Stuxnet Case Study

Minjoo Kim
Georgia Institute of Technology
Atlanta, GA, USA
Email: mkim908@gatech.edu

If you were designing security for Natanz, what prevention and detection methods would you recommend?

It would be best to assume that perpetrators can infiltrate into the system. It would be best for the security team to design the system so that they could limit the amount of damage done by identifying the endpoint compromise early on.

First, I would place strict control on all USB drives and contractor laptops since the first compromise was due to infected USB drives. Every USB usage must be limited, logged, and scanned using separate devices before encountering control systems. It may even be a better idea to ban USB usage entirely and supplant it with one-way data transfer systems, such as data diodes.

Application whitelisting could be used so that only approved programs and PLC code could run in the system. Stuxnet succeeded because it was able to run signed binaries that seemed valid and injected malicious ladder logic into Siemens PLCs. Whitelisting should not only be applied to executables, but also to PLC logic blocks, firmware image, changes in configurations, and more, ideally with cryptographic singing process to increase security.

I would apply segmentations inside the air-gapped network to prevent malware from laterally propagating. Each system in the network should never trust one another and infected machine should not be allowed to spread the malware.

Log management is crucial when it comes to early detection of cyberattacks. This could help to identify strange behaviors with new malware. These strange behaviors could be activities such as installing new drivers, granting new admin rights, running hidden processes, and more.

Lastly, I would implement a new metric that monitors any changes in the PLC code. It is obvious that PLC logic should not be changed often, and any frequent changes in the code should alert the security team to a potential suspicious activity.

Iran air-gapped their actual control systems. This causes operational issues and is therefore avoided in all but the highest security environments. Given that it failed anyway, would you still use it? If not, what would you lose by not doing it? If so, how would you detect a compromise of your air-gapped environment?

Air-gapping should still be used because it makes it more difficult for cyberattacks to succeed. Since the attackers must still bypass such hurdles, the attacks become a lot more expensive and deter weaker attacks. It would be possible to forgo air-gapping, allowing the systems to patch faster and make logging easier. However, the system risks losing protection from internet-based attacks.

As apparent it is from the case study; however, air-gapping should not be used by itself as it does not guarantee well-defined security. Malware can still infiltrate the system via physical devices. It is important that the security system is designed so that it tracks every single file and program and alerts the team to see if there is any new change in the system. Also, it could be beneficial to separate both manual and automatic processes and behaviors and monitor them independently to seek any anomalies.

The zero-day attacks in this case were published earlier, but not known to the vendor. Is there a way to protect against this?

It is practically infeasible to prevent zero-day attacks based on unknown malware and methods; however, it is possible to limit the amount of damage after the infiltration occurs. Systems must be designed under the assumption that trust fails.

References

[1] R. Langner, “Stuxnet: Dissecting a cyberwarfare weapon,” *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49–51, 2011.

[2] N. Falliere, L. O. Murchu, and E. Chien, “W32.Stuxnet dossier,” Symantec Security Response, White Paper, 2011.

[3] K. Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon*. New York, NY, USA: Crown Publishers, 2014.

[4] Cybersecurity and Infrastructure Security Agency (CISA), “Securing industrial control systems,” 2023.

[5] MITRE Corporation, “MITRE ATT&CK® for industrial control systems,” 2023.