Introduction and Security Challenges

Indian Computer Emergency Response Team
Department of Information Technology
Ministry of Communications & Information Technology
New Delhi

Ruchi Gola,Scientist-C
ruchi@cert-in.org.in

Top Security Trends & Threats for 2012

- **Mobile devices & Applications** — a new vector for attacking the network and critical systems.
- **APTs** and merger of Cyber Threats with Physical and Critical Infrastructure
- **SSL** Gets Caught in the Crossfire
- **DDoS** Moves Up the Stack

“mobile Internet devices”

- - iPhones, BlackBerry devices, Android phones, Windows Mobile devices, etc. -- pocket size devices that can access the Internet via cellular/3G/4G, WiFi, etc.

- -tablet computers such as the iPad/iPad2 ,conventional laptops, regular cell phones, etc

Attacks dealt with mobiles

- Many mobile Internet apps, not just Opera Mini, rely on services provided by back end servers -- sometimes servers which run locally, othertimes servers which run "in the cloud."

- If those servers go down, your service may be interrupted. This is a real risk and has happened multiple times to BlackBerry users; some examples include:
  -- "International Blackberry Outage Goes Into Day 2," March 9th, 2010, http://tinyurl.com/intl-outage-2nd-day
  -- "BlackBerry users hit by eight-hour outage," December 23rd, 2009, www.cnn.com/2009/TECH/12/23/blackberry.outage/index.html
  See http://www.dataoutagenews.com/ for more outages.
- **Email On Your Mobile Device May Be Routinely Monitored, At Least In Some Jurisdictions-----**India is the canonical example of this, heavily pressuring Research In Motion to provide email intercept solutions for traffic involving BlackBerries in India.

Beware *Fake* Jailbreaking Apps

Fake iPhone jail-breaking tool packed with malware

http://www.zdnet.com/blog/security/fake-iphone-jail-breaking-tool-packed-with-malware/7381

Fake iPhone jail-breaking tool packed with malware

By Ryan Naraine | September 20, 2010, 10:51pm PDT

Summary

Malicious hackers are preying on iPhone users who want to jail-break their devices, exploiting the increased interest around jail-breaking tools to launch malware attacks.

Topics

Apple iPhone, Malware, Ryan Naraine, Tool, Spyware, Adware & Malware, Smart Phones, Cyberthreats, Hacking, Productivity, *more +*

Blogger Info

Ryan Naraine
Bio Contact

Dancho Danchev
Bio Contact

Malicious hackers are preying on iPhone users who want to jail-break their devices, exploiting the increased interest around jail-breaking tools to launch malware attacks.

According to Kaspersky Lab's Costin Raiu (see disclosure), a rumored jail-breaking utility for iPhone 4 comes with a nasty surprise:

> *Cybercriminals have definitely been riding the buzz around the supposed jailbreaking tool. It's presumed to be called "Greenpois0n" and it's expected to be released any day now. Not surprisingly, we've seen a number of fake "Greenpois0n" Trojans.*
>
> *If you search for the Greenpoison on torrent sites you might be in for a surprise:*

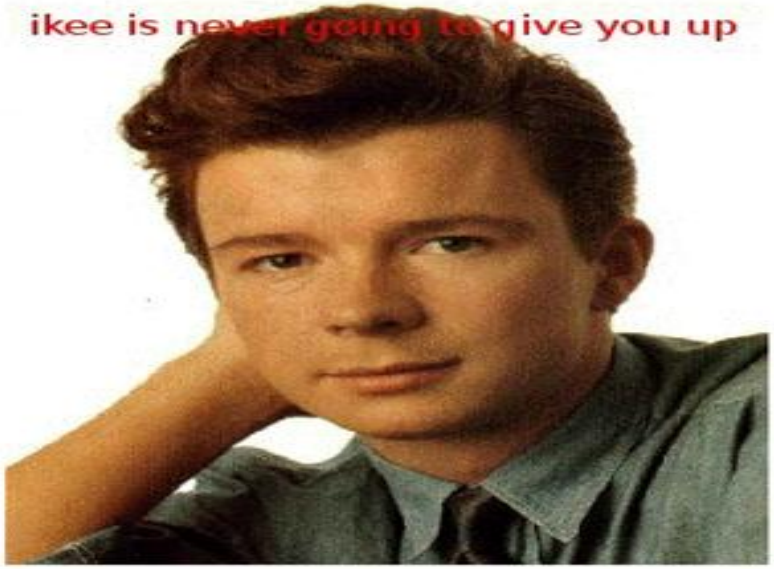
Raiu said all the existing "greenpois0n" archives at the moment contain Trojans designed to steal passwords and other private data from infected systems.

