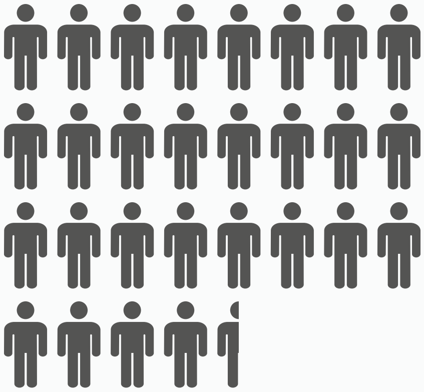
Trustwave
SpiderLabs

CYBERSECURITY IN THE HEALTHCARE INDUSTRY

Actionable Intelligence for an Active Threat Landscape

Contents

Introduction



28.5 million

HEALTHCARE RECORDS BREACHED IN 2022

$10.1M

vs

$4.4M

AVERAGE COST OF A DATA BREACH IN HEALTHCARE COMPARED TO ALL OTHER INDUSTRIES

Data security is a challenge in the healthcare industry that's bordering on a crisis.

By its very nature, health-related data represents the most intimate and personal information we possess. Consequently, personal health information (PHI) has become a highly coveted target for attackers, who exploit its confidential nature to extort payers, providers, and other entities within the healthcare ecosystem.

The U.S. Department of Health and Human Services reports that more than 28.5 million healthcare records were breached in 2022, a significant increase from 21.1 million in 2019. Notable recent headlines include the MediBank data breach that impacted 9.7 million customers, a ransomware attack on PharMerica that exposed medical data of 5.8 million patients, and SMP Health, a hospital that was forced to shut down after its inability to recover from a ransomware attack.

Due to the sensitive nature of healthcare data and the regulatory requirements that healthcare organizations must comply with, the financial impact of a breach in the healthcare industry far surpasses other industries. In 2022, the average cost of a data breach in healthcare was $10.1 million, which is more than double the industry average of $4.4 million, according to data from the Ponemon Institute.

The gravity of the situation goes far beyond the compromise of data or the risk of financial impact. In the healthcare sector, the stakes involve matters of life and death. Ransomware attacks causing disruptions in hospitals have already been linked to multiple patient fatalities, and the American Hospital Association warns that the resultant delays and interruptions in healthcare delivery increase the risk of adverse outcomes, including more deaths.

Given these circumstances, it is crucial for the healthcare sector to minimize its risk and prioritize information protection. Unfortunately, reality paints a different picture, with the industry often lagging behind in this area. Several key factors contribute to this discrepancy:

- **Legacy Systems:** Many healthcare providers still use legacy systems that are no longer supported by vendors or are difficult to patch and update. These systems are often more vulnerable to cyberattacks, and healthcare providers must take extra precautions to protect them.
- **Third-Party Reliance:** Healthcare entities commonly engage with numerous third parties, further expanding the number of endpoints and users involved, thereby contributing to a growing threat surface.

This report's objective is to thoroughly examine the multitude of threats that pose challenges to the healthcare industry. We will begin by highlighting the significant trends currently affecting the industry and discuss the appropriate responses that healthcare entities should adopt. Subsequently, we will analyze the attack flow specific to the healthcare sector, offering actionable intelligence and recommended mitigations for each stage to illustrate how organizations can proactively identify and prevent attacks to avoid lasting impact.

The Health Insurance Portability and Accountability Act (HIPAA) maintains detailed data security requirements healthcare organizations must meet to remain compliant. Organizations that attempt to comply and maintain strong cybersecurity protocols, but are still victimized, will receive a lower penalty than those who ignore regulations.

With that in mind, there are three types of HIPAA violations, all which carry varying degrees of impact:

- An organization has made reasonable efforts to comply with HIPAA, but was still victimized by an attack.
- The failing was attributable to lack of monitoring or oversight.
- The organization made little or no effort to comply with HIPAA despite knowing it had to.

HIPAA uses a four-tiered system to assess culpability and issues fines based on the organization’s compliance with HIPAA regulations. Fines range from $127 per violation to $1.9 million.

1. Lack of knowledge.
2. Reasonable cause.
3. Willful neglect.
4. Willful neglect not corrected within 30 days.

This report contains several actionable items to help an organization meet its HIPAA requirements.

Emerging and Prominent Trends

Artificial Intelligence and Generative AI

ARTIFICIAL INTELLIGENCE AND GENERATIVE AI

Unique implications and risks due to the sensitive nature of the data potentially being shared with these tools, as well as advances in phishing.

The Threat

Generative AI and Large Language Models (LLMs) have taken the world by storm. While AI isn't new, the advances made in Generative AI and LLMs are setting new benchmarks for what's possible for healthcare organizations and for both adversaries and defenders as well. For healthcare, the risks are further heightened due to the sensitive nature of the data potentially being shared with these tools.

How This Could Affect You

Healthcare leaders are significantly concerned about the potential for unintentional breaches of patient data by internal teams who utilize LLMs to enhance efficiency and scalability, considering the sensitive nature of the data involved. While the potential benefits of these tools could be substantial, the security of these systems has not yet been proven. Therefore, it is essential to adopt a risk-benefit approach and carefully consider the implications with the CISO leading the way.

Moreover, healthcare organizations face an increased risk of exposure due to their reliance on third-party vendors who may incorporate Generative AI or LLMs into their products, raising concerns about the potential loss of control over patient data used for training these models.

Lastly, social engineering attacks can become more sophisticated as LLMs have the capability to create highly personalized and targeted messages.

> “Like many organizations, we're closely monitoring the development and impact of Generative AI. Instead of adopting a restrictive approach or implementing blanket bans, we have chosen to establish internal structures to govern and educate our employees on its usage. We have found that integrating security measures into our existing organizational frameworks and meeting our employees where they already are yields the best results.”
>
> **NATE LESSER**
> **CISO OF CHILDREN'S NATIONAL HOSPITAL**

WHAT TRUSTWAVE SPIDERLABS IS SEEING

Trustwave is monitoring the progress and attacker implementation of both Generative AI and LLMs. Based on observations to date, Trustwave sees the primary areas of concern are the increased speed and quality that phishing emails can be drafted and exploit code can be enhanced. This will require security vendors to adjust their detection and response capabilities accordingly.

While LLMs and other technologies categorized as AI seem to have matured at a near-miraculous rate over the past year, we don't have any indication that LLMs have "changed the game" in any substantive way beyond the existing cat-and-mouse games we've always worked against in the security industry.

Trustwave continues to monitor this emerging trend in novel ways threat actors use it and opportunities for risk reduction on the defenders' side. While we explore methods of integrating LLMs to augment our workflow, we see promising trends in identifying PoC exploit code, reverse-engineering malware, and processing large amounts of log files to identify and prioritize threats that must be addressed.

DETERMINE HOW TO GOVERN THE TOOLS VERSUS INSTITUTING BROAD-BASED BANS.

Mitigations to Reduce Risk

- Evaluate your security solutions with Generative AI and LLMs in mind. Choose security tools or partners that can detect AI-generated threats like advanced phishing.
- Create robust internal policies and employee training for proper data usage and data sharing to help minimize the risk of data breaches.
- The reality of the current landscape is that Generative AI is here to stay. While the tools still have inherent risks, healthcare organizations, like all entities, will need to determine how to govern the tools versus instituting broad-based bans.
- Consider instituting an internal AI Infosec working group across relevant teams (like Legal, Privacy, IT, etc.) to deal with governance and data sharing guidelines.

Ransomware Groups Targeting Healthcare

RANSOMWARE GROUPS TARGETING HEALTHCARE

Threat groups previously considered healthcare-related targets off limits, or protected, but are now widely attacked.

24%

OF CRITICAL INFRASTRUCTURE RANSOMWARE ATTACKS TARGET HEALTHCARE

The Threat

According to the FBI, there were more reports of ransomware attacks targeting the healthcare sector than any other critical infrastructure sector in 2022, accounting for 24% of all ransomware attacks.

The largest ransomware attack on a hospital in 2022 was the US-based CommonSpirit ransomware attack that compromised the data of 623,000 patients. Just last month, in June 2023, the Clop ransomware group stole the personal and health information of 490,000 individuals in a ransomware attack on IntelliHARTx, a healthcare payments technology.

Illustrating the financial toll that ransomware can take, US-based Scripps Health not only paid $3.5 million to the victims of its 2021 data breach, but due to a month-long outage, cited a loss of $113 million in revenue.

How This Could Affect You

Threat groups previously considered healthcare-related targets off limits, or protected, but are now widely attacked. Ransomware attacks will continue to be a major threat to the healthcare sector, with attackers exploiting vulnerabilities in healthcare systems to encrypt critical patient data and demand ransom payments.

The use of double-extortion tactics, which is when ransomware groups not only encrypt a victim's data, but also threatens to expose it publicly unless a ransom is paid, and the increasing sophistication of ransomware attacks will make it more difficult for healthcare providers to defend against such attacks.

What Trustwave SpiderLabs Is Seeing

According to Trustwave SpiderLabs' ransomware research, the top 5 most prevalent ransomware groups targeting the healthcare industry today are:

- LockBit 3.0
- ALPHV/BlackCat
- Clop
- DMA Locker
- Royal

BlackCat specifically stooped to a new low for ransomware groups when it published photos of breast cancer patients as part of its extortion of Lehigh Valley Health Network, a Pennsylvania-based healthcare network.

Later sections will provide details from Trustwave SpiderLabs about how HTML smuggling and Qakbot malware were used to deploy ransomware. Through its investigations, Trustwave SpiderLabs also encountered the following ransomware groups in the last year:

- Babuk
- Magniber
- LockBit
- Black Basta
- RansomHouse

SpiderLabs research found multiple examples of healthcare data for sale on the Dark Web, providing strong evidence of the added component of victim extortion.

Mitigations to Reduce Risk

- Remember the best defense is a good offense. The subsequent sections will dive into each of these further but regularly train and test employees, make sure policies and patches are up to date, and deploy layered email security to help detect and cleanse malicious emails.
- Regularly back up your data to help ensure the ability to recover from a ransomware attack or other types of data loss. Be sure to store backups offsite and verify that they can be restored.
- Ransomware and other malware gangs target Remote Desktop Protocol (RDP), the Microsoft protocol that allows users to execute remote operations on other computers. Secure exposed RDP services, patch known vulnerabilities, and/or disable them if not necessary.

Software Vendor and Internet of Things (IoT) Exposure

The Threat

The healthcare industry heavily depends on third-party vendors, including cloud-based web hosting providers and software companies, to support its operations. Unfortunately, cybercriminals often target these third parties as a strategic maneuver – if they successfully breach a third-party vendor, they gain access to the targeted company's data. This poses a significant threat to healthcare organizations since many of these vendors lack robust cybersecurity measures and data breach protection.

