STUXNET

CSEC 742 - Mehul Sen – 11/29/2021

AGENDA

1. Stuxnet Attack Cycle
2. Attribution
3. Aftermath

STUXNET ATTACK CYCLE

INFILTRATION

1) Infected USB connected to a PC by Industrial Facility's Employee/Shared Drives From Infected Machines
2) Use three Zero-Day Vulnerabilities to install itself on the system (CVE-2010-2568) and then escalate privileges (CVE-2010-2743, Unpatched Windows Task Scheduler Vulnerability)
3) Install Stuxnet into the Infected Machine by writing 6 files
   - C:\WINDOWS\inf\oem7A.PNF
   - C:\WINDOWS\inf\oem6C.PNF
   - C:\WINDOWS\inf\mdmcpq3.PNF
   - C:\WINDOWS\inf\mdmeric3.PNF
   - C:\WINDOWS\system32\Drivers\mrxnet.sys
   - C:\WINDOWS\system32\Drivers\mrxcls.sys
4) Spread across the network, bouncing from one computer to the other using a previously known vulnerability (CVE-2008-4250) and a zero-day vulnerability (CVE-2010-2729)

INFILTRATION PT.2

5) Stuxnet also made use of stolen legitimate certificates. These legitimate certificates were stolen from two hardware manufacturers in Taiwan.
6) Once the malware has infiltrated the infrastructure, it then begins searching for its target, specifically the facility's Industrial Control System (ICS).
6) When it gets control over an ICS, it looks for the software Step7 from Siemens. On finding the software, it exploited a hardcoded username and password 'Basisk' within the software that provided it with a backdoor. It then injects itself to any Step7 project files it can find.
7) As soon as it found a Programmable Logic Controller, it escalates privileges and gains control over it.

NOTE: Originally designed to infect three additional machines and erase after 21 days if target was not found. It also has a kill date of June 24, 2012. On that date, the worm will stop spreading and delete itself.

ROOTKITS AND UPDATES

Included two Rootkits that were created in the USB flash memory

- User-Mode Rootkit (~WTR4141.TMP)
- Kernel-Mode Rootkit (MRxNet)

NOTE: MRxNet contained a debug message

`b:\\myrtus\\src\\objfre_w2k_x86\\i386\\guava.pdb`

Which contains the word “myrtus” , a Hebrew Word, that could point towards Israel or a false positive.

It also had an updating mechanism using two methods

1) Updating via the Internet
   - www.mypremierfutbol.com
   - www.todaysfutbol.com
2) Updating via Peer-to-Peer Connection
   - set up an RPC server and communicate with peers

PAYLOAD

1) Once it had complete control over its target system (PLC), Stuxnet then looked for two microchips that control the rotation speed of centrifuges, these microchips manufactured by:
   - Vaasa Control Ltd.
   - Fararo Paya

If not found, it would terminate its operation. However, if it successfully found them, it would look for rotating centrifuges between the speed of 807 Hz to 1210 Hz.

2) Stuxnet would then sit and wait for weeks, listening and recording for normal behavior.
3) After a couple weeks, it then instructed the centrifuge to significantly increase its revolutions per second for 15 minutes.
4) If centrifuge did not break, it would slow down the revolutions per second to barely spin, and then back to normal spin speed.

IMPACT ON URANIUM ENRICHMENT

Uranium gets enriched when hot uranium gas is injected into a rapidly rotating centrifuge.
Gas Centrifuges used to enrich uranium are highly sensitive.
If done correctly, it leads to Nuclear Fission which can be used as:

- Fuel for Nuclear Power Plant
- Nuclear Bomb

If done incorrectly:

- Wastage of Rare and Expensive Uranium 235
- Degradation of 1000 centrifuges
- Set back Iran's Nuclear Program by almost three years

DETECTION EVASION AND DISCOVERY

Stuxnet heavily relied on remaining covert.
It accomplished this by replacing the sensor data sent to the technician's monitor with a pre-recording.
It also "saved" the original software used to run the centrifuges which it would present to programmers debugging the PLC.

However, there was a bug in Stuxnet.
The malware was NOT spreading only to three new computers at a time. It spread beyond the target network on Nantanz, infecting systems all over the world.

On June 17, 2010, Virusblokada discovered this malware several months after its creation. Soon afterwards, Iran shut down their facilities and wiped the malware off all systems. By September 30, 2010, Symantec presented a comprehensive analysis of Stuxnet.

ATTRIBUTION

STUXNET'S PROPERTIES

Stuxnet was built with precision and a very specific objective in mind.
- Step7
- Vaasa Control & Fararo Paya
- 807 Hz and 1210 Hz

= Attackers had prior knowledge about the victim's infrastructure.

Stuxnet was designed to be covert.
- Secretly install itself onto the target machines
- Avoid getting detected by antivirus
- Covertly modify the centrifuge speed
- Send out false sensor data to technicians

= Attackers wanted persistence and gradually disrupt the centrifuges.

Stuxnet was highly sophisticated.
- Used multiple zero-day exploits
- Unprecedentedly complicated
- Roughly 150,000 code lines

= Attackers had the large amount of time and resources to develop this malware.

