Stuxnet: Anatomy of a Cyber Weapon

By: Efrem Mickael

Introduction:

In June 2010, a sophisticated worm named Stuxnet was discovered in Iran` s nuclear facility at Natanz by a Belarusian Security firm by the name VirusBlokAda.

To make things a bit clarified: The first to detect this virus was a senior analyst, goes by the name Sergey Ulasen. One of the major things he discovered about this unknown malware was that, it was exploiting numerous " Zero-day" vulnerability. *(I will not discuss the term " Zero-day" due to its complexities and the desire to keep this essay on focus to avoid confusion.)*

According to the CRS Report for Congress "*...the Malicious software (malware) were designed specifically to attack a particular type of ICS: one that controls nuclear plants, whether for power or uranium enrichment".*[1]

In this essay I will briefly discuss about Stuxnet also known as Computer worm, W32.stuxnet or cyberweapon, its origin, how it works, its impact, future potential scenarios of Stuxnet or Stuxnet-like cyberattacks and their enigma and the lesson learned from the attack on Iran` s nuclear facility.

The Origin of Stuxnet

The origin of the Stuxnet malware is strongly linked to the "Iranian nuclear enrichment facility at Natanz". The amazingly sophisticated design of the malware and its attack on the Iranian nuclear facility left many analysts around the world shocked. This malware was using a skillful rootkit to cloak itself and make it self-invisible to antivirus engines, it was using a shrewd zero-day exploit to propagate from machine to machine- an exploit that attacked a function so fundamental to the windows operation system, it put millions of computers at risk of infection. [2]

According to P. Farwell and Rohozinski, who are both an expert in the field of cyber warfare and cyber security, this malware successfully managed to infect over 60,000 computers. More than half of them in Iran, but many other countries has been affected. To mention: countries including India, China, Indonesia, Azerbaijan, South Korea, Malaysia, the United States, the United Kingdom, Australia, Finland, and Germany.[3]

[1] *Kerr P. (2010).The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability, Available from: The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability (fas.org) ,[Accessed 26/02/23]*

[2] *Zetter Kim (2014) : Countdown to Zero Day*

[3] *Farwell P. J. & Rohozinski R. (2011) Stuxnet and the Future of Cyber War, Available from: Stuxnet and the Future of Cyber War (duke.edu) ,[Accessed 01/03/23]*

Who created Stuxnet? The creation of Stuxnet is uncertain. But hypotheses regarding the mastermind behind this sophisticated & complex design points towards, the USA *(The United States of America)* & Israel. Due to lack of public statement from any party or actor, it remains enigma. Generally, to avoid the political aspect of this matter, this essay will not provide a clear answer on this issue.

Evaluation of Stuxnet Functionality

What makes Stuxnet worm a complex cyber weapon is its ability to achieve its goal/attacks with minimal interface and it does it by not being detected. The malware is designed to evade detection and it can simply affect computer systems through effected USB-driver.

Once the system is infected, the worm will remain in the system in a passive state till it has accomplished it purpose, in any case to sabotage & perhaps to destroy the target. This was exactly what the worm tried to accomplish, when it was injected into Iran`s nuclear facility at Natanz. To destroy the centrifuges Iran was using to enrich uranium as part of its nuclear program.[4]

To gain a thorough understanding of how the malware works, we should break down its steps into six.[5]

- Infection
- Search
- Update
- Compromise
- Control
- Deceive and Destroy

Infection:

The malware infects all systems running Microsoft Windows via. a USB drive/stick. By providing the system a digital certificate which seems to be provided by a trusted source. By doing so the malware evade most detection and antivirus systems.

Search

Through searching the malware detects if the system or computer is the targeted industrial-control system or if that system is part of the targeted system made by Siemens model S7-315 and S7-417 [6], just like the ones that were installed at the Iran`s nuclear facility.

Update

If the Stuxnet malware detects and finds the targeted system, the worm will attempt to gain access to the internet and update itself to a newer or latest version. This will allow the worm to carry out new instructions or changes to its behavior. Its capability to continuously change and adapt to its surrounding makes the worm hard to evade.

[4] *Fruhlinger J.(2022) : Stuxnet Explained: the first known cyberweapon, Available from: Stuxnet explained: The first known cyberweapon | CSO Online [Accessed 24/02/2023]*

[5] *Kushner D. (2013) The Real Story Of Stuxnet, Available from: The Real Story of Stuxnet - IEEE Spectrum (duke.edu) . [Accessed 27/02/2023]*

[6] *Shakarian P. (2011) Stuxnet : Cyberwar Revolution in Military Affairs , Available from: https://www.academia.edu/694528/Stuxnet_Cyberwar_Revolution_in_Military_Affairs?email_work_card=thumbnail . [Accessed 25/02/2023]*

Compromise

At that stage, the targeted logic controllers have already been compromised by exploiting “Zero day” vulnerabilities, software that wasn`t known to security professionals.