The “ikee” Worm

Ikee Worm Rickrolls Jailbroken iPhones | Symantec Connect

http://www.symantec.com/connect/blogs/ikee-worm-rickrolls-jailbroken-iphones

Many users who have jailbroken their iPhones in order to customize them have not changed their SSH password, allowing others to log in to their phone. In the case of Ikee, the worm scans random IP ranges and also specifically targets Optus, Vodafone, and Telstra's IP ranges, which are the common telephony providers in Australia. Once a vulnerable iPhone is found, the worm changes the wallpaper to a picture of Rick Astley (a prank known as Rickrolling), deletes the SSH daemon, and begins scanning the network for other vulnerable phones. Note that some of these telephony networks use NAT (network address translation)—such that iPhones may not actually be reachable by Ikee's scans.

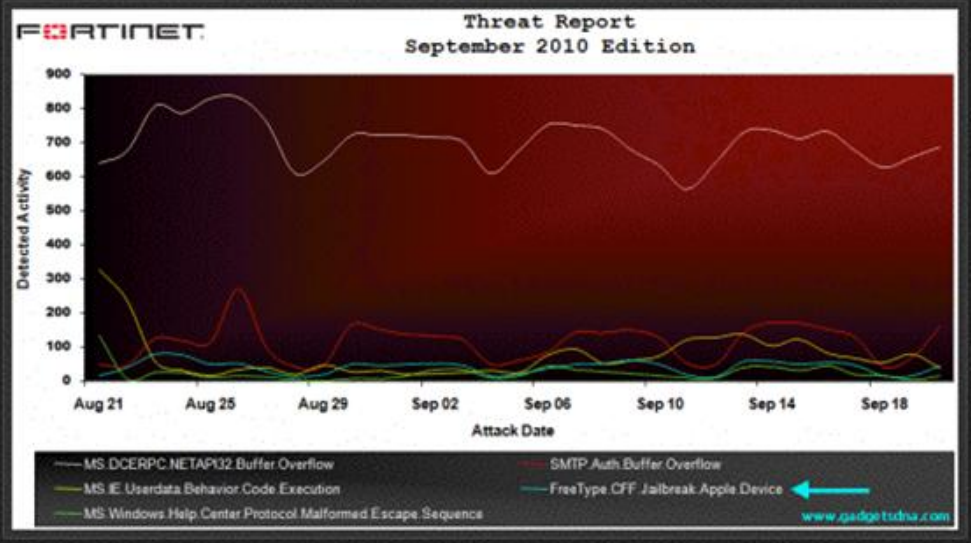


Unfortunately, the first variant worm also had a slight bug. This bug can cause the background of an infected user’s iPhone to be picked up and sent to new infections, instead of the picture of Rick Astley. Later variants of the worm corrected this problem.

PDF Vulnerabilities on the iPhone

PDF Vulnerability Being Used For Malicious Purposes On iPhone iOS

By _GadgetNews - October 3, 2010



The security firm Fortinet has shown a new vulnerability (CVE-2010-2972) that is being used to exploit jailbroken Apple iPhones leveraging the PDF file format. A few weeks back, Apple fixed the security vulnerability (CVE-2010-1797) associated with viewing malicious PDF files in iOS 4.0.2 and iPad 3.2.2 firmwares.

The problem lies in the Compact Font Format, which is supported in popular document formats such as PDF. The interesting aspect here though is that this it is often used intentionally to jailbreak devices. However, as with any vulnerability, a scenario could exist where an attacker could jailbreak a phone for malicious purposes. The exploit **FreeType.CFF.Jailbreak.Apple.Device.Buffer.Overflow** jumped into fourth position in **last month report**.

More than 600,000 Macs infected with Flashback botnet

Russian antivirus company says half the computers infected with malware designed to steal personal information are in the U.S. -- with 274 located in Cupertino.

by Steven Musil | April 4, 2012 6:25 PM PDT

Advanced Persistent Threats

.

