Stuxnet is a type of malware computer worm denotified “Malworm” that made an appearance in 2010. It was discovered by the antivirus company VirusBlokAda. The malicious software was “Trojan-Spy.0485” and “Malware-Cryptor.Win32.Inject.gen.2”, the intention was to use a USB device for propagation. It means that all it requires was to insert a USB device to infiltrate the target. In simple terms, the way it works was using an exploit in Windows Shell.

“The Icon loading vulnerability” in Microsoft: On Windows systems loading an icon file uses “**.LNK**” as a shortcut to the original source path. When an existing shortcut is loaded it runs from a library known as “**DLL**” (Dynamic Link Libraries) a library that contains functions, resources such as icons, images, and files. When “**DLL**” loads it will call for Windows API(*Win32*) known as “**LoadLibrary”** from the Windows Control Panel, where users can configure system-level tasks. The Control Panel considered items you have to be installed in one or another way. When prompted it's too trusting of what is installed as a Control Panel item.

Many USB controllers are “**DMA**” (Direct Memory Access) devices that bypass Operating System security that directly read & write memory on the computer. Now imagine when a USB containing the malicious software is being plugged in, Windows by default will initiate “**autorun.inf”** a configuration set to automatically run the driver thus “creating” the environment for the “Malworm” to operate.

The Stuxnet was made of different sophisticated malware such as Trojan Horse, Computer Worm, and Rootkit. Trojan Horse(malware) being insidious may perform as normal, but running malicious tasks in secret. The payload can be like granting user access rights(Control Panel) without any signs of notification. While Computer Worm will propagate without human interaction and will spread by self-replication. Once the worm infests the system it also survives a system reboot by modifying *Windows Registry(database for system startup).* The latter described being “**mrxnet.sys”** and “**mrxcls.sys**” hides and injects from the USB. Like the names mentioned in the beginning, it implies Trojan and Win32-Inject are placed in the “*%SystemRoot%\System32\drivers*” directory.

Another thing was the malworm driver hide these malicious codes being “**~wtr4132.tmp**” and “**~wtr4141.tmp**”. Both of these contained a genuine Digital Certificate by two companies respectively, *JMicron* and *Realtek* in Taiwan, later revoked by the US company *Verisign*. That’s why the corrupted driver could gain access to kernel-mode (system-level) without the user being notified. This was later identified as “**Rootkit.Tmphider**” & “**SScope.Rookit.TmpHider.2**” by Sergey Ulasen. He gradually discovered that this type of malware was nothing like the ordinary, but something more sinister. Information spread fast amongst infosec forums and controversies about this being not a big concern unless it was targeting Nuclear power plants.

Frank Boldewin another researcher pointed out it was targeting specific hardware like Siemens PLC*(Programmable Logic Controllers)*, WinCC SCADA system, operating on Microsoft Windows machines. These PLCs operate automation of machines at an industrial scale that controls power plants. A report shows that most of the infected system was nuclear facilities at Bushehr and Natanz in Iran. The compromised machines were strategically sabotaged. Operational centrifuges rotors that enrich “u-235” were self-destructive.

Speculations show that compromised computers with Stuxnet inject with a technique, a “**Step 7**” basically hide from the user and create copies and repeat. One of the exploits checks for a value equal to “**19790509**” if valid the code will exit which means the computer has already been marked as infected. If by coincidence the value might refer to the death of a jewish political person. Stuxnet used string with names that potentially have significant meaning. One file named “**Guava**” in this *path: “b:\***myrtus***\src\objfre_w2k_x86\i386 \***guava***.pdb”* could lead to several possible meanings. In Latin guava plant in myrtle(Myrtus) family. MyRTUs could be standing for RTU which is a synonym for similar PLCs in some environments. While in Hebrew it may be an allusion to the Jewish Queen *Esther*, her original name was *Hadassah,* which means myrtle. In the *Book of Esther,* her salvation saved her people from dying.

Analyst at leading infosec company *Kaspersky* suspected the government has been involved in the creation of Stuxnet because it was difficult for an outsider to find these vulnerabilities without accessing Windows source code. The largest number of infections were in Asia, significant in Iran. Western governments have been trying to halt Iran's nuclear program since 2003, followed by several assassinations of Iranian nuclear scientists. High-level Stuxnet analyst groups concluded that Stuxnet was a joint covert operation of the U.S and Israeli intelligence. The genesis of Stuxnet still remains as the U.S government either admits or denied being part of Stuxnet.

Stuxnet literally was the first cyber-weapon targeting industrial infrastructures. To public disclosure deliberately or “leaked” shows cyber threats like Stuxnet can cause damage, possible casualties, and pose threat. This is a gray area in the cyber-world anonymous elites attributed or unattributed crossing the Rubicon, to say end justify the means.

References

The CPL Icon Loading Vulnerability. (n.d.). Www.geoffchappell.com. https://www.geoffchappell.com/notes/security/stuxnet/ctrlfldr.htm

BetaFred. (n.d.). Microsoft Security Bulletin MS10-046 - Critical. Docs.microsoft.com. https://docs.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-046

Archiveddocs. (n.d.). How Flash Drives and Social Engineering can Compromise Networks. Docs.microsoft.com. Retrieved February 20, 2022, from https://docs.microsoft.com/en-us/previous-versions/technet-magazine/cc137730(v=msdn.10)?redirectedfrom=MSDN

Experts Warn of New Windows Shortcut Flaw — Krebs on Security. (n.d.). https://krebsonsecurity.com/2010/07/experts-warn-of-new-windows-shortcut-flaw/

Trojan-Spy.0485 And Malware-Cryptor.Win32.Inject.gen.2 Review Kupreev Oleg Ulasen Sergey VirusBlokAda. (n.d.). https://archive.f-secure.com/weblog/archives/new_rootkit_en.pdf

News | VirusBlokAda. (n.d.). Anti-Virus.by. Retrieved February 20, 2022, from http://anti-virus.by/en/tempo.shtml

Jennings, R. (2010, July 19). Critical Windows vuln. in .LNK files = Stuxnet (and IE IV). Computerworld.

https://www.computerworld.com/article/2468584/critical-windows-vuln--in--lnk-files---stuxnet--and-ie-iv-.html

Rootkit.TmpHider. (n.d.). Wilders Security Forums. Retrieved February 20, 2022, from https://www.wilderssecurity.com/threads/rootkit-tmphider.276994/#post-1712134

“Stuxnet” Worm Far More Sophisticated Than Previously Thought – Krebs on Security. (n.d.). https://krebsonsecurity.com/2010/09/stuxnet-worm-far-more-sophisticated-than-previously-thought/

Security Response Contents. (n.d.). https://docs.broadcom.com/doc/security-response-w32-stuxnet-dossier-11-en

Clues emerge about genesis of Stuxnet worm. (2010, October 1). Christian Science Monitor. https://www.csmonitor.com/World/terrorism-security/2010/1001/Clues-emerge-about-genesis-of-Stuxnet-worm

The Man Who Found Stuxnet – Sergey Ulasen in the Spotlight. (n.d.). Eugene.kaspersky.com. https://eugene.kaspersky.com/2011/11/02/the-man-who-found-stuxnet-sergey-ulasen-in-the-spotlight/

Gross, M. J. (2011, March 2). A Declaration of Cyber-War. Vanity Fair. https://www.vanityfair.com/news/2011/03/stuxnet-201104