Executive Summary:

Current and Emerging Healthcare Cyber Threat Landscape

This report is a collaboration between Health-ISAC and Booz Allen Hamilton Cyber Threat Intelligence (CTI).

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.

Introduction

Time and again, cybersecurity incidents like SolarWinds, Log4j, and geopolitical events such as the Russia-Ukraine War have sent shockwaves throughout the cybersecurity community — impacting the operability of thousands of organizations globally. When thinking about how targeted organizations align to some of the top global industries including Manufacturing, Oil and Gas, Finance and Healthcare, it is easy to understand why threat actors, whether financially or politically motivated, value such targets: the societal criticality, privacy and confidentiality needs, and vulnerability of these organizations make them attractive to extortion, espionage, and product abuse.

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.

I: Survey Results

Survey Background

In a November 2022 survey, executives (n=288) across Health-ISAC, CHIME and the Health Sector Coordinating Council completed a survey and rank ordered the Top Five ***"greatest cybersecurity concerns"*** facing their organizations for both 2022 and 2023. 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.

Survey Findings (2022 and 2023)

Executives reported the same Top Five Cyber Threats facing their organizations both retroactively for 2022 and looking ahead towards 2023.

The rank ordering of the Top 5 Cyber Threats was unchanged from 2022 to 2023. However, compared to the prior year's survey for 2022 concerns, Social Engineering is now the 5th Greatest threat replacing Insider Threat (now number 6).

Top Five Threats for 2022 and 2023 were:

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

II: The Current Threat Landscape

As cyber adversaries continue to evolve and innovate, healthcare industry IT and Information Security professionals need to increase awareness of the current threat landscape. To protect healthcare organizations, security teams and senior leadership need to know the groups targeting the healthcare sector; the tools and methods they are using to do so; and recent successful attacks. Such knowledge is essential to formulating an effective information security and overall risk strategy that should also influence training, security roadmaps, and other facets that compose the industry's cybersecurity posture for 2023 and beyond.

To expand situational awareness of the threat landscape, this section examines cybercriminal, nation-state, and geopolitical activities and trends, broadly across industries and also as they relate to the healthcare industry.

Cybercriminal Activity

Despite increasing sanctions and arrests of Ransomware as a Service (RaaS) gang members, and even the potential for civil penalties against victims who pay ransoms, we do not anticipate that the rate at which organizations are impacted by ransomware will decrease in the coming years because the RaaS model supplies a return on investment for cybercriminal gangs and their affiliates that far outweighs the cost of continuing such operations.

For example, we have observed a trend in which threat actors who have successfully monetized initial accesses for financial gain are integrating with RaaS groups to further obscure operating models and attribution efforts. Access sellers and RaaS groups are two elements of the same exploitation lifecycle: a domain admin access to a multinational company with billions in revenue could result in a multi-million-dollar ransomware payoff, yet the access may only cost the RaaS operator USD $10,000 to purchase. The criminal monetization process is continuously improving and gaining in sophistication as these actors are learning to mitigate and defeat end-point security and anti-virus tools. Malicious operators develop their malware to achieve long-term persistence and victims may be subject to multiple extortion and/or ransom techniques, ranging from cryptojacking to ransomware; however, the motivation is almost always financial.

Ransomware operators attack victims based on opportunity. They leverage vulnerabilities, misconfigurations, access sales on forums, and use access gained by affiliates to proliferate encryption payloads across network endpoints.

Geopolitical Activity

Because geopolitical conflict has become increasingly intertwined between the kinetic and digital worlds, businesses operating within these regions must not only consider the physical implications of conflict, but the cybersecurity implications as well. Since the start of the Russia-Ukraine War, the world has observed an increase in pro-Russian and pro-Western activity ranging from Distributed Denial-of-Service (DDoS) attacks to state-sponsored propaganda, and threats against critical infrastructure. Businesses that operate in regions that are a potential flashpoint for geopolitical tension should assess the impact such activity may have on company operations. In times of peace, businesses must also consider the risk to operating in certain regions of the world, as technical education is ever improving, and the lack of effective law enforcement coupled with tacit approval from central governments will provide the flexibility and space for cybercriminals to improve their craft with near impunity. Large multinational companies will suffer the most from this activity as global cooperation for rules governing the exchange of data and its protection is dictated by geopolitical differences.

