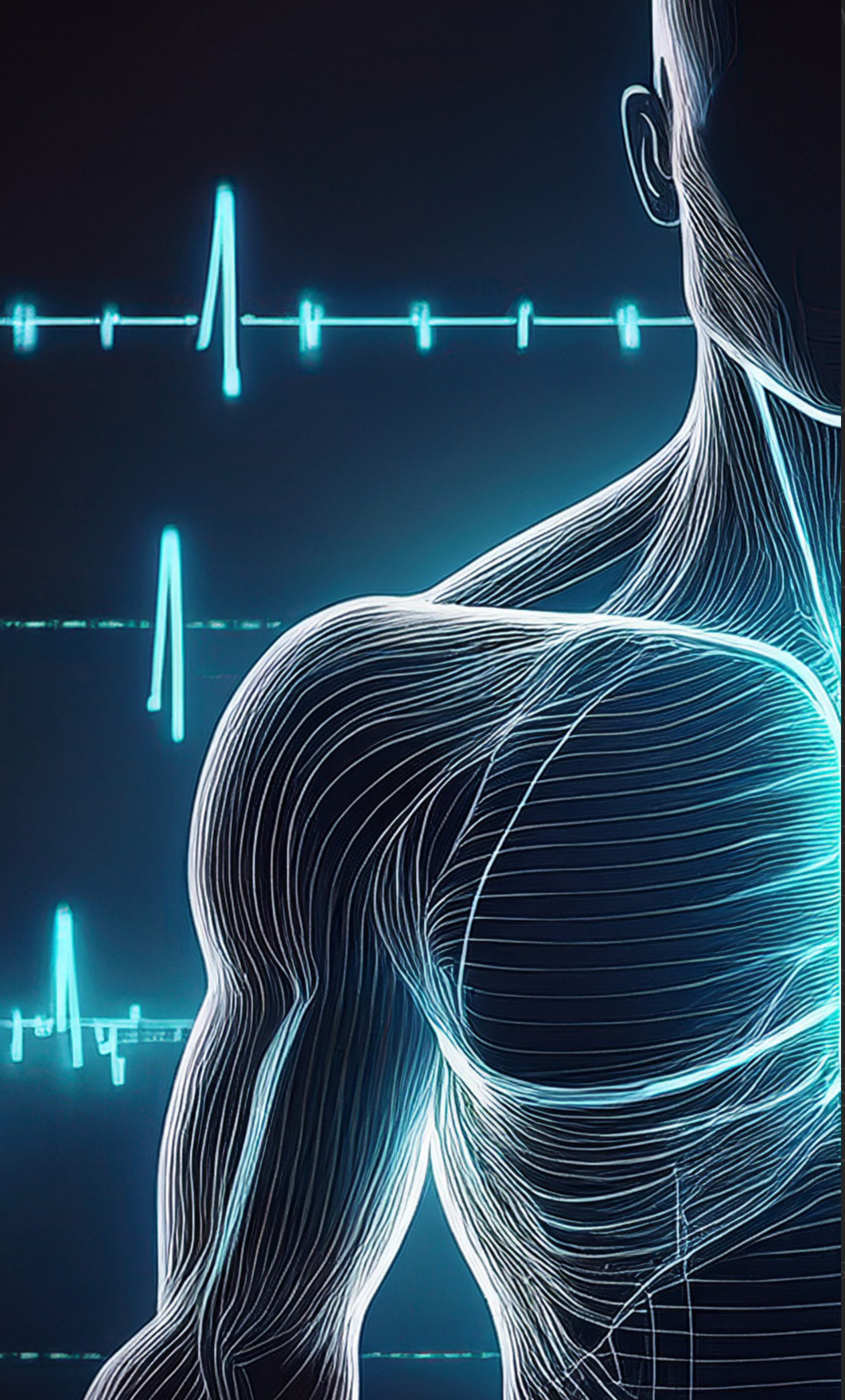


Trustwave SpiderLabs

2025

Trustwave Risk Radar Report

Healthcare Sector

Trustwave®

Contents

The healthcare landscape is undergoing rapid digital transformation, bringing unprecedented advancements in patient care. Yet, this evolution has also ushered in a new era of cybersecurity challenges. Building upon our previous Healthcare Threat Intelligence Briefing, which dissected the attack flows specific to this vital sector, our 2025 report delves deeper into the emergent threats confronting healthcare organizations.

The Trustwave SpiderLabs team has conducted in-depth analysis of emerging cyber adversary tactics, identifying the key trends reshaping the industry's risk profile. We've structured these findings into a comprehensive breakdown of attack stages, providing healthcare organizations with actionable intelligence to strengthen their defensive posture. In addition, Trustwave SpiderLabs has produced two detailed analyses focusing on pressing areas of concern: the rapid rise of ransomware and an examination of common security gaps discovered through a healthcare red team.

