ROOTING THE WORLD'S FIRST CYBER SUPER-WEAPON: STUXNET

Abstract
Stuxnet is considered to be the first cyber super weapon. It was able to begin a new era of malware as it exploited multiple aspects at once including Windows OS, SCADA platforms, Windows based software, Humans, etc. Main objective of this report to analyze the technical constraint of Stuxnet and analyze the social, political, financial and technical aspects cause by it. Even though it has been 10 since the first discovery of this attack, level of details of this attack still amaze the security researchers all over the world.

It it a renowned fact that if a world war 3 to ever occurred, it would be happens in cyber space[1]. For years this claim was doubted but once the Stuxnet was discovered, needless to say the doubt become cleared once and for all. Analyzing such sophisticated malware would be extremely difficult. But renowned cyber security researchers such as Ralf Rosen, Andreas Timm, Ralph Langner, Amr Thabet and organizations such as Symantec and ESET has put their time and effort into this so the people who want to further study Stuxnet would not be have to gone through the same pain. In this report I have used research papers published by above individuals and organization therefor I believe actual and accurate information have been included in this report. Technical narrative section of this report is targeted for tech savvy individuals as it contains deep technical terms while the rest can be easily understand by the general public with very little of technical knowledge.

I. BACK TO THE BEGINNING

After the massacre of Japan due to Atomic bombs, a number of countries made the concern regarding the use of nuclear weapons. In the post WW2 era, the anti-nuclear movement raised and demanded the ban of all nuclear weapons. Some unions such as European Union decided to go along and decided to ban all nuclear weapons[2]. However at the end of the 90s and at the beginning of the millennium, a number of countries including Pakistan, Libya and Iran though otherwise started nuclear programs. Among those countries Iran made strong headlines. Due to this, in 2003 EU3 (Britain, Germany and France) [3] requested Iran to suspend their nuclear enrichment activities for a period of time. Iran actually agreed upon this. However in 2006, Iran's newly elected president Mahmoud Ahmadinejad decided to restart the nuclear enrichment program as they have found a workaround of per-said agreement.

Stuxnet worm specifically targeted Siemens PLCs (Programmable Logic Controls) which were mainly used by Iran's Natanz nuclear facility. Number of cyber security experts claims that Stuxnet was too large and complex for a single or group of hacktivist to create as it required an actual test environment with nuclear reactor materials and radioactive components. Which means the malware developers had access to sensitive facilities and resources. Therefor so many speculations arose that this is a nation state attack backed by the US and Israel. It estimate that it took 8 to 10 extremely talented people and about six months to develop the whole malware[4].

From a financial of view, Iran sure suffered from this attack. Other than that umber of SCADA platforms all over the world suffered from this attack. As it's primary target was Iran, it is safe to say Stuxnet almost fulfilled it's purpose as it was able to hold the Iran's nuclear program for a short period of time, but unable to complete as it was discovered.

From a technical perspective, this begin a new era for malware. Hundreds of security researchers and reverse engineers have tried to find the complete source code of the malware nut as it is too large and complex, still they were not able to fully recover the source code. The need for the behavior based antivirus software, software signing, SCADA (Supervisory control and data acquisition) security raised with the Stuxnet and it is definitely a win for information security.

From a political and social point of view, Stuxnet discredited Iran on a larger scale as it was unable to secure it most sensitive infrastructure from a cyber attack. At the same time as the original creator of the worm is unknown, Iran was not able to retaliate either. This clearly made Iran government look weak as then president Mohammad Ahmadinejad claimed to be a hardliner.

II. TECHNICAL NARRATIVE

Initial infection mechanism of the Stuxnet is USB drives. By this method it was able to access air-gaped systems inside the nuclear facility. Overall process of the Stuxnet can be shown as below,

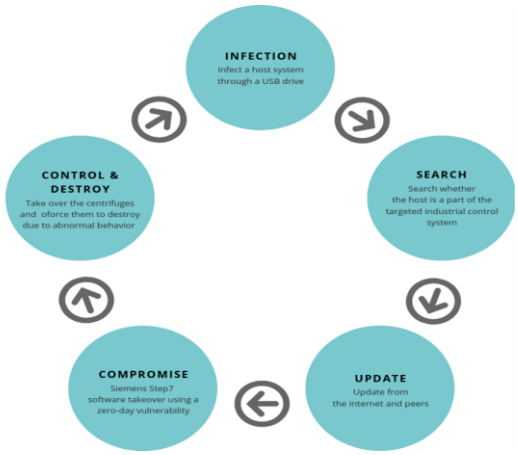

Figure 1: Stuxnet attack's life cycle

Centrifuge referred to a machine that turns a container round very quickly, causing the solids and liquids inside it to separate by centrifugal action[5].

