Booz | Allen | Hamilton®

H-ISAC® HEALTH - ISAC

March 2022

CURRENT AND EMERGING HEALTHCARE CYBER THREAT LANDSCAPE

Executive Summary

This report is a collaboration between Health-ISAC and Booz Allen Hamilton

The report is TLP WHITE and may be shared without restriction.

For Health-ISAC members – be sure to download the full version of the report from the Health-ISAC Threat Intelligence Portal (HTIP). Contact Membership Services for assistance.

Current & Emerging Healthcare Cyber Threat Landscape

INTRODUCTION

2021 was a challenging year in cybersecurity with several high-profile compromises involving large vendors and large-scale vulnerabilities. The concerns of healthcare organizations remained largely unchanged between 2020 and 2021 with ransomware ranking as the primary concern of most organizations. Ransomware may disrupt operations, possibly causing a negative impact to patient care. There are also immediate financial implications of the ransom, the cost of remediation, brand damage, and more. Attacks against supply chains and operational technology environments show that the attackers are continuing to evolve and refine their tactics.

We must do the same.

Health-ISAC surveyed its members in the fall of 2021 to rank order the "greatest cybersecurity concerns" and the results of the survey are summarized here. The cyber threat perspective was prepared independent of the survey results to find and address any gaps between the concerns of leaders and cybersecurity practitioners in the healthcare sector. There were no considerable gaps in the concerns of the survey respondents and our evaluation of the threat landscape. This report should serve as an informational perspective of threat trends and top concerns of organizations across the healthcare landscape.

The Current & Emerging Healthcare Cyber Threat Landscape report covers the top cyber threats to healthcare organizations The intent of this report is to help influence cybersecurity budget and investment decisions for senior leaders and practitioners in the healthcare sector by providing an overview of the current cyber threat landscape and projections going forward. The analysis of this report was created between analysts from Health-ISAC and Booz Allen Hamilton to give the most diverse and experienced perspective possible.

SURVEY RESULTS

In a November 2021 survey, executives (n=132) across Health-ISAC completed a survey and rank ordered the Top 5 "greatest cybersecurity concerns" facing their organizations for both 2021 and 2022. The survey included cyber (e.g., CISO) and non-cyber executives (e.g., CFO), multiple healthcare subsectors (e.g., Providers, Pharma, Payers, Medical Device Manufacturers, Health IT) as well as healthcare organizations of varying size and IT/IS budget.

Executives reported the same Top Five Cyber Threats facing their organizations both retroactively for 2021 and looking ahead towards 2022. In addition, in comparing Cybersecurity Executives, IT Executives, and non-IS/IT Executives, no meaningful differences were observed. It was also found that the size of an organization did not impact the perception of the primary threat in 2021 or 2022.

Top Five Threats for 2021 and 2022:

1. Ransomware Deployment
2. Phishing/Spear-Phishing Attacks
3. Third-Party/Partner Breach
4. Data Breach
5. Insider Threats

CYBER THREAT INTELLIGENCE ANALYSIS

Nation State Threats

Nation-state threats against the healthcare sector continued in 2021 and increased in impact and scope. With the ongoing evolution of the COVID-19 pandemic, nation-state threat actors continued cyber espionage priorities to gather treatment and vaccine information. While many countries engage in sophisticated cyber-attacks including espionage, theft of intellectual property, ransomware, and destructive attacks, we chose to focus here on state-sponsored activities conducted by Russia and China.

Chinese Nation State Threats

Historically, nation-state threats to healthcare include attacks in 2014, 2018, and 2020 by Chinese state-sponsored Advanced Persistent Threat (APT) groups. These groups include APT 41, APT 1, and APT 18, respectively.

Russian Nation State Threats

Russian nation-state actors continue to be one example of those continuing to openly target healthcare institutions globally. APT 29, for instance, also referred to as CozyBear or The Dukes, remains prevalent throughout the COVID-19 pandemic as an espionage group attributed to Russian intelligence services.[i] This threat actor leverages spear-phishing, publicly available exploits, and custom malware to conduct data theft and information stealing, particularly from healthcare organizations focused on developing COVID-19 vaccines. They primarily focus on COVID-19 R&D in Canada, the United States, and the United Kingdom.[iii]

CYBER THREAT INTELLIGENCE ANALYSIS (continued)

2022 Nation State Threat Projections

With many nations making efforts to move beyond the pandemic, we assess that nation-state activity against healthcare will increase, especially with changes in strategic priorities around the globe. Tensions between Russia and Ukraine, as well as Chinese activity regarding Taiwan, are examples of nation-states returning to standard geopolitical strategies, which will reflect in cyberspace.

