VECTRA
SECURITY THAT THINKS

INDUSTRY RESEARCH REPORT

The 2020 Spotlight Report on Healthcare

INTELLIGENT
THREAT DETECTION
AND RESPONSE

CLOUD-NATIVE

ENTERPRISE

TABLE OF CONTENTS

Vectra® protects business by detecting and stopping cyberattacks.

As a leader in network detection and response (NDR), Vectra® AI protects your data, systems and infrastructure. Vectra AI enables your SOC team to quickly discover and respond to would-be attackers —before they act.

Vectra AI rapidly identifies suspicious behavior and activity on your extended network, whether on-premises or in the cloud. Vectra will find it, flag it, and alert security personnel so they can respond immediately.

Vectra AI is Security that thinks®. It uses artificial intelligence to improve detection and response over time, eliminating false positives so you can focus on real threats.

EMEA doubled the amount of data moving to external destinations over the five-month period from January-May 2020.

HIGHLIGHTS

- There is an increase in the upward trending of command-and-control behaviors, which indicate remote access of internal system and a doubling of data exfiltration behaviors, which indicates that data is leaving internal healthcare networks to external destinations like cloud services.
- Comparing the rate of growth in data exfiltration behaviors across all industries in 2020 shows that the dramatic increase within healthcare organizations is unique.
- Lateral movement detections, the strongest indicator that threats are spreading inside a compromised infrastructure and propagating across internal devices, remain relatively flat with a slight decrease in May.
- There is a significant increase in smash-and-grab behavior, which occurs when a large volume of data is sent to an uncommon external destination, like a hosted cloud site, in a short period of time.
- Also increased is data smuggler activities, a behavior that occurs when an internal host device consolidates a large amount of data from one or more internal servers and subsequently sends a significant amount of data to an unexpected external system.

Cloud services and remote healthcare create new exploitable attack surfaces

The COVID-19 pandemic is spurring adoption of cloud services across all industries as they rapidly pivot to support remote work and collaboration. This is particularly true for healthcare providers at the front line as they leverage remote access and cloud analytics to scale operations.

While the pandemic will likely dissipate, the long-term impact for healthcare providers is likely to be profound – leaving business leaders and security professionals tasked with protecting an attack surface that to date has been uncharted.

The COVID-19 pandemic has influenced the world more than any other recent event, from changes in our day-to-day environment, to innovations in manufacturing, finance, healthcare, leisure, retail and supply chain, and almost every other industry.

In healthcare, some areas of influence are clear and obvious, such as the acceleration of digital transformation, which changes how organizations operate and provide care to patients. There is also an increased demand for cloud computing, which provides most of the foundation, tools and infrastructure to fuel this digital transformation.

Some world leaders in the cybersecurity space, including the World Economic Forum[1] (WEF), predict that this rapid and unplanned move will result in a cyberpandemic down the road. But what does this mean?

The primary concerns during COVID-19 have been the provision of clinical care and attempts to control the pandemic. Remote access and timely

collaboration between clinical administrators, healthcare professionals and researchers could mean the difference between life and death. Cloud benefits, such as scalability and redundancy, are vital in supporting these tools. This trend will mostly likely persist after the pandemic as we can expect the increased level of remote work to continue.

Yet, while the use of cloud computing to optimize resources in the healthcare sector has great potential, there are also risks. This is especially true when cloud adoption happens faster than proper due diligence can be applied by information security.

[1] https://www.weforum.org/agenda/2020/06/covid-19-pandemic-teaches-us-about-cybersecurity-cyberattack-cyber-pandemic-risk-virus/

Analysis of security in the healthcare industry from January-May 2020

The 2020 Spotlight Report on Healthcare is based on observations and data from the behaviors and trends in networks from a sample of 31 opt-in enterprise organizations. These healthcare organizations range from small (0-5,000 hosts), medium (5,001 – 25,000 hosts) and large (25,001 or more hosts).

This increase in remote access and data transmitted to external destinations aligns with the rapid adoption of cloud services in healthcare during the COVID-19 pandemic.

These enterprise organizations utilize the Cognito® Network Detection and Response (NDR) platform from Vectra, which detects and correlates attacker behaviors against host devices, assigns a threat-severity score, and prioritizes the highest-risk threats. NDR is an effective approach for the detection and response to attackers that have circumvented or defeated defensive controls and gained an operating capability inside an organization's infrastructure.

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.

When specifically examining cybersecurity statistics for healthcare in 2020, there is an increase in two trends during the first five months of the year. The first is the upward trending of command-and-control behaviors, which indicate remote access of internal systems. The second is the doubling of data exfiltration behaviors, which indicates that data is leaving internal healthcare networks to external destinations like cloud services.

This increase in remote access and data transmitted to external destinations aligns with the rapid adoption of cloud services in healthcare during the COVID-19 pandemic.