This malware functionality has three main phases.

1. First stage: This targets Windows system vulnerabilities including multiple zero day exploits to take over the systems. Then this replicates itself over the network and takes over further vulnerable machines.
2. Second stage: Takes over Siemens step7 software (Windows based software) which used to control and program industrial control systems using another zero day exploit.
3. Third stage: Compromise the logical controllers eventually takes over the whole control system[1].

As the second and third sections are relevant to industrial and electronic engineering, comprehensive explanation has not taken in this report.

- Stuxnet malware

From a technical point of view, it has a sophisticated life cycle.

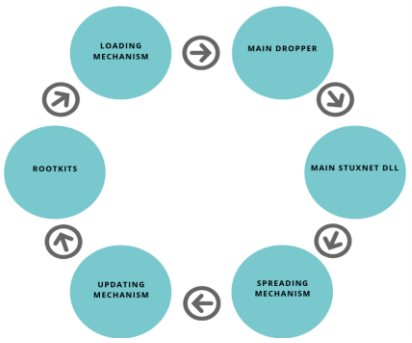

Figure 2: Life cycle of the malware

This malware contains four zero-day Windows exploits and a Zero-day exploit for the Siemens software. It is considered remarkable that Stuxnet used five Zero-day exploits as malware writers almost never use more than one zero-day exploit in a single malware[6].

- The main dropper

This is a Windows DLL (Dynamic Link Library) file loaded into the Explorer.exe. It's execution begins with searching for the ".stub" section in itself. This section contains all the major DLL files of Stuxnet. And this DLL contains all the functions, mechanisms and rootkits of the Stuxnet.

Apart from the DLL, ".stub" section includes configuration data of Stuxnet which are required for spreading mechanism, updating mechanisms, etc. Once the DLL is found, it does not load into the memory right away. Firstly, it allocates memory buffers for the DLL. Secondly, change 6 ntdll.dll APIs with below names.

i. ZwMapViewOfSection;

ii. ZwCreateSection;

iii. ZwOpenFile;

iv. ZwClose;

v. ZwQueryAttributesFile;

vi. ZwQuerySection;

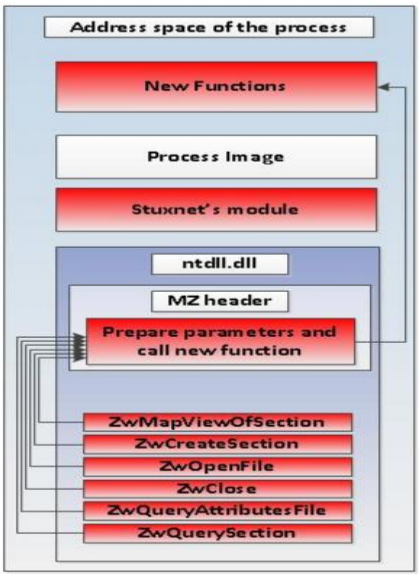

Figure 3: ntdll.dll injection process

[7]

These alterations will make LoadLibraryA to load a DLL file from the memory, unlike from the hard-disk as usual. Then only the main DLL will execute.

- Main Stuxnet DLL

Main DLL works in two steps.

1. Privilege escalation

At the beginning DLL will check whether the admin rights are present. If not, it uses one of two zero-day exploits for the privilege escalation.

CVE-2010-2743, Win32K.sys Keyboard Layout Vulnerability, CVE-2010-3338,Windows Task Scheduler Vulnerability. These two exploits allow the malware to run with escalated privileges using either a new process ("csrss.exe") or a new task in Task Schedule.

When the newly created process is required to execute a module, it looks for a process and replaces the process image with the module. Prior to the injection, the above process will look for the presence of an antivirus program in the system. If none, "Iass.exe" process will be used for the injection. AV availability is detected by looking for the process in the below table.

Antivirus Vendor	Process
Kaspersky KAV	Avp.exe
McAfee	Mcshield.exe
AntiVir personal edition	Avguard.exe
BitDefender switch agent	Bdagent.exe
ETrust configuration engine from Computer Associates International	UmxCfg.exe
F-Secure	Fsdfwd.exe
Symantec real time virus scan service	Rtcscan.exe
Symantec service framework	Ccsvchst.exe
ESET	Ekren.exe
PC-cillin from TrendMicro	Tmproxy.exe

[7]

Based on the AV main image version, Stuxnet will determine whether it's by-passable or not. If is is not by-passable injection will fail. Otherwise it will select a potential process according to the below table.

