Advanced Persistent Threats

Advanced Persistent Threats (APTs) have been around in the cyber world for years, targeting various kinds of corporation. Through a network attack where an unauthorized person gains access to a company’s network and stays there undetected for a period of time, APT allows professional hackers to steal valuable intellectual property such as confidential project descriptions, contracts, and patent information. Knowing this cybercrime category has been around for years, it is essential to understand the characteristics of APT and the difficulties with preventing these types of attacks, how security analytics can be used to understand and predict cyber-attacks, approaches for building a security architecture for APT, and lastly the methods for responding to these security breaches.

There are several characteristics of an APT attack. First, the victim of this target is chosen based on political, commercial and security interests with high-value information, such as national defense, manufacturing and the financial industry. With all of the intellectual property, it attracts hackers to try to gain access and steal data without causing any damage to the organization. Second, unlike any other attacks, the goal of the attack is not to get in and out but to achieve ongoing access. Some APT attacks are so complex that they require a full time administrator, making it difficult to identify as the theft of data can never be completely invisible. Lastly, this attack involves an organized human activity instead of hackers running an automated piece of code (Damballa). Therefore, not only these criminal operators have a specific objective, they also are skilled, motivated, and well-funded.

Security analytics play a huge role as one of the important tools to combat cybercrime especially APT. Security analytics help to identify the potential risks and assesses the vulnerability of critical assets and operations specific to the APT. Through the risk identification,
corporations are able to minimize those risks and prevent any future threats from happening. Security analytics can also act as company’s alarm that monitors patterns across a company’s computer network and alerts for any unusual activities in regards to an APT attack. Hence, it gives corporation a better chance to prevent the compromise or loss of critical information.

Building a security architecture is important to combat APT. It includes implementing defense in depth, continuous monitoring, and increasing security awareness across the corporation. One way in implementing defense in depth is to deploy defenses at the endpoint. This will work to secure any browsing applications and transaction signing devices, provide security at the navigation layer to monitor session navigation behavior and compare it with normal patterns, and even give protection at the linking layer to analyze the relationships between internal and external entities to detect collusive cyber-criminal activities (Computer Weekly). Next, a continuous monitoring can start with a narrow focus on security controls at the information system level. Monitoring inherently weak information systems may allow corporation to waste its resources, however, the allocation of resources toward continuous monitoring of security controls for information could help building stronger, and better systems (Nige). Lastly, security awareness among all employees is important as the people in the organization are the most valuable asset a business has. By providing adequate level of training, employees will have an equal level of security awareness to know how to identify any suspicious activity in regards to APT.

There are some methods for responding to APT. A simple one would be to subscribe to a regular feed of threat data. These subscription companies normally take feeds for thousands of end points and sources, then analyze trends and anomalies for valuable data to come up with various reports that are catered to specific industries including vulnerability reports that
addresses security holes in software. Additionally, sharing data and threat intelligence at levels from analyst to senior leaders across industries will help responding to APT as well. The relevant security officers from each company will meet periodically through conferences to aggregate and further analyze the trend reporting and perhaps collaborate on conducting a research on combating APT. In addition to sharing data, sharing strategic and technical reports among individuals, business, and government entities is a great weapon in responding to this kind of security breaches as the benefits of having quality assurance in the trusted network of business will outweigh the costs.

APT has been around for years yet they are still difficult to identify and prevent. As a result, APTs have led to many of the major data breaches of all kinds of corporations. The fact that dealing with an APT attack is one of the hardest things a corporation can do, it is important for businesses to know what APT is, its characteristics, and to build and maintain security architecture to help detect, analyze, and respond to these attacks before damage is done.
Work Cited

