Healthcare’s legacy infrastructure of unmanaged devices exposes a vulnerable attack surface.
# TABLE OF CONTENTS

- Challenges in today's healthcare networks ........................................ 3
- Analysis of the healthcare industry from July-December 2018 ............. 4
- Behaviors consistent with botnet attacks ........................................... 6
- Behaviors consistent with command-and-control communications ........ 7
- Behaviors consistent with internal reconnaissance ............................. 8
- Behaviors consistent with lateral movement ...................................... 9
- A note about ransomware ................................................................. 10
- Behaviors consistent with data exfiltration ....................................... 10
- Conclusion ....................................................................................... 11
The proliferation of healthcare IoT devices deployed on unpartitioned networks with limited access controls and the use of legacy systems has created a vulnerable attack surface.

Cybercriminals intent on stealing personally identifiable information (PII) and protected health information (PHI) can easily exploit this broad attack surface and simultaneously disrupt healthcare delivery processes.

Gaps in policies and procedures can result in unintentional errors by staff members that create security risks. This sometimes takes the form of improper handling and storage of patient files, which is a soft spot for cybercriminals who are looking for weaknesses to exploit.

Confirming what Vectra® observed from its own healthcare customers, the Verizon 2018 Data Breach Investigations Report indicates that a key security risk for the healthcare industry is its susceptibility to internal errors and misuse. The report shows that the healthcare industry faces the highest risk from accidental or intentional insider threats than external threats.

**Actions within Healthcare**

<table>
<thead>
<tr>
<th>Incidents</th>
<th>Error</th>
<th>Malware</th>
<th>Hacking</th>
<th>Misuse</th>
<th>Social</th>
<th>Physical</th>
<th>Environmental</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incidents</td>
<td>203</td>
<td>185</td>
<td>139</td>
<td>138</td>
<td>105</td>
<td>87</td>
<td>0</td>
</tr>
</tbody>
</table>

This means that human errors pose a bigger risk in healthcare, most often in the form of misdelivery (62%), which Verizon describes as sending something intended for one person to a different recipient, followed by a grouping of misplaced assets, misconfigurations, publishing errors and disposal errors.

Verizon cites misuse as privilege abuse – such as using logical access to assets, often databases, without having a legitimate medical or business need to do so – in 74% of cases. This abuse of access to sensitive information is driven by a combination of curiosity and financial gain motives.

**Challenges in today’s healthcare networks**

- Many healthcare legacy systems lack essential cybersecurity controls
- Downtime to patch systems is a challenge as healthcare operations run 24x7
- Healthcare supports a wide variety of clients, with an average of three devices for every person
- Many IP-addressable devices connect to the network without vetting for security

Saving lives and treating patients is the top priority for healthcare organizations, and they rarely can afford to have their systems down to be patched – even for just a few hours. Having 24x7 access to patient data is crucial. Consequently, outdated systems and software are common among healthcare providers.

Doctors and other caregivers have seamless access to patient electronic health records, medical images and medications. The staff needs access to an array of healthcare delivery, productivity and administrative applications. Use of the cloud is rising, and healthcare systems are migrating to Microsoft Office 365.

Medical IoT devices offer new ways to monitor patients and equipment while improving care and lowering costs. But many of these smart devices have unknown security protections. Connected medical devices – from Wi-Fi-enabled infusion pumps to smart MRI machines – increase the attack surface of devices sharing information.

The patient experience is important, too. Patients and their families use the guest Wi-Fi network to stay connected with each other and to entertainment while waiting for appointments or during a hospital stay.

These Wi-Fi networks, with their large amounts of unmanaged devices, further expand the healthcare attack surface. Although most guest Wi-Fi networks are segregated from production networks, there are cases where hospital systems share the same network as patients and guests.

Often bringing in their own personal devices, physicians employed by outside, independent medical groups work on-site at multiple hospitals. Medical students at teaching hospitals also have access to critical healthcare information.

Even when healthcare organizations enforce strong device management policies, employees, physicians and other staff do not always want to allow access to their own personal devices.

