Cyberattacks [Graded-Optional, 10/7-20/7]

Stuxnet: The Cyberweapon Behind Operation Olympic Games

Yahoo

(2021) Dependency Confusion: Hacked Into Apple, Microsoft and Dozens of Other Companies

Display replies flat, with oldest first

Settings

The cut-off date for posting to this forum is reached so you can no longer post to it.

Stuxnet: The Cyberweapon Behind Operation Olympic Games
by رسول کامکار - Thursday, 13 Mehr 1402, 1:23 PM

Operation Olympic Game

The Olympic Games operation, a covert cyberattack jointly conducted by the United States (NSA) and Israel (Unit 8200), had a profound impact on the Iranian nuclear program. Targeting Iran's uranium enrichment facilities, this operation utilized the Stuxnet worm to sabotage centrifuges, significantly delaying Iran's nuclear ambitions. The operation showcased the strategic use of cyber weapons, underlining their potential to disrupt critical infrastructure and alter the course of international relations.

Started under the administration of George W. Bush in 2006, Olympic Games was accelerated under President Obama, who heeded Bush's advice to continue cyber attacks on the Iranian nuclear facility at Natanz. Bush believed that the strategy was the only way to prevent an Israeli conventional strike on Iranian nuclear facilities.

The Birth of Stuxnet

IN JANUARY 2010, inspectors with the International Atomic Energy Agency visiting the Natanz uranium enrichment plant in Iran noticed that centrifuges used to enrich uranium gas were failing at an unprecedented rate. The cause was a complete mystery.

Five months later a seemingly unrelated event occurred. A computer security firm in Belarus was called in to troubleshoot a series of computers in Iran that were crashing and rebooting repeatedly. Again, the cause of the problem was a mystery. That is, until the researchers found a handful of malicious files on one of the systems and discovered the world's first digital weapon. 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.

The reason for the discovery at this time is attributed to the virus accidentally spreading beyond its intended target (the Natanz plant) and forcing ordinary computers to restart repeatedly, due to a programming error introduced in an update and launched by Unit 8200, without informing NSA.

Why "stux+net"?

The original name given by VirusBlokAda was "Rootkit.Tmphider". Symantec however called it "W32.Temphid" later changing to "W32.Stuxnet" Its current name is derived from a combination of some keywords in the software (".stub" and "mrxnet.sys").

The Maze to Natanz

It was hard to imagine that a piece of malicious software was responsible. After all, Iran's nuclear facilities were air gapped — meaning they weren't connected to a network or the Internet. For a malware attack to occur on the air gapped uranium enrichment plant, someone must have consciously or subconsciously added the malware physically, perhaps through an infected USB drive.

Stuxnet utilized multiple Zero-Day in order to spread and also hide its presence, the worm could spread via USB flash drives using the Windows Autorun feature or through a victim's local network using the print-spooler zero-day exploit that Kaspersky Lab, the antivirus firm based in Russia, and Symantec later found in the code.

To get their weapon into the plant, the attackers launched an offensive against computers owned by four companies. All of the companies were involved in industrial control and processing of some sort, either manufacturing products and assembling components or installing industrial control systems.

Based on the log files in Stuxnet, a company called *Foolad Technic* was the first victim. after that, Stuxnet struck machines belonging to its second victim—a company called *Behpajooh*, It was an engineering firm based in Esfahan in the business of installing and

programming industrial control and automation systems, including Siemens systems. The company's website made no mention of Natanz, but it did mention that the company had installed Siemens S7-400 PLCs, as well as the Step 7 and WinCC software and Profibus communication modules at a steel plant in Esfahan. This was, of course, all of the same equipment Stuxnet targeted at Natanz. Nine days after Behpajooh was hit, Stuxnet struck computers at *Neda Industrial Group*, as well as a company identified in the logs only as *CGJ*, believed to be *Control Gostar Jahed*. Both companies designed or installed industrial control system.

Where Did It Hurt?

An early version of the attack weapon manipulated valves on the centrifuges to increase the pressure inside them and damage the devices as well as the enrichment process. Centrifuges are large cylindrical tubes—connected by pipes in a configuration known as a "cascade"—that spin at supersonic speed to separate isotopes in uranium gas for use in nuclear power plants and weapons. At the time of the attacks, each cascade at Natanz held 164 centrifuges, which is the exact array number experts found in the reversed engineered code, that's how Stuxnet knew it found its target.