Russia-Ukraine

Russian hackers have also reportedly used information stealer malware to target organizations in the Ukrainian government, critical infrastructure, defense, security, and law enforcement sectors.[1] As a result of the war, over 1,000 companies have either curtailed or completely withdrawn operations from Russia, according to the Yale School of Management, which has tracked this information since the start of the invasion. Although the original intention appears to serve as a "comprehensive record" of the exodus, hacktivists have also closely followed this list to identify new targets.[2] This suggests that companies perform or update cost-benefit analyses of continuing operations in the region, to include cybersecurity risk.

European Energy Crisis

The European Union engaged with Russia in an economic conflict to apply pressure on Russia to cease the military effort in Ukraine. Due to Russia's extensive natural gas resources, natural gas has become the object of scrutiny.[3] For example, Russia stopped exporting to the EU after it placed a price cap on Russian gas imports.[4] Most recently, on September 26, 2022, the Nord Stream pipelines, which run through the Baltic Sea and are crucial to supplying energy from Russia to Europe, were sabotaged. At the time of writing, both Nord Stream One and Nord Stream Two were rendered inoperable.[5] In response, and to identify the culprit, the EU sent independent inspectors to assess the damage, which resulted in allegations of sabotage carried out by the Russian government. As attribution is not yet definitive, the action would have powerful political implications if the Russian Government is culpable, and investigators cannot prove the damage's cause. Resolution to the Russia-Ukraine War will be more difficult as negotiations with Russia will likely include updated terms surrounding the repair of the natural gas pipelines. As the energy crisis worsens and the path to resolution becomes increasingly complex, the healthcare sector should maintain awareness around the impact this might have to subsectors such as decreased pharmaceutical exports from European suppliers and European hospitals without adequate energy to properly care for patients. At the time of writing, hospitals have been spared from the energy rationing efforts, but this exemption may not last if the crisis worsens.[6]

[1] Ionut Ilascu, "Russian Hackers Use New Info Stealer Malware Against Ukrainian Orgs," 15 September 2022, https://www.bleepingcomputer.com/news/security/russian-hackers-use-new-info-stealer-malware-against-ukrainian-orgs

[2] "Over 1,000 companies have curtailed operations in Russia - Some Remain," Yale, 14 December 2022, https://som.yale.edu/story/2022/over-1000-companies-have-curtailed-operations-russia-some-remain

[3] "Russia's Natural Gas Pipeline Exports to Europe Decline to Almost 40-Year Lows." Eia.gov, 9 August 2022, https://www.eia.gov/todayinenergy/detail.php?id=53379

[4] Pavlova, Uliana and Cooban, Anna. "Russia Cuts Off Gas Exports to Europe Via Nord Stream Indefinitely." CNN Business, 2 September 2022, https://www.cnn.com/2022/09/02/energy/nord-stream-1-pipeline-turned-off/index.html

[5] Plucinska, Joanna. "Nord Stream Gas 'Sabotage:' Who's Being Blamed and Why?" Reuters, 6 October 2022, https://www.reuters.com/world/europe/qa-nord-stream-gas-sabotage-whos-being-blamed-why-2022-09-30/

[6] Saric, Ivana. "Russian Attacks on Ukrainian Utilities Prompt Energy Rationing." Axios, 20 October 2022, https://www.axios.com/2022/10/20/russia-attack-ukraine-infrastructure-energy-saving

China-Taiwan

As President Xi Jinping continues to consolidate total power over China and the Communist Party of China (CPC), it is possible the world may witness a China-Taiwan conflict in the coming years, particularly as President Xi Jinping's rhetoric becomes increasingly forceful regarding "reunification."[7] Absent current, direct conflict, however, threat actors continue to carry out hacktivist-style attacks against Taiwanese businesses and organizations on behalf of the CPC.[8]