- --> Some nation-state sponsored attacks are targeting corporations specifically for their **intellectual property, sensitive business negotiations and national security designs and technology.**

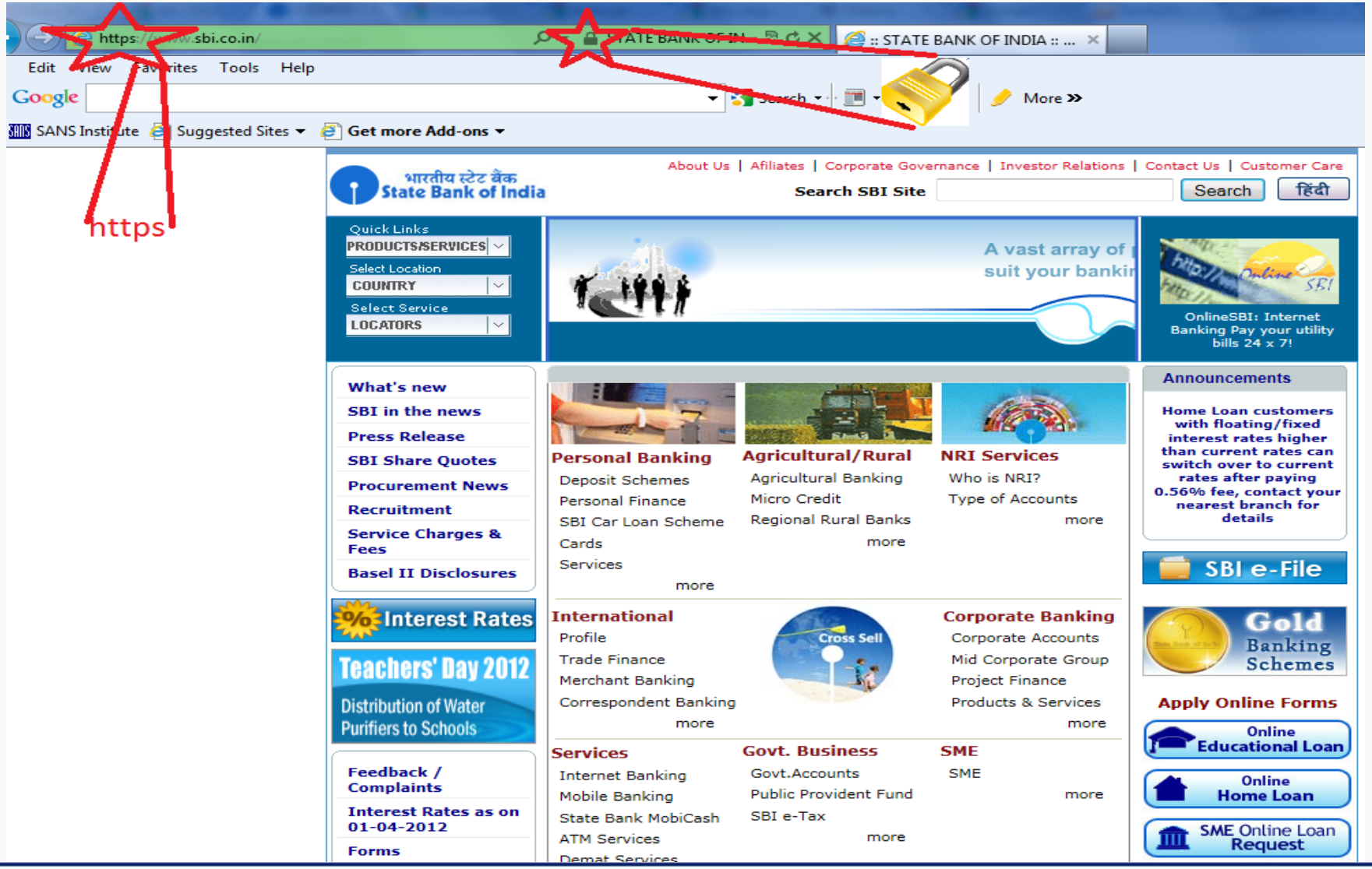
- --> **Operation Aurora, Night Dragon and Shady Rat** are all examples of critical industries being victimized by targeted, persistent cyber attacks

- --> The adversaries behind these attacks were able to **exfiltrate design sche-matics and sensitive field negotiations for new oil and gas explora-tion.**

- --> These threats are, **strategic in nature**. They require a high level of sophistication far beyond the rudimentary skills of hacktivists. Since the goal is to remain covert, they must involve a lot of testing resources to obfuscate the source of the attack."

