Brian Sowers

30/10/2022

Adversarial Behavior

1. Summarize the recent history of adversarial behavior and attacks for your chosen sector.

Industrial Control Systems (ICS) in the energy sector have been a target for both nation-state actors and technically capable adversaries, because, “historically, industrial infrastructure has been a key target for attacks with political motives” (2022 Cortex Xpanse Attack Surface Threat Report, 7). ICS contain two major subcategories, Distributed Control Systems (DCS) and Supervisory Control and Data Acquisition (SCADA), that, should they be compromised, create dire consequences of such a magnitude that are impossible to ignore. To put into perspective, “a short disruption of the control process in an ICS can have devastating effects ranging from environmental disasters to significant financial losses, or even loss of life” (Keliris et al, 1). Most famously in 2009, a worm known as Stuxnet targeted programmable logic controllers in Iran’s nuclear program to surreptitiously destroy its centrifuges over an extended period of time. Stuxnet came to reportedly be the work of an American-Israelian joint project intended to set back Iran’s nuclear developments. In more modern times, Ukraine’s energy sector has once again been the target of Russia due to the Ukrainian-Russian war. In April 2022, an attempted cyber-attack on a Ukrainian energy provider would have “deprived roughly two million people of electricity and made it difficult to restore power” (*UKRAINE: Timeline of Cyberattacks on Critical Infrastructure and Civilian Objects*, 1) had it not been prevented. The West has not been immune to these categories of cyber-attacks either. In the summer of 2021, a Texas based company known as Colonial Pipeline suffered an attack when one of its oil pipelines was made inoperable after an adversary compromised that system with a single known password. As a result, the East Coast suffered shortages in energy.

2. Evaluate the emerging threat climate for the sector of your choice. Identify two or more areas of vulnerability where the sector will be at future risk.

Two areas of vulnerability in the energy sector are the adoption of IT devices in OT networks and networking and security infrastructure. For the former, ICS have been upgrading and modernizing to increase efficiency and connectivity. The upside is that ICS have lower production and maintenance costs, but the downside is that ICS have been adopting "general-purpose Commercial-Off-The-Shelf (COTS) hardware and software" and the security vulnerabilities that come with them (Keliris et al, 1). For instance, the use of an RDP or FTP server contains vulnerabilities that can "be promptly ported to industrial environments, extending the cyber-security threat landscape of ICS. In addition, common IT protocols used for ICS communication have known vulnerabilities and exploitation techniques, enabling elaborate attacks" (Keliris et al, 1). For networking and security infrastructure, misconfigurations are inevitable and will expose those critical infrastructure. For instance, the use of a web server may be misconfigured and allow inbound/outbound internet access from the OT network, which is a major security risk and an invitation for malicious actors.

Works Cited

“2022 Cortex Xpanse Attack Surface Threat Report.” *Palo Alto.* Accessed: 30 October 2022.

Cairl, Brian, and Keliris, Anastasis, and Khorrami, Farshad, and Krishnamurthy, Prashanth, and Hossein Salehghaffari. “Machine Learning-based Defense Against Process-Aware Attacks on Industrial Control Systems.” Accessed: 30 October 2022.

“UKRAINE: Timeline of Cyberattacks on Critical Infrastructure and Civilian Objects.” *Cyber Peace Institute.* 08 June 2022. https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks/. Accessed: 30 October 2022.