



Stuxnet Cyber Attacks

Jackson Smith, Ishaan Singh, Justin Ingram,
Aiden England, and Arjun Bhalodia

Discovery

- In 2010, inspectors with the International Atomic Energy Agency (IAEA) noticed that Iran was replacing centrifuges at an alarming rate. Centrifuges usually are replaced at an 10% rate; however, Iran was replacing them at an almost 25% rate. This led to increased scrutiny from the IAEA
- An engineer working at the Natanz power plant was affected as his computer was infected by the virus, which lead to the virus spreading wildly in Iran when he took the computer home, as the virus was now connected to the internet
- Then, an IT security company was contacted when Iran reported arbitrary shutdowns and reboots on computers at Natanz. When they found that the issue persisted after reinstalling Windows, as well as finding it on the engineer's home computers, they knew it was a malicious attack



<https://gizmodo.com/the-incredible-tale-of-stuxnet-a-weapon-for-the-digital-1656811897>

History and Context

- Highly anticipated Iranian election between Mahmoud Ahmadinejad and challenger Mir-Hossein Mousavi two weeks preceding the Stuxnet attack on the Natanz uranium enrichment plant. The suspicion behind the elections resulted in civil unrest throughout the country, namely the nation's capital of Tehran.
- The attack was conducted on the Natanz uranium enrichment plant due to speculation that the Iranian government was using the plant for the development of nuclear weapons. This then necessitated the 2015 multi-national Iran Nuclear Deal




How Stuxnet Worked

- Utilized an unprecedented FOUR zero day exploits
- Initially spread through USB flash drives and then computer to computer
- Malware targeted Windows 7, Industrial Software and Siemens P7 PLC machinery.
- If criteria met, would change the frequency of centrifuges to cause damage.
- Implemented a man in the middle attack to fake process control signals to prevent shutdown due to irregular behavior.

According to the Washington Post, cameras installed in the Natanz nuclear facility recorded the dismantling and removal of 900-1,000 centrifuges.





“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], Stuxnet 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

Reaction & Significance

- For the first time ever a virus was used to infect industrial hardware which used the Siemen P7 Programmable Logic Controller (PLC) and capabilities to affect power stations.
- This was the cyber attack of the highest profile.
- Rumored that this worm was made by the intelligence agency of The United States and Israel to overthrow the Iran's nuclear powers.
- Was also used to interfere in the internal affairs of Iran.



Who Did It?

Israel



- Many speculate that Israel was behind the creation of stuxnet, through their unit 8200, an Israeli Intelligence Corps similar to the NSA
- "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" - Scott Borg, United States Cyber-Consequences Unit

United States



- Many leaks and reports hint that the United States wanted to destroy Iran's nuclear program by targeting their computer systems
 - John Bumgarner, a former intelligence officer of the United States published an article covering a possible cyber attack on centrifuges before Stuxnet was discovered.
-
- Gholam Reza Jalali, an Iranian government official, stated that the United States and Israel worked together on Stuxnet after an investigation
 - Differing code styles in Stuxnet suggest multiple groups could have collaborated on it
 - Edward Snowden also claimed that the United States and Israel were responsible for Stuxnet
 - Both countries deny any involvement, and the real origin is unknown to this day



Discussion Questions

- Is the United State's alleged vault of exploits ethical?
- How does this attack set the precedent for warfare or future conflicts?



Sources

- <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>
- <https://www.vanityfair.com/news/2011/03/stuxnet-201104>
- <https://www.newscientist.com/article/dn19504-why-the-stuxnet-worm-is-like-nothing-seen-before/>
- <https://www.ft.com/content/69f150da-25b8-11e5-bd83-71cb60e8f08c>
- https://www.theregister.com/2013/07/08/snowden_us_israel_stuxnet/
- <https://gizmodo.com/the-incredible-tale-of-stuxnet-a-weapon-for-the-digita-1656811897>
- <https://www.stripes.com/news/cone-of-silence-surrounds-u-s-cyberwarfare-1.158090>