AV Vendor	Injected Process
KAV v1 to v7	Lass.exe
KAV v8 to v9	KAV process
McAfee	Lass.exe
BitDefender	Lass.exe
ETrust v5 to v6	Fails to inject
Etrust (Other)	Lass.exe
F-Secure	Lass.exe
Symantec	Lass.exe
ESET NOD32	Lass.exe

[7]

It is important to note that it does not look for the mentioned processes form the task manager to inject rather create the certain process under the suspended status with the use of "CreateProcess" function.

Once the process is created, it's unloaded from the memory and re-loaded another PE file from the previously mentioned DLL resources. While doing this, it makes sure to add a new section to the beginning named ".verif" so the new PE file size matches the file size of previously uploaded PE file's size. As well as the entry-point of the unloaded module rewrites with the "jmp" instruction to the entry-point of the new PE file. Finally it copies the .stub section and the main malicious DLL and maps those into the new process.

2. Host infection

Before beginning the installation, Stuxnet checks for configuration data to make sure installation can start. Also it checks for registry entry named "NTVDM TRACE" with the value of 19790509.

While this could have multiple meanings, most relevant possibility could be the May 9, 1979 execution of Jewish Iranian businessman and philanthropist Habib Elghanian.

After that, it installs itself by adding 6 new Windows directory entries. This includes 4 encrypted files and 2 device drivers.

Files:

i. C:\WINDOWS\inf\oem7A.PNF

ii. C:\WINDOWS\inf\mdmeric3.PNF

iii. C:\WINDOWS\inf\mdmcpq3.PNF

iv. C:\WINDOWS\inf\oem6C.PNF

Device drivers

i. C:\WINDOWS\system32\Drivers\mrxnet.sys

ii. C:\WINDOWS\system32\Drivers\mrxcls.sys

Once this is done, drivers will be written to the registries therefor it will run each time the computer boots up. After

that Stuxnet loads the mrxnet driver bay calling ZwLoadDrive. Meanwhile its privileges are being adjusted to "SeLoadDriverPrivileges" by the "AdjustTokenPrivileges" function.

As the end of this stage, it modifies the Windows Defender firewall rules to allow all the Stuxnet related communications through the firewall. It changes defender registry values from the SOFTWARE\Microsoft\Windows Defender\Real-Time Protection entry. EnableUnknownPrompts, EnableKnownGoodPrompts, ServicesAndDriversAgent are set to zero. so it won't get detected by the system.

Kernel32dll: FindFirstFileW, FindNextFileW, FindFirstFileExW

Ntdll.dll: NtQueryDirectoryFile, ZwQueryDirectoryFile.

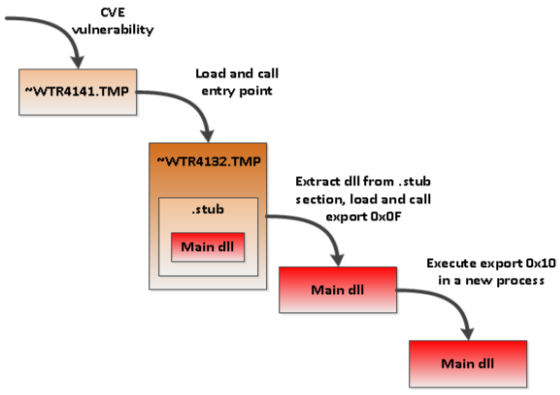

Figure 4: Stub section and main DLL execution

[7]

- Spreading mechanism

USB is considered to be the initial spreading medium of this attack. apart from that as this is a worm class malware, network spreading was also used.

1. USB infection

Windows sends WM_DEVICECHANGE when a media is inserted and removed from the system. Stuxnet waits for this message to identify when a USB drive is inserted into the machine. Once identified, it writes 6 files into the USB drive.

4 shortcut files:

i. Copy of Shortcut to.lnk

ii. Copy of Copy of Shortcut to.lnk

iii. Copy of Copy of Copy of Shortcut to.lnk

iv. Copy of Copy of Copy of Copy of Shortcut to.lnk

2 executable DLL files: ~WTR4132.tmp, ~WTR4141.tmp

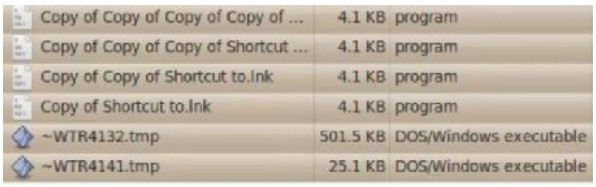

Figure 5: Initial dropper files preview from a GNU/Linux OS

These shortcuts are vulnerable to the CVE-2010-2568,Windows Shell LNK Vulnerability. This misuses the way Windows uses to load the icons for LNK files.