SSL Trust Gets Caught in the Crossfire

Motivation behind the use of SSL



Weaknesses in SSL certification exposed by Comodo security breach

news.cnet.com/8301-31921_3-20048525-281.html

Search | YouTube Downloader | Updated Software | Video | Weather

FBI probes Comodo Web security breach

FBI and Italian police investigate how hacker managed to convince N.J. security firm to issue it digital certificates for Google, Yahoo, Microsoft, other major Web sites.

by Declan McCullagh | March 29, 2011 4:07 PM PDT

Follow

The FBI is investigating how a hacker tricked a New Jersey company into issuing fraudulent digital certificates for Google, Yahoo, Microsoft, and other major Web sites, the firm's chief executive said today.

Comodo CEO Melih Abdulhayoglu told CNET this afternoon that "it is an ongoing investigation" that has drawn in both the FBI and Italian law enforcement.

IP Address Location	
IP Address	212.95.136.18
City	Tehran
State or Region	Tehran
Country	Iran, Islamic Republic of
ISP	Pishgaman TOSE Ertebatat Tehran Network.
Latitude & Longitude	35.696111 51.423056

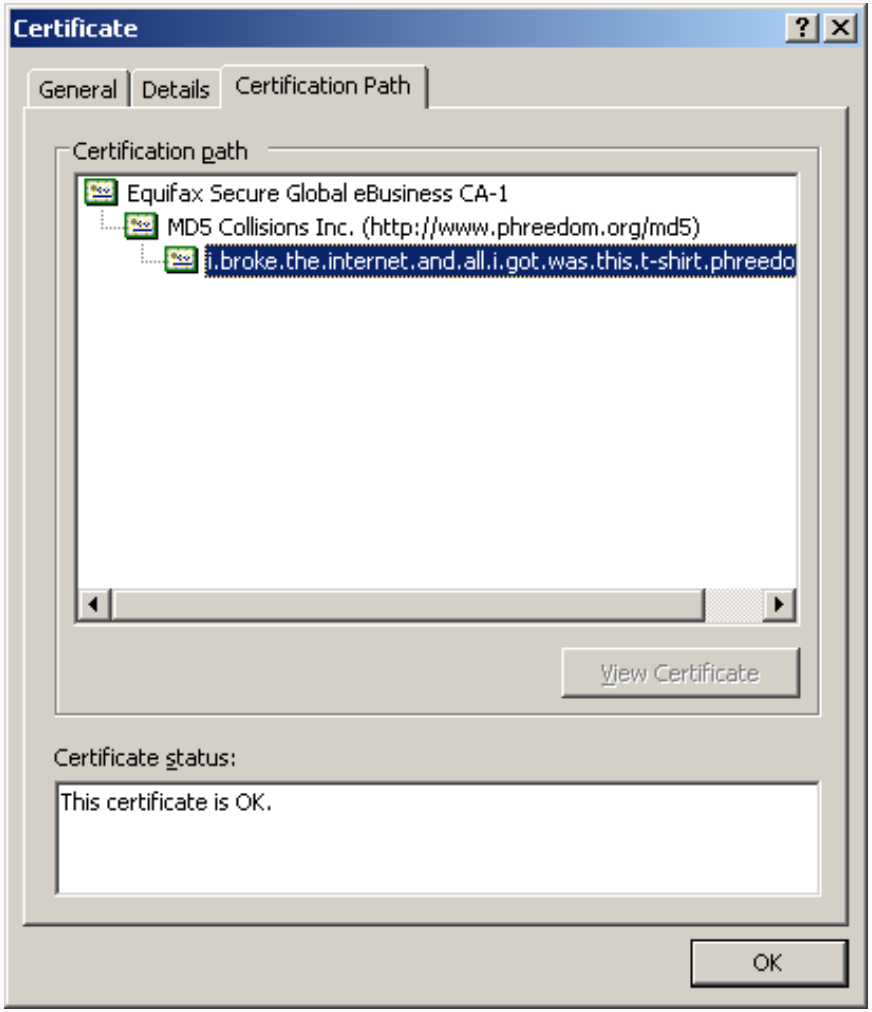
Compromise related to fraudulent digital certificates is traced to IP addresses in Iran, Comodo says.
(Credit: Comodo)

Abdulhayoglu confirmed that a reseller in Italy called GlobalTrust had its network compromised by a hacker traced to Iran. That person, or multiple people, obtained fake digital certificates for nine Web sites that also included Skype and Mozilla. Those certificates, which have since been revoked, allowed someone to impersonate the secure versions of those Web sites--the ones that are used when encrypted connections are enabled.

