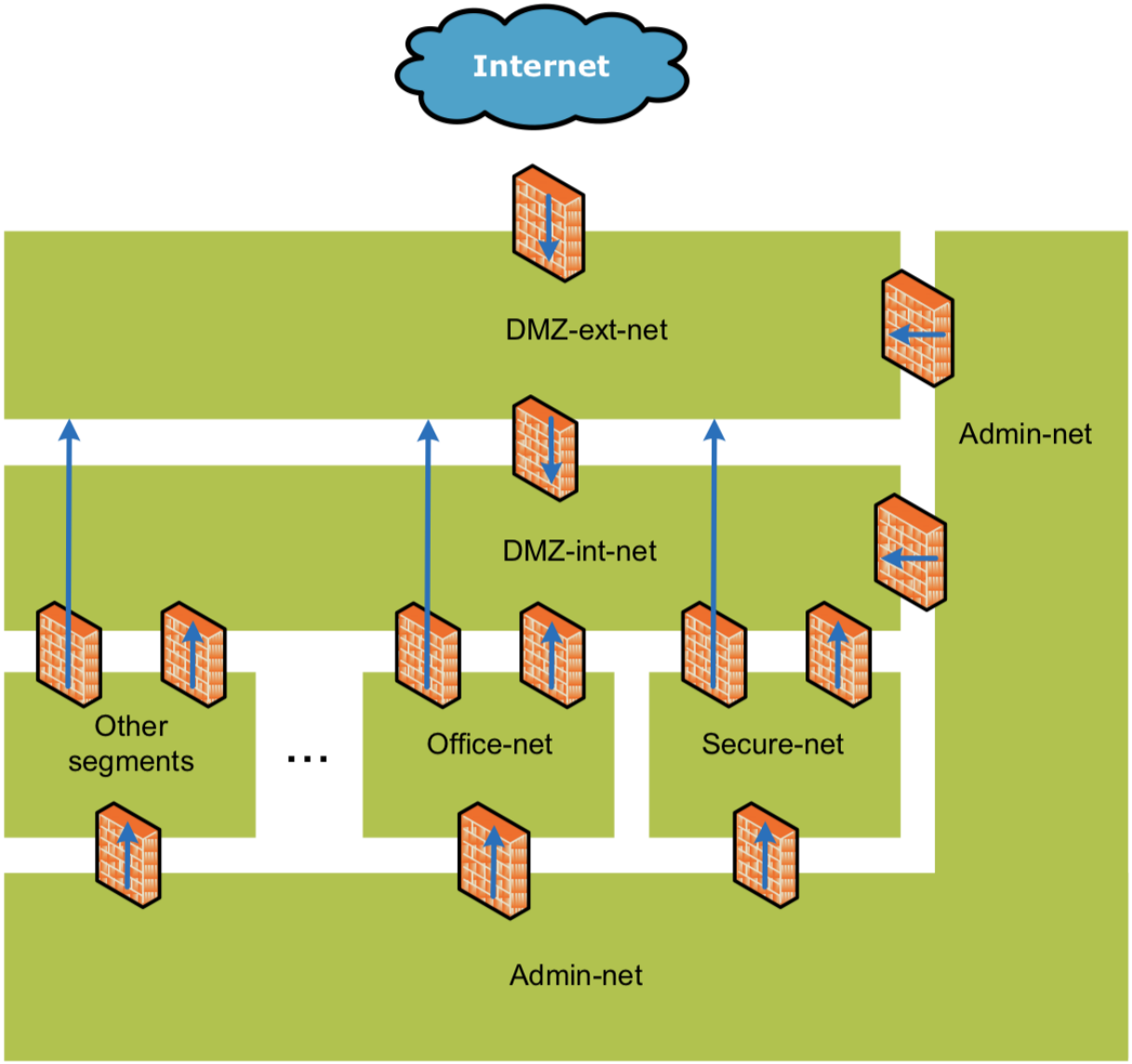


- L'indagine mostra che i server web nella zona demilitarizzata esterna (*DMZ-ext-net*) furono il primo punto di accesso per l'intruso il 17 giugno 2011, a causa delle vulnerabilità lasciate dai software non aggiornati.
- Tali server venivano usati per scambiare file tra sistemi interni ed esterni, con script utili come file manager rudimentali.
- Tra il 17 ed il 29 giugno vennero compromessi i sistemi nella Office-net e successivamente nella Secure-net (1 luglio): la sottorete che ospitava i server della *certificate authority*.
- Sono stati recuperati tool per creare tunnel che permettessero all'attaccante di creare una connessione con i sistemi interni.
- Furono recuperati anche password cracking tool.

