Stuxnet

Stuxnet is a malicious computer worm first uncovered on June 17, 2010, and thought to have been in development since at least 2005. Stuxnet targets supervisory control and data acquisition (SCADA) systems and is believed to be responsible for causing substantial damage to the Iran nuclear program. Although neither the United States nor Israel has openly admitted responsibility, multiple independent news organizations claim Stuxnet to be a cyberweapon built jointly by the two countries in a collaborative effort known as Operation Olympic Games. The program, started during the Bush administration, was rapidly expanded within the first months of Barack Obama's presidency.

Stuxnet specifically targets programmable logic controllers (PLCs), which allow the automation of electromechanical processes such as those used to control machinery and industrial processes including gas centrifuges for separating nuclear material. Exploiting four zero-day flaws in the systems, Stuxnet functions by targeting machines using the Microsoft Windows operating system and networks, then seeking out Siemens Step7 software. Stuxnet reportedly compromised Iranian PLCs, collecting information on industrial systems and causing the fast-spinning centrifuges to tear themselves apart. Stuxnet's design and architecture are not domain-specific and it could be tailored as a platform for attacking modern SCADA and PLC systems (e.g., in factory assembly lines or power plants), most of which are in Europe, Japan and the United States. Stuxnet reportedly destroyed almost one-fifth of Iran's nuclear centrifuges. Targeting industrial control systems, the worm infected over 200,000 computers and caused 1,000 machines to physically degrade.

Stuxnet has three modules: a worm that executes all routines related to the main payload of the attack, a link file that automatically executes the propagated copies of the worm and a rootkit component responsible for hiding all malicious files and processes to prevent detection of Stuxnet. It is typically introduced to the target environment via an infected USB flash drive, thus crossing any air gap. The worm then propagates across the network, scanning for Siemens Step7 software on computers controlling a PLC. In the absence of either criterion, Stuxnet becomes dormant inside the infected rootkit onto the PLC and Step7 software, modifying the code and giving unexpected commands to the PLC while returning a loop of normal operation system values back to the users.

Discovery

Stuxnet, discovered by Sergey Ulasen from a Belarusian antivirus company VirusBlokAda, initially spread via Microsoft Windows, and targeted Siemens industrial control systems. While it is not the first time that hackers have targeted industrial systems, nor the first publicly known intentional act of cyberwarfare to be implemented, it is the first discovered malware that spies on and subverts industrial systems, and the first to include a programmable logic controller (PLC) rootkit.

The worm initially spreads indiscriminately, but includes a highly specialized malware payload that is designed to target only Siemens supervisory control and data acquisition (SCADA) systems that are configured to control and monitor specific industrial processes. Stuxnet infects PLSs by subverting the Step-7 software application that is used to reprogram these devices.

Different variants of Stuxnet targeted five Iranian organizations, with the probable target widely suspected to be uranium enrichment infrastructure in Iran; Symantec noted in August 2010 that 60 percent of the infected computers worldwide were in Iran. Siemens stated that the worm caused no damage to its customers, but the Iran nuclear program, which uses embargoed Siemens equipment procured secretly, was damaged by Stuxnet. Kaspersky Lab concluded “with nation-state support.” F-Secure’s chief researcher Mikko Hyppönen, when asked if possible nation-state support were involved, agreed: “That’s what it would look like, yes.”

In May 2011, the PBS program Need To Know cited a statement by Gary Samore, White House Coordinator for Arms Control and Weapons of Mass Destruction, in which he said, “we’re glad they [the Iranians] are having trouble with their centrifuge machine and that we - the U.S. and its allies - are doing everything we can to make sure that we complicate matters for them,” offering “winking acknowledgement” of United States involvement in Stuxnet. According to The Daily Telegraph, a showreel that was played at a retirement party for the head of the Israel Defense Forces (IDF), Gabi Ashkenazi, included references to Stuxnet as one of his operational successes as the IDF chief of staff.

On 1 June 2012, an article in The New York Times reported that Stuxnet was part of a US and Israeli intelligence operation named Operation Olympic Games, devised by the NSA under President George W. Bush and executed under President Barack Obama.

On 24 July 2012, an article by Chris Maryszczyk from CNET reported that the Atomic Energy Organization of Iran e-mailed F-Secure’s chief research officer Mikko Hyppönen to report a new instance of malware.

On 25 December 2012, an Iranian semi-official news agency announced there was a cyberattack by Stuxnet, this time on the industries in the southern area of the country. The malware targeted a power plant and some other industries in Hormozgan province in recent months.