These shortcuts are linked to CPL files, usually Windows control panel item shortcuts. In this case those shortcut files have multiple PIDs including control panel PID as the first. PID change ends with an item containing filename and the path of Stuxnet DLL (~WTR4141.tmp).

Multiple shortcut files contain different paths to the DLL file so it would be compatible with all the versions of Windows OS. These shortcut paths execute Stuxnet by Explorer.exe. Meanwhile Explorer.exe calls "shell32.LoadCPLModule" API to load the icons for the shortcuts. It executes the ~WTR4141.tmp with the help of LoadLibraryA.

As soon as the rootkit starts the execution, these files will become hidden. And two new files named "mrxcls" and "mrxclnet" will be generated in the drivers directory. "Mrxcls" uses to invoke the Stuxnet on a reboot while "mrxnet" uses to hide the files. Initially these files were signed using Realtec digital signature. But once its revealed developers revoke it. However malware developers had given thoughts to such scenario as new variant came to the with digital certificates signed with "JMicron Technology Corp".

2. Network spread

Network spreading of the Stuxnet was done using one of the two vulnerabilities.

CVE-2008-4250 -Windows Server Service NetPathCanonicalize() Vulnerability, CVE-2010-2729 - Windows Print Spooler Service Vulnerability.

CVE-2008-4250 is not a zero-day exploit. Stuxnet looks for c$ and admin$ shares on remote machines and copies itself as "DEFRAGxxxxx.TMP" in the first writable directory. After it tries to execute the following command with the scheduled task set to be executed on the next day.

rundll32.exe "DEFRAGxxxxx.TMP",DllGetClassObjectEx

CVE-2010-2729 is a zero-day exploit. It allows guests to write to the system directories of the machines with shared printers. Stuxnet copies two files into such directories.

Windows\System32\winsta.exe

Windows\System32\wbem\mof\sysnullevnt.mof

First file is the Stuxnet dropper and the second file executes it under some conditions.

- Updating mechanism

Stuxnet update itself through the internet. It checks the internet connectivity by using below two legitimate web sites of ,

www[.]windowsupdate[.]com & www[.]msn[.]com

If successful, then it establishes a HTTP connection to malicious web sites,

i. www[.]mypremierfutbol[.]com

ii. www[.]todaysfutbol[.]com

Once the request is sent to the web site, the server will reply with the update data as an encrypted payload.

Once a machine is infected with the Stuxnet, it makes itself a RPC server. It sets to listener mode for incoming RPC requests from other computers in the system.

First, it sends the RPC version and validates whether it's the latest. If so, it sends the Stuxnet DLL to it's clients. Then the clients inject it into the pre-selected process.

If the server is not the latest version, then the client prepares a never version of Stuxnet and sends it to the RPC server. This is quite useful as some of the computers won't be having direct access to the internet.

- Rootkits

1. User mode rootkit

This is a DLL file loaded by the LNK vulnerability. This loads the main Stuxnet dropper as well as hides it in the flash memory working as a user mode rootkit.

This rootkit hooks the file management API as the first job. Then the Stuxnet installation step begins. After it's done,this rootkit is no longer required as the operation is transferred to a kernel rootkit.

2. Kernel mode rootkit (MRxNet)

This rootkit adds itself to the system drivers chain which are responsible for the file handling of the OS. Once it's done, rootkit will receive the system requests to the drivers before legitimate drivers receive them. This allows rootkit to alter such requests. Main objective of this rootkit is to alter the output of the drivers.

- Loading mechanism

1. User Mode rootkit

This is loaded by the LNK vulnerability. This is used to load the main Stuxnet dropper.

2. MRx driver

This is a complex and sophisticated process. This was done in several steps. It has been identified that this part of the worm was created separately from the rest as this does not contain any features which were used by Stuxnet. As well as this signed from Realtec to show this as a legitimate application.

i. Initialization :Register the Mrx driver as an automatic startup program.

ii. stage one: Kernel module data injection.

iii. stage two: Kernel32 injection with entry-point overwriting.

iv. Stage three: User mode Stuxnet execution.

- Code injection the Siemens PLC

From a single USB drive, Stuxnet only infect three systems to avoid being detected. Once infected it will look for the Siemens Step 7 development software in the system. If found, system driver and Step 7 project files will be infected.

