LBMC Information Security Cybersecurity Sense Podcast Show Notes
Author: Bill Dean
Episode: 30
Date: October 3, 2018

Targeted Attacks Compared to Opportunistic Attacks

- This topic is something we discuss often here at LBMC Information Security, both internally and externally, as it is very important to understand the differences. These thoughts are further conveyed by a post from Kayla Elliot on the techtalk site. The post is titled, *"Targeted Attacks or Untargeted Attacks—Which is Most Common?"* There are some very good points in the article that I want us to add to.
- While the article references "untargeted attacks," and is applicable, we like to refer to these as "opportunistic attacks." Opportunistic attacks are not focused on an organization nor its specific information. These attacks are more focused on vulnerabilities and computing power to conduct other types of attacks. Commons examples are:
    - Remote Desktop services available to the Internet. This is an opportunity to gain access to the systems to perform many nefarious acts:
        - Install Bitcoin miners
        - Deploy ransomware
        - Use these systems to obfuscate the attacks on other targeted attacks
    - Spam emails to infect internal systems with ransomware
    - Phishing emails to gather mailbox access for future spear phishing attempts
    - Previously identified vulnerabilities that can now be exploited for benefit of future attacks
    - Web application platforms vulnerable to specific types of attacks
- Essentially, opportunistic attacks are focused on the benefit of compromising your systems in their endeavors. This can be mining Bitcoins, getting a ransom payment, sending trusted phishing emails, harvesting credentials, etc.
- The point here is that they are not focused on YOU or your organization as far as the specific data types or the value of the data that you have.
- If you don't provide what they seek, they move on to another organization to meet their needs
- As the referenced article summarizes, what we call "opportunistic" *"attacks are when hackers have no specific vertical, business, or person they are attacking."*
- However, while we call it "opportunistic," the impact can still be very serious. The organization, while not "targeted," still faces:
    - Potential business outages and ransom payments from ransomware infections
    - Potential brand issues when spear phishing emails requesting credentials are sent to clients and prospects
    - Additional brand issues if a website is defaced or infected with malware
    - Potential disclosure issues if mailboxes are accessed that contain PII, ePHI, or payment information
    - System performance issues from malware infections mining Bitcoins (best case scenario)
- Now, let's talk about targeted attacks.
    - Let's begin by disclosing that I am not a motivational speaker. I have been leading incident response engagements for more than a decade.

    - In a targeted attack, your systems are not the objective, your data is. You have something they want. It can be anything from ePHI, intellectual property, trade secrets, financial information, M&A information, etc. This information is specific to your organization.
    - If the attacker group cannot find a vulnerability, they do not quit and move on. You are the target, and they persist. They do not quit easily.
    - These are the high-profile attacks we hear about such as RSA, Heartland, Equifax, Target (no pun), Home Depot, and thousands of cleared defense contractors that we will never hear about, and numerous other entities that do not have a duty to disclose publicly (law firms).
    - This is where the marketing term "APT" came from. An advanced persistence threat does not concede when their first attempts fail; they continue until they succeed.
    - Most defenses depend on known "bad" signatures. The attackers develop new malware and attack approaches not previously seen.
    - They will exploit vulnerabilities not previously known (0-day).
    - They will compromise the networks of small companies that are soon to be acquired. When the infected networks join the clean networks, all is not infected.
        - Example: pediatrician "well room/sick room" analogy
        - This approach has produced many of the data breach case studies that we have cringed after reading.
- Now, I will be honest that many organizations do not fall into this category. I will also disclose that many are vulnerable because they do not know they are in this category.
- Some basic questions to help are:
    - Do we have information that is valuable to nation states?
    - Do we have information that cannot be obtained somewhere else?
    - Are we part of a supply chain for valuable products?
    - Do we have patents pending?
    - A link in the references below clearly outlines information that a specific nation state seeks. I have used a slide with this information in my incident response talks for years. Over the past year or so, they have exchanged the term "materialize" with R&D numbers. Make no mistake, they seek this information from us. Do you have any of the information they seek? If so, you are a target.

Takeaways

- Opportunistic and targeted attacks are not the same. While the objectives are different, the impact can still be devastating if they succeed.
- All companies are subject to opportunistic attacks. Do you know if you are subject to a targeted attack based on the data you generate or maintain?

Action

- Routine vulnerability assessments and penetration tests, along with social engineering will help build your resilience against opportunistic attacks.
    - In addition, stay abreast of vulnerability disclosures between tests for protection.
- Targeted attack protection builds on that with:
    - Purple-teaming exercises to ensure your security controls are effective
    - Adversary simulation exercises help you understand how well you can defend yourself against a targeted attack and assist in improving your controls

References:

- https://techtalk.pcpitstop.com/2018/09/13/untargeted-targeted-attacks-untargeted/
- http://www.china.org.cn/china/2012-09/24/content_26607377.htm

Bill Dean is a Senior Manager at LBMC Information Security. While involved in various aspects of LBMC's security services, he is also the practice lead for the organization's incident response, forensics, and litigation support practice.