According to Eugene Kaspersky, the worm also infected a nuclear power plant in Russia. Kaspersky noted, however, that since the power plant is not connected to the public Internet, the system should remain safe.

History

The worm was first identified by the security company VirusBlockAda in mid-June 2010. Journalist Brian Krebs’s blog post on 15 July 2010 was the first widely read report on the worm. The original name given by VirusBlockAda was “Rootkit.Tmphider;” Symantec, however, called it “W32.Temphid,” later changing it to “W32.Stuxnet.” Its current name is derived from a combination of keywords found in the software (“.stub” and mrxnet.sys”). The timing of the discovery has been attributed to the virus accidentally spreading beyond its intended target due to a programming error introduced in an update. This may have caused the worm to spread to an engineer’s computer connected to the centrifuges, further propagating when the engineer later connected to the internet at home.

Kaspersky Lab experts initially estimated that Stuxnet began spreading around March or April 2010, but the first variant of the worm appeared in June 2009. On 15 July 2010, the day the worm’s existence became widely known, a distributed denial-of-service attack targeted the servers of two leading mailing lists on industrial-systems security. This attack, from an unknown source but possibly related to Stuxnet, disabled one of the lists, interrupting a key information source for power plants and factories. Separately, researchers at Symantec uncovered a version of the Stuxnet computer virus that was used to attack Iran’s nuclear program in November 2007, with evidence indicating it was under development as early as 2005, when Iran was still setting up its uranium enrichment facility.

The second variant, with substantial improvements, appeared in March 2010, reportedly due to concerns that Stuxnet was not spreading fast enough. A third variant, with minor improvements, followed in April 2010. The worm contains a component with a build timestamp from 3 February 2010. On 25 November 2010, Sky News in the United Kingdom reported receiving information from an anonymous source at an unidentified IT security organization claiming that Stuxnet, or a variation of the worm, has been traded on the black market.

In 2015, Kaspersky Lab reported that the Equation Group has used two of the same zero-day attacks prior to their use in Stuxnet, in another malware called fanny.bmp. Kaspersky Lab noted that “the similar type of usage of both exploits together in different computer worms, at around the same time, indicates that the Equation Group and the Stuxnet developers are either the same or working closely together.”

In 2019, Chronicle researchers Juan Andres Guerrero-Saade and Silas Culter presented findings indicating that at least four distinct threat actor malware platforms collaborated in developing the different versions of Stuxnet. The collaboration was referred to as ‘GOSSIP GIRL’, a name derived from a threat group mentioned in classified CSE slides that included Flame. GOSSIP GIRL is described as a cooperative umbrella encompassing the Equation Group, Flame, Duqu, and Flowershop (also known as ‘Cheshire Cat’).

In 2020, researcher Facundo Muñoz presented findings suggesting that Equation Group may have collaborated with Stuxnet developers in 2009 by providing at least one zero-day exploit, and one exploit from 2008 that was actively used by the Coficker computer worm and Chinese hackers. In 2017, a group of hackers known as The Shadow Brokers leaked a collection of tools attributed to Equation Group, including new versions of both exploits compiled in 2010. Analysis of the leaked data indicated significant code overlaps, as both Stuxnet’s exploits and Equation

Group’s exploits were developed using a set of libraries called the “Exploit Development Framework”, also leaked by The Shadow Brokers.

Affected countries

A study of the spread of Stuxnet by Symantec showed that the main affected countries in the early days of the infection were Iran, Indonesia and India:

Iran was reported to have fortified its cyberwar abilities following the Stuxnet attack, and has been suspected of retaliatory attacks against United States banks in Operation Ababil.

Operation

Unlike most malware, Stuxnet does little harm to computers and networks that do not meet specific configuration requirements; “The attackers took great care to make sure that only their designated targets were hit … It was marksman’s job.” While the worm is promiscuous, it makes itself inert if Siemens software is not found on infected computers, and contains safeguards to prevent each infected computer from spreading the worm to more than three others, and to erase itself on 24 June 2012.

For its targets, Stuxnet contains, among other things, code for a man-in-the-middle attack that fakes industrial process control sensor signals so an infected system does not shut down due to detected abnormal behavior. Such complexity is unusual for malware. The worm consists of a layered attack against three different systems:

1. The Windows operating system,
2. 2. Siemens PCS 7, WinCC and STEP7 industrial software applications that run on Windows and
3. One or more Siemens S7 PLCs.