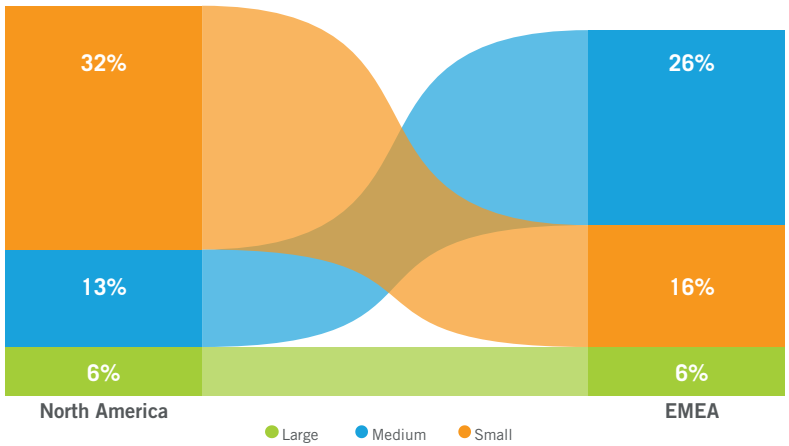

Figure 1: Healthcare by geography and size

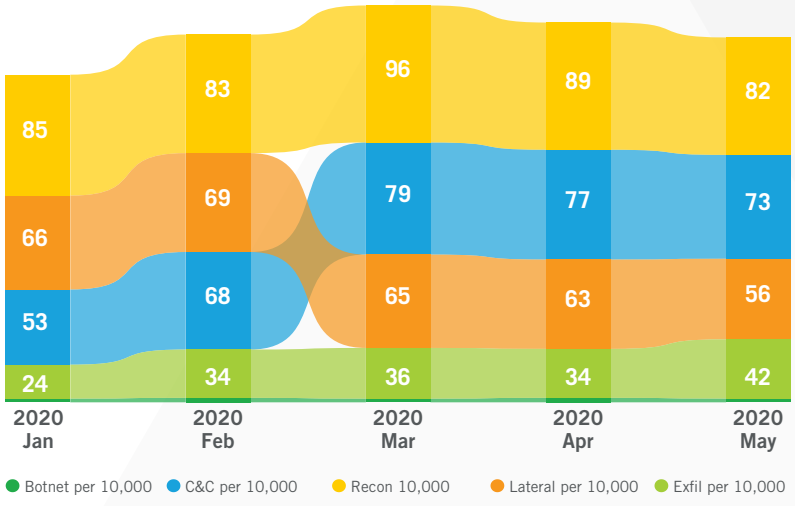

Figure 2: Potential attacker behaviors in healthcare by month per 10,000 devices

"This year we observed a stark and sudden growth in data movement outside of our organization's traditional boundaries. That growth is most likely due to how the National Health Service has traditionally worked in siloed data centers behind a firewall and has now shifted to the COVID-19 world of cloud-based collaboration."

David Willis
Head of Cyber, Governance and Assurance
Greater Manchester Health and Social Care Partnership
The National Health Service, United Kingdom

External threats targeting healthcare are not leading to increased internal threat activity

Despite the increased attack surface, lateral movement detections remain relatively flat with a slight decrease in May. Lateral movement detections are the strongest indicator that threats are spreading inside a compromised infrastructure and propagating across internal devices.

The lateral movement within healthcare often reflects administrative activity as organizations deal with lean staff, old controls, and unsecured protocols like FTP. Overall, lateral movement in 2020 is trending downward for healthcare.

This flat trend in lateral movement is positive as the World Health Organization (WHO) indicated seeing a five-fold increase in phishing and ransomware over the same time period. The WHO also refers to the compromise of external databases and user accounts that can be used against healthcare workers in a cyberattack.

The same trend of increased phishing attacks against healthcare organizations has been seen by email and firewall vendors. In March and April, security researchers, the U.S. Department of Homeland Security, and other federal agencies warned that attackers were taking advantage of the increase in remote workers and the COVID-19 crisis.

These warnings ranged from launching ransomware, hijacking videoconferencing, targeting virtual private networks (VPNs), and ramping-up business email compromise schemes and fraud attempts. But were these opportunistic attacks successful? Did these phishing campaigns lead to further damage and compromise of healthcare networks?

The research indicates no. Although opportunistic attacks against healthcare were up – and some might have succeeded – this external activity does not appear to have led to internal activity normally observed in successful attacks. Healthcare organizations in general are doing a good job of mitigating inbound attack attempts.

A larger concern is the increase in data that leaves the internal infrastructure to external destinations not seen before. This is likely the result of large volumes of health-related data rapidly propagating within cloud services. The problem of data going to new and unmanaged cloud services compounds the existing issue of unmanaged medical devices that are already widespread in healthcare.

