Report: A vulnerable attack surface exists in healthcare enterprise IT networks

Vectra research highlights precarious security risks in the healthcare industry due to legacy infrastructures and unmanaged devices

April 24, 2019

Vectra today announced that the proliferation of healthcare internet-of-things (IoT) devices, along with unpartitioned networks, insufficient access controls and the reliance on legacy systems, has exposed a vulnerable attack surface that can be exploited by cybercriminals determined to steal personally identifiable information (PII) and protected health information (PHI), in addition to disrupting healthcare delivery processes.

Published in the Vectra 2019 Spotlight Report on Healthcare, these findings underscore the importance of utilizing machine learning and artificial intelligence (AI) to detect hidden threat behaviors in enterprise IT networks before cybercriminals have a chance to spy, spread and steal.

“Machine learning and AI can assist healthcare organizations in better securing networks, workloads and devices, and provide data security by analyzing behaviors across systems,” said Jon Oltsik, senior principal analyst at Enterprise Strategy Group. According to ESG research, “12 percent of enterprise organizations have already deployed AI-based security analytics extensively, and 27 percent have deployed AI-based security analytics on a limited basis. We expect these implementation trends will continue to gain.”

Gaps in policies and procedures can result in errors by healthcare staff members. Examples of these errors include improper handling and storage of patient files, which is a soft spot for cybercriminals when they target global organizations and industries looking for weaknesses to exploit.

“The increase in medical IoT is beneficial for patients but makes securing healthcare systems a challenge due to limited security controls around these devices,” said Brett Walmsley, chief technology officer at Bolton NHS Foundation Trust, which provides in-patient and out-patient healthcare services to over 140,000 people in Bolton and the surrounding area northwest of Manchester, England. “Having the visibility to quickly and accurately detect threat behaviors on and between all devices is the key to good security practice, regulatory compliance and managing risk.”

The 2019 Spotlight Report on Healthcare is based on observations and data from the 2019 RSA Conference Edition of the Attacker Behavior Industry Report, which reveals behaviors and trends in networks from a sample of 354 opt-in enterprise organizations in healthcare and eight other industries. Motivated attackers often mask their malicious actions by blending in with existing network traffic behaviors.

From July through December 2018, the Cognito threat-detection and response platform from Vectra monitored network traffic and collected metadata from more than three million workloads and devices from customer cloud, data center and enterprise environments. The analysis of this metadata provides a better understanding about attacker behaviors and trends as well as business risks, enabling Vectra customers to avoid disastrous data breaches.

Key findings from the 2019 Spotlight Report on Healthcare

- The most prevalent method attackers use to hide command-and-control communications in healthcare networks was hidden HTTPS tunnels. This traffic represents external communication involving multiple sessions over long periods of time that appear to be normal encrypted web traffic.
- The most common method attackers use to hide data exfiltration behaviors in healthcare networks was hidden domain name system (DNS) tunnels. Behaviors consistent with exfiltration can also be caused by IT and security tools that use DNS communication.
- Vectra observed a spike in behaviors consistent with attackers performing internal reconnaissance in the form of internal darknet scans and Microsoft Server Message Block (SMB) account scans. Internal darknet scans occur when internal host devices search for internal IP addresses that do not exist on the network. SMB account scans occur when a host device rapidly makes use of multiple accounts via the SMB protocol that is typically used for file sharing.
- While many healthcare organizations experienced ransomware attacks in recent years, the report found that ransomware threats were not as prevalent in the second half of 2018. It is still important to catch ransomware attacks early, before files are encrypted and clinical operations are disrupted.
- Botnet attacks are opportunistic and are not targeted at specific organizations. While botnet attacks persist everywhere, their rate of occurrence in healthcare is lower than other industries.

“As emerging new medical technologies are adopted to improve healthcare delivery, it becomes increasingly important to strengthen security by understanding the technologies you have, how those technologies are being used, and receiving timely alerts when unauthorized use occurs,” said Robert Rivera, senior security engineer at Cooper University Health Care, a leading academic health system in Camden, New Jersey.

“Healthcare organizations struggle with managing legacy systems and medical devices that traditionally have weak security controls, yet both provide critical access to patient health information,” said Chris Morales, head of security analytics at Vectra. “Improving visibility into network behavior enables healthcare organizations to manage risk of legacy systems and new technology they embrace."

The Cognito platform accelerates network threat detection and response using sophisticated artificial intelligence to collect, enrich and store network metadata with the right context to detect, hunt and investigate hidden threats in real time. The Cognito platform scales efficiently to the largest organization’s networks with a distributed architecture that includes a mix of physical, virtual and cloud sensors to provide 360-degree visibility across cloud, data center, user and IoT networks, leaving attackers with nowhere to hide.