Centrifuges spin at extraordinarily fast speeds, creating a force many times faster than gravity in order to separate elements in uranium gas. The worm manipulated the centrifuges' operating speed using PLCs, creating enough stress to damage them. Stuxnet took its time, waiting weeks to slow down the centrifuges after accelerating them temporarily, making its activities hard to detect.

Stuxnet also sent fake industrial process control sensor signals to monitoring devices, in order to hide its presence and malicious activity. In addition, Stuxnet was also able to drop a rootkit. Rootkits can give a threat actor control of a system at its core. With a rootkit installation, Stuxnet was more capable of furtive action.

We Can Do This Too!

The Natanz attack proved to be only a temporary setback in any case. Not only did the program come roaring back stronger than before, and Iran rapidly build a Cyber Army of young people bent on defending their country, but the Iranians mounted cyber attacks of ".their own, successfully targeting Saudi Aramco and several U.S. banks. Their message was clear: "We can do this too

Nitro Zeus

Referring to unnamed sources within the CIA and NSA, the documentary film *Zero Days* claims that the Stuxnet/Olympic Games malware was just a small part of a much larger mission to infiltrate and compromise Iran—"Nitro Zeus" (NZ).

A Mission that makes Olympic Games look like a sandbox game. Aimed to "disrupt, degrade and destroy" Iran's infrastructure, the program would mean "a full scale cyber war," in the words of one expert, a war in which the U.S. would be subject to the same sort of attacks.

References

- The Documentary Film "Zero Days"
- https://en.wikipedia.org/wiki/Stuxnet
- https://www.malwarebytes.com/stuxnet
- https://www.rogerebert.com/reviews/zero-days-2016
- https://www.spiritualityandpractice.com/films/reviews/view/28235/zero-days
- https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet
- https://en.wikipedia.org/wiki/Nitro_Zeus
- https://en.wikipedia.org/wiki/Operation_Olympic_Games

I really advise you to watch the documentary "Zero Days"

Sum of ratings: 50 (1) Permalink

در پاسخ به: Stuxnet: The Cyberweapon Behind Operation Olympic Games
by سحر رمضانی جلفائی - Saturday, 15 Mehr 1402, 12:29 AM

you know, one thing we gotta think about is how these cyberattacks mess with stuff on the world stage and the whole cybersecurity scene. It could be interesting to check out how these operations are messing with diplomatic peeps trying to set the rules in cyberspace

Permalink Show parent

در پاسخ به: Stuxnet: The Cyberweapon Behind Operation Olympic Games
by رسول کامکار - Saturday, 15 Mehr 1402, 4:38 PM

that's a very good point. as it was said in "Zero Days" the problem with today's cyber space is there are no treaties, there are no international rule, anybody can do anything they want.
there's no cyberwarfare equivalent to the treaties governing nukes or biological warfare. Although President Obama has talked of the need to negotiate international agreements, it's not clear how you monitor a digital weapon that can be hidden on something no larger

than a thumb drive. And because all these cyber programs have grown up in the dark — which is now intelligence agencies like them — the public has had little knowledge of, much less influence over their shape and purpose.
basically, everybody wants power, and nobody wants to talk about it.

Sum of ratings: 20 (1) Permalink Show parent

در پاسخ به: Stuxnet: The Cyberweapon Behind Operation Olympic Games
by مهسا ساحلی - Saturday, 15 Mehr 1402, 7:00 PM

If I want to explain the name of this attack, Stuxnet, according to the information stated in the Zero Days documentary, I must say:

The main name of this attack was "Operation Olympic Games" or "Attack on Natanz," which is the code name of this program in the cybersecurity institutions of America and Israel, namely NSA and Section 8200 in the Cyber Intelligence Organization of Israel. However, after it was identified to be known worldwide by a single name, the coders chose the name Stuxnet by using the words in its binary code and connecting them together.

For more explanation about the Stuxnet virus, you can refer to the following content:

Stuxnet is a virus whose code is 20 times larger than a normal malicious code. The code of this virus is very dense, and each part of it has a specific task. However, there are no security bugs in it, which is one of the features that has attracted the attention of programmers. A code with this volume, density, complexity, and without security bugs cannot have been written by one or more people alone; it must have had government support.