Windows infection

Stuxnet attacked Windows systems using an unprecedented four zero-day attacks (plus the CPLINK vulnerability and a vulnerability used by the Conficker worm). It is initially spread using infected removable drives such as USB flash drives, which contain Windows shortcut files to initiate executable code. The worm then uses other exploits and techniques such as peer-to-peer remote procedure call (RPC) to infect and update other computers inside private networks that are not directly connected to the Internet. The number of zero-day exploits used is unusual, as they are highly valued and malware creators do not typically make use of (and thus simultaneously make visible) four different zero-day exploits in the same worm. Amongst these exploits were remote code execution on a computer with Printer Sharing enabled, and the LNK/PIF vulnerability, in which file execution is accomplished when an icon is viewed in Windows Explorer, negating the need for user interaction. Stuxnet is unusually large at half a megabyte in size, and written in several different programming languages (including C and C++)

which is also irregular for malware. The Windows component of the malware is promiscuous in that it spreads relatively quickly and indiscriminately.

The malware has both user mode and kernel mode rootkit ability under Windows, and its device drivers have been digitally signed with the private keys of two public key certificates that were stolen from separate well-known companies, JMicron and Realtek, both located at Hsinchu Science Park in Taiwan. The driver signing helped it install kernel mode rootkit drivers successfully without users being notified, and thus it remained undetected for a relatively long period of time. Both compromised certificates have been revoked by Verisign.

Two websites in Denmark and Malaysia were configured as command and control servers for the malware, allowing it to be updated, and for industrial espionage to be conducted by uploading information. Both of these domain names have subsequently been redirected by their DNS service provider to Dyanadot as part of a global effort to disable the malware.

Step 7 software infection

According to researcher Ralph Langner, once installed on a Windows system, Stuxnet infects project files belonging to Siemens' WinCC/PCS 7 SCADA control software (Step 7), and subverts a key communication library of WinCC called s7otbxdx.dll. Doing so intercepts communications between the WinCC software running under Windows and the target Siemens PLC devices, when the two are connected via a data cable. The malware is able to modify the code on PLC devices unnoticed, and subsequently to mask its presence from WinCC if the control software attempts to read an infected block of memory from the PLC system.

The malware furthermore used a zero-day exploit in the WinCC/SCADA database software in the form of a hard-coded database password.

PLC infection

Stuxnet's payload targets only those SCADA configurations that meet criteria that it is programmed to identify.

Stuxnet requires specific subordinate system to be attached to the targeted Siemens S7-300 controller system: variable-frequency drives (frequency converter drives) and its associated modules. It only attacks those PLC systems with variable-frequency drives from two specific vendors: Vacon based in Finland and Fararo Paya based in Iran. Furthermore, it monitors the frequency of the attacked motors, and only attacks systems that spin between 807 Hz and 1,210 Hz. This is a much higher frequency than motors typically operate at in most industrial applications, with the notable exception of gas centrifuges. Stuxnet installs malware into memory block DB890 of the PLC that monitors the Profibus messaging bus of the system. When certain criteria are met, it periodically modifies the frequency to 1,410 Hz and then to 2 Hz and then to 1,064 Hz, and thus affects the operation of the connected motors by changing their rotational speed. It also installs a rootkit - the first such documented case on this platform - that hides the malware on the system and masks the changes in rotational speed from monitoring systems.

Removal

Siemens has released a detection and removal tool for Stuxnet. Siemens recommends contacting customer support if an infection is detected and advises installing Microsoft updates for security vulnerabilities and prohibiting the use of third-party USB flash drives. Siemens also advises immediately upgrading password access codes.

The worm’s ability to reprogram external PLCs may complicate the removal procedure. Symantec’s Liam O’Murchu warns that fixing Windows systems may not fully solve the infection; a thorough audit of PLCs may be necessary. Despite speculation that incorrect removal of the worm could cause damage, Siemens reports that in the first four months since discovery, the malware was successfully removed from the system of 22 customers without any adverse effect.

Control system security

Prevention of control system security incidents, such as from viral infections like Stuxnet, is a topic that is being addressed in both the public and the private sector.

The US Department of Homeland Security National Cyber Security Division (NCSD) operates the Control System Security Program (CSSP). The program operates a specialized computer emergency response team called the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), conducts a biannual conference (ICSJWG), provides training, publishes recommended practices, and provides a self-assessment tool. As part of a Department of Homeland Security plan to improve American computer security, in 2008 it and the Idaho National Laboratory (INL) worked with Siemens to identify security holes in the company’s widely used Process Control System 7 (PCS 7) and its software Step 7. In July 2008, INL and Siemens publicly announced flaws in the control system at a Chicago conference; Stuxnet exploited these holes in 2009.