In addition to the risks associated with third-party vendors, the proliferation of Internet of Things (IoT) devices in healthcare further amplifies the potential attack surface and vulnerability of the industry's infrastructure.

How This Could Affect You

Recent supply chain headlines, like 3CX or the infamous SolarWinds, underscore the exposure that third-party vendors can expose healthcare organizations to. Because of healthcare entities' classification as critical infrastructure, they are an attractive target for threat actors who aim to exploit their widespread access to compromise multiple entities across various sectors and industries. Supply chain attacks can pose a risk even to healthcare entities that protect their digital networks perfectly well.

Due to the recent zero-day vulnerability in MOVEit, a file transfer software, there has been a lot of discussion about the risks associated with data-sharing among organizations within an economy's supply chain or critical infrastructure. The MOVEit software specifically is used by multiple organizations in the Healthcare and Public Health (HPH) sector, including hospitals, clinics, and health insurance groups The U.S. Department of Health and Human Services (HHS) was impacted, stating that "attackers gained access to data by exploiting the vulnerability in the MOVEit Transfer software of third-party vendors."

From an IoT perspective, healthcare devices such as heart monitors or pacemakers, are often developed with a hardware-first approach. However, when it comes to connecting these devices to a network, there is often a lack of thorough security evaluation. As stated by the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3), "Medical device hardware often remains active for 10-30 years, however, underlying software life cycles are specified by the manufacturer, ranging from a couple months to maximum life expectancy per device allowing cyber threat actors time to discover and exploit vulnerabilities."

It is crucial for organizations to prioritize ensuring their suppliers adhere to stringent security measures to mitigate potential risks.

SOFTWARE VENDOR AND INTERNET OF THINGS EXPOSURE

The risks associated with third-party vendors and the proliferation of Internet of Things (IoT) devices in healthcare further amplifies the potential attack surface and vulnerability of the industry's infrastructure.

MEDICAL DEVICE HARDWARE OFTEN REMAINS ACTIVE FOR 10-30 YEARS, HOWEVER, UNDERLYING SOFTWARE LIFE CYCLES ARE SPECIFIED BY THE MANUFACTURER, RANGING FROM A COUPLE MONTHS TO MAXIMUM LIFE EXPECTANCY PER DEVICE ALLOWING CYBER THREAT ACTORS TIME TO DISCOVER AND EXPLOIT VULNERABILITIES.

What Trustwave SpiderLabs Is Seeing

During a penetration test conducted by Trustwave SpiderLabs, a convergence of third-party risk and IoT exposure was uncovered with the identification of two Reflected XSS vulnerabilities in third-party software for Canon Medical's Vitrea View.

Exploitation of these vulnerabilities could potentially lead to unauthorized access to patient information, stored images, scans, and the ability to manipulate data based on session privileges. Additionally, sensitive information and credentials associated with various services integrated with Vitrea View could be compromised. These vulnerabilities were assigned CVE-2022-37461.

Another vulnerability was discovered by Trustwave SpiderLabs in the Sinilink Wi-Fi-connected thermostat. These discoveries highlight the pressing need for IoT system developers to implement robust and secure protocols wherever feasible. This particular vulnerability enables an attacker to replay identical or similar data, potentially granting unauthorized control over the relay-connected device without requiring authentication. Exploitation of this vulnerability capitalizes on the absence of endpoint verification, allowing an attacker to send commands directly to the targeted device via the User Datagram Protocol.

Mitigations to Reduce Risk

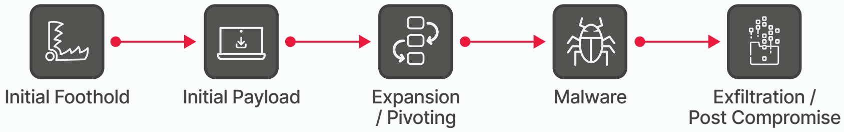
- Healthcare providers must ensure both their own systems and those belonging to third-party partners are secure and protected by the latest security measures. This can be achieved through regular penetration tests and vulnerability scans.
- Maintain an inventory management system for all medical devices and associated software, including vendor-developed software components, operating systems, version and model numbers.
- Implement a routine vulnerability scan before installing any new medical device or technology onto the operating IT network.

Dissecting the Attack Flow for Healthcare

Attack Flow Overview

While the specifics and details of every breach and compromise may vary, there is typically a specific attack flow that occurs from the initial security bypass to escalation, compromise, followed by persistent home on your network and exfiltration and/or destruction of valuable data. The following analysis presents an overview of the attack flow specific to the healthcare sector, incorporating insights from the Trustwave SpiderLabs team and offering actionable mitigations for organizations to implement.

At each stage of the attack flow, the recommended mitigations provide proactive guidance to minimize the potential risks of financial, reputational, regulatory, or physical impacts to a healthcare organization. The typical sequence of events unfolds as follows:



Attack Flow Steps

Initial Foothold

This is the step where the attacker successfully triggers a security bypass that will give them the ability to expand their access to suit their motives and goals. This initial foothold can take various forms, ranging from successful phishing attacks to vulnerability exploitation or even logging into public-facing systems using previously acquired credentials.

In this section, we will explore the most common methods through which attackers gain this initial foothold in healthcare organizations, like phishing, logging in, vulnerability exploitation, and the supply chain.

Initial Payload

Once the attackers have established a foothold on the network, they will proceed to download more sophisticated tools and malware.

In this section, we will specifically concentrate on real-world examples of the types of payloads that frequently target the healthcare sector.

Expansion / Pivoting

The initial foothold typically involves a low-value workstation, such as a phishing victim's laptop, or a network appliance like a VPN endpoint.

In this section, we will showcase how once armed with the necessary tools, attackers can target higher-value accounts and systems, such as Domain Admins, root accounts, Active Directory Systems, and Database servers.

Malware

There are a variety of malware types with a myriad of uses. We’re talking about Remote Access Toolkits (RATs), Infostealers, Ransomware, and many others.

In this section, we will focus on the types of malware that are prevalent in the healthcare Industry.

Exfiltration / Post Compromise

In most cases, the primary motive behind compromises is data theft.

In this section, we will explore the types of data that are targeted and exfiltrated in healthcare-related compromises. Additionally, we will present real-world examples of healthcare data breaches to provide concrete illustrations.

In this section, we will examine many of the most prevalent threat tactics and threat actors operating across healthcare and throughout the attack chain, including:

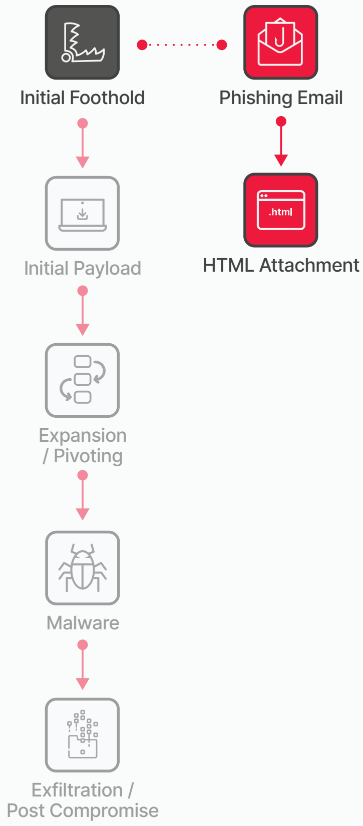
THREAT ACTORS

- LockBit 3.0
- ALPHV/BlackCat
- Clop
- DMA Locker
- Royal
- Babuk
- Magniber
- Royal
- Black Basta
- RansomHouse

THREAT TACTICS

- Phishing/BEC
- Vulnerability Exploitation
- Logging In with Valid Credentials (Unsecured, Default, Low Complexity, or Purchased)
- Existing Tools (Powershell, LOLBins)
- Webshells and Stolen Sessions
- Malware (Infostealers, RATs, Ransomware)
- DDoS

For additional information about the most prevalent threat actors, please go to the Appendix.



Initial Foothold: Phishing and Business Email Compromise (BEC)

The Threat

Phishing stands out as the most commonly exploited method for gaining an initial foothold in an organization. Instead of attempting to exploit the software or systems on the network, attackers direct their focus towards targeting the individuals operating the keyboard.

Using a persuasive and time-sensitive email, the attacker successfully convinces their victim to take specific actions, such as opening an attachment, clicking on an embedded URL, or following instructions to transfer funds to a purported "stranded CEO."

TYPICAL PHISHING GOALS:

- **Credential theft: example:** Invoice from a customer includes a link. When the link is clicked it prompts the user for their password before “access is granted to the document”
- **Malware insertion:** via Powershell scripts, Javascript, Macros
- **Triggering some action:** e.g., wire transfer for “stranded CEO” (BEC)

Trustwave SpiderLabs Insights

Our Trustwave SpiderLabs team is dedicated to monitoring email-based threats including opportunistic phishing, targeted/spear-phishing, and Business Email Compromise (BEC). Over the last year our team flagged both Emotet and Qakbot as the most common trend amongst phishing attacks targeting healthcare organizations. These have employed a number of different delivery methods during the last year, including:

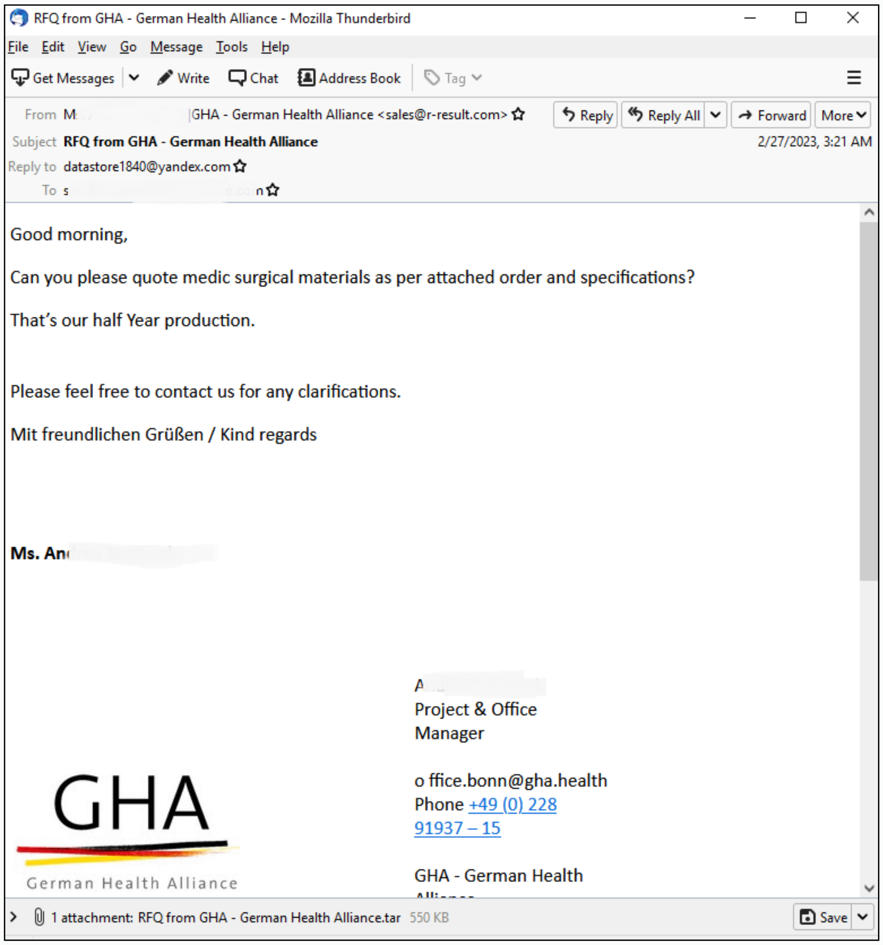
NOVEL PHISHING ATTACHMENT TYPES:

- Document files with macros
- OneNote Attachments with embedded links (Trustwave SpiderLabs research here and here)
- HTML attachments, which deliver or redirect to credential phishing sites, or employ HTML smuggling to hide malware (Trustwave SpiderLabs research here and here)
- PDFs with embedded URL links

These emails are crafted to convince the recipient to perform an action, like clicking on a malicious link or opening a malicious attachment. A common lure in phishing emails is the impersonation of a ‘Request for Quote.’ Below are some of the more common 'Subjects' our Email Security team found targeting healthcare entities in the last 3 months:

- ENQUIRY MEDICAL DEVICES SUPPLIES
- REQUEST FOR MEDICAL EQUIPMENT SUPPLIES
- Purchase Order List of PO for Medical Supplies and Equipment
- March 2023 Medical Equipment Order
- Inquiry Order | Required Quotation For Medical Supplies

Below is an example of a health-related RFQ phishing email below. It purports to be from the German Health Alliance. The attachment was an archive that contained an executable known as Guloader, a loader used as an initial payload.



From M[redacted]GHA - German Health Alliance <sales@r-result.com>

Subject **RFQ from GHA - German Health Alliance**

2/27/2023, 3:21 AM

Reply to datastore1840@yandex.com

To s[redacted]n

Good morning,

Can you please quote medic surgical materials as per attached order and specifications?

That’s our half Year production.

Please feel free to contact us for any clarifications.

Mit freundlichen Grüßen / Kind regards

Ms. An[redacted]

A[redacted]
Project & Office
Manager

o ffice.bonn@gha.health
Phone +49 (0) 228
91937 – 15

GHA - German Health
Alliance

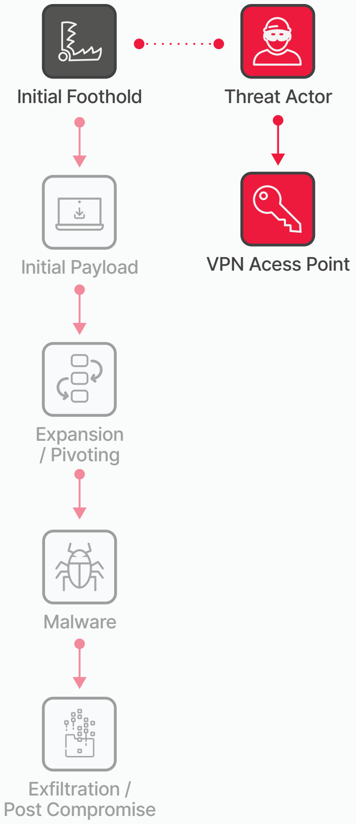
1 attachment: RFQ from GHA - German Health Alliance.tar 550 KB

Additionally, Trustwave SpiderLabs has been monitoring the effect of AI and LLMs like ChatGPT on phishing attacks. Many of the red flags that we teach users to identify phishing emails include items like picking out misspellings, grammar mistakes, and general clumsiness of writing that may indicate that the author is not a native speaker.

The quick maturity and expanded use of LLM technology is making the crafting these emails even easier, more compelling, highly personalized, and harder to detect. Trustwave SpiderLabs has detected multiple spearphishing attacks with malicious attachments or links being used against healthcare entities. Creating these targeting, compelling spearphishing emails will likely be made easier for attackers with LLM technology.

Mitigations to Reduce Risk

- Consistently conduct mock phishing tests to assess the effectiveness of anti-phishing training and retrain repeat offenders.
- Implement robust anti-spoofing measures, including deploying technologies on email gateways.
- Deploy layered email scanning with a solution like MailMarshal to provide better detection and protection. Trustwave's email security MailMarshal provides 99% malware and exploit capture rate and <0.001% spam false positives.
- Utilize techniques to detect domain misspellings, enabling the identification of phishing and BEC attacks.



Initial Foothold: Logging in

The Threat

Sometimes attackers gain access to your network simply by logging in. This could occur if the default credentials for a device have not been changed, if weak passwords are used and vulnerable to brute-forcing, or if credentials have been purchased from an underground forum. Beyond simple credentials, attackers can purchase access to a webshell or active sessions already in place in a target organization.

Trustwave SpiderLabs Insights

The Trustwave SpiderLabs team performs proactive threat hunts in our client's environment to identify breaches or compromises that have yet to be identified. In the course of these engagements, the team regularly finds the following issues that directly contribute to this threat.

VALID ACCOUNTS

The team commonly finds administrative accounts with passwords older than one year. The longer a password goes unchanged, the higher the likelihood that those credentials could be leaked, compromised, or brute-forced. During hunts for our healthcare clients, 30% of findings were related to valid accounts.

UNSECURED CREDENTIALS

Making up 22% of findings in a hunt, unsecured credentials make the attacker's job an easy one. Trustwave SpiderLabs often comes across unsecured plaintext files containing credentials, as well as scripts or custom applications passing credentials in cleartext in environments. If a malicious actor is able to sniff the password from these applications or gain access to unsecured files, they will have additional access.

Sometimes all an attacker needs to do is purchase credentials directly via underground forums and the Dark Web. Our Trustwave SpiderLabs team performs on-going monitoring of these shadowy areas of the Internet.

WEBSHELLS

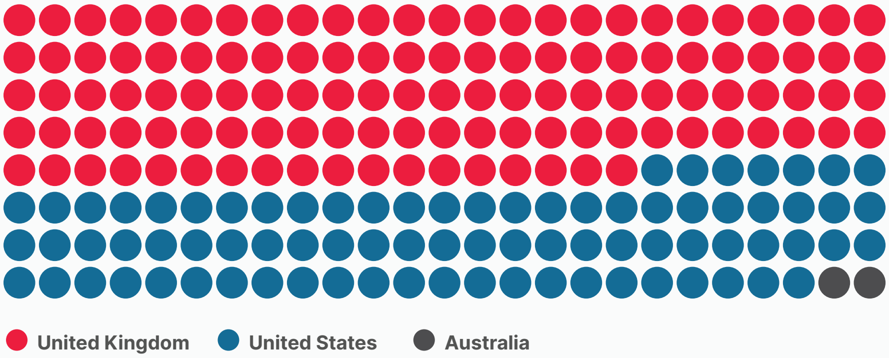
One consistent service offering is the sale of webshells. These webshells are typically inserted into compromised webservers to provide persistent access. In a recent search, our team found an instance when the actor was selling a webshell to a private pharmaceutical company in the US, at a blitz price of $160 on underground forums on the Dark Web. The advertisement claims the webshell will allow access to the Active Directory of the organization with Local Admin privileges.

Another advertisement from the same source affords access to a Korean drugstore chain, with revenue of around $1 billion a year. This access with workgroup admin rights in Active Directory will cost a malicious actor $500.

INFOSTEALERS

As the name suggests, infostealers focus on that exact activity as its primary function. The stolen information is then typically offered up for sale.

The RussianMarket forum is a popular underground marketplace. Our team analyzed posts offering the sale of Infostealer logs that were specific to domain names associated with healthcare organizations. From January 2022 to May 2023, we found close to 20,000 ads offering these types of logs. These included over 10,000 logs claiming to be from UK healthcare orgs, about 8000 from the USA, and nearly 200 from Australia.

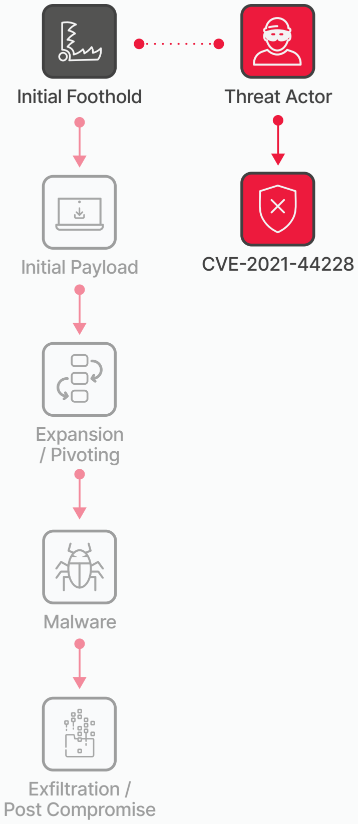


The Trustwave SpiderLabs team provides detection logic for our Trustwave Managed Services team and monitors incidents generated there. The team found the most common form of Credentialed Access relied almost exclusively on password brute force attacks. When a password like “Password123!” passes your company’s password policy, you can be sure that bad actors will capitalize on that weakness.

Finally, we unfortunately see that default credentials often go unchanged. This could be due to a multitude of reasons, but often it is simply overlooked. Default credential libraries are as easy to look up as a Google search.

Mitigations to Reduce Risk

- Regularly rotate passwords (e.g., every quarter) to mitigate issues related to valid accounts.
- Implement password complexity requirements to enhance security.
- Enable multi-factor authentication (MFA) to provide an additional layer of protection for accounts.
- Securely store credentials in programs like KeePass to prevent credential abuse.
- Encrypt credentials when used in scripts to safeguard sensitive information.
- Audit local administrative accounts regularly and obfuscate admin accounts by not using admin in the name.
- Use LAPS on Windows systems to manage local accounts.
- Implement Privileged Access Management (PAM) and Privileged Identity Management (PIM) solutions to deepen defense-in-depth strategy.



Initial Foothold: Vulnerability Exploitation

The Threat

When it comes to information security, vulnerability exploitation is often the first concept that comes to mind. This topic encompasses discussions on Zero Days, Patch Agility, Proof-of-Concept exploits, and Vulnerability Disclosure.