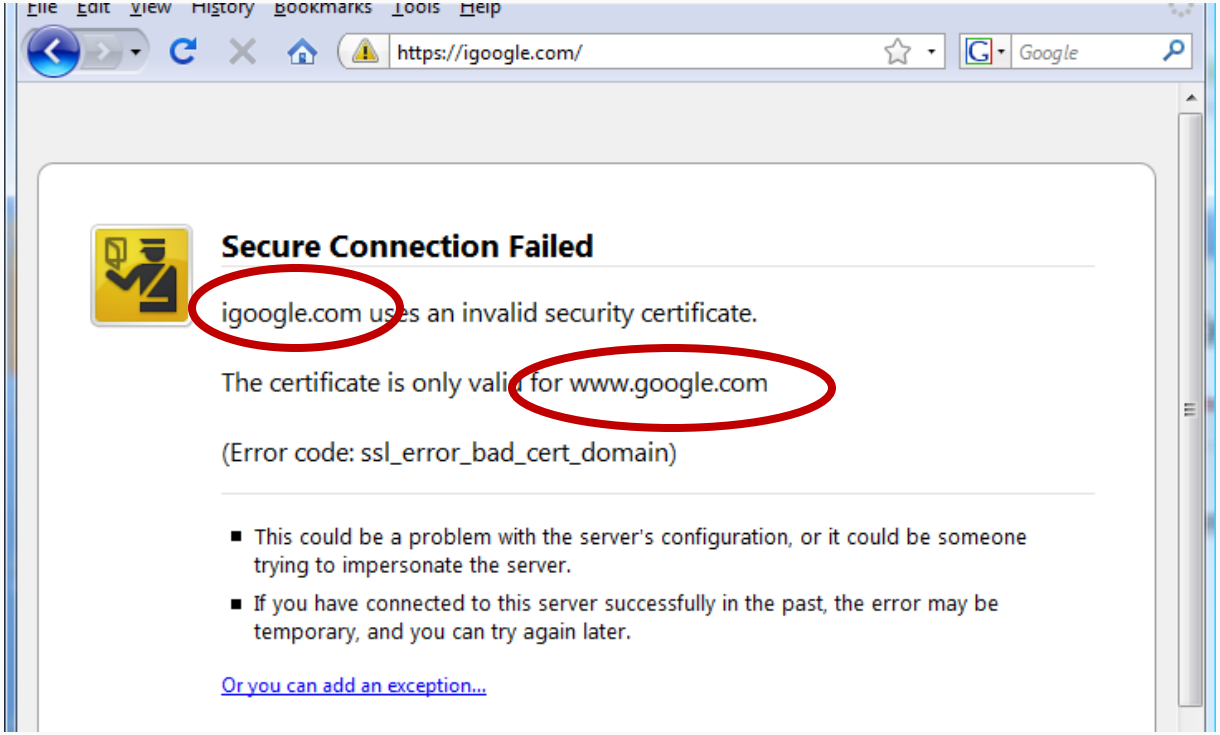
"We're letting the government agencies handle the issue and figure out what exactly has happened here," Abdulhayoglu said.

The FBI did not immediately respond to a request for comment.

A Rogue Certificate



Invalid Certificate Warning



- Four clicks to get Firefox 3 to accept certificate
- Page is displayed with full HTTPS indicators

Comodo

- Comodo is one of the trusted CAs
  - Its certificates for any website in the world are accepted by every browser
- Comodo accepts certificate orders submitted through resellers
  - Reseller uses a program to authenticate to Comodo and submit an order with a website name and public key, Comodo automatically issues a certificate for this site

COMODO
Creating Trust Online®

Comodo Break-In

- Iranian hacker broke into instantSSL.it and globalTrust.it resellers, decompiled their certificate issuance program, learned credentials of their reseller account and Comodo API
  - username: gtadmin, password: globaltrust
- Wrote his own program for submitting orders and obtaining Comodo certificates
- On March 15, 2011, got Comodo to issue 9 rogue certificates for popular sites
  - mail.google.com, login.live.com, login.yahoo.com, login.skype.com, addons.mozilla.org, “global trustee"

Consequences

- Attacker needs to divert users to an attacker-controlled site instead of Google, Yahoo, Skype (connection hijacking), but then…
  - For example, use DNS to poison the mapping of mail.yahoo.com to an IP address
- … “authenticate” as the real site
- … decrypt all data sent by users
  - Email, phone conversations, Web browsing

Q: Does HTTPS help?