The complexities of modern healthcare, with its intricate network of interconnected medical devices, electronic health records (EHRs), and legacy systems, create a fertile ground for cyberattacks. The health records (EHRs), and legacy systems, create a fertile ground for cyberattacks. The expanding adoption of telehealth, Internet of Medical Things (IoMT), and cloud-based solutions has broadened the attack surface, introducing new vulnerabilities that threat actors are adept at exploiting. Beyond the staggering financial implications, with average data breach costs exceeding $9.7 million – which is double the cross-industry average of $4.8 million – the true cost lies in the potential for compromised patient safety.

A cyberattack in healthcare can directly impact human lives. A compromised infusion pump, ventilator, or patient monitoring system can lead to incorrect dosages, system malfunctions, and potentially fatal outcomes. Moreover, the stringent compliance requirements of HIPAA and other regulations underscore the imperative of robust cybersecurity.

Our findings emphasize that cybersecurity in healthcare is not just about protecting data—it's about safeguarding lives. It's a fundamental obligation to ensure that the technologies designed to heal do not become instruments of harm. We aim to equip healthcare professionals with the knowledge and strategies necessary to navigate this complex terrain, ensuring that patient safety, data integrity, and regulatory compliance remain paramount in the face of evolving cyber threats.

Key Report Findings for the Healthcare Sector

45%

of attacks originated from exploiting public-facing applications

9%

of ransomware attacks were conducted by Ransomhub

51%

of ransomware attacks targeted the US

56%

of public-facing applications exploited were against Log4j

21%

of ransomware attacks targeted public health and government healthcare

Healthcare's Unique Threat Landscape

Patient Safety and Data Integrity:

- At the heart of healthcare cybersecurity lies the absolute necessity to safeguard patient safety and data integrity. A breach at a healthcare facility can have immediate, life-threatening consequences. Medical devices, from infusion pumps to ventilators, are now interconnected, creating potential for vulnerabilities that, if exploited, could directly harm patients. Adding to the urgency, healthcare data is exceptionally valuable to threat actors, often fetching high prices on the dark web due to its comprehensive nature.

- The sensitivity of Protected Health Information (PHI) adds another layer of complexity. Breaches not only violate patient trust but also incur severe regulatory penalties under frameworks like HIPAA in the United States, GDPR in Europe, and similar legislation worldwide. The global healthcare community, while diverse in its delivery models, shares this fundamental commitment to patient safety and data protection, making robust cybersecurity a universal imperative.

Complex Compliance and Regulation:

- Healthcare operates within a highly regulated environment, with stringent compliance requirements that vary by jurisdiction. In addition to data privacy laws, healthcare organizations must adhere to industry-specific standards and regulations related to medical device security, data interoperability, and patient consent. For example, the GDPR in Europe requires organizations to report data breaches within 72 hours, with potential fines of up to 4% of annual global turnover. This regulatory landscape is constantly evolving, requiring organizations to maintain agility and vigilance.

- Additionally, the global nature of healthcare, with cross-border collaborations and remote patient monitoring, necessitates a harmonized approach to cybersecurity, balancing national regulations with international best practices. The sheer volume and sensitivity of healthcare regulations places a significant burden on organizations to ensure compliance while maintaining operational efficiency.

Legacy Systems and Cutting-Edge Technology:

- Healthcare grapples with the challenge of integrating legacy systems with modern technologies. Hospitals often rely on outdated EHR systems and medical devices that lack robust security features. However, the rapid adoption of telehealth, IoMT, and cloud-based solutions has expanded the attack surface, creating new vulnerabilities. A typical US hospital has between 10 and 15 medical devices per bed, which means a 1,000-bed hospital could have around 15,000 medical devices.

- The convergence of these disparate systems necessitates a holistic cybersecurity approach that addresses both legacy vulnerabilities and emerging threats. This challenge is compounded by the fact that many healthcare organizations lack the resources and expertise to modernize their infrastructure while maintaining operational continuity.

The Human Element:

- Healthcare is inherently a people-centric industry, making it particularly susceptible to social engineering attacks. Phishing, ransomware, and other forms of cybercrime often target healthcare employees, exploiting their empathy and urgency to gain access to sensitive data or systems.

- The human element is a critical vulnerability that requires ongoing training and awareness programs. Healthcare must prioritize the security awareness of its workforce to mitigate the risk of social engineering attacks.

Global Interconnectedness and Supply Chain Risks:

- The global supply chain for medical devices and pharmaceuticals introduces another layer of complexity. Vulnerabilities in third-party systems or devices can have cascading effects, impacting healthcare organizations worldwide. This interconnectedness necessitates a collaborative approach to cybersecurity, with information sharing and coordinated responses across national borders.
- The global nature of medical research and development also creates a target-rich environment for intellectual property theft and espionage.