To put it simply, a vulnerability refers to a bug in software that introduces security risks. Attackers develop specialized software or scripts to exploit the vulnerability and circumvent security controls, such as authorization, authentication, and audit controls. Once the vulnerability is exploited, the attacker takes advantage of the ability to bypass a security control and introduce a payload, which can manifest as various types of malware, as we will explore later.

A software **patch** provided by the vendor resolves the bug responsible for the vulnerability and prevents exploitation.

Trustwave SpiderLabs Insights

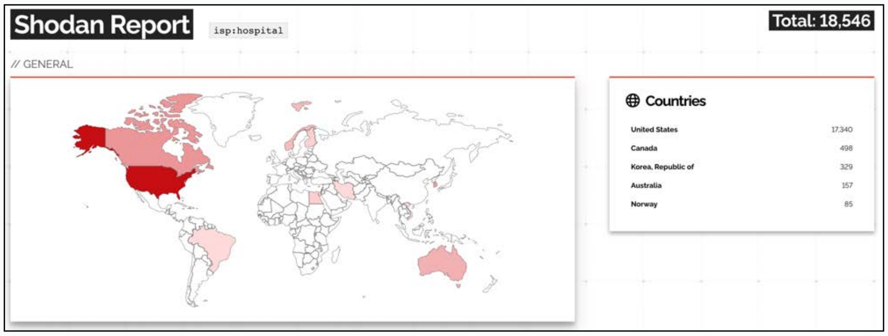
Through active monitoring of our Trustwave Managed Services clients, Trustwave SpiderLabs identified the most common exploits targeting our clients in the healthcare industry.

- Apache Log4J (CVE-2021-44228)
- Spring Core RCE (CVE-2022-22965)
- HTSearch (CVE-2000-0208)
- Jive Openfire (CVE-2008-6508)
- HTTP Directory Traversal
- HTTP SQL injection

Trustwave SpiderLabs conducts hundreds of penetration tests and Digital Forensics and Incident Response (DFIR) engagements every year and has found that the vulnerability of healthcare organizations is expanded due to other factors unique to the industry:

- Custom applications designed for healthcare organizations often lack adequate security testing and code auditing, leading to undiscovered vulnerabilities.
- The healthcare industry typically has a higher number of connected physical devices, such as heart monitors and imaging hardware, which often prioritize functionality over software security.
- Healthcare organizations are often hesitant to implement changes quickly due to concerns about compliance with oversight agencies and compatibility issues with existing software and hardware.
- The focus on patient safety and avoiding unexpected disruptions, like system crashes, leads healthcare organizations to be more cautious about adopting software patches or making changes that could jeopardize patient care.

Additionally, a recent Trustwave SpiderLabs search of Shodan, which scans all public IP addresses on the internet, turned up about 20,000 hospitals and clinics with open ports, service banners and/or application fingerprinting. Most of the ports open on those hosts were very common; TCP ports like 443 (https) and 80 (http) were the two most common, but other open ports gave us pause. For instance, TCP/161 was in the top five open ports across those 20,000 hosts. TCP/161 is used for SNMP, which is often abused to gather more information about the target environment or to take over the SNMP software and use it to further their access to the network.



Shodan Report `isp:hospital` Total: 18,546

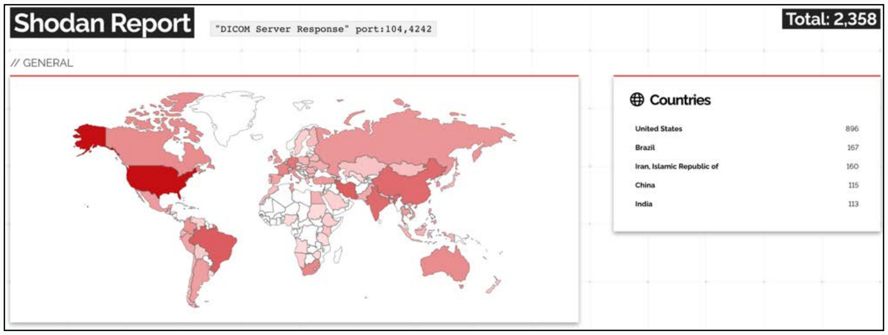
// GENERAL

Countries

United States	17,340
Canada	498
Korea, Republic of	329
Australia	157
Norway	85

Hospital systems on Shodan

Another common service we saw exposed publicly are DICOM servers. DICOM is a standard for medical imaging, X-rays, CT scans, MRI scans, etc. Having any such device accessible from the Internet will potentially give access to private medical information.



Shodan Report `"DICOM Server Response" port:104,4242` Total: 2,358

// GENERAL

Countries

United States	896
Brazil	167
Iran, Islamic Republic of	160
China	115
India	113

DICOM servers on Shodan

Trustwave SpiderLabs found slightly over 2,300 publicly exposed DICOM servers. Additionally, we uncovered over 34,000 ACR/NEMA DICOM honeypots based in China.

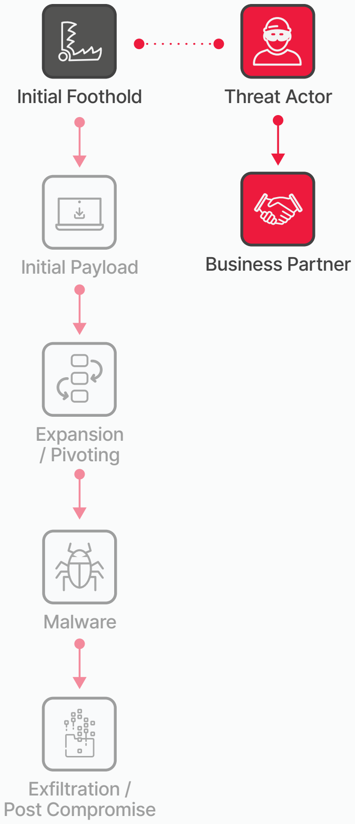
Finally, some of the services exposed on those public ports were vulnerable to a variety of exploits. That includes the following Remote Code Execution vulnerabilities:

- HTTP.sys Cloud RCE (CVE-2015-1635)
- EternalDarkness Microsoft SMBv3 RCE (CVE-2020-0796)
- Microsoft Exchange RCE (Proxyshell) (CVE-2021-31206)

These unpatched vulnerabilities range from 2-8 years old.

Mitigations to Reduce Risk

- Utilize vulnerability assessments and penetration testing to identify vulnerable servers. Pay close attention to systems that store PHI like DICOM systems.
- Databases that store patient PHI should be a priority for system and software patching. Database auditing tools like Trustwave's DbProtect Pro that can flag misconfiguration and user rights can also help eliminate risk.
- Place all servers behind the firewall and practice proper network segmentation for enhanced access control.
- Strengthen access controls to minimum necessary levels for authorized users.
- Promptly patch critical vulnerable systems.
- Recognize the significance of patching in the healthcare sector, where it can be challenging due to reliance on legacy systems.



Initial Foothold: Supply Chain

The Threat

Supply chain attacks are increasingly prevalent. Instead of directly targeting multiple large entities, attackers concentrate their efforts on trusted third-party partners frequently utilized by these entities. This strategy is sometimes referred to as "the Domino Risk," as the attackers aim to topple one domino, causing a chain reaction that affects numerous others.

The return on investment for this type of attack appears to be substantial, considering its current popularity and the alarming compromise incidents we often encounter in headlines.

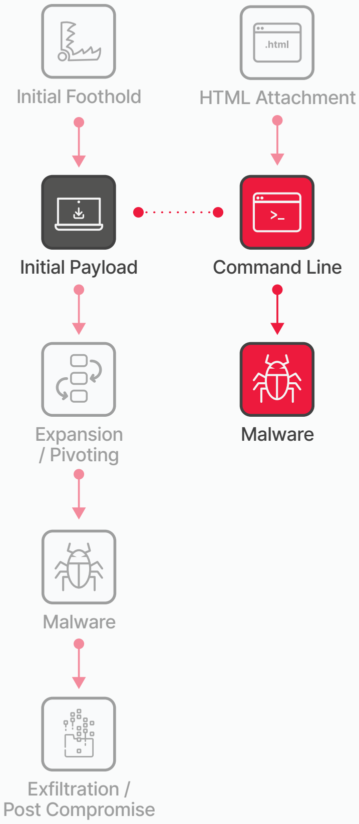
Trustwave SpiderLabs Insights

The healthcare industry, like many others, relies heavily on third-party vendors such as cloud-based web hosting and service or software providers. Cybercriminals commonly prefer to attack these third parties in a sort of flanking maneuver—if the attack succeeds, they gain access to the targeted company’s data. These third parties pose a grave risk to healthcare organizations because most don’t have proper cybersecurity plans or data breach protection.

Recent supply chain headlines, like SolarWinds and 3CX, underscore the exposure that third-party vendors can expose healthcare organizations to. Because of healthcare entities’ classification as critical infrastructure, they are an attractive target for threat actors who aim to exploit their widespread access to compromise multiple entities across various sectors and industries.

Mitigations to Reduce Risk

- Prioritize the security and protection of your systems and those of third-party partners.
- Implement the latest security measures to ensure the safety of the healthcare ecosystem.
- Recognize that the security of the ecosystem is dependent on the strength of its weakest link.



Initial Payload

The Threat

Once a foothold is established, the attacker generally does not anticipate having complete control over the entire network. Often, they have gained access to a low-value system with limited network privileges. They will proceed to download more sophisticated tools and malware to enhance their foothold or leverage existing tools such as PowerShell or LOLBins (Living-off-the-Land Binaries).

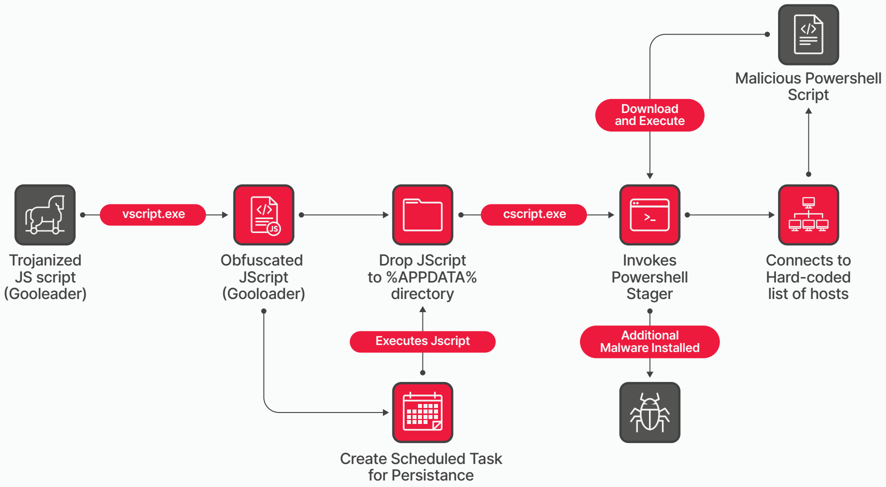
Trustwave SpiderLabs Insights

Between April 2022 and March 2023, Trustwave SpiderLabs has found 85% of initial execution by threat actors is malware that has been downloaded, versus 15%, which utilized Powershell. The use of PowerShell in attacks is a common technique due to its prevalence in Windows environments and its ability to bypass traditional security measures. Attackers can use PowerShell to execute commands and scripts on compromised systems, as well as to download and run malicious payloads.