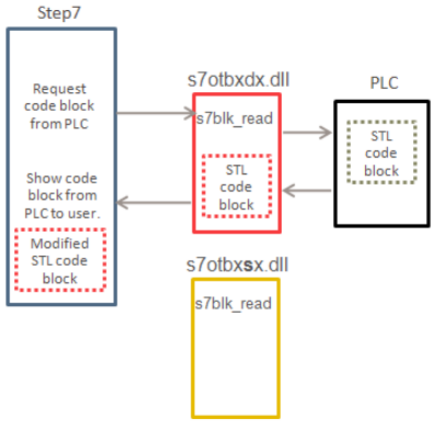

Figure 6: Step7 data maipulation

[8]

III. DETECTION OF THE MALWARE

As Stephan Hawking, the one of the greatest scientists of the human history once said, "Perfection simply doesn't exist[9]. World most sophisticated cyber super weapon (at that time) was no exception. Such a small imperfection leads to the discovery of this malware in the June 2010.

Stuxnet was created to be discrete and to attack only the Iran's nuclear facilities. But is has been found that infected systems were all over the world. It was a serious question how did it spread worldwide as it was designed not to be. There are multiple theories have been made for this. More comprehensive version was presented by Roel Schouwenberg, a senior antivirus researcher at Kaspersky Lab[10]. According to him. Malware developers created a more complex edition as the first version did not achieve its targets.

Back in the days from time to time Windows Blue screen of death was a common windows issue. But having such system crashes very often was abnormal. This was what happened with the Stuxnet discovery. Belarusian malware detection firm got a request from a client who has this PC getting blue screen of death continuously. While looking for the root cause, malware analyst Sergey Ulasen found the possible infected files which were caused by the Stuxnet.

As a results of this malware, nuclear centrifuges were damaged in an unusual rate. Even though the number was unclear it was climbed that more than 2000 units were defected within few months[11]. However no one suspected it was caused by a malware. As the malware was not designed to damage windows systems, it was undetectable to the computer users and AV softwares.

By that time almost all the IPS, IDS and antivirus softwares were based in the signature based detection. As this was a new malware, those controls were not able to detect this malware. At the same time as the Stuxnet used zero-day exploits for critical tasks, it could not be detected by the antivirus softwares.

Device driver singing is a strong control mechanism against the drive manipulation. As forging such certificate is almost impossible this provides a strong foundation for the driver software security. But as the Stuxnet used legitimate certificates, it could not be detected by this.

When it comes to process injection, most of the time this is a part where behavior based malware detection comes into play. Eve though this method was at the early stage, injecting a legitimate process would raise alarm in any antivirus platform. But in the case of Stuxnet, it does not tries to inject the first process it can identify. Instead of that, first it will look for the presence of an AV software. Then it will find a potential process to inject which would bypass the AV detection capabilities. Therefor AV platforms were not able to detect this operation either.

When it comes to malwares, the most common way of detection is command and control traffic. If a system in a controlled environment tries to contact an outside party, it could be an indicator of compromise. But in the case of Stuxnet, it checks the internet accessibility by accessing the legitimate windows and Bing web sites. As this it is a windows systems trying to access windows systems it wont raise any alarms. Second step is when the C&C communication is taking place, it uses encrypted payloads. At that time Next-Gen firewalls with HTTPS decryption capabilities were not available. Therefore systems were not able to identify the content of such traffic. Likewise such controls were useless against Stuxnet.

Earlier versions of Stuxnet only infected three hosts from a single USB drive. As well as in the propagation step, it will only carry out for the maximum of 21 days. These steps were taken to avoid the detection. By this method, it takes much time to reach the target but this wont raise any alarms. However this has changed in the new variant. As mentioned above, change of this precaution eventually led to the discovery of this malware.

IV. TECHNICAL IMPACT ANALYSIS

When it comes to technical affect from a malware, it can be divided into two aspect. Physical and logical. From the physical aspect, Stuxnet only affected and damaged centrifuges. It has been found that Stuxnet damaged the centrifuges by changing the rotor speed to too-low and too-high speeds (as low as 2 Hz and high as 1410 Hz)[12]. This abnormal variation caused centrifuges to damaged by wore out in an increased rate. It has been claimed that Natanz facility had over 8700 centrifuges installed. And at a given year it would be normal to replace around 10% of them. But due to Stuxnet, it has been discovered that Iran replaces over 1000 centrifuges within few months[11].

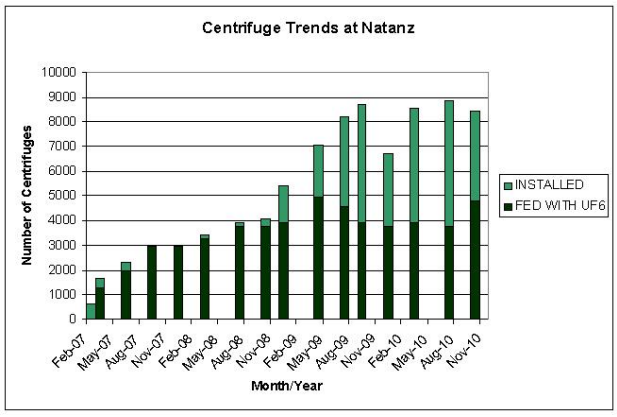

Figure 7: Natanz centrifuges' statistics

[13]

In general it does not seems to be a weapon of mass destruction as the centrifuge damage rate not increased in a larger scale. Therefor it's safe to say that physical destruction

of Stuxnet not in a mass scale. However it has been fond that due to the centrifuge damage, nuclear production rate becomes significantly lower that prior to the attack[13].