We assess the majority of nation-state threat activity against healthcare will center around Intellectual Property (IP) theft, and activity focused on economic strategies such as obtaining sensitive data on trade deals, negotiations, and supply routes in competitive global markets. It is likely some nation-state actors may utilize cybercriminal organizations as part of their cyber operations to obfuscate their activity using ransomware attacks as a method to extract sensitive data.

There is no indication that nation-state actors intend on using destructive malware or conduct activity that would put lives at risk due to the implication of cyber threat activity which results in civilian deaths being considered an act of war by the global community.

CYBER CRIMINALS & RANSOMWARE

Over the last decade, the healthcare industry benefited immensely from technological advances, resulting in major advances in medical care and the breadth of information available to save lives. However, these advancements led to greater interconnectivity and cloud-based infrastructures, making the industry a target for malicious threat actors. The healthcare industry is especially at risk due to the value of sensitive personally identifiable information (PII) housed within systems, an increase on the Internet of Medical Things (IoMT), insufficient cybersecurity protection, the need for data transparency, and ineffective employee awareness training. Often, healthcare providers rely on legacy systems; outdated computer systems that are still in use and provide less protection and increased susceptibility for an attack.[iii]

Recent Attacks Against Healthcare

The shift from paper health records to electronic health records has made patient health information more accessible, however, these records are more vulnerable to attacks and are extremely lucrative due to the sensitivity of their content. Threat actors can expect to receive $1 per stolen Social Security Number or credit card number but can demand $50 for a partial health record. If sensitive patient information is not protected, healthcare providers face costly legal, ethical, and moral dilemmas. Remote medical devices are less secure and are not easily updated, creating more endpoints for threat attackers to target sensitive health data. When the healthcare industry is targeted, it can result in disruptions to patient records, surgical services, medical devices, appointment systems, all with the potential to disrupt emergency or life-saving care and result in loss of life.[iv]

COVID-19 has created many exploitation opportunities for threat actors due to the value of vaccine research and data, a rapid deployment of remote systems to support remote workforces, and an amplified opportunity to target individuals via phishing campaigns to gain access to systems.[v]

CYBER CRIMINALS & RANSOMWARE (continued)

2022 Cybercriminal Projections

Cyber criminals' transition to a Ransomware-as-a-Service (RaaS) model will continue in 2022 and likely become the most common operating model for cyber-criminal gangs. The RaaS model will cause attribution to become more difficult and tools used in ransomware attacks will no longer be an adequate method of determining the identity of an attacker. We assess the RaaS model will make cybercriminal gangs more agile, and their potential for exploiting publicly disclosed vulnerabilities will increase to as quickly as 24 to 48 hours from the release of a Proof-of-Concept to active exploitation depending on the severity of the vulnerability and the projected monetary gain from a vulnerability's exploitation. We assess that in 2022, cybercriminals will target critical systems to the operations of healthcare organizations as a means to force healthcare organizations to pay a ransom quickly and not allow time for investigation or forensic examination prior to paying the ransom demanded.

Medical devices remain a viable vector of approach for cybercriminal operations due to legacy systems and irregular software updates, but there is no indication that cybercriminal gangs intend on threating the lives of patients as a method to extract ransom from a healthcare organization. Cybercriminal gangs' targeting of healthcare organizations is focused on brand damage, loss of production, and delay of basic care to motivate organizations to pay their ransom. Cybercriminal gangs are also aware of the strict regulatory environment regarding patients' Protected Health Information (PHI) and will threaten the disclosure of such information to encourage healthcare organizations to pay their ransom without delay.

Due to the huge growth in cybercrime and large ransomware payouts, sophisticated and organized criminal groups will be able to invest heavily into R&D and develop new ways to conduct automated and effective scams. The criminals will leverage machine learning, artificial intelligence and deep fakes to perpetrate efficient and effective criminal campaigns.

CYBER CRIMINALS & RANSOMWARE (continued)

Supply Chain

Large supply chain compromises highlight the change in threat actor attack strategies and how they are finding success in compromising IT providers, Managed Service Providers and Enterprise Management Software Systems to gain access to a larger group of victims. In 2021 incidents involving SolarWinds, Kaseya and Accenture, for example, created supply chain compromises that increased 4x over the previous year. Likely, heading into 2022, threat actors will evolve this tactic and focus on compromising cloud providers to gain access to the sensitive data of multiple victims.[vi]

In April 2021, the American Hospital Association (AHA) and Health-ISAC produced a strategic intelligence analysis report to identify what other "SolarWinds" like issues might be lurking in enterprise networks.