Several industry organizations and professional societies have published standards and best practice guidelines providing direction and guidance for control system end-users on how to establish a control system security management program. The basic premise that all of these documents share is that prevention requires a multi-layered approach, often termed defence in depth. The layers include policies and procedures, awareness and training, network segmentation, access control measures, physical security measures, system hardening, e.g., patch management, and system monitoring, anti-virus and intrusion prevention system (IPS). The standards and best practices also all recommend starting with a risk analysis and a control system security assessment.

Target and origin

Experts believe that Stuxnet required the largest and costliest development effort in malware history. Developing its abilities would have required a team of capable programmers, in-depth knowledge of industrial processes, and an interest in attacking industrial infrastructure. Eric Byres, who has years of experience maintaining and troubleshooting Siemens systems, told Wired that writing the code would have taken many man-months, if not man-years. Symantec estimates that the group developing Stuxnet would have consisted of between five and thirty people, and would have taken six months to prepare. The Guardian, the BBC and The New York Times all claimed that (unnamed) experts studying Stuxnet believe the complexity of the code indicates that only a nation-state would have the abilities to produce it. The self-destruct and other safeguards within the code implied that a Western government was responsible, or at least is responsible for its development. However, software security expert Bruce Schneier initially condemned the 2010 news coverage of Stuxnet as hype, stating that it was almost entirely based on speculation. But after subsequent research Schneier stated in 2012 that “we can now conclusively link Stuxnet to the centrifuge structure at the Natanz nuclear enrichment lab in Iran.

In January 2024, de Volkskrant reported that Dutch engineer Erik van Sabben was the saboteur who had infiltrated the underground nuclear complex in the city of Natanz and installed equipment infected with Stuxnet.

Iran as a target

Ralph Langner, the researcher who identified that Stuxnet infected PLCs, first speculated publicly in September 2010 that the malware was of Israeli origin, and that it targeted Iranian nuclear facilities. However Langner more recently, at a TED conference, recorded in February 2011, stated that, “My opinion is that the Mossad is involved, but that the leading force is not Israel. The leading force behind Stuxnet is the cyber superpower - there is only one; and that’s the United States.” Kevin Hogan, Senior Director of Security Response at Symantec, reported that most infected systems were in Iran (about 60%), which has led to speculation that it may have been deliberately targeting “high-value infrastructure” in Iran including either the Bushehr Nuclear Power Plant or the Natanz nuclear facility. Langner called the malware “a one-shot weapon” and said that the intended target was probably hit, although he admitted this was speculation. Another German researcher and spokesman of the German-based Chaos Computer Club, Frank Rieger, was the first to speculate that Natanz was the target.

Natanz nuclear facilities

According to the Israeli newspaper Haaretz, in September 2010 experts on Iran and computer security specialists were increasingly convinced that Stuxnet was meant “to sabotage the uranium enrichment facility at Natanz - where the centrifuge operational capacity had dropped over the past year by 30 percent.” On 23 November 2010 it was announced that uranium enrichment at Natanz has ceased several times because of a series of major technical problems. A “serious nuclear accident” (supposedly the shutdown of some of its centrifuges) occurred at the site in the first half of 2009, which is speculated to have forced Gholam Reza Aghazadeh, the head of the Atomic Energy Organization of Iran (AEOI), to resign. Statistics published by the Federation of American Scientists (FAS) show that the number of enrichment centrifuges operational in Iran mysteriously declined from about 4,700 to about 3,900 beginning around the time the nuclear incident WikiLeaks mentioned would have occurred. The Institute for Science and International Security (ISIS) suggests, in a report published in December 2010, that Stuxnet is a reasonable explanation for the apparent damage at Natanz, and may have destroyed up to 1,000 centrifuges (10 percent) sometime between November 2009 and late January 2010. The authors conclude:

The attacks seem designed to force a change in the centrifuge’s rotor speed, first raising the speed and then lowering it, likely with the intention of inducing excessive vibrations or distortions that would destroy the centrifuge. If its goal was to quickly destroy all the centrifuges in the FEP [Fuel Enrichment Plant], Stixnet failed. But if the goal was to destroy a more limited number of centrifuges and set back Iran’s progress in operating the FEP, while making detection difficult, it may have succeeded, at least temporarily.

The Institute for Science and International Security (ISIS) report further notes that Iranian authorities have attempted to conceal the breakdown by installing new centrifuges on a large scale.

