Keith Ecker

Andy Achenreiner

CS639

2/5/2019

Thinking Like an Attacker

1. The Stuxnet attack was engineered to disrupt the Iranian nuclear weapon program. Stuxnet did this by infecting the program logic controllers of the Iranian nuclear facility at Natanz. The malicious program would target the centrifuges of the plant and discreetly and slowly continue to damage these essential pieces to annoy the engineers of the plant while still keeping the malware a secret. It was discovered that there was two different Stuxnet attacks. The first and larger one infected the PLCs and would manipulate the centrifuges by giving these controllers fake data by acting as a gateway between the actual data and the controller.
2. The Stuxnet attack was able to infect the controllers at Natanz by infected the computers of contractors who would then connect their infected machines to the Natanz systems. This was likely spread through USB flash drives and eventually penetrating the industrial systems.
3. What is different about this type of attack from previously published ones.

“It was the first time anyone had seen digital code in the wild being used to physically destroy something in the real world.” (1) It was also more complex and targeted than previous attacks.

1. This attack is really two attacks.
   1. The attack started on infected USB sticks which would load a DLL file onto the machine if it had Siemens Step7 software. The DLL file “would intercept commands going from the Step7 software to the Programmable Logic Controller and replace them with its own malicious commands.” (1)

“The new version self-replicated, spreading within trusted networks and via USB drives to all sorts of computers, not just to those that had the Siemens configuration software for controllers installed.” (2)

* 1. Both versions of the attack were complex. The second system is described to have been simpler. “it was much simpler and much less stealthy than its predecessor.” (2) Its method of damaging the centrifuges via the rotor speeds seems more straightforward. On the other hand, the second version was equipped with four zero-days and several stolen digital certificates, so that makes it sound more complex.
  2. The attack tried to damage the centrifuges at the Natanz uranium-enrichment plant. The first variant tampered with the protection system for the centrifuges in a way that led to too much pressure. This could lead to the uranium hexafluoride solidifying which is damaging to the centrifuge. The second variant tried to increase the rotor speeds in the centrifuges to a speed that would cause damage.

Citations:

1) <https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/>

2) https://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/