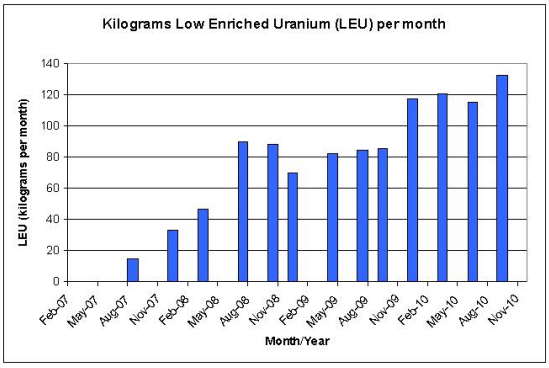

Figure 8: Natanz Uranium production statistics

[13]

Other than this from a logical aspect, Stuxnet directly affected four major software platforms. Windows OS, Siemens Step 7 software, antivirus vendors and Realtec driver certificates.

In Windows, Stuxnet exploited not only one, but three zero-day vulnerabilities. Microsoft strongly practices " security though obscurity" by keeping their softwares closed source. Which has been debated over decades and found to be not so secure as it claims to be.

If the security of a system is maintained by keeping the implementation of the system a secret, the entire system collapses when the first person discovers how the security mechanism works - and someone is always determined to discover these secrets[14].

Microsoft released security patches as soon as the vulnerabilities were found but the harm had been done by then. As this affected almost all the windows versions had by then, and as the vulnerabilities exposed privilege escalation capabilities, it was a serious risk to any infrastructure running on Windows OSs.

Siemens step 7 software used to control and develop new controls for SCADA platform components. As SCADA platforms are being used to control critical infrastructures such as electric plants, water plants and even nuclear missile silos, exploiting such a critical software platform could lead to a catastrophic failure of an country's entire infrastructure. Not to mentions the fact that exposure of a nuclear missile silo could possibly be start the next world war.

Stuxnet was able to bypass almost all the major antivirus vendors at that time. One could argue it was possible because the AV softwares are meant to protect Windows OSs but the worm was designed to damage completely different target. But in reality as Stuxnet exploited multiple windows exploits, inject legitimate processes, escalate privileges etc, AV could have detected one of the act as malicious if they were built to detect anomaly based detection rather than signatures. By the time almost all the AV vendors relied on signature detection. Not only by then, still some AV vendors rely on signature detection which has proven over and over again to be ineffective. If any system or an infrastructure is still rely on signature based detection, needless to say it would rather not have a such AV installed.

Device drivers plays a major part in OSs as it has direct access to the OS kernel. Therefor compromise of such a driver is critical. This is what happened with Stuxnet. As it uses compromised Realtec driver certificate to act like a legitimate driver, it was able to hide its activity from the users, AVs and was able to successfully launch the attack. Once its reveled Realtec revoked the certificate, but the harm was done by then. Therefor when it comes to driver security and validation, strong methods and mechanisms are required. As driver softwares are a complement of any critical infrastructure, compromise of such drivers put the entire system at a jeopardy.

Other than these targets, there has been numerous claims that Stuxnet worm killed India's INSAT-4B satellite as the India's Space Research Organization used vulnerable Siemens software for their SCADA platforms. While this remains doubtful, if true billions of dollars worth of equipments alongside with thousands of man hours of engineering was lost due to Stuxnet[15].

V. BUSINESS IMPACT ANALYSIS

In general, Stuxnet attacked Iran's Natanz nuclear facility's centrifuges. It increased the damaging rate of the centrifuges. By the time Iran had pressure from outside world to stop the nuclear program. Therefor it was almost impossible for Iran to purchase required centrifuges fro the outside world. On the other hand as the nuclear production rate did not increased as expected. Due to this Iran had a very some serious financial difficulties regarding this project from a cost-benefit ratio perspective. Due to the low production rate, Iran forced to buy enriched Uranium for other countries.

Other than Iran, multiple other countries were hit by Stuxnet. While the total cost of the worldwide damage is unclear, we can only imagine millions of USD of damage were included.