The worm worked by first causing an infected Iranian IR-1 centrifuge to increase from its normal operating speed of 1,064 hertz to 1,410 hertz for 15 minutes before returning to its normal frequency. Twenty-seven days later, the worm went back into action, slowing the infected centrifuges down to a few hundred hertz for a full 50 minutes. The stresses from the excessive, then slower, speeds caused the aluminium centrifugal tubes to expand, often forcing parts of the centrifuges into sufficient contact with each other to destroy the machine.

According to The Washington Post, International Atomic Energy Agency (IAEA) cameras installed in the Natanz facility recorded the sudden dismantling and removal of approximately 900 - 1,000 centrifuges during the time the Stuxnet worm was reportedly active at the plant. Iranian technicians, however, were able to quickly replace the centrifuges and the report concluded that uranium enrichment was likely only briefly disrupted.
On 15 February 2011, the Institute for Science and International Security released a report concluding that:

Assuming Iran exercises caution, Stuxnet is unlikely to destroy more centrifuges at the Natanz plant. Iran likely cleaned the malware from its control systems. To prevent re-infection, Iran will have to exercise special caution since so many computers in Iran contain Stuxnet. Although Stuxnet appears to be designed to destroy centrifuges at the Natanz facility, destruction was by no means total. Moreover, Stuxnet did not lower the production of low enriched uranium (LEU) during 2010. LEU quantities could have certainly been grated, and Stuxnet could be an important part of the reason why they did not increase significantly. Nonetheless, there remain important questions about why Stuxnet destroyed only 1,000 centrifuges. One observation is that it may be harder to destroy centrifuges by use of cyber attacks than often believed.

Iranian reaction

The Associated Press reported that the semi-official Iranian Students News Agency released a statement on 24 September 2010 stating that experts from the Atomic Energy Organization of Iran met in the previous week to discuss how Stuxnet could be removed from their systems. According to analysts, such as David Albright, Western intelligence agencies had been attempting to sabotage the Iranian nuclear program for some time.

The head of the Bushehr Nuclear Power Plant told Reuters that only the personal computer of staff at the plant had been infected by Stuxnet and the state-run newspaper Iran Daily quoted Reza Taghipour, Iran’s telecommunications minister, as saying that it had not caused “serious damage to government systems”. The Director of Information Technology Council at the Iranian Ministry of Industries and Mines, Mahmud Liaii, has said that: “An electronic war has been launched against Iran… This computer worm is designed to transfer data about production lines from our industrial plants to locations outside Iran.”

In response to the infection, Iran assembled a team to combat it. With more than 30,000 IP addresses affected in Iran, an official said that the infection was fast spreading in Iran and the problem had been compounded by the ability of Stuxnet to mutate. Iran had set up its own systems to clean up infections and had advised against using the Siemens SCADA antivirus since it is suspected that the antivirus contains embedded code which updates Stuxnet instead of removing it.

According to Hamid Alipour, deputy head of Iran’s government Information Technology Company, “The attack is still ongoing and new versions of this virus are spreading.” He reported that his company had begun the cleanup process at Iran’s “sensitive centres and organizations.” “We had anticipated that we could root out the virus within one to two months, but the virus is not stable, and since we started the cleanup process three new versions of it have been spreading”, he told the Islamic Republic News Agency on 27 September 2010.

On 29 November 2010, Iranian president Mahmoud Ahmadinejad stated for the first time that a computer virus had caused problems with the controller handling the centrifuges at its Natanz facilities. According to Reuters, he told reporters at a news conference in Tehran, “They succeeded in creating problems for a limited number of our centrifuges with the software they had installed in electronic parts.”

On the same day two Iranian nuclear scientists were targeted in separate, but nearly simultaneous car bomb attacks near Shahid Beheshti University in Tehran. Majid Shahriari, a quantum physicist, was killed. Fereydoon Abbasi, a high-ranking official at the Ministry of Defence was seriously wounded. Wired speculated that the assassinations could indicate that whoever was behind Stuxnet felt that it was not sufficient to stop the nuclear program. That same Wired article suggested the Iranian government could have been behind the assassinations. In January 2010, another Iranian nuclear scientist, a physics professor at Tehran University, was killed in a similar bomb explosion. On 11 January 2012, a director of the Natanz nuclear enrichment facility, Mostafa Ahmadi Roshan, was killed in an attack quite similar to the one that killed Shahriari.