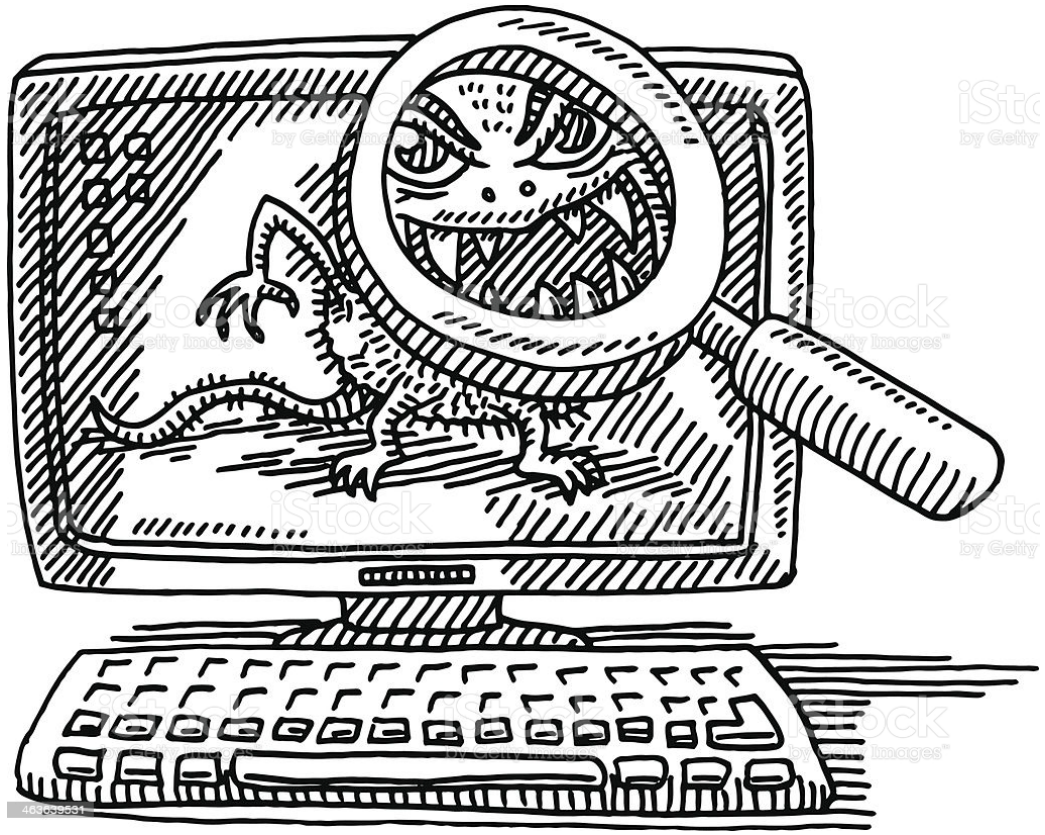
WHAT WE KNOW

All these different clues, led security researchers to believe that such an attack could only be conducted by a nation state actor.

Two Potential Nations
- United States of America
- Israel

“Olympic Games” was the codename given to the joint American-Israeli operation.
This operation began during the Bush Administration and continued through the Obama Administration. A 2011 retirement video for the head of Israeli Defense Forces listed Stuxnet as one of their success.

Kaspersky Lab estimated that it took a team of ten coders 2-3 years to create Stuxnet.



AFTERMATH

REPRECUSSIONS

- As soon as it was discovered, Iran assembled a team to combat Stuxnet however they faced difficultly because of Stuxnet's fast spreading and mutating abilities, with newer versions of the malware showing up frequently.
- Iran officially claimed that it believed United States and Israel were behind the creation of Stuxnet.
- In the next couple of years, Iran beefed up its cyber capabilities.
- Leaked NSA document suggested that Iran was learning from these cyberattacks and replicating the techniques to conduct their own attacks.
- Iran also created the "1390 Program"

LEGACY OF STUXNET

One year after Stuxnet was exposed, Doqu was discovered by security researchers in Hungary.
Doqu shared common pieces of code as Stuxnet. Unlike Stuxnet, Doqu was used for espionage.

Six months later, another malware, Flame was discovered. It had small similarities indicating the same author.
It was twenty times as complex as Stuxnet with over 3,000,000 lines of code.

Other malware that appear to have inherited characteristics from Stuxnet are:

- Havex (2013)
- Industroyer (2016)
- Triton (2017)
- Unnamed (2018)

WHAT DOES THE FUTURE HOLD?

Stuxnet showed us that malware and digital virus could be used to sabotage physical equipment with extreme sophistication and precision.
Stuxnet proved that countries were now no longer restricted to Air, Land and Sea and Space for their warfare, cyberweapons could now be designed to hit their target's key infrastructure and be used to wage wars against each other.

This also brings forth the notion that Stuxnet was discovered back in 2010 due to a bug in their code. Over 10 years after this attack, it's almost a certainty, that many such attacks have taken place without any major exposure or leaks. A massive cyberattack could be underway as we speak, and we might never find out about it.

REFERENCES

(1) https://www.zdnet.com/article/attack-code-published-for-unpatched-stuxnet-vulnerability/ -
(2) https://malicious.life/episode/episode-8-stuxnet-part-2/ -
(3) https://darknetdiaries.com/transcript/29/ -
(4) Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon
(5) https://hakk.gg/stuxnet-detail-analysis-and-mechanism/
(6) https://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html?sh=4a9447b851e8 -
(7) https://arstechnica.com/information-technology/2011/08/serious-security-holes-found-in-siemens-control-systems-targeted-by-stuxnet/ -
(8) https://bits.blogs.nytimes.com/2010/09/24/malware-hits-computerized-industrial-equipment/
(9) https://docs.broadcom.com/doc/security-response-w32-stuxnet-dossier-11-en -


THANK YOU