Change Healthcare Breach Impact Doubles to 190M People

January 2025, **Dark Reading**

Ransomware Attack Forces 100 Romanian Hospitals to Go Offline

February 2024, **Bleeping Computer**

Trustwave SpiderLabs

With more than 250 cybersecurity experts across the globe, the Trustwave SpiderLabs team puts its resources to task researching the top threats in today's landscape. We are uniquely positioned to do so, as we perform over 200,000 hours of penetration tests and uncover tens of thousands of vulnerabilities annually. We also have a dedicated email security team analyzing millions of phishing URLs validated daily, including 10k per day that are uniquely identified by Trustwave SpiderLabs. Our diverse coverage of infosec disciplines, including Advanced Continuous Threat Hunting, Digital Forensics and Incident Response, Malware Reversal, and Database Security, give us insight into identifying how these breaches occur, as well as mitigations and controls that your organization can put in place to prevent these compromises.

This report examines the myriads of threats facing the healthcare industry. In addition to supplemental reports focused on the rapid rise of ransomware and common security gaps, Trustwave SpiderLabs will offer recommendations to help healthcare organizations mitigate risks and keep their operations undisrupted.

Notable and Prominent Trends in Healthcare

Ransomware Groups Continue to Target Healthcare

The Threat

We explore the rapid rise of ransomware in depth in our accompanying report. At a high level, here are some key points to consider:

Ransomware has emerged as one of the most disruptive and dangerous cyber threats targeting healthcare facilities, with attacks against hospitals, research institutions, medical suppliers, and healthcare educational facilities increasing at an alarming rate.

Cybercriminals infiltrate healthcare networks, encrypt critical systems, and demand ransom payments, often leaving organizations unable to access patient records, process medical procedures, or operate essential equipment. Given the life-critical nature of healthcare services, these attacks not only pose financial risks but can also result in patient endangerment, delayed treatments, and loss of critical medical data.

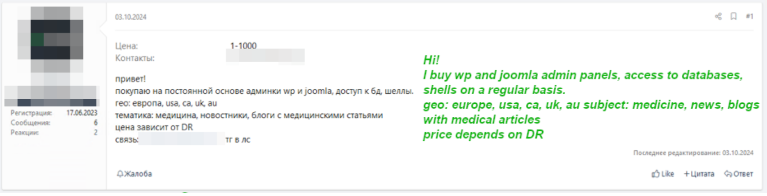
Unlike other industries, hospitals and healthcare providers cannot afford prolonged downtime, making them more likely to pay ransom demands to restore operations quickly. This reality has made healthcare a prime target for ransomware gangs, who see it as a high-pressure, high-payoff sector.

The healthcare industry has become a lucrative target for cybercriminals, with network access to hospitals, clinics, and medical institutions being actively sold on the Dark Web.

11 Big Pharma Firms Affected in Cencora Cyber Attack

May 2024, **Cyber Daily**

Cybercriminal marketplaces and forums offer access to compromised remote desktop (RDP) credentials, VPN logins, and administrator accounts, providing attackers with a direct gateway into hospital networks. These illicit sales fuel a growing underground economy, where ransomware groups, data brokers, and all types of actors compete to exploit healthcare vulnerabilities for financial gain, intelligence gathering, or even disrupting critical medical operations.



Цена: 1-1000
Контакты: [redacted]

привет!
покупаю на постоянной основе админки wp и joomla, доступ к бд, шеллы.
гео: европа, usa, ca, uk, au
тематика: медицина, новостники, блоги с медицинскими статьями
цена зависит от DR
связь: [redacted] тг в лс

Hi!
I buy wp and joomla admin panels, access to databases, shells on a regular basis.
geo: europe, usa, ca, uk, au subject: medicine, news, blogs with medical articles
price depends on DR

Последнее редактирование: 03.10.2024

Figure 1: Threat actor on the Dark Web seeking various types of access to healthcare facilities

What Trustwave Is Seeing

In 2024, ransomware attacks continued to pose a significant threat across various industries, with several groups dominating the landscape.

Trustwave SpiderLabs analyzed ransomware incidents targeting the healthcare sector and identified Ransomhub and LockBit 3.0 as the predominant groups operating in this space. The data reveals that Ransomhub had the greatest number of reported incidents with 62 victims, followed closely by LockBit 3.0 and Dispossessor, each claiming 55 attacks. These numbers indicate that multiple groups remain highly active, leveraging various attack vectors to infiltrate organizations.

This trend highlights the persistent evolution of ransomware tactics, with groups constantly refining their encryption methods, extortion techniques, and targeting strategies. The increasing diversity in attack sources also suggests greater fragmentation within the cybercriminal ecosystem, making it more challenging for law enforcement and cybersecurity professionals to track and mitigate threats effectively.