Control

Stuxnet spooks on operations of the targeted system and use the information gathered to take control over the system and carry out its mission. In the case of Iran`s nuclear facility at Natanz, the malware took control of the centrifuges and made them spin to failure.

Deceive and Destroy

The worm generates misleading feedback to external controllers, by doing so it effectively delay their ability to detect it or track the worm and they won`t notice anything is amiss until it`s too late to do anything.

Impact of Stuxnet

As previously noted, this sophisticated computer worm is designed to target mainly industrial control systems, to be specific those installed & used at Natanz nuclear facility. The worm was able to pass through the system and surprisingly alter their code. This caused a significant damage to the centrifuges used for Uranium enrichment.

According to paper provided by the Cyber Conflict Studies Association- call for papers 2012, “the cyber-attack on Natanz successfully delayed the Iranian nuclear program for at least a year and demonstrated the power of a nation-state grade cyber weapon; there was no need for any additional forces.

The impact of Stuxnet can be compared to awakening from a bad dream for the global community. It has proven it`s tremendous power both in terms of its technical capabilities and its role in geopolitical.

Technical capabilities:

Stuxnet has demonstrated its power and its potential to target and sabotage essential infrastructures.

Geopolitical impact:

According to experts, ***“Stuxnet is the world`s first cyber-weapon of geopolitical significance.”*** [7]

It has demonstrated its potential to harm physical damage to critical infrastructures. The attack in Iran`s nuclear program, remains a historical example of cyber warfare and it use in international conflict. “Even after 12 years Stuxnet remains one of the most successful and visible shows of what a cyber-attack can accomplish.” [8]

Stuxnet has opened a new chapter in modern history as technology being used as a weapon in international conflicts. As nations around the globe eagerly pursue their desire to evolve and deploy software-based weapons to shape the future military power, it is essential to examine the geopolitical implications of such arm. The event at Natanz nuclear facility serves as a critical lesson and emphasizes

[7] *Holger Stark(8 August 2011) Stuxnet Virus Opens New Era Of Cyber War, Available from: [Mossad's Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War - DER SPIEGEL] [Accessed 01/03/2023]*

[8] *Myers – Cyber Security : Cybercrime, Attacks and Terrorism (2020) Available from: [1st-cyber-attacks-un-day.pdf (odu.edu)] [Accessed 02/03/2023]*

the need of more robust security measures to combat such attacks/threats.

The geopolitical impact of Stuxnet or any other forms of cyber warfare is significant. To gain a better understanding of its geopolitical implications , the international community need a thorough study of cyber warfare and the challenges it brings to the global security in a term of ethical and legal considerations.

Lesson learned & Takeaways

Though the takeaways are broad , we can draw out some of the most important lessons the world have learned from the attack on Natanz`s nuclear facility.

- Cyberattack: It is a real threat to the world, and it can have a tremendous physical damage to industrial control systems. And it should be taken seriously.
- Zero-days vulnerabilities: The importance of identifying and patching Zero-days vulnerabilities. Stuxnet has utilized multiple zero-day vulnerabilities , which has demonstrated the value of Zero-day vulnerabilities.
- The Origin of Stuxnet: Even though there have been several accusations and speculations, the true origin of Stuxnet has not been officially claimed by any party. This underlines the challenges occur when identifying the responsible actor or country.
- Collaborations: Many claim that Stuxnet is a result of collaboration between USA & Israel. The joint effort by this to countries- if "TRUE" can be taken as a lesson, hence it has demonstrated the potential of collaboration between several parties to carry out a cyberattack.
- The need of improving security practices: The impact on critical infrastructures and industrial control systems has demonstrated the need for a better security measure.

Future scenarios of Stuxnet-like Cyberattacks and their Enigma

As the world becomes more computerized, it is more likely for future Stuxnet-like attacks to occur. Both in the form of cybercriminals or state-sponsored actors , with the main purpose of targeting a critical infrastructure such as a nuclear facility, water purification plants, telecommunications networks, healthcare facilities, food production and distribution systems, transportation systems etc.