In all these examples, healthcare systems are exposed to outside networks with limited security controls.
Analysis of the healthcare industry from July-December 2018


These enterprise organizations utilize the Cognito® platform from Vectra, which detects and correlates behaviors consistent with attacker behaviors with host devices, assigns a threat-severity score, and prioritizes the highest-risk threats.

The 2019 RSA Conference Edition of the Attacker Behavior Industry Report provides a breakdown of behavior-detection statistics by industry. The charts that follow show network behaviors consistent with threats across the attack lifecycle – botnet monetization, command and control, internal reconnaissance, lateral movement and data exfiltration.

While these behaviors are not always related to a cyberattack, they are strong indicators of potential risk and exposure.

Security analysts must decide and label the behavioral detections that are approved and those that are unapproved to understand where to focus their investigations. The unapproved behaviors can lead to intentional and unintentional theft of information or disruption of healthcare delivery services.

Figure 2 shows the volume of behavioral detections that were triggered in each industry per 10,000 host devices. This view shows how each industry fared on a per-capita basis as well as which industries generated the most behavioral detections by volume.
Healthcare exhibited a lower volume of behavioral detections consistent with command-and-control communication and exfiltration compared to the industry average. Behavioral detections consistent with internal reconnaissance and lateral movement in healthcare organizations were relatively the same as the industry average.

The combination of behavioral detections consistent with phases of the attack lifecycle – as well as the context of specific behavioral detections – are potentially strong threat indicators. Figure 4 shows host-device severity scores – critical, high, medium and low – in the healthcare industry per 10,000 host devices by month.
Behaviors consistent with botnet attacks

Botnets represent opportunistic attacks that are not targeted at specific organizations. While botnet attacks persist everywhere, their occurrence is not significant in healthcare and are more often associated with user desktops that browse the web.

Figure 5: Healthcare botnet behaviors per 10,000 host devices by month
Behaviors consistent with command-and-control communications

Hidden HTTPS tunnels are the most common behavior detected in healthcare. This traffic represents external communication involving multiple sessions over long periods of time that appear to be normal encrypted web traffic.

When attackers hide their command-and-control communications in HTTPS tunnels, it often looks like service provider traffic. The results are shown in blue in Figure 6.

A challenging aspect of security involves validating that a device’s connectivity to remote locations is working as intended. It is unclear to a healthcare security operations team what ports should be allowed to communicate inside and out of the network because service providers set their own requirements and documentation often lags behind versions and upgrades.

Behaviors that point to the use of external remote access tools are the second most-common detections in healthcare. Although these behaviors are consistent with cyberattack command-and-control communications, as shown in Figure 6, these behaviors also occur when healthcare organizations communicate with independent labs, imaging centers and other service providers.

External remote access occurs when an internal host device connects to an external server and the external server appears to be in control of the communications.

Remote access is commonly triggered by IT services logging into user machines and high volumes of outsourced hosted services, such as help desks. The spike in external remote access in November and December was due to a change in how Vectra reported external remote access and may not be a proper reflection of the healthcare environments monitored.

Figure 6: Healthcare command-and-control behaviors per 10,000 host devices by month
Behaviors consistent with internal reconnaissance

Vectra observed a spike in behaviors consistent with internal reconnaissance in healthcare. These behaviors are consistent with a cyberattacker performing internal darknet scans and SMB account scans, as shown in Figure 7. Internal darknet scans occur when internal host devices search for internal IP addresses that do not exist on the network.

In healthcare, a darknet scan detection can occur when IoT devices scan the network to reauthenticate as they move around and require a specific address. For example, darknet scans occur due to a short DHCP time that requires IoT devices to constantly look for a new IP address.

An SMB account scan can occur when a host device makes rapid use of multiple accounts via the SMB protocol, which can be used for file sharing, RPC and other lateral movements. SMB account scans often occur when internal users log into multiple systems.

Figure 7: Healthcare internal reconnaissance behaviors per 10,000 host devices by month
Behaviors consistent with lateral movement

Lateral movement detections can occur when connected systems and devices communicate with each other across the network. Figure 8 shows a high level of behaviors associated with authentication. Detections consistent with Kerberos and SMB brute-force attacker behaviors were the most common.