Top Ransomware Groups Targeting Healthcare

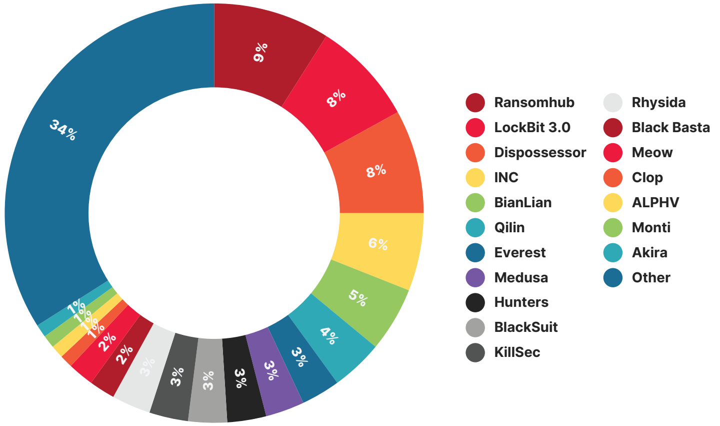


Figure 2: Top ransomware groups targeting healthcare

From a global perspective, ransomware groups exhibit a clear focus on certain regions, with the United States bearing the brunt of attacks. 51% of the incidents in the dataset target US-based companies, highlighting their prominence in global healthcare and their perceived capacity to pay high ransoms.

India and Canada share second place albeit with a significant gap from the US with 4% of reported incidents. Meanwhile, the UK ranks third in the number of ransomware attacks.

Top Countries Impacted

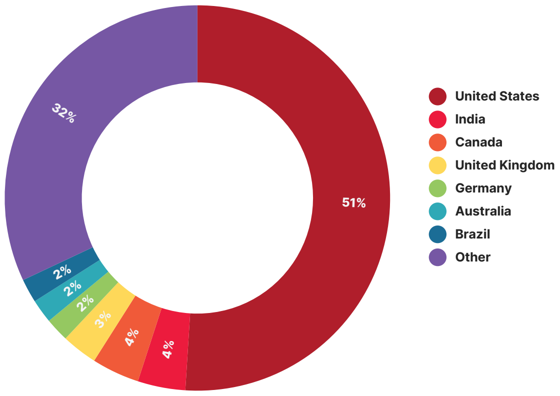


Figure 3: Healthcare organizations affected by ransomware by country

Top Subindustries Impacted

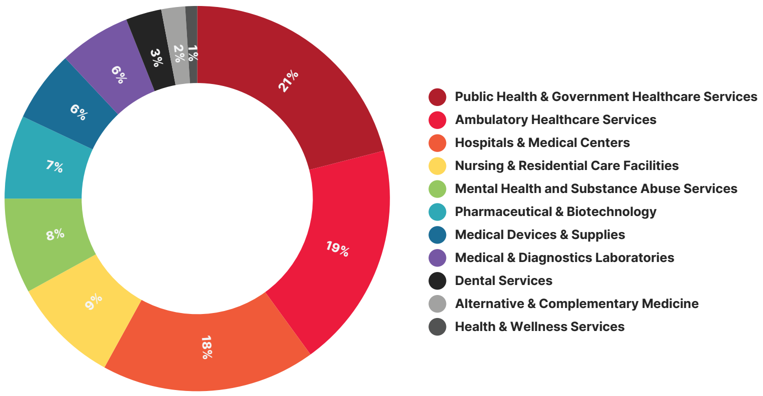


Figure 4: Ransomware attacks by healthcare type

The public health and government healthcare services subindustry is the top target for ransomware attacks, accounting for 21% of incidents, followed closely by ambulatory healthcare services and hospitals and medical centers, accounting for 19% and 18%, respectively. It's important to note that no subsector is immune from these attacks. This distribution underscores the need for robust cybersecurity measures across all healthcare subsectors.

23andMe Settles Data Breach Lawsuit for $30 Million

September 2024, **Reuters**

Mitigations to Reduce Risk

- **Enhance Cybersecurity Hygiene and Patch Management:** Many ransomware attacks exploit known vulnerabilities, especially in legacy systems. Health providers should ensure that all systems, including OT and IT infrastructure, are regularly updated with the latest security patches. The CISA Known Exploited Vulnerabilities (KEV) catalog is a useful resource for identifying and prioritizing patches for critical systems.

- **Implement Robust Backup and Recovery Plans:** Maintaining regular, encrypted backups of critical systems and data is essential to mitigating the impact of a ransomware attack. Backups should be stored offline or in isolated environments to prevent them from being encrypted during an attack. Healthcare organizations should also regularly test their recovery plans to ensure that systems can be restored quickly and with minimal operational disruption.

- **Employee Training and Awareness:** Phishing emails and credential theft are common entry points for ransomware attackers. Educating employees on recognizing phishing attempts, practicing good password hygiene, and reporting suspicious activities can reduce the risk of initial compromise. Healthcare entities should also conduct regular security training and simulated phishing exercises to reinforce these practices.

