Stuxnet

Justina Choi, Kyle Holzinger, Timothy Lau

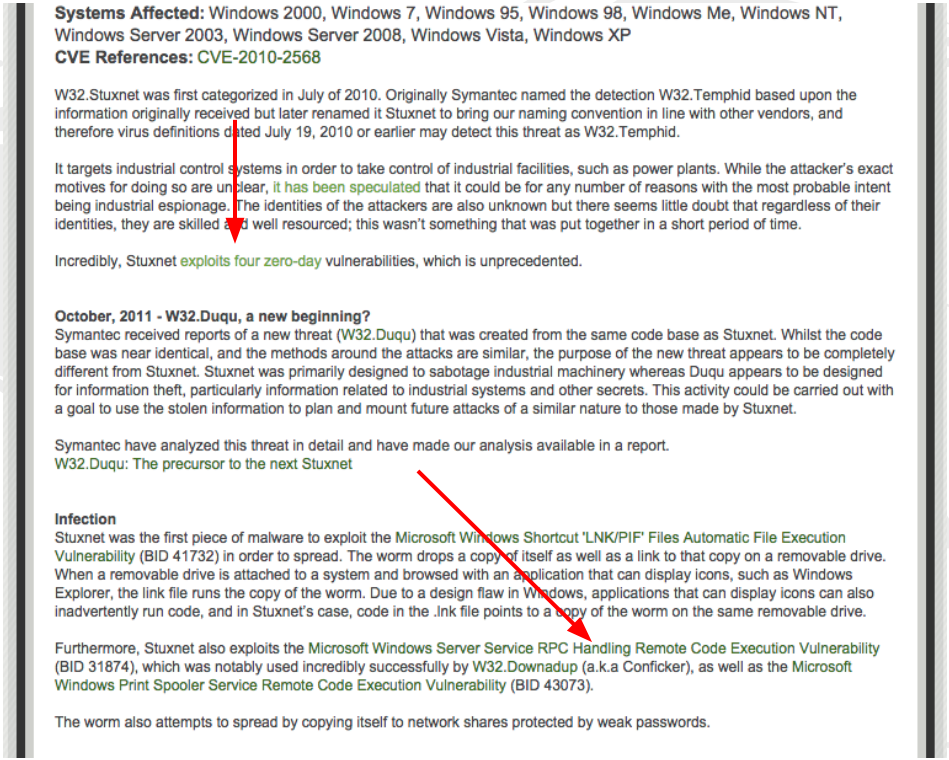
Background

- Who wrote it?
- What does it do?
- Who was affected?

Technical Issues - Spread

- used a valid signed certificates stolen from two Taiwanese hardware makers
  - RealTek and JMicron were both headquartered in the the same business park
- nothing spread through internet, all LAN
- 4 zero-day vulnerabilities
- updates online to two command-and-control servers and P2P

Lies!



Systems Affected: Windows 2000, Windows 7, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Server 2008, Windows Vista, Windows XP
CVE References: CVE-2010-2568

W32.Stuxnet was first categorized in July of 2010. Originally Symantec named the detection W32.Temphid based upon the information originally received but later renamed it Stuxnet to bring our naming convention in line with other vendors, and therefore virus definitions dated July 19, 2010 or earlier may detect this threat as W32.Temphid.

It targets industrial control systems in order to take control of industrial facilities, such as power plants. While the attacker's exact motives for doing so are unclear, it has been speculated that it could be for any number of reasons with the most probable intent being industrial espionage. The identities of the attackers are also unknown but there seems little doubt that regardless of their identities, they are skilled and well resourced; this wasn't something that was put together in a short period of time.

Incredibly, Stuxnet exploits four zero-day vulnerabilities, which is unprecedented.

October, 2011 - W32.Duqu, a new beginning?
Symantec received reports of a new threat (W32.Duqu) that was created from the same code base as Stuxnet. Whilst the code base was near identical, and the methods around the attacks are similar, the purpose of the new threat appears to be completely different from Stuxnet. Stuxnet was primarily designed to sabotage industrial machinery whereas Duqu appears to be designed for information theft, particularly information related to industrial systems and other secrets. This activity could be carried out with a goal to use the stolen information to plan and mount future attacks of a similar nature to those made by Stuxnet.

Symantec have analyzed this threat in detail and have made our analysis available in a report.
W32.Duqu: The precursor to the next Stuxnet

Infection
Stuxnet was the first piece of malware to exploit the Microsoft Windows Shortcut 'LNK/PIF' Files Automatic File Execution Vulnerability (BID 41732) in order to spread. The worm drops a copy of itself as well as a link to that copy on a removable drive. When a removable drive is attached to a system and browsed with an application that can display icons, such as Windows Explorer, the link file runs the copy of the worm. Due to a design flaw in Windows, applications that can display icons can also inadvertently run code, and in Stuxnet's case, code in the .lnk file points to a copy of the worm on the same removable drive.

Furthermore, Stuxnet also exploits the Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability (BID 31874), which was notably used incredibly successfully by W32.Downadup (a.k.a Conficker), as well as the Microsoft Windows Print Spooler Service Remote Code Execution Vulnerability (BID 43073).

The worm also attempts to spread by copying itself to network shares protected by weak passwords.

