Sarah Walterman, Liz Ottati, Hamad Mohammed
Business Information Systems- Cybersecurity Term Project
Stuxnet Virus

The Stuxnet Virus was discovered in June 2010; however, it is said that the development started as early as 2005. It is a "500-kilobyte computer worm that infected the software of at least 14 industrial sites in Iran."[9] Malware exists in many forms, that is, worms, scareware, Trojans, spyware, and adware. Each of these programs has a unique way of compromising the way a computer functions. Over the years, there have been malware programs reported as threats to networks. As an instance, Stuxnet is one such malware existing in PCs.

While it's not known exactly who created Stuxnet, the most realistic guess is that the United States and Israel worked together to make it. The original purpose was to "derail, or at least delay, the Iranian program to develop nuclear weapons."[8] Most worms are created to just infect a computer, but Stuxnet was created to cause "real-world physical effects."[8] Developers of the malware made it in such a way that it attacks devices that meet a specific requirement. The worst-hit country was Iran. The state's top companies, especially those dealing with uranium infrastructure, were infected by Stuxnet.[10] Stuxnet is believed to be spread using flash drives.

"Stuxnet, as it came to be known, was unlike any other virus or worm that came before. Rather than simply hijacking targeted computers or stealing information from them, it escaped the digital realm to wreak physical destruction on equipment the computers controlled."[6] It was programmed to make the nuclear plant's centrifuges spin faster than they were meant to and it eventually destroys them. The worm moved through the use of USBs in purposely infected computers.[7]

The Stuxnet virus is an incredibly complex piece of malware with layers of operational conditions, capabilities, and safeguards including zero-day exploits, a Windows rootkit, the first

ever PLC rootkit, antivirus evasion, security response techniques, complex process injection and hooking code, network infection routines, peer-to-peer updates, and a command and control interface.[3] Essentially, it functioned like so: "one component was designed to send Iran's nuclear centrifuges spinning wildly out of control… the computer program also secretly recorded what normal operations at the nuclear plant looked like, then played those readings back to plant operators, like a pre-recorded security tape in a bank heist, so that it would appear that everything was operating normally while the centrifuges were actually tearing themselves apart."[5] A variety of safeguards were in place within the malware: It only infected three computers from a given infected flash drive and is hardcoded to stop spreading itself after June 24, 2012.[4] It also only attacked very specific technology responsible for critical infrastructures in the Iranian nuclear research facilities. In all other instances of infected hardware, the worm lies dormant. It accomplished this by looking for a particular model of Programmable Logic Controller made by Siemens. Research suggests that the Stuxnet virus had an extensive list of features to ensure the cyber-attack was successful with little collateral damage. According to the authors of W32 Stuxnet Dossier, these include (in their unadulterated jargon):

- Self-replicates through removable drives exploiting a vulnerability allowing auto-execution.
- Microsoft Windows Shortcut 'LNK/PIF' Files Automatic File Execution Vulnerability (BID 41732)
- Spreads in a LAN through a vulnerability in the Windows Print Spooler.
- Microsoft Windows Print Spooler Service Remote Code Execution Vulnerability (BID 43073)
- Spreads through SMB by exploiting the Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability (BID 31874).
- Copies and executes itself on remote computers through network shares.
- Copies and executes itself on remote computers running a WinCC database server.
- Copies itself into Step 7 projects in such a way that it automatically executes when the Step 7 project is loaded.
- Updates itself through a peer-to-peer mechanism within a LAN.

- Exploits a total of four unpatched Microsoft vulnerabilities, two of which are previously mentioned vulnerabilities for self-replication and the other two are escalation of privilege vulnerabilities that have yet to be disclosed.
- Contacts a command and control server that allows the hacker to download and execute code, including updated versions.
- Contains a Windows rootkit that hide its binaries.
- Attempts to bypass security products.
- Fingerprints a specific industrial control system and modifies code on the Siemens PLCs to potentially sabotage the system.
- Hides modified code on PLCs, essentially a rootkit for PLCs.[3]

The three primary structural components are a worm, an .LNK file, and a rootkit. "The worm executes all routines related to the main payload of the attack. It uses certain vulnerabilities for its propagation and execution of certain routines. It implements a Microsoft Remote Procedure Call to execute certain functions, enabling affected systems to communicate with one another. It also tests for an active Internet connection on the affected system to communicate with a remote server. It is also the component responsible for attempting to access a database consistent with one used in Siemens WinCC systems."[2] The "specially crafted .LNK file automatically executes the propagated copies of WORM_STUXNET. It exploits a vulnerability in the way Windows displays the icons of shortcut files and is basically employed by STUXNET for automatic execution."[2] The "rootkit component is mainly responsible for hiding all malicious files and processes. This is done in order to keep the infection from being traced by the user."[2] It propagated via three unpatched vulnerabilities which have since been patched, or made harder to become infected; and two additional still unpatched vulnerabilities which allowed Stuxnet to be recognized as a computer administrator.

Given its capabilities, Stuxnet's origin is still unknown. The common belief about its source is that the Israel and US intelligence organizations joined forces to build the malware. Further, reports indicate that the worm's development has been ongoing in both President Bush

and Obama's eras. Additionally, the malware was intended to delay Iran's nuclear weapon advancements. Through derailments, the US government administrators believed that a war between Israel and Iran would be prevented. Stuxnet was only intended to affect the Iranian nuclear plant in Natanz.

The attacks were not fully successful: Some parts of Iran's operations ground to a halt, while others survived, according to the reports of international nuclear inspectors. Nor is it clear the attacks are over: Some experts who have examined the code believe it contains the seeds for yet more versions and assaults.[1]

Iran refused to reveal the extent of the damages caused by the attack or their method of removal but Siemens has since released anti-virus software for the technology which was collaterally infected and still contains the dormant version of the Stuxnet virus.

Bibliography

[1]https://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html#23f29f3e51e8

[2]https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/54/stuxnet-malware-targets-scada-systems

[3]http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[4]https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf

[5]https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1&ref=general&src=me&pagewanted=all

[6]https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

[7] Franceschi-Bicchierai, 2016

[8] Fruhlinger, 2017

[9] Kushner, 2013

[10] Combs, 2011

Franceschi-Bicchierai, L. (2016, August 9). *The History of Stuxnet: The World's First True Cyberweapon*. Retrieved from Motherboard: https://motherboard.vice.com/en_us/article/ezp58m/the-history-of-stuxnet-the-worlds-first-true-cyberweapon-5886b74d80d84e45e7bd22ee

Fruhlinger, J. (2017, August 22). *What is Stuxnet, Who Created It, and How Does it Work*. Retrieved from CSO: https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html

Kushner, D. (2013, February 23). *The Real Story of Stuxnet*. Retrieved from IEEE Spectrum: https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

Combs, Marcia M. "Impact of the Stuxnet Virus on Industrial Control Systems." XIII International Forummodern Information Society Formation Problems, Perspectives, Innovation Approaches (2011): 5-10.