If not utilizing local utilities already installed on the victim's system (like Powershell), the type of malware that is initially downloaded is typically called a "Loader" since its primary purpose is to load additional malware.

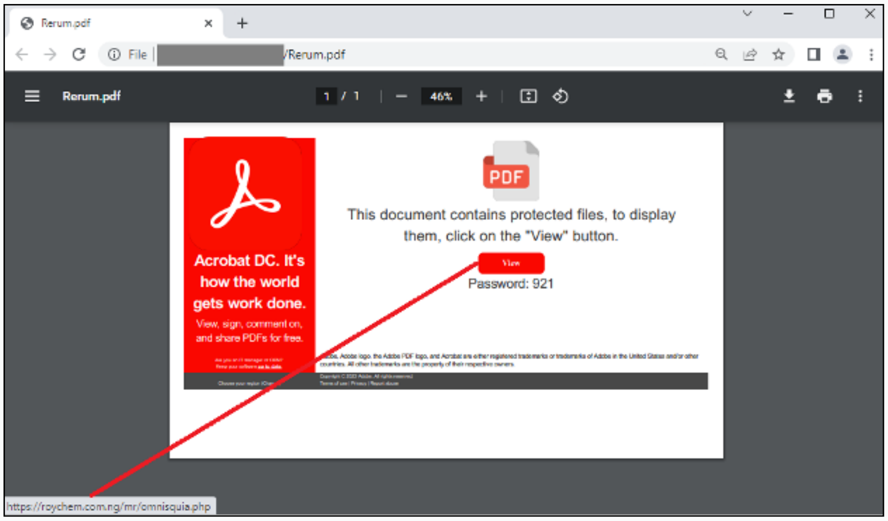
Across these Loaders, the most prevalent seen by our Malware Analysis team is Gootkit, a JavaScript loader typically downloaded by victims via SEO poisoning. This JavaScript kicks off the infection chain, using Powershell scripts. Trustwave SpiderLabs has observed samples abusing VLC Media player to perform DLL sideloading to execute a malicious file, leading to deploying of a Cobalt Strike beacon.

GOOTKIT DELIVERY CHAIN


Malicious Powershell Script
Download and Execute
Trojanized JS script (Gooleader)
vscript.exe
Obfuscated JScript (Gooloader)
Drop JScript to %APPDATA% directory
cscript.exe
Invokes Powershell Stager
Connects to Hard-coded list of hosts
Executes Jscript
Additional Malware Installed
Create Scheduled Task for Persistance

Our Trustwave SpiderLabs team confirms this in their threat hunting engagements. Additionally, they note that due to the many custom applications that are utilized within the healthcare industry, it can be difficult to spot malware without a proper inventory of approved applications, services, and scripts.

Two other Loaders we see quite often are Emotet and Qakbot. In 2022, Qakbot was used by affiliates deploying Black Basta ransomware. According to HHS, the Black Basta group, first observed in April 2022, targeted several health and public health sector organizations in the US and stole personal identifiable information (PII) of members, customers and employees.



Acrobat DC. It's how the world gets work done.

View, sign, comment on, and share PDFs for free.

This document contains protected files, to display them, click on the "View" button.

Password: 921

Adobe, Adobe logo, the Adobe PDF logo, and Acrobat are either registered trademarks or trademarks of Adobe in the United States and/or other countries. All other trademarks are the property of their respective owners.

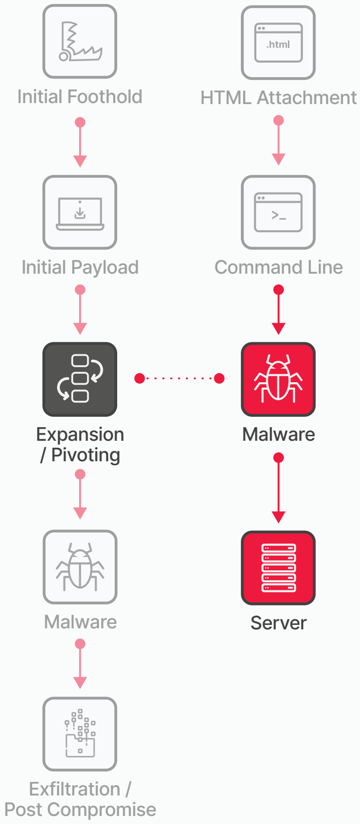
https://roychem.com.ng/mr/omnisquia.php

PDF with embedded URL link leading to Qakbot malware download

Also in 2022, Emotet was a prominent cyberthreat targeting healthcare, according to Health Sector Cybersecurity Coordination Council (HC3). In that year, HC3 also mentioned that trojans accounted for almost 80% of malware found on computer systems in healthcare, with Emotet being the most prevalent.

Mitigations to Reduce Risk

- Conduct regular audits of all applications operating within the environment.
- Implement highly granular whitelisting of applications on specific hosts to minimize exposure.
- Prevent malicious actors from deploying applications that masquerade as known apps to execute malicious commands.
- One of the best ways to identify malicious actions is through the commands that are being run.
- Apply additional privilege restrictions to prevent unprivileged sources from running different shells.



Expansion / Pivoting

The Threat

Since the initial foothold typically occurs on a low-value workstation, such as the laptop of a phishing victim, or a network appliance like a VPN endpoint, the attacker now is going to target higher-value accounts and systems with the appropriate tools at their disposal. These can include Domain Admins, Root Accounts, Active Directory Systems, and Database servers.

Trustwave SpiderLabs Insights

From that initial foothold, often on an employee or contractor's workstation (phishing), an internal IP address (remote access like RDP or VPN), or software implanted from a compromised third party (SolarWinds, 3CX), the goal now is privilege escalation and expansion. Because an attacker is behind an organization's perimeter, things become a bit easier. This step is often referred to as "pivoting" or "lateral movement."

The techniques used in this stage echo those used in the Initial Foothold steps, with the benefit of having at least low-level access and authorization. Infostealers are often used at this point to grab organization credentials from this internal perch.

Credential grabbing also tends to be easier from this perch. Security tends to fall off internally. Often this is due to an "it's behind the firewall" mentality of prioritizing security controls. We used to refer to this as "crab security," a hard shell with a soft interior.

It is also during this stage when the attacker will try to establish persistence in the network so they can share access with others on their team or come back at a future time to continue the attack.

SCHEDULED TASK/JOB

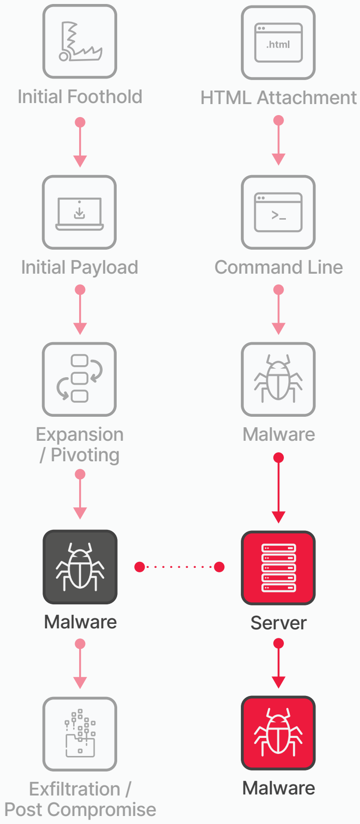
One of the best tools adversaries use to maintain persistence is to set up scheduled tasks to continuously execute malicious code on a regular basis. This is a scenario that the Threat Hunt team has observed in many cases.

Trustwave® SpiderLabs®

Trustwave SpiderLabs conducts 100K hours of pentesting each year

Mitigations to Reduce Risk

- Conduct regular audits of all applications in the environment to combat adoption of custom applications that could result in vulnerabilities.
- Implement a highly detailed whitelist of applications on designated hosts to minimize exposure, which will prevent malicious actors from introducing applications disguised as legitimate ones and executing harmful commands.
- Impose additional restrictions on privileges to prevent unauthorized execution of different shells from unprivileged sources.



Malware: Infostealers

The Threat

As the name may suggest, Infostealers are specialized malware designed with the primary function of stealing information. While various types of malware, such as Remote Access Trojans (RATs) and certain ransomware families, may possess this capability, Infostealers specifically focus on this function, often targeting specific types of data for theft. Infostealers primarily seek data both at rest and in transit.

In-place Infostealers primarily target local data stored on compromised storage devices, aiming to exfiltrate information such as contacts, cached passwords, cryptocurrency wallets, and system details (e.g., operating system, patch level, installed software).

In-transit Infostealers, on the other hand, are focused on stealing data that users enter but is not stored as a file on the system. These Infostealers usually manifest as malicious web browser plug-ins that act as proxy servers for specific connections. For example, they may monitor connections to your bank's website and manipulate the connection to steal your account information or perform unauthorized actions, such as initiating a wire transfer, by utilizing your access.

Trustwave SpiderLabs Insights

Trustwave SpiderLabs and threat operations teams have insights into potential Infostealers in our clients' environments obtained through delivery of our managed services, threat hunts, DFIR, and malware analysis teams across clients worldwide.

The two Infostealers we have spotted most often in the healthcare sector over the last six months are Redline Stealer and Racoon Stealer.

REDLINE STEALER

Redline is a .Net compiled executable that can check a range of system information such as OS version, running processes and installed programs. It can harvest credentials from browsers, target cryptocurrency wallets, and steal credentials from a range of programs, for example NordVPN and FileZilla.

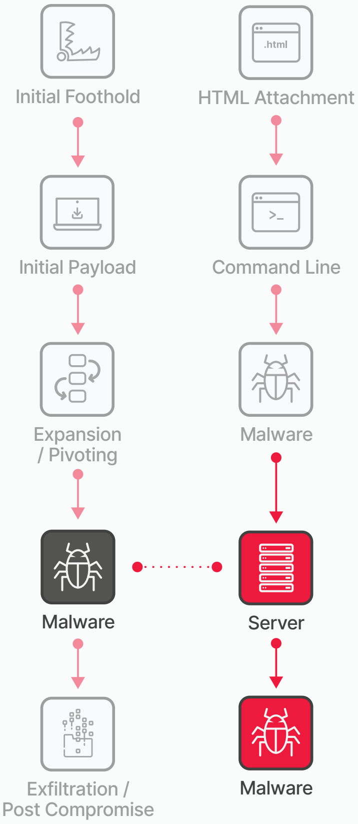
Trustwave SpiderLabs published an analysis of Redline Stealer in conjunction with an analysis of the Lapsu$ hacker group in 2022.