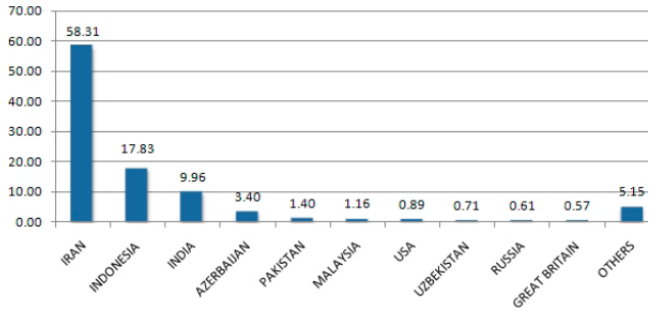

Figure 9: Stuxnet worldwise infection statistics

[13]

After the attack was discovered, like any responsible government would do, Iran decided to develop their cyber security capabilities. While there are no actual evidence, Comodo, a digital certificate vendor claims that Iran hacked into their system in order to steal the digital certificated which later used on multiple cyber attacks against US [16].

Not only this, as per developing the cyber security space, Iran has spent insanely significant amount of assets. Just to get a clear idea on this, Atlantic council panel discussion at 2015 revealed that "Over the past three years, Iran's budget for cyber security has increased 1,200 percent". Therefor it is safe to say Iran has to decrease the cost for number of other projects in order to develop the cyber security capabilities.

As mentioned in the Technical impact assessment section, as a result of the loss of the satellite, over 70% of Indian's direct to home services were down. This includes services such as TV, data services, etc. . As a result, those companies were forced to use a satellite owned by a Chinese organization. From a financial perspective, as India had to pay for the Chinese satellite, it was considerable loss to their national economy. On the other hand billions of dollars worth of equipment were lost as well and making a new satellite would take much more time, effort and money. Therefor it is safe to say, if the claims are true, Stuxnet paralyzed India's Direct-To-Home (DTH) services and the India's Space Research Organization.

VI. PREVENTION AND MITIGATION

Stuxnet like malwares are too large and sophisticated to mitigate using a single control mechanism. It needs much more than that. It means the mighty "defense in depth" strategy has to take place. As this is not only limited to a single platform like Windows, GNU/Linux, etc. different types of security controls are required. Specifically in this case, SCADA security controls mechanisms and controls are required.

As Bruce Schneier, one of the most important cryptographers in the world once said, "If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology". Because humans claimed to be the weakest link of the security. Therefor technological controls won't alone solve the security problems. Likewise not only the technological but human controls are required for security as well.

Security comes with the development of bot defensive and offensive technologies. Therefor the Mitigation can be break into two steps. Preventive and reactive. Both steps consist of active and passive components and with regards to the severity, it can break down as below.

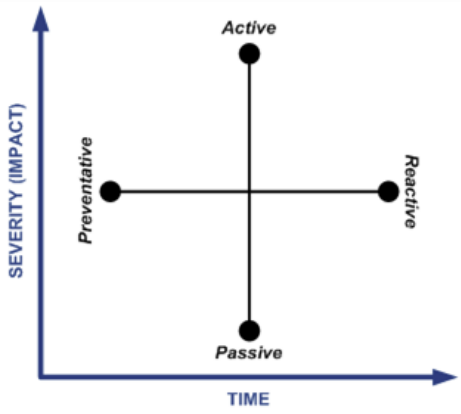

Figure 10: Mitigation strategy

[17]

- Preventive - passive

1. Implement effective security policies, guidelines and procedures. And review them in a scheduled manner
2. Carry out information security awareness sessions among the employees
3. Security policies and procedures should follow isa-99 standard[18]
4. Disable USB device access to the systems
5. Implement restrictions for unauthorized softwares
6. Follow vendor guidelines for system hardening
7. Adhere US "Cyber Security Procurement Language for Control Systems" for security controls systems[19]
8. Implement schedules comprehensive vulnerability scans
9. Implement comprehensive patch management

Preventive -active

1. Host systems should be safeguarded with host based firewalls, host based IPS/IDS, antivirus platforms.
2. Accountable logging and events and backup them in a separate location
3. Use of whitelisting based security applications rather has blacklisting
4. Firewalls should follow deny by default rule
5. Utilize code singing tasks
6. Implement NG firewalls with HTTPS decryption capabilities
7. Network segmentation

Reactive - passive

1. Implement SIEM (Security Incident ad Event Management) solutions.
2. Implement IPS/IDS, extrusion detection systems and integrate them with the SIEM platform.
3. Implement a SCADA honeypot

reactive-active

1. Isolate the compromised target once detected
2. Once detected, all the communications should be closely monitored
3. Reactive plans, incident response plans, disaster recovery plans should be in place and tested before
4. Business continuity plan should be in place and tested before
5. Carry out intensive digital forensics process once isolated. System integrity should be carefully validates when reinstating.