- **Multi-Factor Authentication (MFA) and Strong Credential Management:** Many ransomware groups gain access to systems through stolen credentials. Implementing MFA across all systems, especially for remote access, can significantly reduce the risk of unauthorized entry. Health providers should also ensure that access to critical systems is restricted to only those who need it, and credentials should be regularly updated.

- **Incident Response Planning:** A comprehensive incident response plan is essential to minimizing the impact of a ransomware attack. This plan should include clear steps for containing and mitigating the attack, restoring systems, and communicating with stakeholders. Healthcare entities should test their incident response plans through tabletop exercises and ensure that external cybersecurity experts are ready to assist if needed.

- **Collaboration with Law Enforcement:** In the event of an attack, healthcare organizations should report the incident to relevant law enforcement agencies. These organizations can assist in tracking down perpetrators, identifying trends, and offering support for recovery. Additionally, collaborating with other industry players and cybersecurity experts can help to stay informed about emerging threats and best practices.

Unmasking Security Gaps in Healthcare

The Threat

We explore a red team assessment with a healthcare client in depth in our accompanying report. At a high level, here is an overview of what was discovered and lessons learned:

A United States-based health system hired Trustwave SpiderLabs to perform a Red Team on its environments, focusing specifically on achieving privilege escalation or abusing user privileges to attempt further exploitation of the environment. The assessment spanned multiple weeks and was conducted with several variations.

The health system's overall security posture was on par with more mature organizations in similar industries. While the organization did have security tooling, Trustwave SpiderLabs observed a high dependency on Application Control, which is not uncommon. For the operation's duration, a high level of privilege was obtained in a brief period of time.

What Trustwave Is Seeing

Trustwave SpiderLabs identified several issues related to the company's Virtual Desktop Infrastructure (VDI) instance, which allowed arbitrary code execution and the means to establish a foothold within the company's network. In addition, even though Trustwave SpiderLabs was allowed to pivot – eventually achieving Domain Administrator privileges, there are multiple aspects in which SpiderLabs would have been caught at the start of the exploitation event, and the instance of exploitation would have been remediated.

Trustwave SpiderLabs was able to access a wide range of files, backups, and prove the ability to worm ransomware. Again, this was only possible in the light of the client working with Trustwave SpiderLabs to highlight the detection events and allow the team to continue.

Summary of Key Findings

- **Credential Mismanagement:** Weak password policies, credential reuse, and exposed accounts with low security measures were identified across various systems, enabling privilege escalation and lateral movement.
- **Vulnerability in Sensitive Systems:** Critical systems, including medical devices, shared drives, and web applications, were found to be improperly secured, exposing PHI, PII, and internal credentials to unauthorized access.
- **Privilege Escalation:** The ability to escalate privileges, both within the network and to Domain Admin levels, was demonstrated. This provides attackers with the potential for broad access across the entire environment.
- **Misconfiguration in Network Segmentation:** Vulnerabilities in the segmentation of sensitive areas, such as patient rooms and camera systems, were found, leaving them exposed to lateral movement and exploitation.

Mitigations to Reduce Risk

- **Credential Hardening:** Enforce strong password policies, utilize MFA, and implement a more rigorous approach to credential management to prevent reuse across services and devices. Additionally, ensure that files do not contain plaintext credentials. Implementing a secrets management program can help securely store and handle sensitive information.

- **Network Segmentation:** Ensure that critical systems (e.g., medical devices, cameras) are properly segmented from other network resources and that access is restricted based on least privilege.

- **EDR and Security Monitoring:** Enhance EDR mechanisms and ensure that security monitoring tools are in place to detect and mitigate suspicious activities, such as arbitrary code execution and privilege escalation. Utilize best practices when implementing exclusions to prevent inadvertently assisting threat actors.

- **Regular Vulnerability Scanning and Patch Management:** Regularly audit and patch systems for known vulnerabilities, especially those with default credentials or outdated software. Keeping critical software up to date is essential to mitigate basic exploitation, such as default credentials or exploits that require limited effort.

- **Review and Mitigate Misconfigured Shared Drives**: Perform thorough reviews of shared drives across the network, addressing any misconfigurations that expose sensitive information, such as PHI and PII. Implement access controls to ensure that only authorized users can access sensitive data.

- **User Permissions Audits:** Conduct regular user permissions audits to ensure that groups or users do not inherit more permissions than they need. This will help minimize the risk of privilege escalation or lateral movement through the network.