Healthcare records are transitioning to cloud services at an accelerated rate

Comparing the rate of growth in data exfiltration behaviors across all industries in 2020 shows that the dramatic increase within healthcare organizations is unique. Other industries have either remained stable in the volume of detections per month or exhibited a downward trend in data transfers to external destinations. This trend of less data aligns with the temporary shut-down of global business operation, such as in the retail sector, due to the spread of the COVID-19 pandemic.

Breaking down the healthcare threat data by geography shows that Europe, the Middle East and Africa (EMEA), as well as North America, experienced an increase in the volume of external data movement. EMEA doubled the amount of data moving to external destinations over the five-month period from January-May 2020. In North America, healthcare providers experienced an initial spike in external data movement activity that settled down over time.

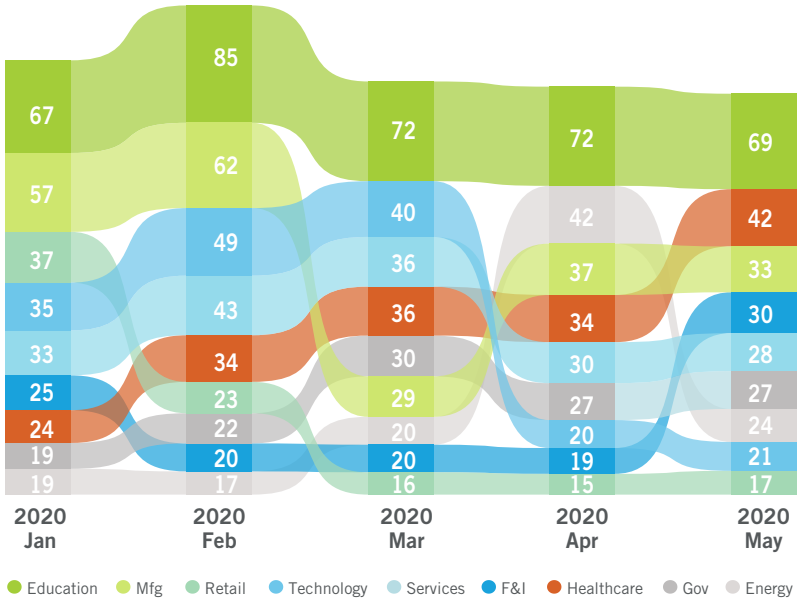

Figure 3: Data exfiltration behaviors across all industries by month per 10,000 devices

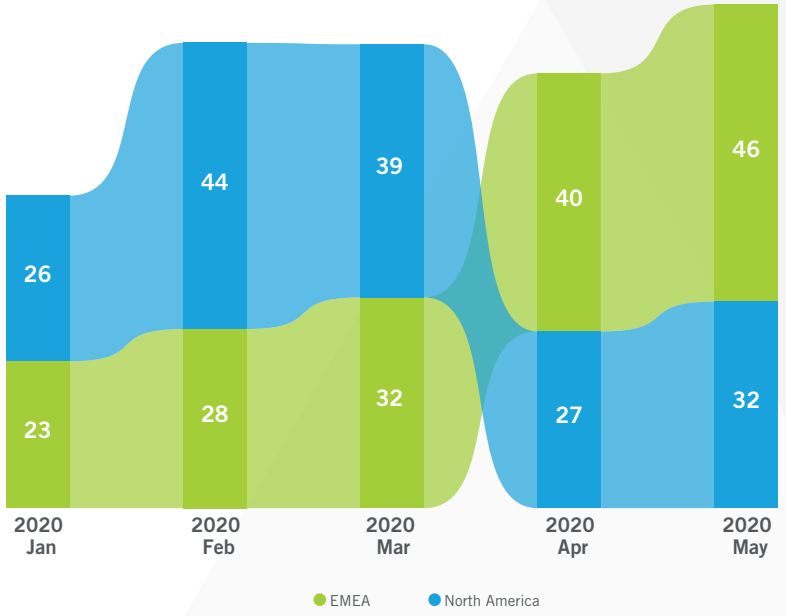

Figure 4: Data exfiltration behaviors in healthcare by geography per 10,000 devices

Drilling down further into the EMEA growth activity, the specific exfiltration behaviors point to a significant increase in two specific types of data movement behaviors.

The first is the smash-and-grab behavior, which occurs when a large volume of data is sent to an uncommon external destination in a short period of time. An example is a medical device that quickly sends large volumes of data to a hosted cloud site.

While the cloud providers might be HIPAA-compliant and secure in design, the responsibility for ensuring adequate protection falls on the user and not the cloud provider.

Using the cloud enables medical devices to wirelessly collect data for storage, computation, accessibility, and sharing. Specific examples include the use of cloud services to provide real-time glucose insights for patients with diabetes, or probes that use high-resolution optical and imaging techniques to identify cancerous and precancerous cells in epithelial tissue.