Message from Attacker

http://pastebin.com/74KXCaEZ

I'm single hacker with experience of 1000 hacker, I'm single programmer with experience of 1000 programmer, I'm single planner/project manager with experience of 1000 project managers …

When USA and Isarel could read my emails in Yahoo, Hotmail, Skype, Gmail, etc. without any simple little problem, when they can spy using Echelon, I can do anything I can. It's a simple rule. You do, I do, that's all. You stop, I stop. It's rule #1 …

Rule#2: So why all the world got worried, internet shocked and all writers write about it, but nobody writes about Stuxnet anymore?... So nobody should write about SSL certificates.

Rule#3: I won't let anyone inside Iran, harm people of Iran, harm my country's Nuclear Scientists, harm my Leader (which nobody can), harm my President, as I live, you won't be able to do so. as I live, you don't have privacy in internet, you don't have security in digital world, just wait and see...

DigiNotar Break-In

- In June 2011,same “ComodoHacker”

broke into a Dutch certificate authority, DigiNotar

  - Message found in scripts used to generate fake certificates:

    “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"

- Security of DigiNotar servers
  - All core certificate servers in a single Windows domain, controlled by a single admin password (Pr0d@dm1n)
  - Software on public-facing servers out of date, unpatched
  - Tools used in the attack would have been easily detected by antivirus… if it had been present

Consequences of DigiNotar Hack

- Break-in not detected for a month
- Rogue certificates issued for *.google.com, Skype, Facebook, www.cia.gov, and 527 other domains
- 99% of revocation lookups for these certificates originated from Iran
  - Evidence that rogue certificates were being used, most likely by Iranian government or Iranian ISPs to intercept encrypted communications
    - Man-in-the-middle attack using DNS poisoning
  - 300,000 users were served rogue certificates

Another Message from Attacker

http://pastebin.com/u/ComodoHacker

Most sophisticated hack of all time … I'm really sharp, powerful, dangerous and smart!

My country should have control over Google, Skype, Yahoo, etc. […] I'm breaking all encryption algorithms and giving power to my country to control all of them.

You only heards Comodo (successfully issued 9 certs for me -thanks by the way-), DigiNotar (successfully generated 500+ code signing and SSL certs for me -thanks again-), StartCOM (got connection to HSM, was generating for twitter, google, etc. CEO was lucky enough, but I have ALL emails, database backups, customer data which I'll publish all via cryptome in near future), GlobalSign (I have access to their entire server, got DB backups, their linux / tar gzipped and downloaded, I even have private key of their OWN globalsign.com domain, hahahaa).... BUT YOU HAVE TO HEAR SO MUCH MORE! SO MUCH MORE! At least 3 more, AT LEAST!

DDoS Moves Up the Stack

- **Compared to Q2 2011**
- 50 percent increase in total number of DDoS attacks
- 11 percent increase in infrastructure (Layer 3 & 4) attacks
- Shorter attack duration: 17 hours vs. 26 hours
- 63 percent higher packet-per-second (pps) volume
- 55 percent decline in average attack bandwidth
- **Compared to Q1 2012**
- 10 percent increase in total number of attacks
- 8 percent rise in Layer 3 and 4 infrastructure attacks
- Average attack duration declines to 17 hours from 28.5

Q2 2012 DDoS Attack Report

- **Q1 2012 – Financial services firms get hammered**
  Prolexic logged a significant increase in attack traffic directed at financial services clients.
- **Q4 2011 – Attacks become more concentrated and damaging**
  Prolexic recorded a dramatic rise in packet-per-second volume this quarter and significant attack activity against e-Commerce businesses.
- **Q3 2011 – DDoS attackers change strategies**
  Prolexic saw changing tactics where attackers were starting to target the DDoS mitigation infrastructure directly, specifically routers, most of which do not have the capacity to process high packets-per-second attacks.

Thank you