An analysis by the FAS demonstrates that Iran's enrichment capacity grew during 2010. The study indicated that Iran's centrifuges appeared to be performing 60% better than in the previous year, which would significantly reduce Tehran's time to produce bomb-grade uranium. The FAS report was reviewed by an official with the IAEA who affirmed the study.

European and US officials, along with private experts, told Reuters that Iranian engineers were successful in neutralizing and purging Stuxnet from their country's nuclear machinery.

Given the growth in Iranian enrichment ability in 2010, the country may have intentionally put out misinformation to cause Stuxnet's creators to believe that the worm was more successful in disabling the Iranian nuclear program than it actually was.

Israel

Israel, through Unit 8200, has been speculated to be the country behind Stuxnet in multiple media reports and by experts such as Richard A. Flakenrath, former Senior Director for Policy and Plans within the US Office of Homeland Security. Yossi Melman, who covers intelligence for Israeli newspaper Haaretz and wrote a book about Israeli intelligence, also suspected that Israel was involved, noting that Meir Dagan, the former (up until 2011) head of the national intelligence agency Mossad, had his term extended in 2009 because he was said to be involved in important projects. Additionally, in 2010 Israel grew to expect that Iran would have a nuclear weapon in 2014 or 2015 - at least three years later than earlier estimates - without the need for an Israeli military attack on Iranian nuclear facilities; "They seem to know something, that they have more time than originally thought", he added. Israel has not publicly commented on the Stuxnet attack but in 2010 confirmed that cyberwarfare was now among the pillars of its defense doctrine, with a military intelligence unit set up to pursue both defensive and offensive options. When questioned whether Israel was behind the virus in the fall of 2010, some Israeli officials broke into "wide smiles", fueling speculation that the government of Israel was involved with its genesis. American presidential advisor Gary Samore also smiled when Stuxnet was mentioned, although American officials have suggested that the virus originated abroad. According to The Telegraph, Israeli newspaper Haaretz reported that a video celebrating operational successes of Gabi Ashkenazi, retiring Israel Defense Forces (IDF) Chief of Staff, was shown at his retirement party and included references to Stuxnet, thus strengthening claims that Israel's security forces were responsible.

In 2009, a year before Stuxnet was discovered, Scott Borg of the United States Cyber-Consequences Unit (US-CCU) suggested that Israel may prefer to mount a cyberattack rather than a military strike on Iran’s nuclear facilities. In late 2010 Borg stated, “Israel certainly has the ability to create Stuxnet and there is little downside to such an attack because it would be virtually impossible to prove who did it. So a tool like Stuxnet is Israel’s obvious weapon of choice.” Iran uses P-1 centrifuges at Natanz, the design for which A. Q. Khan stole in 1976 and took to Pakistan. His black market nuclear-proliferation network sold P-1s to, among other customers, Iran. Experts believe that Israel also somehow acquired P-1s and tested Stuxnet on the centrifuges, installed at the Dimona facility that is part of its own nuclear program. The equipment may be from the United States, which received P-1s from Libya’s former nuclear program.

Some have also cited several clues in the code such as a concealed reference to the word MYRTUS, believed to refer to the Latin name myrtus of the Myrtle tree, which in Hebrew is called hadassah. Hadassah was the birth name of the former Jewish queen of Persia, Queen Esther. However, it may be that the “MYRTUS” reference is simply a misinterpreted reference to SCADA components known as RTUs (Remote Terminal Units) and that this reference is actually “My RTUs”-a management feature of SCADA. Also, the number 19790509 appears once in the code and may refer to the date 1979 May 09, the day Habib Elghanian, a Persian Jew, was executed in Tehran. Another date that appears in the code is “24 September 2007”, the day that Iran’s president Mahmoud Ahmadinejad spoke at Columbia University and made comments questioning the validity of the Holocaust. Such data is not conclusive, since as noted by Symantec, "...attackers would have the natural desire to implicate another party”.

United States

There has also been reports on the involvement of the United States and its collaboration with Israel, with one report stating that “there is vanishingly little doubt that [it] played a role in creating the worm.” It has been reported that the United States, under one of its most secret programs, initiated by the Bush administration and accelerated by the Obama administration, has sought to destroy Iran’s nuclear program by novel methods such as undermining Iranian computer systems. A leaked diplomatic cable showed how the United States was advised to target Iran’s nuclear abilities through ‘convert sabotage’. An article in The New York Times in January 2009 credited a then-unspecified program with preventing an Israeli military attack on Iran where some of the efforts focused on ways to destabilize the centrifuges. A Wired article claimed that Stuxnet “is believed to have been created by the United States”. Dutch historian Peter Koop speculated that the Tailored Access Operations could have developed Stuxnet, possibly in collaboration with Israel.