For instance, following Nancy Pelosi's visit to Taiwan as Speaker of the U.S. House of Representatives, threat actors compromised Taiwanese information systems to display a slew of propaganda across business menu boards and train station platforms. Just a day after the visit,[9] China fired missiles near Taiwan in its biggest drills in the Taiwan Strait, signaling its displeasure over the visit. It is possible that state-sponsored groups, likely at the behest of China's Ministry of State Security (MSS), conducted the accompanying information attack. Still, like other countries, China has a domestic brew of cyber activists and cybercriminals that are allowed, and sometimes encouraged, to conduct such activity on behalf of the CPC. Large multinational companies are attractive targets because attacks are disruptive and can impact economic, political, and international conditions. Such incidents are likely to continue as countries appear less willing to engage in outright warfare, with obvious exceptions, and will instead attempt to use cyber warfare to coerce adversaries towards a favorable direction. In anticipation of such activity, companies with business operations in China, Taiwan, or, more generally, the Asia Pacific region, should consider risk assessments and contingency planning to mitigate, or remove the threat to, assets and business operations in the region.

[7] "Full Text of Xi Jinping's Report at the 19th CPC National Congress." Xinhua, Full text of Xi Jinping's report at 19th CPC National Congress -Xinhua | English.news.cn (xinhuanet.com)

[8] "Full Text of the Report to the 20th National Congress of the Communist Party of China," Ministry of Foreign Affairs of the People's Republic of China, Full text of the report to the 20th National Congress of the Communist Party of China (fmprc.gov.cn)

[9] Sarah Wu and Eduardo Baptista, "From 7-11s to Train Stations, Cyber Attacks Plague Taiwan Over Pelosi Visit," Reuters, 4 August 2022, https://www.reuters.com/technology/7-11s-train-stations-cyber-attacks-plague-taiwan-over-pelosi-visit-2022-08-04/

III: Cyber Threat Intelligence Analysis

Nation State Threats

The health sector is also a lucrative target for nation-state backed threat actors (also known as Advanced Persistent Threats or APTs) due to the vast amount of sensitive information organizations within this sector must safeguard, including intellectual capital, Protected Health Information (PHI), Personally Identifiable Information (PII), and informational and operational technologies. For example, in July 2022, the U.S. Federal government issued a warning stating North Korean threat actors had been targeting the healthcare sector for over a year.[10] Their objective appeared to be financial gain due to the ransomware used in these attacks; however, North Korea is known to conduct attacks for both espionage and financial purposes. We chose to focus here on state sponsored activities conducted by North Korea, and China.

Chinese Nation State Threats

Active since 2012, APT41 uses a combination of public and private malware and spearphishing to steal credentials and to establish backdoors with a predilection for healthcare systems, pharmaceutical companies, and high-tech industries.[11] APT41 is associated with the Chinese Ministry of State Security (MSS), which is known to target industries and intellectual property that are aligned with China's most recent Five-Year Plan.

APT27, also known as Emissary Panda, targeted multiple German companies with watering hole and spearphishing attacks in multiple sectors including pharmaceuticals in 2022.

North Korea: Kimsuky, and Maui

On the other side of the world, Kimsuky, a North Korean state-sponsored group active since 2012, was observed targeting healthcare with spearphishing and watering hole attacks; however, it primarily targets South Korea.[12] In July 2022, North Korean threat actors targeted the healthcare sector using malware called "Maui" to collect financial ransoms.

[10] "North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target Healthcare and Public Health Sector." Cisa.gov, 7 July 2022. https://www.cisa.gov/uscert/ncas/alerts/aa22-187a

[11] "Chinese APT leveraged zero days — Including Log4j — To compromise US state governments." SC Media, 8 March 2022, https://www.scmagazine.com/analysis/apt/chinese-apt-leveraged-zero-days-including-log4j-to-compromise-u-s-state-governments

[12] "Researchers Uncover Kimusky Infra Targeting South Korean Politicians and Diplomats." The Hacker News, 25 August 2022, https://thehackernews.com/2022/08/researchers-uncover-kimusky-infra.html

Medical Device Cybersecurity

Like Operational Technology (OT), the proliferation of the Internet of things (IoT) and the Internet of medical things (IoMT) in the healthcare environment warrant safeguarding. These devices can interact with the environment; in medical devices, that interaction point is often a patient or caregiver. Healthcare companies with a higher percentage of connected medical devices experienced more cyberattacks and were more likely to experience multiple attacks.