RACCOON STEALER

Raccoon Infostealer was originally sold as a Malware-as-a-Service (MaaS) model, until the main developer was arrested in March 2022. However, it didn't take long for new actors to rebuild Racoon from the ground up and re-release it in June of that year. The new version uses C/C++ and includes new features throughout the infrastructure including the types of data available for theft. Raccoon Stealer can access browser credentials, stored credit cards, cryptocurrency wallets, email data, and various other types of sensitive data from numerous applications.

Mitigations to Reduce Risk

- Use host-based anti-malware tools that can assist in identifying and quarantining specific malware, but understand they have limitations and are often circumvented by custom malware packages.
- If prevention of infection is not possible, audit controls become crucial indicators of potential compromise. This involves enabling system logs on valuable systems and workstations, as well as implementing network logging through flows, Network Monitoring Solutions, or IDS devices on ingress and egress channels.
- Implement active monitoring. Merely enabling logs is insufficient; if logs are not monitored, they lose their effectiveness. Regular monitoring helps establish a baseline of regular activity, making abnormal behavior or traffic more conspicuous.
- Establish and regularly practice a formal Incident Response process.
- Perform ongoing Underground and Dark Web monitoring for information leakage that may have been missed.



Malware: RATs

The Threat

A Remote Access Trojan (RAT) is malware whose primary function is to provide an administrative level backdoor to a compromised system. A RAT typically has a wide variety of additional features that allow the attacker to:

- Download any files from the system
- Capture sensitive data similar to Infostealers
- Take screenshots
- Execute any binary on the system
- Upload and execute additional malware to the system
- Activate the webcam and/or microphone
- Sniff network traffic

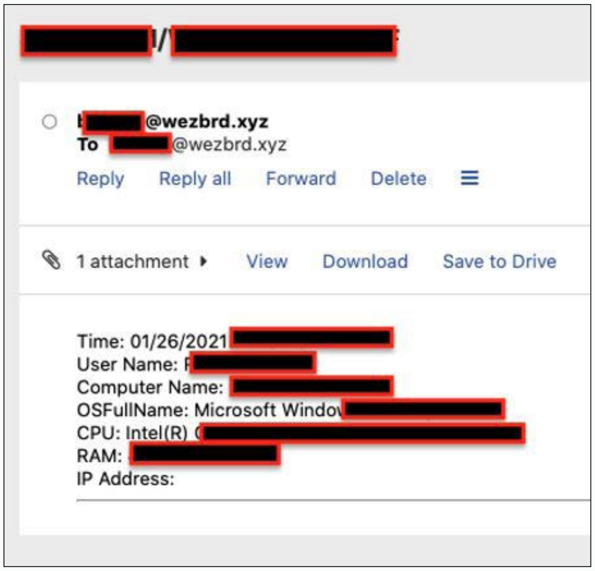
Trustwave SpiderLabs Insights

We've witnessed two major RATs targeting the healthcare industry:

AGENT TESLA

Agent Tesla is a RAT most commonly deployed via phishing emails with archive or disc image attachments. Agent Tesla has the capability to steal a variety of data, making it quite popular. It includes a keystroke logger, the ability to access anything on the clipboard, and can search the hard drive for any other valuable data. It also has a very flexible command and control channel and can connect up to the C2 via HTTP, HTTPS, Email, or in a Telegram channel.

Trustwave SpiderLabs encounters Agent Tesla quite often, typically attached to phishing campaigns.


[redacted]/[redacted]

[redacted]@wezbrd.xyz
To [redacted]@wezbrd.xyz

Time: 01/26/2021 [redacted]
User Name: [redacted]
Computer Name: [redacted]
OSFullName: Microsoft Windo[redacted]
CPU: Intel(R) [redacted]
RAM: [redacted]
IP Address:

Email showing system data exfiltrated from an Agent Tesla infection and sent back to the C2

ASYNC RAT

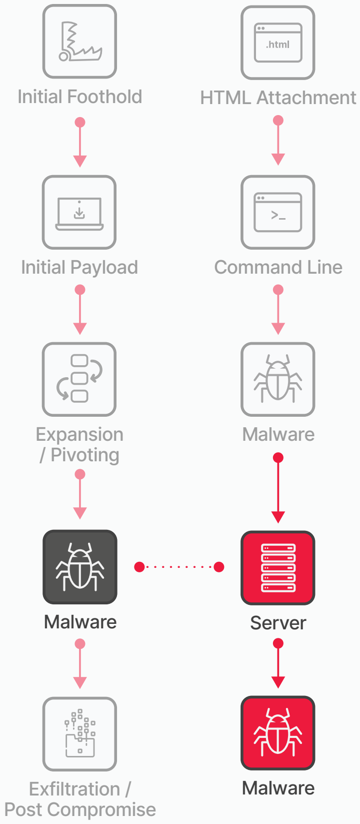
The Async RAT is another common RAT. One reason for its popularity is that it is free and open source. The RAT is typically deployed via phishing emails and uses a chain of .BAT, .PS1, and .VBS files to evade detection. It has a lot of common options like:

- View and record the victim's screen
- Log all keystrokes
- Chat mechanism with the victim
- Disable Windows Defender
- Access to upload, download, and delete files

Trustwave MDR Elite offers an MTTA of 15 minutes and MTTR of >30 minutes

Mitigations to Reduce Risk

- Use host-based anti-malware tools that can assist in identifying and quarantining specific malware, but understand they have limitations and are often circumvented by custom malware packages.
- If prevention of infection is not possible, audit controls become crucial indicators of potential compromise. This involves enabling system logs on valuable systems and workstations, as well as implementing network logging through flows, Network Monitoring Solutions, or IDS devices on ingress and egress channels.
- Implement active monitoring. Merely enabling logs is insufficient; if logs are not monitored, they lose their effectiveness. Regular monitoring helps establish a baseline of regular activity, making abnormal behavior or traffic more conspicuous.
- Establish and regularly practice a formal Incident Response process.
- Perform ongoing Underground and Dark Web monitoring for information leakage that may have been missed.



Malware: Ransomware

The Threat

Ransomware is a type of malware that typically encrypts or locks data and then demands the victim pay a ransom to provide access to that data again. Modern ransomware campaigns prevent recovery by also attempting to remove access to backup files and deleting Volume Shadow Copies.

More recently, ransomware groups have added an extortion component to these attacks. They will exfiltrate valuable data prior to deploying the ransomware and then publicly post proof of the attack in order to scare/shame the victim organization into paying the ransom. If the ransom isn't paid, the threat actors still have a dataset they can turn around and sell. This is commonly referred to as a double extortion tactic.

Threat actors will go to great lengths to get paid. Triple extortion techniques have also been seen where threat actors will strategically deploy a Distributed Denial of Service (DDOS) attack as a third layered extortion tactic. Worse yet, is when they target the victims of the breach and threaten to release their data if they don't pay, as seen in the Vastaamo data breach, a Finnish psychotherapy provider.

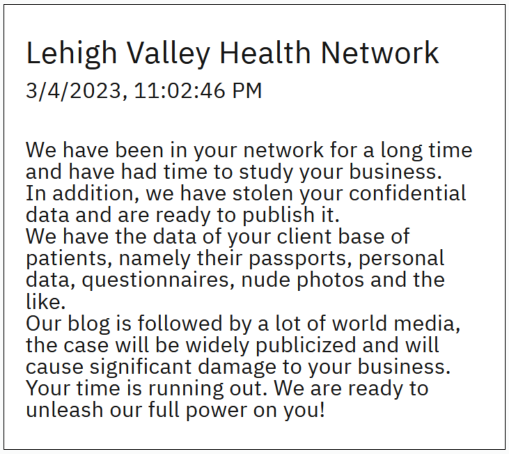
Trustwave SpiderLabs Insights

Trustwave SpiderLabs and threat operations teams continually encounter Ransomware in their recurring engagements. Here is a summary of the ransomware families encountered most often.

BLACKCAT

The BlackCat (aka AlphV) Ransomware group has targeted healthcare organizations directly and unapologetically. This includes attacks on FONASA, Chile's National Health Fund, and NextGen Healthcare, an Atlanta-based third-party health record vendor with over 2,000 healthcare organizations as clients.

BlackCat also compromised the Lehigh Valley Health Network, a Pennsylvania-based healthcare network, and published sensitive photos of female breast cancer patients as part of its extortion campaign.


Lehigh Valley Health Network

3/4/2023, 11:02:46 PM

We have been in your network for a long time and have had time to study your business.
In addition, we have stolen your confidential data and are ready to publish it.
We have the data of your client base of patients, namely their passports, personal data, questionnaires, nude photos and the like.
Our blog is followed by a lot of world media, the case will be widely publicized and will cause significant damage to your business.
Your time is running out. We are ready to unleash our full power on you!

Extortion post from Blackcat

CLOP

The Clop Ransomware group is currently associated with a massive campaign targeting an SQLi zero-day vulnerability in the popular MOVEit file transfer software. This ransomware group has also been known to use valid accounts to infiltrate healthcare organizations. In a recent attack on a large medical diagnostics company, Clop used stolen credentials to gain access to the network and deploy its ransomware.

LOCKBIT

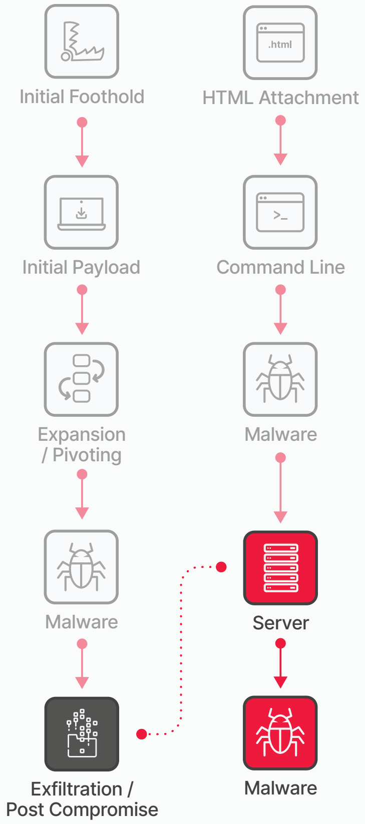
In a recent attack against a US healthcare provider, LockBit ransomware was used to encrypt the organization's data. The attackers reportedly gained access to the network using valid credentials, which were likely obtained through a previous phishing attack. In August 2021, LockBit ransomware targeted a US-based healthcare organization, impacting multiple systems and data. The attack was reportedly initiated through the exploitation of Remote Desktop Protocol (RDP) credentials. The attackers encrypted more than 7 terabytes of data and demanded a ransom of $70 million.