A future attack, using more sophisticated worms or malware targeting these infrastructures, may inflict more serious, longer-lasting damage.[9]

An expert in cyberspace policy and cybersecurity and a former United States national cybersecurity coordinator Melissa Hathaway, was quoted as saying " Proliferation of cyber weapons is a real problem, and no country is prepared to deal with it. All of these computer security guys are scared to death. We have about 90 days to fix this new vulnerability before some hacker begins using it."[10]

[9] *Farwell & Rohozinski (2011)Stuxnet & the Future of Cyber War, Available from: https://courses.cs.duke.edu/common/compsci092/papers/cyberwar/stuxnet2.pdf [Accessed 20/02/2023]*

[10] *Glick C. (2010) Column one: The lessons of Stuxnet- The Jerusalem post, Available from: Column one: The lessons of Stuxnet - The Jerusalem Post (jpost.com)   [Accessed 28/02/2023]*

The statement made by Hathaway may sound overstated, but it underlines the fear of the unknown capability of future Stuxnet-like cyberattack and their impact.

What the future holds regarding cyber-attacks verses security remains enigma as terrorists or a non-state actor do not have to own or create Stuxnet-like malware to use the worm.

Former deputy defense secretary William Lynn stated " Cybercrime organizations have been said to "rent" networks of infected computers, known as **botnets** for use in politically motivated cyber attacks on government websites and computer networks. It may become possible for organizations to develop and either rent or sell malware such as Stuxnet or access to infected computers for malicious use against government or civilian infrastructure." [11]

Meanwhile the cascading effect of future Stuxnet-like attacks remains unknown and the enigma of the future of Stuxnet-like attacks versus cybersecurity remains significant concern for the "good guys party".

Conclusion

In summery Stuxnet is the most sophisticated malware modified to target industrial equipment also known as SCADA(Supervisory Control and Data Acquisition). SCADA systems use (PLCs) programable logical controller to control physical component.

The malware mainly targets PLC`s which runs Siemen`s step 7 software. The worm, further targes the following two models: - the siemens s7-315 and s7- 417.

This worm was first unleashed to attack Iran`s nuclear plant at Natanz with a main purpose of sabotaging Iran`s nuclear program. Evidence proves that the attack was successful and resulted a setback for Iran`s nuclear program of at list by 2 years. [12] This attack led to a very critical question: WHO DID IT & WHY? Several studies & news articles, among others: The Guardian and New York time-newspapers point at USA & Israel. [13] [14] [15] [16] Hence, no party or actor has taken a public stand or claimed responsibility.

The attack at Natanz nuclear plant demonstrated to the world that "Cyber Attack" is not a myth but a significant threat to all humankind.

The attack has illustrated that any secured system in the world can be infiltrated and it`s consequence is catastrophic. Causing physical

[11] *CRSReport.com (2010) The Stuxnet Computer Worm, Available from: https://www.everycrsreport.com/reports/R41524.html#fn13 [Accessed 01/03/2023]*

[12] *Katz Y. (2010) Stuxnet virus set back Iran`s nuclear program by 2 years, Available from: 'Stuxnet virus set back Iran's nuclear program by 2 years' - The Jerusalem Post (jpost.com) [Accessed 09/03/23]*

[13] *Beaumont P. (2010) Stuxnet worm heralds new era of global cyberwar- The Guardian, Available from: https://www.theguardian.com/technology/2010/sep/30/stuxnet-worm-new-era-global-cyberwar [Accessed 10/03/2023]*

[14] *Sanger E. (2012) Obama Order Sped Up Wave Of Cyberattacks Against Iran, Available from: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html [Accessed 10/03/2023]*

[15] *Hounshell B. 6 mysteries about Stuxnet (2010), Available from: https://foreignpolicy.com/2010/09/27/6-mysteries-about-stuxnet/ [Accessed 10/03/2023]*

[16] *A Silent Attack, but Not a Subtle one , , Available from: https://www.nytimes.com/2010/09/27/technology/27virus.html [Accessed 10/03/2023]*

damage to critical infrastructures such as a nuclear facility, water purification plants, telecommunications networks, healthcare facilities, food production and distribution systems, transportation systems etc. There is no doubt that Stuxnet serves as a blueprint , shaping the future of Cyber War.

Stuxnet and Stuxnet-like Cyber-attacks has shown to be low in cost than traditional military action. (*There are no numbers which can confirm this statement, but it is widely believed.)* Furthermore, a Cyber-attack is difficult to stop, and hackers have proven the internet is a viable channel through which to insert malware. [17] Which makes malwares such as Stuxnet attractive to both criminals and state-sponsored Organizations. It is crystal clear that, the more the future technology becomes connected to the internet, the chance of malware -attacks like Stuxnet is likely to increase and accelerate.

Nevertheless, the issue of cyber-attack presents a paradoxical quandary– that remains unclear from both ethical and legal perspective, leaving the future uncertain.

---

[17] *Farwell and Rohozinski- Stuxnet and the Future of Cyber War , Available from: Stuxnet and the Future of Cyber War (duke.edu) [Accessed 10/03/2023]*