For your discussion thread this week, research the Zeus botnet or the BlackEnergy Trojan. If you decide to research both and discuss both, that is fine too. In your discussion, include how pen. testing would be able to uncover the presence of the Zeus botnet or the BlackEnergy Trojan. What clues, tools, processes would you use?

BlackEnergy was identified several years ago as a Trojan malware designed to launch distributed denial-of-service (DDoS) attacks, download custom spam, and banking information-stealer plugins. It was known to have been used to deliver KillDisk. This feature can render systems unusable and destroy critical components on infected systems. BlackEnergy has been reported to possess unique functions that can place Industrial Control Systems (ICS) and/or SCADA (Supervisory Control and Data Acquisition) systems at risk. In fact, initially, the malware appears to have targeted a Ukrainian power facility Prykarpattya Oblenergo and other electricity distribution companies in Ukraine. Fortunately, the Ukraine attack has been attributed to *Sandworm*, a Russian cyberespionage group known to have been harassing Ukrainian officials and their allies as early as 2007. The attack succeeded since the attackers completed comprehensive reconnaissance over months. They knew the specific equipment in use at each facility and established backdoors in Human-Machine Interface (HMI) devices at those facilities. The attackers also determined the recovery protocols and procedures at those facilities. They were also prepared to lock operators out of their consoles. Actually, when asked, the operation employees reported that the cursors on the screens moved and could not be interrupted by the keyboard or mouse at the console. However, BlackEnergy malware may have also been used to target other utilities (Frequently Asked Questions: BlackEnergy, 2016).

A typical attack scenario involves an attacker sending a phishing email that contains a malicious attachment to a victim. To execute the attack, the attacker spoofs the sender address to appear to be coming from Rada (the Ukrainian parliament). Once the victim opens the attachment, they are asked to run the malicious macro in the document, allowing the attacker to run it automatically, and become a real threat to personal and enterprise data security. A good example of this scenario was the attack launched on The Aurora Power Grid. Through a well-crafted phishing email, the attackers used BlackEnergy to deliver KillDisk, which disabled boot capabilities on target systems. Consequently, the systems couldn’t be restored, and Uninterruptable Power Supply (UPS) systems were rendered useless. The damage delayed recovery considerably, and most of the systems could not be used until their firmware had been restored (Cyber-Attack Against Ukrainian Critical Infrastructure, 2016).

That being said, uncovering a malware such as BlackEnergy requires security professionals to be well versed in considering actions that are outside the range of normal activity and specification towards systems. To accomplish this goal, they must know what vulnerabilities exist in their critical infrastructure systems. Hence, penetration testing plays a crucial role in helping industries understand the possible methods of evasion and how to detect them. It also helps in identifying weaknesses across various platforms and integrating these platforms into current security controls such as secure configurations and rigorous patch management. Additionally, the results of careful penetration testing will highlight what Administrators across all industries need to do to protect their systems from malware attacks, focusing their efforts on keeping device operating systems and security software up to date and hardening their infrastructure against open vectors of attack. This is crucial considering how BlackEnergy malware has undergone a dramatic change in its design and target, depending on the groups that use it. In fact, businesses are creating penetration tools against supervisory control and data acquisition (SCADA) systems designed for security testing of ICS environments. These tools have real-world applications for testing the resiliency of the network against malicious actors (Malware Trends, 2016).

Finally, penetration testers can also reveal how keen employees’ exhibit necessary information security awareness and the effectiveness of organizational policies in enforcing such standards.

References

Cyber-Attack Against Ukrainian Critical Infrastructure. (2016). ICS-CERT Alerts, Department of Homeland Security. Retrieved from https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01

Frequently Asked Questions: BlackEnergy (2016). Trend Micro. Retrieved from https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/faq-blackenergy#:~:text=Identified%20several%20years%20ago%2C%20BlackEnergy,What%20does%20it%20do%3F

Malware Trends. (2016). Industrial Control Systems Emergency Response Team (ICS-CERT) and Advanced Analytical Laboratory (AAL), U.S. Department of Homeland Security. Retrieved from https://www.us-cert.gov/sites/default/files/documents/NCCIC\_ICS-CERT\_AAL\_Malware\_Trends\_Paper\_S508C.pdf