Detections consistent with lateral movement within healthcare often reflect administrative activity as the organization deals with lean staff, old controls and unsecured protocols like FTP.

Remote desktops are also common in healthcare. It is difficult to validate administrative models in healthcare due to old internal processes and widely open administrative protocols.

The type of traffic associated with IoT systems and the traditionally weak security of IoT devices creates an opportunity for cyberattackers. They hide their lateral movements and use these systems to move laterally across a healthcare network, jumping across non-critical and critical subsystems, until they find ways to complete their exploitative missions.

For example, behaviors consistent with SMB brute-force occur when an internal host device utilizes the SMB protocol to make multiple login attempts for the same user account, which most often fail.

Healthcare IoT devices can represent a large volume of devices that attempt to automatically log into the network. Sometimes these accounts become locked out and begin continuous logins until authenticated. The same applies to service accounts, which are widely used in the healthcare industry.

IoT devices also display automated replication behaviors by sending very similar payloads to several internal targets. Attackers can leverage these behaviors to hide their own lateral movements inside healthcare organizations.

![Figure 8: Healthcare lateral movement behaviors per 10,000 host devices by month](image-url)
A note about ransomware

Two years ago, healthcare organizations fell prey to a high rate of ransomware attacks. Many healthcare organizations were severely impacted and their ability to deliver quality patient care was disrupted.

However, ransomware attacks were much less prevalent from July-December 2018. Despite this, ransomware remains a concern among healthcare organizations, which should continue to monitor for ransomware attacks early in the attack lifecycle before files are encrypted and healthcare delivery is disrupted.

Behaviors consistent with data exfiltration

The use of hidden DNS tunnels in healthcare networks was the most prevalent behavior consistent with the exfiltration of data in the healthcare industry.

Hidden DNS tunnels indicate that an internal host device is communicating with an outside IP using DNS and another protocol is running over the top of the DNS session. These behaviors are often caused by IT and security tools that leverage DNS communication. However, attackers can use them to hide the exfiltration of data.

In healthcare, the second most-common behavior consistent with data exfiltration is the smash and grab. This occurs when a large volume of data is sent to an external destination not commonly in use, in a short period of time. An example is security cameras that quickly send large volumes of data to a hosted cloud site.

While smash-and-grab behaviors can reflect the normal operation of an IoT device, low and slow attackers who wait and watch can use it to obfuscate their nefarious theft of data. It is important to document and monitor these network behaviors to enable the detection of cyberattackers and protect critical healthcare data.

The final type of behavior consistent with exfiltration in healthcare is data smuggling. This occurs when an internal host device acquires a large amount of data from one or more internal servers and subsequently sends a significant amount of data to an external system.

Figure 10: Healthcare exfiltration behaviors per 10,000 host devices by month
Data smuggling behaviors can occur when patient medical records are transferred, which is a common business process for healthcare providers. As highly valuable assets protected by regulatory mandates, patient medical records must be securely transmitted to the correct destinations.

The potential for errors in medical record transfers is particularly high. To reduce the chances of errors, many healthcare organizations automate and validate large, routine data transfers.

**Conclusion**

It is a never-ending challenge to balance security and policy enforcement with usability and efficiency. Healthcare organizations struggle with managing legacy systems and medical devices that traditionally have weak security controls, yet both are instrumental to ensure that medical teams have instant access to vital information.

Vulnerable processes persist, and weak trust models often stay implemented, creating wider-than-necessary exposure. And healthcare organizations are often unaware of the methods in which their processes violate security policies or what services are being used.

Greater visibility into traffic and behaviors inside the network can help healthcare security teams remain vigilant and more confident as cutting-edge medical technologies are adopted.

Emerging medical technologies will continue to become essential to the quality and speed of healthcare delivery, attracting patients and providing the best patient outcomes.

As this transformation moves forward, healthcare organizations must remain mindful about what technologies are in place, how they are utilized, and when unauthorized actions occur.

To learn more about cyberattacker behaviors seen in other real-world cloud, data center and enterprise environments, get the 2019 RSA Conference Edition of the Attacker Behavior Industry Report from Vectra.