Zero Day Attacks

- Never before seen
- Usually very obscure
- In this case, actual bugs in Windows

Infecting a USB

- Creates a new hidden window “AFC64c313”
- Gets notified of any new USB being plugged in, waits for “WM_DEVICECHANGE”
- Writes 6 files into flash memory drive

Infection by USB

- LNK vulnerability: CVE-2010-2568(MS-10-046) - Windows Shell LNK Vulnerability
- Special file called CPL - Control Panel Applications
- Explorer calls an API named “Shell32.LoadCPLModule” which then calls a library which then executes wtr4141.tmp
- First file infects File Management APIs
- Inserts code to hide files with the same name as the Stuxnet files
- Moves the second DLL file onto infected machine

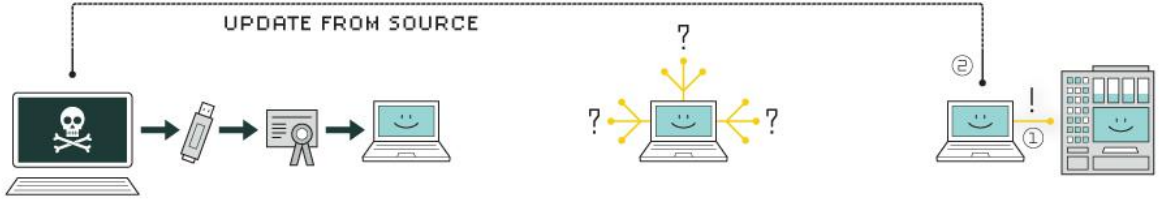
Infection By Network

- CVE-2010-2729(MS-10-061) Windows Print Spooler Service Vulnerability
- Allowed a guest account to communicate over printer network and write files
- Using API ‘GetSpoolFileHandle’, you can get the file handle of the new file
- Once the file is inserted, one can easily use ReadFile and WriteFile APIs to copy infected files over

Technical Issues - Effect

- Specifically targeted computers with Siemens SIMATIC WinCC/Step 7 controller software
- Connect to command-and-control servers
- Exploits Programmable Logic Controller
- Targeted Iranian centrifuges

HOW STUXNET WORKED



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

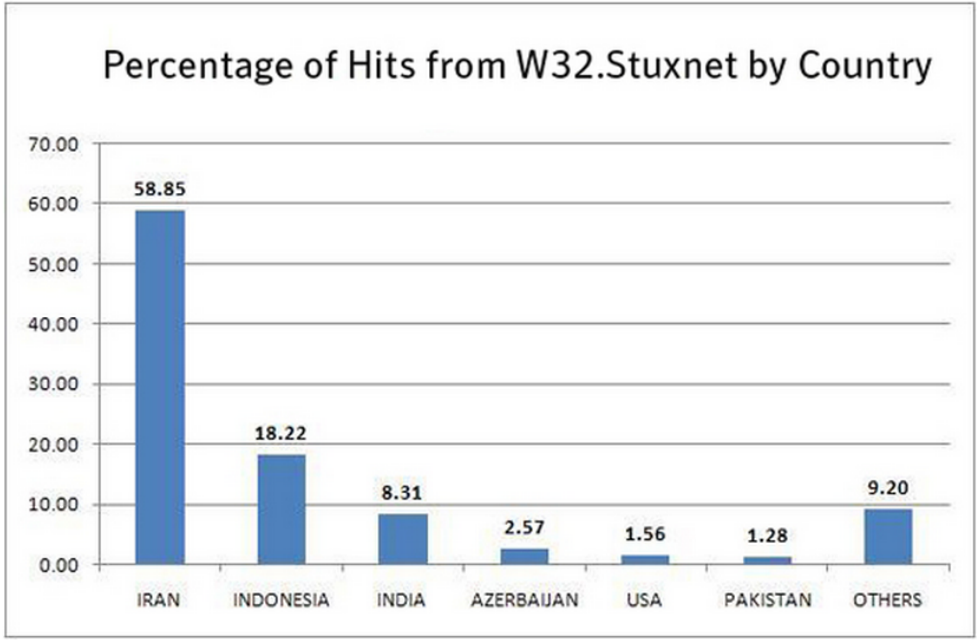
6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Prevention

- UPDATE SOFTWARE!! - Microsoft fixed vulnerabilities
- Turn off guest account access to print spooler
- Turn off autoplay and don’t use untrusted USBs

Incentives

- If US was the attacker: Iran targeted because didn't want Iran to have nuclear facilities
- Other theories



Legal or Ethical Issues

- without attribution -> no consequences
- If U.S./Israel: first state-sponsored cyber attack
- purposely created for sabotage
- “Cyber War”
  - cyber space as new domain of warfare
  - cheaper, faster, easier

Sources

- http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet
- http://krebsonsecurity.com/2015/03/microsoft-fixes-stuxnet-bug-again/
- http://foreignpolicy.com/2013/03/20/if-we-dont-want-to-be-like-the-iranians-and-get-stuxnetted-take-these-4-steps/
- https://www.schneier.com/blog/archives/2010/10/stuxnet.html
- http://arstechnica.com/tech-policy/2011/07/how-digital-detectives-deciphered-stuxnet-the-most-menacing-malware-in-history/
- http://rdist.root.org/2011/01/17/stuxnet-is-embarrassing-not-amazing/
- http://www.darkreading.com/vulnerabilities---threats/our-governments-are-making-us-more-vulnerable/a/d-id/1319147
- http://www.symantec.com/connect/pt-br/blogs/w32stuxnet-installation-details
- http://www.securityfocus.com/bid/41732/exploit