Medical Supply Chain Complexities

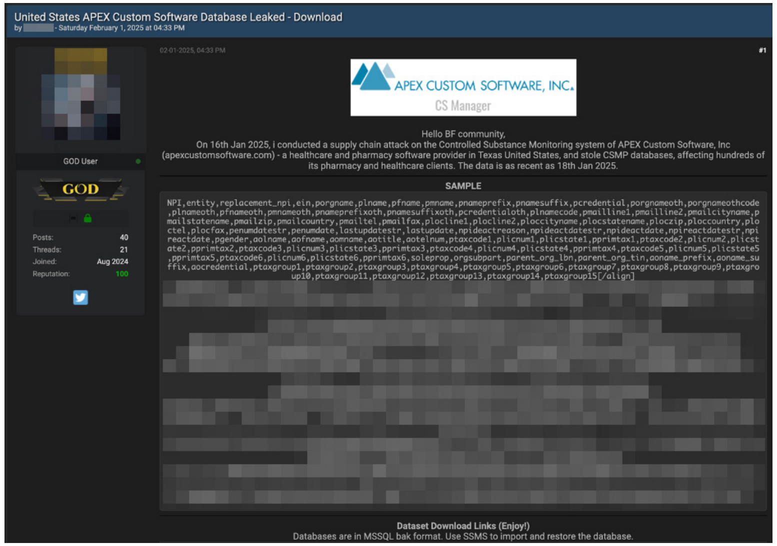
The Threat

The medical supply chain is a critical component of healthcare operations, ensuring that hospitals, clinics, and research institutions receive the necessary equipment, medications, and software to function effectively. These attacks can cause widespread disruptions, from delaying patient care to compromising sensitive medical data.

A successful attack on a single supplier can create a ripple effect across multiple healthcare facilities, affecting everything from hospital management systems to life-saving medical devices. Below, we explore three targets within the medical supply chain and the potential consequences of cyberattacks against them.

What Trustwave Is Seeing

Healthcare institutions rely on specialized software solutions for patient management, medical imaging, billing systems, and electronic health records. Cybercriminals have identified these software providers as high-value targets, knowing that compromising a single vendor could grant them access to multiple hospitals and healthcare facilities at once.



United States APEX Custom Software Database Leaked - Download

by [redacted] - Saturday February 1, 2025 at 04:33 PM

02-01-2025, 04:33 PM

#1

Posts: 40
Threads: 21
Joined: Aug 2024
Reputation: 100

Hello BF community,
On 16th Jan 2025, i conducted a supply chain attack on the Controlled Substance Monitoring system of APEX Custom Software, Inc (apexcustomsoftware.com) - a healthcare and pharmacy software provider in Texas United States, and stole CSMP databases, affecting hundreds of its pharmacy and healthcare clients. The data is as recent as 18th Jan 2025.

SAMPLE

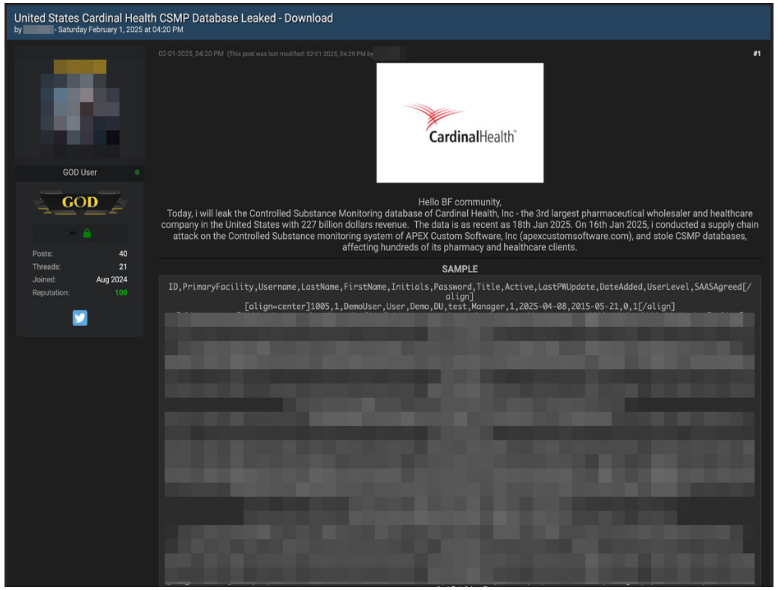
```
NPI,entity,replacement_npi,ein,porgname,plname,pfname,pmname,pnameprefix,pnamesuffix,pcredential,porgnameoth,porgnameothcode
,plnameoth,pfnameoth,pmnameoth,pnameprefixoth,pnamesuffixoth,pcredentialoth,plnamecode,pmailline1,pmailline2,pmailcityname,p
mailstatename,pmailzip,pmailcountry,pmailtel,pmailfax,plocline1,plocline2,ploccityname,plocstatename,ploczip,ploccountry,plo
ctel,plocfax,penumdatestr,penumdate,lastupdatestr,lastupdate,npideactreason,npideactdatestr,npideactdate,npireactdatestr,npi
reactdate,pgender,aolname,aofname,aomname,aotitle,aotelnum,ptaxcode1,plicnum1,plicstate1,pprimtax1,ptaxcode2,plicnum2,plicst
ate2,pprimtax2,ptaxcode3,plicnum3,plicstate3,pprimtax3,ptaxcode4,plicnum4,plicstate4,pprimtax4,ptaxcode5,plicnum5,plicstate5
,pprimtax5,ptaxcode6,plicnum6,plicstate6,pprimtax6,soleprop,orgsubpart,parent_org_lbn,parent_org_tin,aoname_prefix,aoname_su
ffix,aocredential,ptaxgroup1,ptaxgroup2,ptaxgroup3,ptaxgroup4,ptaxgroup5,ptaxgroup6,ptaxgroup7,ptaxgroup8,ptaxgroup9,ptaxgro
up10,ptaxgroup11,ptaxgroup12,ptaxgroup13,ptaxgroup14,ptaxgroup15[/align]
```