Now let's talk about the Stuxnet structure:

The Stuxnet virus uses four unknown zero days to attack, which is a significant number for a malicious code. Out of the millions of malicious codes found each year, only about 12 zero days are detected. This is another reason why it is said that this virus has benefited from the support of one or more governments.

Stuxnet has three main modules:

- Worm

- Link file

- Rootkit

The task of the worm module is to infect the system and create all the necessary conditions to transmit the virus to the device. The link file module is responsible for running worms distributed in each part, and the rootkit is responsible for hiding these processes and keeping the code hidden in the system.

How it works:

In order to achieve low-level access in Windows and remain hidden in the system, Stuxnet must present itself as a non-malicious program with a digital certificate. It must be recognized as authentic by Windows and be able to receive a certificate from Microsoft for its activities. In fact, a part of its code shows valid digital certificates related to two famous companies, Realtek and JMicron.

In the documentary Zero Days, it is mentioned that these digital certificates were stolen from these companies through security agents. However, considering the fact that this code was written by an organization like the NSA, there is no need to steal these certificates. The private keys required for confirming these certificates are all produced with the approval of the NSA and given to different companies. Therefore, all these private keys are with the NSA, and there is no need to steal them. Stealing these certificates is a very difficult task due to their high importance and strict protections, and accessing them is not easy at all; it can even be said that it is impossible.

Stuxnet can be called a revolution in malicious coding because:

Before Stuxnet was written, viruses took instructions from the operator to perform their operations and how to react at each stage or exactly when to start which operation, but Stuxnet was designed in such a way that as soon as it entered the network, it managed all the operations automatically. That is, all the logic needed to attack and reach the desired goal is included in its code, and as soon as it enters the systems, the virus itself starts making decisions.

Whether the place where it is located is Natanz or not? Is the system that is entered related to PLCs or not? Are the PLCs controlled by this system specified as the same type or not? And many other questions that the virus will automatically look for answers to and will begin to operate if it is sure that it has reached the target system.

Comprehensive Course and Method of Sabotage:

Stuxnet remains in Natanz for 13 days without any activity because it takes 13 days to fill the centrifuges with uranium and initiate the enrichment process. The virus is designed in such a way that it does not start its operation when the centrifuges are empty or even during the initiation of the enrichment process. Instead, it activates itself during the midst of the enrichment process, causing the

maximum damage to the systems.

During these 13 days, Stuxnet records the processes that take place in Natanz before the enrichment phase. The centrifuges are connected to a rotor for rotation, and the rotation speed of this rotor is controlled by PLCs. SCADA systems in the control room monitor all the processes carried out by these PLCs. After the initiation of the enrichment process, the rotation speed of the centrifuges reaches 300 meters per second, which is equivalent to the speed of sound.

Since the pipes inside the centrifuges are not completely straight and have curvature, resembling the shape of a banana, they need to be carefully rotated. Any interference in their rotation disrupts their balance and eventually leads to their explosion. What the Stuxnet virus does with the centrifuge rotors is that it first increases their speed from 65,000 revolutions per minute to 80,000 revolutions per minute, and then intermittently reduces their speed until they come to a complete stop. This action, considering the physical structure of the centrifuges mentioned above, causes their explosion.

To better understand this event, one can refer to the example of a spinning top that starts to throw the anchor when it stops spinning, and the slower its speed becomes, the more anchor it throws until it completely stops moving. A similar process occurs in centrifuges, which is why the pipes collide with the outer wall and explode. During this process, the operators in the control room hear a very loud noise from the centrifuges, similar to the sound of a fighter jet engine, but the SCADA devices facing them do not show any reports of malfunction because the Stuxnet virus sends them old reports recorded in advance. As a result, they do not receive any warnings from the PLCs. However, since this sound is very unusual, the operators naturally think of manually shutting down the centrifuges, but the Stuxnet virus does not allow them to do so and prevents the stop command from reaching the PLCs.

Stuxnet is written in the best possible way, but since it does not have access to the outside world of Natanz, it is unable to send reports to its commanders. This is where the role of atomic energy inspectors becomes prominent. After their periodic visits to Natanz, the inspectors include all the events that have taken place there in their reports, and as a result, the United States easily realizes that its operation has been successful and is progressing according to plan.

References:

- Mashreq news agency reviews
- Clarification of US national security
- Zero Days documentary

Permalink Show parent

⇥ Yahoo (2021) Dependency Confusion: Hacked Into Apple, Microsoft and Dozens of Other Companies ⇤