The Capterra 2022 Medical IoT Survey 1 revealed increased medical device data and traffic monitoring are essential, and the breadth of patient care technologies may necessitate more than one tool. To remedy the growing need for medical device security, Health-ISAC recommends:

- Performing risk assessments and develop threat models to identify how devices may be susceptible to cyberattacks and to understand their impacts on patient care.
- Identify and correct those devices with default or poor credentials. Apply patches and updates when available.
- Engage caregivers to better understand the safety and operational implications to patients and care delivery and then develop care contingency plans that will build resilience and proactively prepare for cyber threats into medical technology operations.

IV: Threats on the Horizon

Despite efforts to secure healthcare organization environments and implement improved controls, threat actors are extremely adaptable and recognize that information they can steal can be used in more ways than one to generate monetary gain. Cybercriminal forums advertise ways to purchase access to sensitive information which can be used for multiple objectives, including strategic insight into organizations, a method to gain additional footholds into company networks, and bargaining material to drive extortion demands. There are ample cases to show that the attack surface is quite large, and that there are a myriad of valuable targets including intellectual property, supply chain flows, and customer/employee records.

Healthcare organizations should maintain awareness around emerging risks in the form of operational, financial, and regulatory impacts. Risks that have been traditionally observed in the financial and high-tech sectors are starting to appear in other sectors that have not developed the security controls and processes to address these issues.

Two emerging risks we anticipate will plague the healthcare industry in 2023 include product abuse and synthetic accounts.

Product Abuse

Organizations with internet facing products, such as web login portals and APIs, are easy targets for actors that employ compromised user credentials, proxy networks, and customizable crimeware to carry out account takeovers, or unauthorized access to account. Billions of compromised credentials that have been captured through phishing, malware, and data breachers are available for sale on deep and dark web cybercriminal forums. Credential lists are freely available on many forums; however, attackers can gain access to more restrictive or targeted lists by purchasing credentials in automated credential shops (ACS) or malware marketplaces. For example, an adversary could purchase only credentials that were found in malware logs where the domain the credential was captured is a specific domain for the product(s) they wish to abuse to gain access to health records.

Synthetic accounts

The proliferation of compromised PII and lack of controls that verify individuals (versus validation) is creating opportunities for adversaries to commit fraud, game systems, and even generate individuals digitally out of thin air. Financial institutions and lenders have fallen victim to millions of dollars in losses due to synthetic account creation1313 and identity theft. Cybercriminals will often build a fake credit profile with these accounts over the course of several months and years to strengthen the success rate of their attacks. These accounts have been used to obtain loans, make large purchases, cash out funds, and other fraudulent activity since these accounts are set up to bypass identity checks. The health industry will likely see a rise in these types of attacks to pay for medical billing and other health-related activity.

[13] A synthetic account or identity refers to the creation of an account or identity using falsified information or a combination of real and fake information.

Threat Outlook

Although most organizations understand that threat actors can target sensitive data through access to internal systems, abuse against third-party systems, email accounts, and customer-facing products widen the scope for abuse. Customer-facing products are routinely targeted by attacks designed to extract data with crimeware that threat actors have customized to look and feel like a legitimate customer—whether a consumer, industry practitioner, or third party. Preparing for these attacks require properly aligned controls at the network, application, authentication, and risk layers to protect organizational data and reduce the risk of credential stuffing, account takeovers, carding attacks, and unhealthy account creation.

Closing Thoughts

Health-ISAC continues to place its members at the forefront of our mission, which has resulted in a wide accumulation of knowledge that we aim to aggregate and share within this report. Health-ISAC places security and resiliency of the healthcare sector at the utmost importance and relishes the opportunity to assist in the fight against threats which impact healthcare sector entities and their partners and suppliers.

In 2023, Health-ISAC will continue to bring members actionable and accurate threat intelligence encompassing both the cyber and physical realms. This would not be possible without the use of our greatest asset—our members—who play a significant role in the fight to secure a more secure and resilient future for the healthcare sector.

> **“There is a wealth of knowledge in our community at Health-ISAC where peers are sharing information...the community is there to help, so don’t think you have to go at it alone.”**
>
> —Denise Anderson, President and CEO, Health-ISAC

Feedback and suggestions on this document are encouraged and welcome.

Please email **contact@h-isac.org**