BLACK BASTA

In November 2021, Black Basta ransomware targeted a European hospital, infecting the network through RDP. The attackers demanded a ransom of €700,000 euros in exchange for the decryption key. In another attack on the French healthcare group, Ramsay Santé, Black Basta ransomware terminated various services and processes, including the antivirus software, making it easier for the ransomware to encrypt files undetected.

Mitigations to Reduce Risk

- Use host-based anti-malware tools that can assist in identifying and quarantining specific malware, but understand they have limitations and are often circumvented by custom malware packages.
- If prevention of infection is not possible, audit controls become crucial indicators of potential compromise. This involves enabling system logs on valuable systems and workstations, as well as implementing network logging through flows, Network Monitoring Solutions, or IDS devices on ingress and egress channels.
- Implement active monitoring. Merely enabling logs is insufficient; if logs are not monitored, they lose their effectiveness. Regular monitoring helps establish a baseline of regular activity, making abnormal behavior or traffic more conspicuous.
- Establish and regularly practice a formal Incident Response process.
- Perform ongoing Underground and Dark Web monitoring for information leakage that may have been missed.



Exfiltration / Post Compromise

The Threat

Once attackers have established themselves within a network and systems, they will proceed to execute their final plan. This plan can take various forms depending on their objectives.

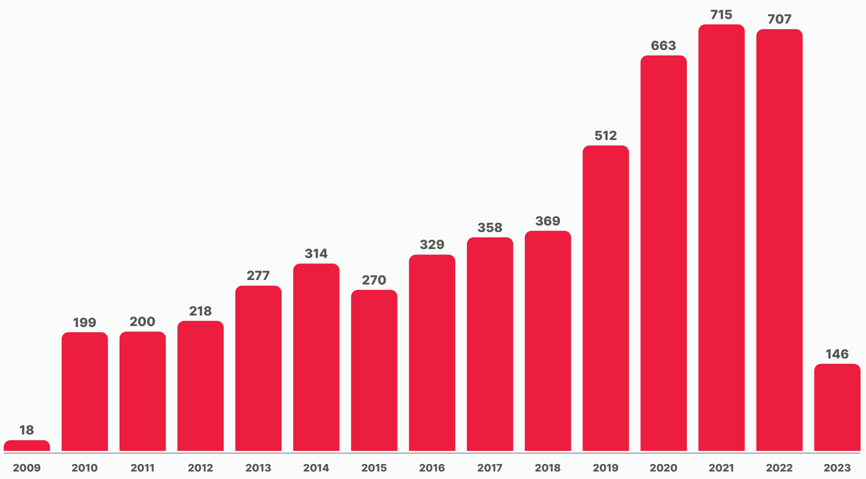
In some cases, attackers may adopt a "smash and grab" strategy, aiming to swiftly gather as much information as possible before making a hasty exit. They will often make efforts to cover their tracks during this process.

On the other hand, certain attackers may have specific targets in mind, such as a particular system, individual, or dataset. In these instances, they will proceed cautiously and meticulously through the network, employing tactics to avoid detection until they achieve their goal.

Other attackers simply aim to cause widespread destruction, prioritizing chaos over theft. They may employ ransomware to render valuable data unusable or resort to deleting and corrupting data as well as backups.

Overall, the number of PHI records breached during a compromise is stunning and is increasing year over year.

HEALTHCARE DATA BREACHES OF 500+ RECORDS (2009 - MARCH 2023)

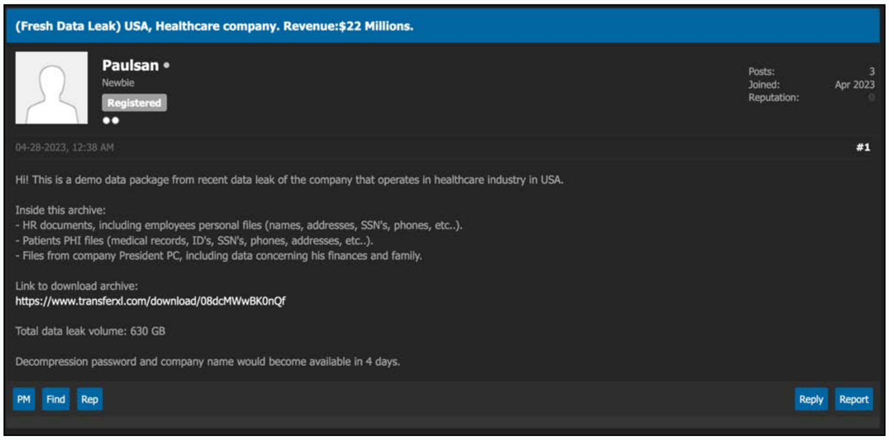


Trustwave SpiderLabs Insights

Stealing PHI is the primary motivating factor for threat actors attacking healthcare systems. The healthcare industry is also considered critical infrastructure and preventing access through ransomware or Distributed Denial of Service (DDoS) attacks have become an additional key motivator to monetizing their attack.

While we have statistics on how much data may have been exposed due to a breach, how much of that data actually ends up exposed either publicly or to a private buyer? Trustwave SpiderLabs continuously monitors a variety of Dark Web forums, open web forums, Twitter accounts, Telegram channels, and more for healthcare-related data.

Here is an example of an advertisement for a PHI data dump from April 2023:



(Fresh Data Leak) USA, Healthcare company. Revenue:$22 Millions.

Paulsan •
Newbie
Registered
●●

Posts: 3
Joined: Apr 2023
Reputation: 0

04-28-2023, 12:38 AM #1

Hi! This is a demo data package from recent data leak of the company that operates in healthcare industry in USA.

Inside this archive:
- HR documents, including employees personal files (names, addresses, SSN's, phones, etc..).
- Patients PHI files (medical records, ID's, SSN's, phones, addresses, etc..).
- Files from company President PC, including data concerning his finances and family.

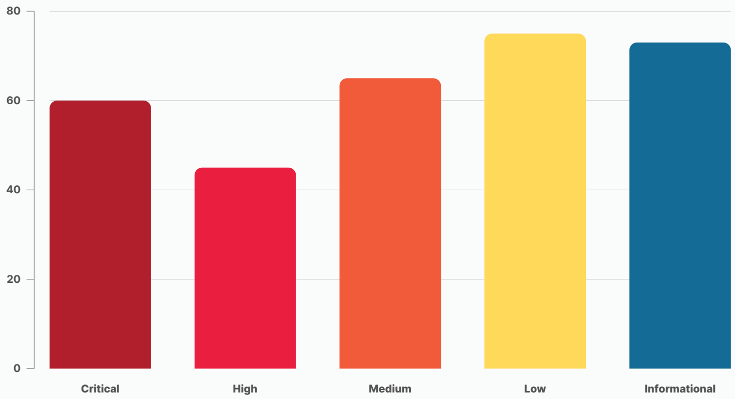
Link to download archive:
https://www.transferxl.com/download/08dcMWwBK0nQf

Total data leak volume: 630 GB

Decompression password and company name would become available in 4 days.

Finally, you hear about agile patching policies, but their importance can't be stressed enough. Through penetration testing, Trustwave SpiderLabs has tracked how long it takes clients to remediate issues reported to them after an assessment. In some cases, critical issues can take two months on average to remediate.

AVERAGE DAYS TO REMEDIATE (BY SEVERITY)



100%

OF TRUSTWAVE'S ADVANCED CONTINUAL THREAT HUNTS RESULT IN THREAT FINDINGS

Mitigations to Reduce Risk

- Monitor the Dark Web on a regular basis for potential compromises.
- Conduct regular penetration tests to proactively identify vulnerabilities and weaknesses in your systems, networks, and applications.
- Decrease the time to remediation to have a significant impact in exposure and reduce the window of exploitation.
- Run continuous Threat Hunting, like Trustwave's Advanced Continual Threat Hunt, through your environments for undetected compromises.
- Formalize and regularly test your Incident Response Policy for the scenarios that will most likely impact you.

Distributed Denial of Service Attacks

The Threat

Distributed Denial of Service (DDoS) attacks belong to a distinct category of attacks. While some attacks aim to compromise and expose data through theft, DDoS attacks specifically target data availability, effectively preventing access for anyone.

Internal compromises typically manifest as the deletion of systems, services, data, or accounts. Externally, DDoS attacks commonly involve overwhelming a public service, such as a web server, with an excessive amount of traffic, thereby rendering the service inaccessible to authorized users.

Trustwave SpiderLabs Insights

Across our healthcare client base, we have seen a variety of DDoS attacks utilizing:

- Samba CVE-2010-1635
- Net-SNMP DoS Vulnerability
- ISC DHCP CVE-2010-2156
- SIP INVITE Method Request Flood

Additionally, we noted resource issues due to Resource Hijacking because of cryptocurrency mining as well as one case of Account Access Removal, where the administrator account was deleted.

KILLNET

Killnet recently launched DDoS attacks on US healthcare systems. From the US Health Sector Cybersecurity Coordination Center

“In the late January 2023 attack, over 90 known orchestrated DDoS attacks took place on healthcare systems (covering multiple hospitals), lone hospitals, and medical centers. Of these, 55% were healthcare systems with at least one hospital and lone hospitals with Level I trauma centers, which provide the most comprehensive and highest level of trauma care to critically ill or injured patients.”

ANONYMOUS SUDAN

Anonymous Sudan claimed ownership of a series of DDoS attacks against Swedish healthcare organizations as a retaliation to the burning of Quran in Sweden. Södersjukhuset (Sos) Hospital and Sahlgrenska University Hospital were among the targets listed.

Mitigations to Reduce Risk

- DDoS attacks are notoriously difficult to prevent.
- Implement a CDN, which will allow you to distribute your content across a network of geographically dispersed servers, reducing the strain on your origin server and increasing its ability to handle high volumes of traffic.
- Deploy an intrusion detection system (IDS) or intrusion prevention system (IPS) capable of monitoring network traffic patterns.

Key Takeaways and Recommendations

Although the healthcare industry isn't alone in facing an elevated threat landscape, the consequences of attacks in this sector can be quite severe and potentially fatal. Attackers are highly motivated by financial gains and continually adapt their methods to outpace defenses.

As demonstrated in our attack cycle, attackers often employ multiple vectors to persistently target healthcare organizations. While the technical aspects of these attacks may change over time, the underlying tactics tend to remain consistent. Traditional methods such as phishing, exploiting known vulnerabilities, and compromising third-party vendors continue to pose significant threats. The emergence of generative AI and LLMs in healthcare introduces new risks, including sophisticated social engineering attacks, unintentional internal data breaches, and vulnerabilities through third-party vendors.