While high-volume data-transfer behaviors from a single host can reflect the normal operation of a medical IoT device, low and slow attackers who wait and watch can use it to obfuscate their 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 second most prevalent data-movement behavior are data smuggler activities. These behaviors occur when an internal host device consolidates a large amount of data from one or more internal servers and subsequently sends a significant amount of data to an unexpected external system.

Data smuggling behaviors can occur when patient medical records are transferred to cloud storage offerings like Microsoft OneDrive, which is a common requirement for collaborating healthcare professionals.

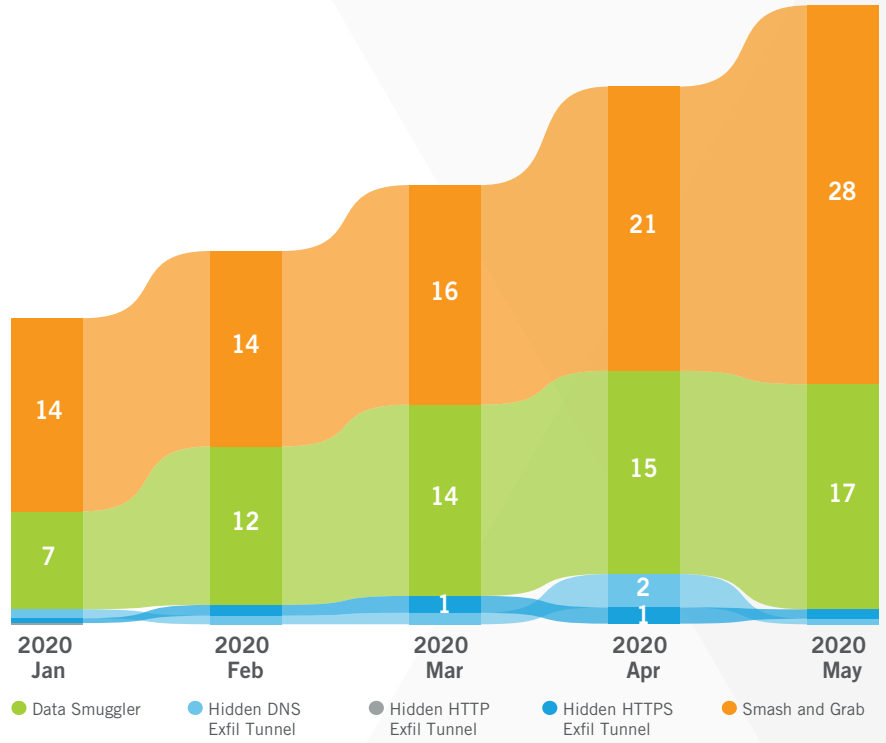

Figure 5: Exfiltration behaviors in healthcare per 10,000 devices throughout the EMEA region

While the cloud providers might be HIPAA-compliant and secure in design, the responsibility for ensuring adequate protection falls on the user and not the cloud provider. This is an important distinction when storing data in the cloud. As highly valuable assets protected by regulatory mandates, patient medical records must be securely transmitted to the correct destinations with appropriate data governance oversight and controls. The potential for errors in medical record transfers is particularly high. To reduce errors, many healthcare organizations automate and validate large, routine data transfers.

Conclusion

Within the current climate, the need for immediate response outweighs the normal policy oversight of ensuring secure data handling processes. Healthcare operations involve never-ending challenges to balance security and policy enforcement with usability and efficiency. Security organizations in healthcare will likely struggle with managing the need for availability of patient information with the policy and controls required for securing and protecting that data in the cloud.

Protected health information (PHI) is any information in the medical record or designated record set that can be used to identify an individual and was created, used, or disclosed in the course of providing a healthcare service such as diagnosis or treatment.

The biggest setback to cloud adoption in healthcare is the possible security risk associated with it. The privacy of patient data must be protected and cloud-hosted healthcare data must be safeguarded against external threats.

The growth in cloud computing means that more companies are putting more data and applications online, which attracts threat actors and cybercriminals eager to benefit from the potential to make easy money through various cloud cybersecurity schemes.

Healthcare organizations must find tools that identify what data is moving to the cloud and how it is being used and shared. Many healthcare providers believed this shift would occur in the future. But it is required now, even though strong security policies might not yet be in place.

Security teams for quite some time will have to grapple with where healthcare data exists and how to get it under control. To do so will require pan-organizational visibility that integrates the cloud and on-premises infrastructure to enable a truly comprehensive threat detection and response capability.

To learn more about cyberattacker behaviors seen in other real-world cloud, data center and enterprise environments, get the 2020 Attacker Behavior Industry Report from Vectra.

Email info@vectra.ai vectra.ai