- L'attaccante ha eseguito il tunnelling della connessione RDP (*Remote Desktop Protocol*), per ottenere una GUI (*Graphical User Interface*) sui sistemi compromessi, inclusi i server CA.
- A questo punto l'attaccante aveva il pieno controllo della rete, dei server CA, dei file di log e del database.
- Per emettere certificati falsi era anche necessario utilizzare una chiave privata attiva nel *netHSM (Hardware Security Module)*.
- Per attivare le chiavi private sono necessarie delle smartcard.
- Nei file di log però si trovano voci riguardo la generazione automatica di CRL (Certificate Revocation List); le CA le emettono a intervalli regolari secondo le politiche scelte.

- Questi CRL sono firmati dalle autorità emittenti e, per fare ciò, è necessario che la chiave privata sia attiva.
- Ciò dimostra che le chiavi private erano effettivamente attive, offrendo così l'opportunità all'attaccante di produrre e distribuire certificati fraudolenti, identici a quelli affidabili.
- Essendo indistinguibili, è necessario ritirare tutti i certificati forniti da *DigiNotar* e rimuovere la società dagli elenchi di fiducia di tutti i software.

Il report di Fox-IT
Network security zones

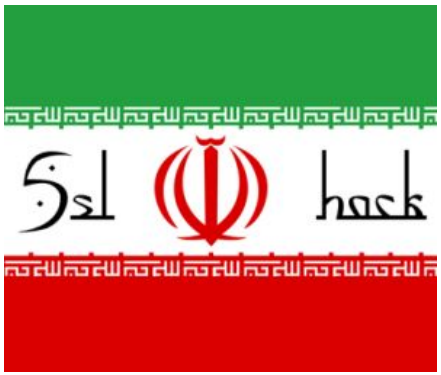


ComodoHacker

Il 5 settembre 2011 su *pastebin.com* appare un post pubblicato da *Comodohacker*, noto da qualche mese per un altro attacco.

- Comodohacker si fa chiamare *Ich Sun* ed è un ragazzo 21enne.
- È uno studente iraniano che sostiene il proprio governo e fa parte di un gruppo di hacker turchi.
- Afferma di aver attaccato *DigiNotar* volendo punire il governo olandese per le azioni svolte nel 1995 a Srebrenica, con 8000 musulmani uccisi durante la *Guerra in Bosnia ed Erzegovina*.

Nonostante le dichiarazioni, questa sembra essere soltanto una copertura escogitata dallo stato iraniano per evitare indagini.



Come detto, *Comodohacker* è già noto un altro attacco che prendeva di mira un'altra CA: *Comodo Group*.

- Il 15 marzo 2011 era riuscito compromettere un account con autorità di registrazione per poter creare un nuovo profilo.
- Con il nuovo account ha creato e pubblicato 9 certificati fraudolenti per 7 domini.
- Entro una settimana Comodo ha ripristinato la situazione revocando i certificati e incrementando le misure di sicurezza.
- L'attacco è stato fatto risalire ad un IP con origine a Teheran in Iran; subito si pensò ad un attacco guidato dallo stato (con il dubbio che l'origine fosse solo un falso indizio).
- Il 26 marzo Comodohacker rivendica l'attacco su *pastebin.com*.

Conclusione

Conclusione

Il disastro che coinvolse *DigiNotar* fu un doloroso campanello d'allarme per il mondo, non solo per il governo olandese.

- La violazione ha avuto notevoli ripercussioni in diverse parti del mondo, in particolare per gli utenti Gmail residenti in Iran.
- Attraverso Internet, le falle di sicurezza di un'azienda possono causare conseguenze terribili in altre parti del mondo.
- Anche le autorità di certificazione sulle quali si basa la fiducia mondiale a livello di rete possono essere vittime di attacchi.
- Non deve essere ammissibile nessun tipo di negligenza a livello di sicurezza interna da parte di queste compagnie.