[redacted]

Dataset Download Links (Enjoy!)
Databases are in MSSQL bak format. Use SSMS to import and restore the database.

Figure 5: Threat actor claims to hack into the healthcare supply chain attack by targeting healthcare software provider

These attacks mostly occur through supply chain vulnerabilities, ransomware deployment, and API exploits. Many healthcare software providers integrate third-party libraries, cloud services, and open-source components, which can introduce security flaws. Attackers also exploit unpatched software or weak authentication mechanisms, using stolen credentials or API vulnerabilities to gain unauthorized access.



United States Cardinal Health CSMP Database Leaked - Download
by [redacted] - Saturday February 1, 2025 at 04:20 PM

02-01-2025, 04:20 PM (This post was last modified: 02-01-2025, 04:29 PM by [redacted]

Posts: 40
Threads: 21
Joined: Aug 2024
Reputation: 100

Hello BF community,
Today, i will leak the Controlled Substance Monitoring database of Cardinal Health, Inc - the 3rd largest pharmaceutical wholesaler and healthcare company in the United States with 227 billion dollars revenue. The data is as recent as 18th Jan 2025. On 16th Jan 2025, i conducted a supply chain attack on the Controlled Substance monitoring system of APEX Custom Software, Inc (apexcustomsoftware.com), and stole CSMP databases, affecting hundreds of its pharmacy and healthcare clients.

SAMPLE

```
ID,PrimaryFacility,Username,LastName,FirstName,Initials,Password,Title,Active,LastPWUpdate,DateAdded,UserLevel,SAASAgreed[/align]
[align=center]1005,1,DemoUser,User,Demo,DU,test,Manager,1,2025-04-08,2015-05-21,0,1[/align]
```

[redacted]

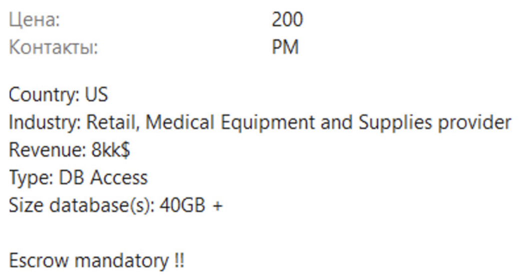
Figure 6: The same actor advertises data claimed to be obtained from the healthcare facility using a supply chain attack against a healthcare software supplier

The consequences of such attacks are severe. A breach at a cloud-based EHR provider could result in thousands of patient records being exfiltrated and sold on the Dark Web. If an attacker compromises a hospital management software provider, scheduling, prescription, and diagnostic processes could be severely disrupted, affecting patient care. Financial and legal ramifications are also significant, with affected healthcare organizations facing lawsuits, regulatory fines, and reputational damage.

Cyberattacks on Retail Healthcare Suppliers and Equipment Vendors

Hospitals and pharmacies rely on retail healthcare suppliers to provide medical devices, pharmaceuticals, and consumables. When a cyberattack targets a major healthcare supplier, it can lead to shortages of essential medical products, directly impacting patient care.

Attackers compromise these suppliers through manipulation of order management systems, financial fraud, and ransomware attacks that halt logistics operations. By infiltrating supplier databases, cybercriminals can reroute shipments, delay deliveries, or falsify invoices, disrupting the flow of critical medical supplies.



Цена: 200
Контакты: PM

Country: US
Industry: Retail, Medical Equipment and Supplies provider
Revenue: 8kk$
Type: DB Access
Size database(s): 40GB +

Escrow mandatory !!