The fact that John Bumgarner, former intelligence officer and member of the United States Cyber-Consequences Unit (US-CCU), published an article prior to Stuxnet being discovered or deciphered, that outlined a strategic cyber strike on centrifuges and suggests that cyber attacks are permissible against nation states which are operating uranium enrichment programs that violate international treaties gives some credibility to these claims. Bumgarner pointed out that centrifuges used to process fuel for nuclear weapons are a key target for cybertage operations and that they can be made to destroy themselves by manipulating their rotational speeds.

In a March 2012 interview with 60 Minutes, retired US Air Force General Michael Hayden - who served as director of both the Central Intelligence Agency and National Security Agency - while denying knowledge of who created Stuxnet said that he believed it had been “a good idea” but that it carried a downside in that it had legitimized the use of sophisticated cyber weapons designed to cause physical damage. Hyden said, “There are those out there who can take a look at this… and maybe even attempt to turn it to their own purposes”. In the same report, Sean McGurk, a former cybersecurity official at the Department of Homeland Security noted that the Stuxnet source code could now be downloaded online and modified to be directed at new target systems. Speaking of the Stuxnet creators, he said, “They opened the box. They demonstrated the capability… It’s not something that can be put back.”

Joint effort and other states and targets

In April 2011, Iranian government official Gholam Reza Jalali stated that an investigation had concluded that the United States and Israel were behind the Stuxnet attack. Frank Reiger stated that three European countries’ intelligence agencies agreed that Stuxnet was a joint United States-Israel effort. The code for the Windows injector and the PLC payload differ in style, likely implying collaboration. Other experts believe that a US-Israel cooperation is unlikely because “the level of trust between the two countries’ intelligence and military establishments is not high.”

A Wired magazine article about US General Keith B. Alexander stated: “And he and his cyber warriors have already launched their first attack. The cyber weapon that came to be known as Stuxnet was created and built by the NSA in partnership with the CIA and Israeli intelligence in the mid-2000s.”

China, Jordan, and France are other possibilities, and Siemens may have also participated. Langner speculated that the infection may have spread from USB drives belonging to Russian contractors since the Iranian targets were not accessible via the Internet. In 2019, it was reported that an Iranian mole working for Dutch intelligence at the behest of Israel and the CIA inserted the Stuxnet virus with a USB flash drive or convinced another person working at the Natanz facility to do so.

Sandro Gaycken from the Free University Berlin argued that the attack on Iran was a ruse to distract from Stuxnet’s real purpose. According to him, its broad dissemination in more than 100,000 industrial plants worldwide suggests a field test of a cyber weapon in different security cultures, testing their preparedness, resilience, and reactions, all highly valuable information for a cyberwar unit.

The United Kingdom has denied involvement in the worm’s creation.

In July 2013, Edward Snowden claimed that Stuxnet was cooperatively developed by the United States and Israel.

Deployment in North Korea

According to a report by Reuters, the NSA also tried to sabotage North Korea's nuclear program using a version of Stuxnet. The operation was reportedly launched in tandem with the attack that targeted Iranian centrifuges in 2009-10. The North Korean nuclear program shares a number of similarities with the Iranian, both having been developed with technology transferred by Pakistani nuclear scientist A.Q.Khan. The effort failed, however, because North Korea's extreme secrecy and isolation made it impossible to introduce Stuxnet into the nuclear faiclity.

Stuxnet 2.0 cyberattack

In 2018, Gholamreza Jalali, Iran's chief of the National Passive Defence Organisation (NPDO), claimed that his country fended off a Stuxnet-like attack targeting the country's telecom infrastructure. Iran's Telecommunications minister Mohammad-Javad Azari Jarhomi has since accused Israel of orchestrating the attack. Iran plans to sue Israel through the International Court of Justice (ICJ) and is also willing to launch a retaliation attack if Israel does not desist.

Related malware

"Stuxnet's Secret Twin"

A November 2013 article in Foreign Policy magazine claims existence of an earlier, much more sophisticated attack on the centrifuge complex at Natanz, focused on increasing centrifuge failure rate over a long time period by stealthily inducing uranium hexafluoride gas overpressure incidents. This malware was capable of spreading only by being physically installed, probably by previously contaminated field equipment used by contractors working on Siemens control systems within the complex. It is not clear whether this attack attempt was successful, but follow-up by a different, simpler, and more conventional attack is indicative that it was not.

