LBMC Information Security Cybersecurity Sense Podcast Show Notes
Author: Bill Dean
Episode: 5
Date: August 22, 2017

Attacker Dwell Time

HIEWatch Article - Clinic Discovers Network Breach that Lasted 15 Months

- Cyber-attacks on healthcare IT systems are headline-grabbing events that can lead to exposure of patient data, service disruptions, time-consuming recovery processes, and high costs in the form of paying a ransom or spending money on new servers, security systems, or consultants.
    - However, that is only when they are aware of the breach.
- Example: Peachtree Neurological Clinic (PNC), which discovered a 15-month breach as the Atlanta-based provider was investigating a recent ransomware attack when it was discovered.
- While PNC was able to restore the encrypted files and there were no further indications of malware, attackers had dwelled on their network from February 2017 until May 2017.
- PNC was unable to determine which, if any, patient files or information were accessed during the 15-month-long breach, but noted that a patient's "name, address, telephone number, social security number, date of birth, driver's license number, treatment/procedure information, prescription information, and/or healthcare insurance information" could have been exposed.
- After notification of this, the patients were likely unconcerned about any ransomware.
- Some network breaches can go on for months or even years when the adversary is seeking value (PII, ePHI, IP, etc.).

Looking for Attackers

- The time elapsed between the initial breach of a network by an attacker and the discovery of that breach by the victim is known as "dwell time," or the "breach detection gap."
- FireEye, an international incident response firm, cites dwell time as 146 days on average, globally.
- To make matters worse, Trustwave reports that 81% of reported intrusions are not detected by internal security processes but rather by news reports, law enforcement notifications, or external fraud monitoring.
- It is important to note that many of these companies take information security very seriously with compliance requirements, appropriate budgets, and talented security personnel. Reported examples include:
    - Michael's credit card breach in 2014—dwell time was 8 months
    - Home Depot's credit card breach in 2014— dwell time was 5 months

    - PF Chang's—dwell time was 11 months
    - Office of Personnel Management (OPM)—dwell time was more than a year
- Unlike ransomware attacks, website defacements, or DDOS attacks that are intentionally loud, persistent compromises work to remain stealth as long as possible to obtain as much valuable data as possible over long periods of time.
- One of the sources of this issue are organizations that rely solely on static-based protections, such as anti-virus and firewalls.
- Advanced attackers rely on undetectable malware to evade static controls. In some instances, the malware may be developed/altered specifically for the target organization, which almost guarantees that static-based protections will not be effective.
- Advanced threats require additional efforts to hunt for undetected malware and network communications.
- Closely monitor and restrict outgoing internet communications.
- Consider blocking uncategorized and unknown websites.
- Start "hunting" for intruders within your network.
- The goal is to take additional steps to honestly answer the question, "Are our systems compromised?"

Key Takeaways:

- Advanced attacks will often circumvent traditional static protections.
- This provides the ability for extensive "dwell time" of attackers on your network.
- Put in place additional network controls. If malware cannot communicate out, it cannot operate.
- "Hunt" for previously undetected malware on your systems.

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.

References:

http://www.hiewatch.com/news/clinic-discovers-network-breach-lasted-15-months

https://www.fireeye.com/company/press-releases/2016/fireeye-releases-first-mandiant-mtrends-emea-report.html

https://www.sans.org/reading-room/whitepapers/analyst/who-what-where-when-effective-threat-hunting-36785

https://www.sans.org/reading-room/whitepapers/analyst/hunter-strikes-back-2017-threat-hunting-survey-37760

http://www.lbmcinformationsecurity.com/services/malware-compromise-assessment