VII. CONCLUSION

In this report I have taken effort to analyses the one the most sophisticated malwares in the world.

First part of this report contains the background story of this malware. As well as how the attacked was happened has been described in a detailed manner.

Second section of this report conclude of technical aspect of the attack. Deep technical approach has been taken to analyze each and every key aspect of the malware. While the PLC infection section may lack of technical details as it does not belong to computing filed, Windows infection section has been built from the surface to the deep down.

Third section includes the detection of the malware. Even though the first ever encounter of this malcode goes back to 2007, as someone uploaded a piece of the malware into the virustotal, there are no valid evidences to prove this point. Therefor it is considered 2010 as the detection year for Stuxnet.

Fourth and fifth section include technical and business impact analysis caused by the Stuxnet. Same as above this section includes deep technical and financial approach alongside with facts and figures from the reputed sources.

Last part of this report includes the prevention techniques for the Stuxnet. Even though there were no actual harm doe to windows systems, as it was able to gain admin rights, having mitigation techniques for Stuxnet is a must.

War is never an option due to it's collateral damages. I believe same goes with the cyber wars. One could argue Cyber wars are somewhat better as no humans are harmed in the act. But Indian satellite was possibly a collateral of Stuxnet. Therefor, as a information security professional I believe either physical or cyber, war is ever an options.

VIII. ACKNOWLEDGMENT

I would like to express my gratitude and thanks to my Network Security lecturer Mr. Kanishka Yapa for his wonderful guidance throughout this project.

I am also grateful to my parents for their continuous support to me throughout this project.

IX. REFERENCES

[1] S. P. Rao, "Stuxnet , A new Cyberwar weapon : Analysis from a technical point of view," Aalto University, 2014.

[2] E. Tuomioja, "It is time to end our reliance on nuclear weapons," 2017.

[3] R. Langner, "To kill a centrifuge," 2013. [Online]. Available: https://www.langner.com/to-kill-a-centrifuge/.

[4] B. Schneier, "The Story Behind The Stuxnet Virus," *Forbes*, 2010.

[5] Cambridge University Press, "Cambridge Dictionary." https://dictionary.cambridge.org/dictionary/english/centrifuge (accessed Dec. 25, 2020).

[6] J. Richmond, "Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?," *Fordham Int. Law J.*, vol. 35, no. 3, p. 54, 2012, [Online]. Available: https://core.ac.uk/download/pdf/144231051.pdf.

[7] ESET, "Stuxnet Under the Microscope," 2012. [Online]. Available: https://www.esetnod32.ru/company/viruslab/analytics/doc/Stuxnet_Under_the_Microscope.pdf.

[8] F. Nicolas, L. O. Murchu, and E. Chien, “W32.Stuxnet Dossier,” 2010. [Online]. Available: https://css.csail.mit.edu/6.858/2014/readings/stuxnet.pdf.

[9] Darlow Smithson Productions, *Into the Universe With Stephen Hawking*. Discovery, 2010.

[10] G. Keizer, “Why did Stuxnet worm spread?,” *Computerworld*, Oct. 01, 2010.

[11] K. Zetter, *Countdown to Zero Day*. Crown, 2014.

[12] P. Mueller and B. Yadegar, “The Stuxnet Worm,” 2012. [Online]. Available: https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/topic9-final/report.pdf.

[13] D. Albright, P. Brannan, and C. Walrond, “Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?,” 2010. [Online]. Available: https://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf.

[14] J. Breithaupt and M. S. Merkow, “Information Security Principles of Success,” 2014. https://securitynotepad.wordpress.com/2019/06/17/information-security-principles-of-success-12-principles/ (accessed Dec. 28, 2020).

[15] J. Carr, “Did The Stuxnet Worm Kill India’s INSAT-4B Satellite?,” *Forbes*, 2010.

[16] R. McMillan, “Comodo hacker claims another certificate authority,” *Computerworld*, Mar. 30, 2011.

[17] SCADAHAcker, “Stuxnet Mitigation.” https://scadahacker.com/resources/stuxnet- mitigation.html (accessed Jan. 02, 2021).

[18] ISA, “ISA99, Industrial Automation and Control Systems Security,” *International Society of Automation*. https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99 (accessed Dec. 28, 2020).

[19] D. of H. Security, “Cyber Security Procurement Language for Control Systems,” *2009*. https://us-cert.cisa.gov/sites/default/files/documents/Procurement_Language_Rev4_100809_S508C.pdf (accessed Dec. 29, 2020).