Alexandre Fernandes Costa

Master of Science in Cyber Security Operations and Leadership

CSOL-580-02-SU20 – Cyber Intelligence

Module 4: Cyber Threat Intelligence Report

University of San Diego

Author Note

In Dedication to Services Pentest (SERPENT) Team

Abstract

This academic paper outlines potential cyber threat actors for the Contoso company, which is in the leading company in the technology sector and responsible for industry-leading innovation and building software for customers across the world.

The Contoso company holds thousands of patents, and intellectual property is a vital part of the company's high-value assets.

Summary Executive

Nowadays, from the global perspective, the amount of data generated by organizations is growing at impressive rates year over year, and the number of threats to this data from cyberattacks and data breaches is increasing equally exponentially.

Cyber incidents may cause organizations to lose money, data, productivity, and consumer trust. In 2019 alone, cybercrime resulted:

- The industry of cyber threats actors committing a crime is estimated to be a $1.5 trillion industry, with countries now focusing on economic activities around cybercrime.
- Security companies estimate that by 2023 cybercriminals will be stealing $ 33 billion records a year.
- According to a recent article in Forbes, analysts predict that the landscape for cybersecurity will change substantially in 2019, with both the manner of attack and defense becoming better than the past.
- Internet-of-Things (IoT) increase exponentially since the incubation of the technology and has expanded the corporate and home networks layer with billions of endpoints, making it easier for anyone to compromise a network.
- Beyond that, malicious attackers can use IoT devices and mobile devices like smartphones to form botnets or initiate DDoS attacks.
- Cloud-Based Attacks, Microsoft reported that in 2019 cloud-based attacks increased by 300%. As flexible and cost-effective as cloud-based solutions are, they have also made it so that many networks are more vulnerable to attack.

- Ransomware Based on the statistics above, Contoso corporation wants to establish the necessary Cyber Threat Intelligence Program in place, Security initiatives, and security controls to improve the posture to protect against a range of cyber threats from Advanced Persistent Threats (APTs) to Insider Threat (IT).

Cyber Threat – Insider Threat

Contoso Corporation will focus on Cyber threats ranging from insider threats to advanced persistent threats (APTs). This white paper will be summarized to the senior leadership team two threats.

Tactics, techniques, and procedures (TTP) will be highlighted for the cyber threats and potential security controls to minimize the risk.

The first cyber threat to be highlighted is the insider threat. It can be described as if advanced persistent threats cannot get access to the target organization through reconnaissance and external means and custom or commodity attacks. The next step on the bag of tricks is to gain access by actively recruiting insiders in the target organization who have a deep or initial level of access to the valuable information needed to conduct attacks.

Advanced threat actors are well-sponsored from the financial point of view and are willing to pay large sums of money to recruit potential insider threats.

Based on HUMAN OSINT, advanced persistent threats will recruit potential insider threats. The insider may assist a range of cybercriminals in a variety of ways, including information theft and internal network access. The insider threat will potentially drop malware, connect a USB port to a workstation or server, and provide credentials or insider knowledge of the infrastructure's overall security architecture.

The way to prevent insider threats is to:

- Conduct different levels of background for full-time employees and temporary employees.
- Ensure and practice the principles of least privilege and need-to-know.
- Enforce multi-factor authentication.
- Enforce strong password policy management.
- Implement network segmentation to reduce the number of systems accessible to an attacker.
- Implement monitoring across all systems.
- Implement endpoint detection and recovery protection.
- Implement user & entity behavior analytics (UEBA).
- Implement network segmentation.

Cyber Threat – APT28

Active since 2007, Advance Persistent Threat (APT28) is an activity group that has been used primarily to target government bodies, diplomatic institutions, and political advisors. Frequent use of zero-day vulnerabilities, spear-phishing, and several other distribution methods, makes APT28 a highly resilient threat.

APT28 targets government agencies, diplomatic institutions, military organizations and installations in NATO member states, and certain Eastern European countries. It has been observed that it targets organizations associated with political activism in Central Asia. Tools, tactics, and procedures of APT28 seek out victim information through open-source intelligence and social media interaction. It uses simple spear-phishing attacks to obtain victims' email account credentials, compiling information for further attacks. It uses email accounts from

generic email providers to imitate the email provider to disguise the spear-phishing emails as a notification from the generic email provider, such as a privacy alert. APT28 persistently sends spear-phishing attacks over many months to the same victims. APT28 attacks higher-value targets with emails that contain lures designed to take control of the victims' machines. APT28 uses a breadth of tactics using lure emails that include:

- URLs to websites containing zero-day exploits
- URLs to websites that use social engineering techniques that cause the victim to download malware
- Document attachments that contain zero-day exploits.
- APT28 usually packages these emails into a lure that might be interesting to the victim. APT28 tries to provide credibility to these emails by associating the sender with a real organization.

APT28 appears to have resources to acquire many zero-day exploits that cover a wide range of software products for these attacks. After a successful attack, APT28 proceeds to get a foothold onto the victim's network. This includes making use of malware backdoors and VPN clients to achieve persistent network access. APT28 has also been observed using Kali Linux (a penetration testing Linux distribution) on the victim's network to explore the victim's computer further. Lateral movement is also commonly used through pass-the-hash and credential dumping using publicly available tools, such as Mimikatz. Exfiltration of information from the victim's network can happen through dedicated command and control (C2) infrastructure. APT28 attempts to hide this traffic through domain names associated with everyday tasks on the network, such as updates and malware checks.

In rare instances, it is observed that APT28 uses legitimate servers, such as local SMTP mail servers, to extract information.

Overall, APT28 tries to blend into the network traffic to avoid suspicion.

The recommended leading security practices and security control for potential defenses are:

- A modern operating system
- latest software versions with the latest security updates.
- Conduct enterprise software security awareness training.
- Build awareness about malware infection prevention.
- Implement second-factor authentication.
- Prepare the infrastructure to be forensically ready.
- Keep personnel and personal data private.
- Critical users should have strict privacy configuration on social profiles.
- Conduct frequent Incident response exercises.
- Conduct Red and Blue team engagements.
- Keep systems and software fully updated.

References

BAZZELLMICHAEL. OPEN SOURCE INTELLIGENCE TECHNIQUES: Resources for Searching and Analyzing Online Information. INDEPENDENTLY PUBLISHED, 2019.

Bodmer, Sean. Reverse Deception: Organized Cyber Threat Counter-Exploitation. McGraw-Hill, 2012.

Bodmer, Sean. Reverse Deception: Organized Cyber Threat Counter-Exploitation. McGraw-Hill, 2012.

by Lastline, Posted, and Lastline. “Cybersecurity Statistics for 2019: The Chances Your Business Will Be Attacked.” Lastline, 20 Feb. 2019, www.lastline.com/blog/cybersecurity-statistics-for-2019/.

Harper, Allen, et al. Gray Hat Hacking: The Ethical Hacker's Handbook. McGraw-Hill Education, 2018.