The paper is meant for all audiences, non-technical and technical, and provides strategic level decision elements that senior leaders, including C-Suite Executives, can use to help understand the risks involved with certain enterprise IT systems in their network environment.

The report contains detailed technical analysis and recommendations for IT and information security teams to help address immediate concerns by providing tactical mitigations and recommendations. For technical readers, the paper presents a detailed analysis of characteristics that allowed the SolarWinds incident to affect multiple industries, organizations, and systems. The ability to extract the characteristics and features of SolarWinds could allow organizations to predict and hopefully prevent the next "SolarWinds"-like event in their enterprise environments

https://h-isac.org/preparing-for-the-next-solarwinds-event-2/

2022 OPERATIONAL TECHNOLOGY AND SUPPLY CHAIN PROJECTIONS

Threat actors will likely focus on supply chains as a viable vector of approach given the successful breach of SolarWinds, Kaseya and the leveraging of Apache's Log4j in late 2021. Cybercriminal gangs and nation-state actors know that a supply chain compromise will give them access to a larger target surface than attempting to compromise individual targets. Operational technology is also an increased focus for threat actors and operational technology compromises will come from a supply chain compromise via a vendor update or vulnerability in Primary Logic Controllers (PLCs).

Cybercriminals may focus more efforts on operational technology because organizations are more likely to pay a ransom quickly rather than shut down production. Nation States will also focus on operational technology for intellectual property (IP) theft and potential supply disruption activities.

RECOMMENDATIONS TO MITIGATE THREATS

Health-ISAC recommends the following general best practices to protect against the threats described above:

- **Layered Defense:** Adopt a layered defense approach, where your organization's security stack is layered with defenses and protection technologies deployed from the perimeter and inwards onto each host on your network.
- **Network Segmentation:** Implementing network segmentation and deploy firewalls, to mitigate the risk posed by advanced threat actors.
- **Endpoint Security:** Deploy an endpoint security product or a Host Intrusion Detection System (HIDS) that is driven by behaviour-based rules and can block execution of PowerShell or cmd.exe spawned from Microsoft Office applications.
- **Access Controls:** Implementing role-based access controls, secure remote access channels, robust and efficient system logging and monitoring to limit the effectiveness of advanced exploits and threats and increase the likelihood of detection.
- **Prevention and Detection:** Implementing countermeasures to mitigate attacks at the perimeter of the network. This includes firewall rules used to block unused ports and deny HTTP requests to non-standard ports, content filtering to allow users to only access trusted sites, restricting users from browsing with local admin privileges on their machines, and intrusion prevention systems to detect and block malicious traffic from entering the environment.
- **Data Backup:** Rely on frequent, segmented, and redundant backups as the best way to restore encrypted files in the event of a ransomware infection.

For a comprehensive set of recommendations, refer to the Health Sector Coordinating Council's Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Publication: *https://healthsectorcouncil.org/hhs-and-hscc-release-voluntary-cybersecurity-practices-for-the-health-industry/*

The publication seeks to raise awareness for executives, health care practitioners, providers, and health delivery organizations, such as hospitals. It is applicable to health organizations of all types and sizes across the industry.

Feedback and suggestions on this document are encouraged and welcome.
Please email contact@h-isac.org

END NOTES

i 27 April 2021; HealthcareIT News; Cybersecurity Roundup: US Agencies Warn of Russian Hacks, Australian Hospitals Struggle to get Back Online; *https://www.healthcareitnews.com/news/cybersecurity-roundup-us-agencies-warn-russian-hacks-australian-hospitals-struggle-get-back*

ii 16 July 2020; Healthcare IT News; Russian Hackers Targeting Healthcare Orgs for Coronavirus Vaccine Info; *https://www.healthcareitnews.com/news/russian-hackers-targeting-healthcare-orgs-coronavirus-vaccine-info*

iii Fall 2021; Journal of Business and Accounting; RANSOMWARE: HEALTHCARE INDUSTRY AT RISK *http://asbbs.org/files/2021/JBA_14.1_Fall_2021.pdf#page=65*

iv September 2021; International Journal For Quality In Health Care; Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health; *https://academic.oup.com/intqhc/article/33/1/mzaa117/5912483?login=true*

v August 2020, Heath IT Security; COVID-19 Impact on Ransomware, Threats, Healthcare Cybersecurity; *https://healthitsecurity.com/news/covid-19-impact-on-ransomware-threats-healthcare-cybersecurity*

vi 16 August 2021; Cyber Talk; 4x increase in supply chain attacks; experts worried; *https://www.cybertalk.org/2021/08/16/4x-increase-in-supply-chain-attacks-experts-worried/*