Duqu

On 1 September 2011, a new worm was found, thought to be related to Stuxnet. The Laboratory of Cryptography and System Security (CrSyS) of the Budapest University of Technology and Economics analyzed the malware, naming the threat Duqu. Symantec, based on this report, continued the analysis of the threat, calling it "nearly identical to Stuxnet, but with a completely different purpose", and published a detailed technical paper. The main component used in Duqu is designed to capture information such as keystrokes and system information. The exfiltrated data may be used to enable a future Stuxnet-like attack. On 28 December 2011, Kaspersky

Lab's director of global research and analysis spoke to Reuters about recent research results showing that the platform Stuxnet and Duqu both originated in 2007, and is being referred to as Tilded due to the ~d at the beginning of the file names. Also uncovered in this research was the possibility for three more variants based on the Tilded platform.

Flame

In May 2012, the new malware "Flame" was found, thought to be related to Stuxnet. Researchers named the program "Flame" after the name of one of its modules. After analysing the code of Flame, Kaspersky Lab said that there is a strong relationship between Flame and Stuxnet. An early version of Stuxnet contained code to propagate infections via USB drives that is nearly identical to a Flame module that exploits the same vulnerability.

Media coverage

Since 2010, there has been extensive international media coverage on Stuxnet and its aftermath. In early commentary, The Economist pointed out that Stuxnet was "a new kind of cyber-attack." On 8 July 2011, Wired then published an article detailing how network security experts were able to decipher the origins of Stuxnet. In that piece, Kim Zetter claimed that Stuxnet's "conts-benefit ratio is still in question." Later commentators tended to focus on the strategic significance of Stuxnet as a cyber weapon. Following the Wired piece, Holger Stark called Stuxnet the "first digital weapon of geopolitical importance, it could change the way wars are fought." Meanwhile, Eddie Walsh referred to Stuxnet as "the world's newest high-end asymmetric threat." Ultimately, some claim that the "extensive media coverage afforded to Stuxnet has only served as an advertisement for the vulnerabilities used by various cybercriminal groups." While that may be the case, the madia coverage has also increased awareness of cyber security threats.

Alex Gibney's 2016 documentary Zero Days covers the phenomenon around Stuxnet. A zero-day (also known as 0-day) vulnerability is a computer-software vulnerability that is unknown to, or unaddressed by, those who should be interested in mitigating the vulnerability (including the vendor of the target software). Until the vulnerability is mitigated, hackers can exploit it to adversely affect computer programs, data, additional computers or a network.

In 2016, it was revealed that General James Cartwright, the former head of the U.S. Strategic Command, had leaked information related to Stuxnet. He later pleaded guilty for lying to FBI agents pursuing an investigation into the leak. On 17 January 2017, he was granted a full pardon in this case by President Obama, thus expunging his conviction.

In popular culture

Besides the aforementioned Alex Gibney documentary Zero Days (2016), which looks into the malware and the cyberwarfare surrounding it, other worlds which reference Stuxnet include:

- In Castle, season 8, episode 18 “Backstabber” Stuxnet is revealed to have been (fictionally) created by MI6, and a version of it is used to take down the London power grid.
- Trojan Horse is a novel written by WIndows utility writer and novelist Mark Russinovich. It features the usage of the Stuxnet virus as a main plot line for the story, and the attempt of Iran to bypass it.
- In Ghost in the Shell: Arise, Stuxnet is the named type of computer virus which infected Kusanagi and Manamura allowing false memories to be implanted.
- In July 2017, MRSA (Mat Zo) released a track named “Stuxnet” through Hospital Records.
- In Ubisoft’s 2013 video game Tom Clancy’s Splinter Cell: Blacklist, the protagonist, Sam Fisher, makes use of a mobile, airborne headquarters (“Paladin”) which is said at one point within the game’s story mode to have been targeted by a Stuxnet-style virus, causing its systems to fail and the place to careen towards the ocean, and would have crashed without Fisher’s intervening.
- In Michael Mann’s 2015 movie Blackhat, the code shown as belonging to a virus used by a hacker to cause the coolant pumps explosion in a nuclear plant in Chai Wan, Hong Kong, is actual Stuxnet decompiled code.
- In the third episode of Star Trek: Discovery, “Context Is for Kings”, characters identify a segment of code as being part of an experimental transportation system. The code shown is decompiled Stuxnet code. Much of the same code is shown in the episode, “Pyre” of The Expanse, this time as a visual representation of a “diagnostic exploit” breaking into the control software for nuclear missiles.