Exploit Research: Stuxnet

Paul Gurke

Exploit Research: Stuxnet

Preface

In 2010, the most complex cyberattack was discovered by the cyber community. What was eventually named Stuxnet, was an unprecedented malware attack that targeted a specific Iranian uranium enrichment facility. The goal was to interrupt operations. The virus achieved this by modifying the logic in industrial controllers that operated the uranium centrifuges. The interfaces to the controllers would report that it was operating nominally, but it was in fact damaging the material and the equipment used to processes it.

Stuxnet

The quality, complexity and target specific details of this attack leads researchers to believe that this was a collaboration of some of the most capable organizations. The creators of Stuxnet have not been positively identified, but according to a McAfee report, it is widely assumed that the NSA, CIA and Israel worked together to create it.

Attack Flow

The first stage of the attack was centered around a number of zero-day flaws in Microsoft systems. McAfee states that, “Stuxnet was a multi-part worm that traveled on USB sticks and spread through Microsoft Windows computers.” (*What Is Stuxnet? | McAfee,* n.d.) This method of propagating through USB devices allowed Stuxnet to bridge into air gapped industrial control networks.

The second stage was to infect machines that had a certain type of engineering/maintenance software that communicated with the Programable Logic Controllers (PLC) that operated the centrifuges used to produce enriched uranium. These PLCs controlled things like the motors that spun the centrifuges as well as valves to separate the product.

Outcome

The result of the attack was that engineers at the enrichment facility were fighting against an invisible adversary. It is not known how early the attack was put into motion. According to *To Kill a Centrifuge*, a paper written by Ralph Langer, a worldwide recognized controls security expert, Iran’s low-tech approach to uranium enrichment was an obsolete European design that was stolen. Because of this, they never managed to get it to operate efficiently. Instead of increasing efficiency, they to performed the lower yield process at a larger scale. Because of all of this, it was much easier for the attack to go unnoticed as it was obscured by the already poor performing system.

Closing Thoughts

What is interesting to note about this cyber attack is that it could have been devastating. As of 2018, Siemens had about 31% of the PLC market. Remember that these PLCs control power distribution, water, waste management, manufacturing and other critical resources. It is apparently easier to cause wide spread destruction rather than such a targeted attack. Several variants piggybacked on the methods and code of Stuxnet to do what we expect from typical viruses; steal, extort and break things. Power companies were the hardest hit with 80% of companies in Mexico and 60% in India falling victim to a variant. (*What Is Stuxnet? | McAfee*, n.d.)

The solution to this problem is typical good IT practices. Application of patches and updates stop the majority of attacks. Stuxnet was special in that most of the vulnerabilities were unknown at the time. But it is clear that an incredible amount of effort and resources were dedicated to creating this cyber-attack. If they were able to keep digital media from entering the facility, the virus would have never been able to reach its target. Industrial control networks have historically relied on air gapped networks for security. Hopefully, this is a lesson that we can learn from in protecting our own critical IT resources.

References

Fruhlinger, J. (2017, August 22). *What is Stuxnet, who created it and how does it work?* CSO Online. https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html

Langner, R. (n.d.). *A Technical Analysis of What Stuxnet's Creators Tried to Achieve*. 37.

Langner—A Technical Analysis of What Stuxnet's Creators Tr.pdf. (n.d.). Retrieved April 19, 2020, from https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

Market Share Of Different PLCs. (n.d.). Retrieved April 19, 2020, from https://ipcsautomation.com/blog-post/market-share-of-different-plcs/

Ralph Langner: Cracking Stuxnet, a 21st-century cyber weapon. (n.d.). Retrieved April 19, 2020, from https://www.youtube.com/watch?v=CS01Hmjv1pQ

What Is Stuxnet? | McAfee. (n.d.). Retrieved April 19, 2020, from https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html