Additionally, ransomware attacks on healthcare organizations have experienced a significant surge, as attackers exploit vulnerabilities and extort ransom payments. As a result, preventative measures remain the most effective defense against all types of cyberattacks. As shared earlier in the previous sections of the attack cycle, the following chart serves as a comprehensive reference for actionable mitigations that can effectively thwart attackers and prevent lasting damage.

Initial Foothold

ACTIONABLE MITIGATION RECOMMENDATIONS:

- ❑ Consistently conduct mock phishing tests, implement robust anti-spoofing measures, deploy layered email scanning, and utilize techniques to detect domain misspellings.
- ❑ Regularly rotate passwords (e.g., every quarter), implement password complexity requirement, securely store and encrypt credentials, and enable multi-factor authentication (MFA).
- ❑ Audit local administrative accounts regularly and obfuscate admin accounts.
- ❑ Implement Privileged Access Management (PAM) and Privileged Identity Management (PIM) solutions.
- ❑ Utilize vulnerability assessments and penetration testing to identify vulnerable servers. Pay close attention to systems that store PHI like DICOM systems.
- ❑ Prioritize databases that store patient PHI for system and software patching.
- ❑ Place all servers behind the firewall, practice proper network segmentation for enhanced access control, and disable Internet access for servers that don't require it
- ❑ Recognize that the security of the ecosystem is dependent on the strength of its weakest link.

Initial Payload & Expansion / Pivoting

ACTIONABLE MITIGATION RECOMMENDATIONS:

- ❑ Conduct regular audits of all applications in the environment to combat the adoption of custom applications that could result in vulnerabilities.
- ❑ Implement a highly detailed whitelist of applications on designated hosts to minimize exposure, which will prevent malicious actors from introducing applications disguised as legitimate ones and executing harmful commands.
- ❑ Impose additional restrictions on privileges to prevent unauthorized execution of different shells from unprivileged sources.

Malware

ACTIONABLE MITIGATION RECOMMENDATIONS:

- ❏ Use host-based anti-malware tools that can assist in identifying and quarantining specific malware, but understand they have limitations and are often circumvented by custom malware packages.
- ❏ If prevention of infection is not possible, audit controls become crucial indicators of potential compromise. This involves enabling system logs on valuable systems and workstations, as well as implementing network logging through flows, Network Monitoring Solutions, or IDS devices on ingress and egress channels.
- ❏ Implement active monitoring. Merely enabling logs is insufficient; if logs are not monitored, they lose their effectiveness. Regular monitoring helps establish a baseline of regular activity, making abnormal behavior or traffic more conspicuous.
- ❏ Establish and regularly practice a formal Incident Response process.
- ❏ Perform ongoing Underground and Dark Web monitoring for information leakage that may have been missed.

Exfiltration / Post Compromise

ACTIONABLE MITIGATION RECOMMENDATIONS:

- ❏ Monitor the Dark Web on a regular basis for potential compromises.
- ❏ Conduct regular penetration tests to proactively identify vulnerabilities and weaknesses in your systems, networks, and applications.
- ❏ Decrease the time to remediation to have a significant impact in exposure and reduce the window of exploitation.
- ❏ Run continuous Threat Hunting, like Trustwave’s Advanced Continual Threat Hunt through your environments for undetected compromises.
- ❏ Formalize and regularly test your Incident Response Policy for the scenarios that will most likely impact you.

Appendix/Reference

Threat Groups

ALPHV/BlackCat

- The group BlackCat/ALPHV first appeared in late 2021. This ransomware group was the fourth most active in the second quarter of 2022 and third most active in the third quarter 2022. Intel471 reported the group was responsible for about 6.5% of the total reported ransomware cases during this period. While the amount is smaller compared to LockBit or Black Basta, newcomer BlackCat has managed to stand out from the crowd. The group developed a search function in July 2022 for indexed stolen data that had not been seen previously. The group claimed this was done to aid other cybercriminals in finding confidential information which can be used to add pressure to victim organizations forcing them to pay the ransom. This idea was quickly copied with LockBit adding its own, lighter version to its toolset.
- ALPHV has also set other trends. According to the FBI, ALPHV was the first group to successfully utilize Rust to ransom a victim, well before Hive made the switch. ALPHV's ability to develop capabilities and functionality that are quickly adopted by other threat actors most likely indicates that its members are most likely ransomware veterans and there are indications the group was linked to the infamous Darkside and BlackMatter gangs.

Babuk

- Babuk is a RaaS malware that has been used since at least 2021 (sharing a significant codebase and artifacts with Vasa Locker). The operators of Babuk employ a "Big Game Hunting" approach to targeting major enterprises and operate a leak site to post stolen data as part of their extortion scheme.
- Babuk lacks a stable internal structure. After claiming retirement following an attack on the Metropolitan Police Department and pressure from U.S. law enforcement, some members of the group splintered off and relaunched as Babuk V2, shifting focus from RaaS to data-theft extortion.
- The cybercriminals behind Babuk employ similar TTPs as other RaaS families. They exploit popular entry vectors, including email phishing with malware loaders, exploiting unpatched vulnerabilities in remote access software, web servers, network edge hardware, and firewalls, and gaining access through weakly protected RDP accounts with credentials obtained from infostealers.

Black Basta

- One of the newest ransomware groups is Black Basta. The group has had alleged ties to other gangs, such as Conti, REvil, and Fin7 (aka Carbanak). These ties come in the form of possible former members/affiliates, in the case of Conti, or custom tools, which are potentially linked to Fin7. With potentially experienced members, the group was able to publish more than 20 organizations to its name-and-shame blog within the first two weeks of the group being identified in April 2022, according to Intel471. Since the initial identification of the group, they have compromised over 90 organizations as of September 2022 with no sign of slowing down.
- The group has had unprecedented success for the short period that they have been active. This success can be linked to a couple of factors. First, Black Basta does not publicly recruit affiliates and most likely only collaborates with actors with whom it has worked with previously. This collaborative methodology is possible because it has been assessed that the Black Basta was formed from members of other successful ransomware groups, so they know other actors. Additionally, the group outsources its capabilities utilizing established tools, such as QakBot and Cobalt Strike, or network access brokers, allowing the group to have a high success rate once inside a victim's environment.

Clop

- Clop is a ransomware family that was first observed in February 2019 and has been used against retail, transportation and logistics, education, manufacturing, engineering, automotive, energy, financial, aerospace, telecommunications, professional and legal services, healthcare, and high tech industries. Clop is a variant of the CryptoMix ransomware.
- In addition to exploiting a previously undisclosed vulnerability (CVE-2023-34362) in MOVEit Transfer, the group has a history of conducting similar campaigns using zero-day exploits, targeting Accellion File Transfer Appliance (FTA) devices in 2020 and 2021, as well as Fortra/Linoma GoAnywhere MFT servers in early 2023.

DMA Locker

- The initial report of DMA Locker occurred in January 2016. This ransomware specifically targets Windows operating systems. Previous iterations were susceptible to decryption because of a program flaw, but the latest updates have effectively addressed this problem. DMA Locker possesses notable capabilities, such as encrypting unmapped network shares and targeting files outside specific folders or lacking specific extensions.
- Among others, the Neutrino exploit kit was discovered to be utilized for the dissemination of malware, in addition to manual deployment by the attackers. DMA Locker was also observed to be combined with banking malware, as well as other ransomware strains such as CryptXXX and Cerber.

LockBit 3.0

- LockBit has continued its reign as the most prominent ransomware group in 2022. For those that don't closely follow these groups, LockBit is and continues to be, the group that dominates the ransomware space. They utilize high payments for recruiting experienced malicious actors, purchasing new exploits, and even run a bug bounty program that offers high-paying bounties - a first for a ransomware group to identity of one of its users. With all these programs and the continued effectiveness of the group, it is forecasted that it will remain the most active and effective group for the foreseeable future.
- As for developments, the group has developed LockBit 3.0, the newest iteration of the ransomware. The updated version, released in June 2022, and includes additional features that can automate permission elevation, disable Windows Defender, a "safe mode" to bypass installed Antivirus, and the ability to encrypt Windows systems with two different ransomware strains to decrease the chance of decryption from a third party. With these new features, the group has been able to conduct successful attacks, accounting for roughly 44% of successful attacks in 2022 according to Infosecurity Magazine.
- On a law enforcement note, a member of the LockBit group was recently arrested in Canada and is awaiting extradition to the United States. A dual Russian and Canadian national has allegedly participated within the LockBit campaign and has been charged with conspiracy to intentionally damage protected computers and to transmit ransom demands. The charges carry a maximum of five years in prison.

Magniber

- The initial detection of the Magniber ransomware took place towards the end of 2017, when it was observed employing the Magnitude Exploit Kit for malvertising attacks specifically targeting users in South Korea. Despite its early identification, the ransomware has remained active and has continuously enhanced its strategies by adopting novel methods of obfuscation and evasion. In April 2022, Magniber gained infamy for masquerading as a Windows update file, enticing victims into unwittingly installing it. Subsequently, it began propagating through JavaScript starting in September 2022.
- In early 2022, Magniber distributed itself through fake installers in APPX and MSI formats. The ransomware was executed using the MSI CustomAction table, which called a malicious DLL within the package. The installer also dropped a malware file called Fodscript, used for privileged escalation. Magniber employed various tactics, including posing as fake installers, Windows updates, and COVID-19-related files to deceive users. Additionally, it utilized malformed digital signatures to bypass execution blocks and exploit vulnerabilities such as CVE-2022-44698.

Royal

- Royal is ransomware that first appeared in early 2022; a version that also targets ESXi servers was later observed in February 2023. Royal employs partial encryption and multiple threads to evade detection and speed encryption. Royal has been used in attacks against multiple industries worldwide--including critical infrastructure.
- Royal operates as a private group, distinguishing themselves from other cybercrime operations by purchasing direct access to corporate networks from underground Initial Access Brokers (IABs). Security researchers have identified similarities in the encryption routines and TTPs used in Royal and Conti attacks and noted a possible connection between their operators (the group suspected of being primarily composed of former members of the Conti ransomware group operates discreetly and in a secretive manner. This group, referred to as Team One, consists of ex-members who have come together to form this new entity).
- Royal has been observed employing various methods to gain initial access to vulnerable systems, often including - callback phishing, SEO poisoning and exploiting exposed RDP accounts. Once they have successfully gained access, the group utilizes a range of tools to facilitate their intrusion operations. These tools include Chisel, a TCP/UDP tunneling software, and AdFind, an Active Directory query tool, among others.