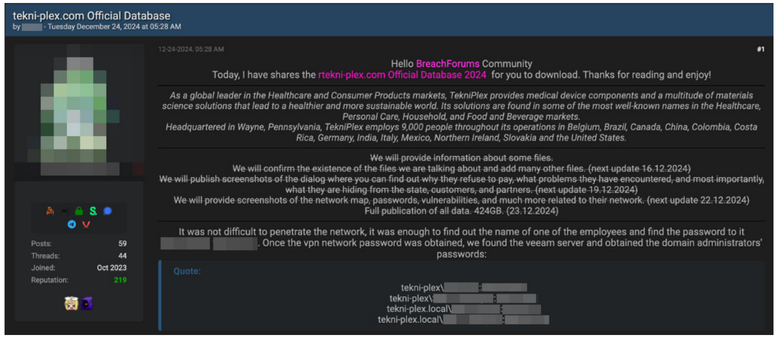
Figure 7: Threat actor sells access to a medical equipment supplier in US

Financially motivated hackers also target payment processing systems used by healthcare suppliers, aiming to steal credit card details, insurance claims, and patient data. Ransomware attacks on suppliers can shut down warehouse operations, making it impossible for hospitals to receive the medical products they need.

The consequences of these attacks include delays in delivering essential medical equipment, financial fraud resulting in substantial losses for hospitals, and the exploitation of stolen customer data to launch targeted phishing attacks against healthcare facilities.

Cyberattacks on Medical Materials and Science Solution Providers

Some companies that develop medical-grade materials, pharmaceuticals, and biotech solutions are also high-value targets for cybercriminals. These companies supply raw materials for drug manufacturing, laboratory reagents, and specialized research tools that are essential for medical treatments and scientific advancements. Cyberattacks on these firms often involve espionage, supply chain manipulation, and operational disruption.



tekni-plex.com Official Database
by [redacted] - Tuesday December 24, 2024 at 05:28 AM

12-24-2024, 05:28 AM #1

Hello BreachForums Community
Today, I have shares the rtekni-plex.com Official Database 2024 for you to download. Thanks for reading and enjoy!

As a global leader in the Healthcare and Consumer Products markets, TekniPlex provides medical device components and a multitude of materials science solutions that lead to a healthier and more sustainable world. Its solutions are found in some of the most well-known names in the Healthcare, Personal Care, Household, and Food and Beverage markets.
Headquartered in Wayne, Pennsylvania, TekniPlex employs 9,000 people throughout its operations in Belgium, Brazil, Canada, China, Colombia, Costa Rica, Germany, India, Italy, Mexico, Northern Ireland, Slovakia and the United States.

~~We will provide information about some files.~~
~~We will confirm the existence of the files we are talking about and add many other files. (next update 16.12.2024)~~
~~We will publish screenshots of the dialog where you can find out why they refuse to pay, what problems they have encountered, and most importantly, what they are hiding from the state, customers, and partners. (next update 19.12.2024)~~
~~We will provide screenshots of the network map, passwords, vulnerabilities, and much more related to their network. (next update 22.12.2024)~~
~~Full publication of all data. 424GB. (23.12.2024)~~

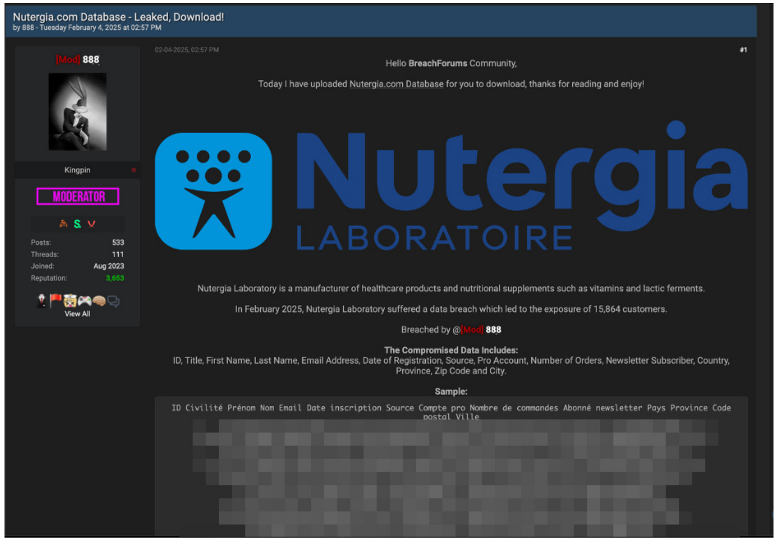
It was not difficult to penetrate the network, it was enough to find out the name of one of the employees and find the password to it [redacted] [redacted]. Once the vpn network password was obtained, we found the veeam server and obtained the domain administrators' passwords:

> Quote:
>
> tekni-plex\[redacted]:[redacted]
> tekni-plex\[redacted]:[redacted]
> tekni-plex.local\[redacted]:[redacted]
> tekni-plex.local\[redacted]:[redacted]

Figure 8: Threat actor shares databases and credentials from a compromised global healthcare materials and science solutions supplier

Intellectual property theft is a major concern, as hackers target pharmaceutical and biotech companies to steal proprietary drug formulas, vaccine research, and medical innovations. Compromised research data can be sold on the Dark Web, used by competitors, or exploited for financial gain.

Cybercriminals can also manipulate supply chain data, causing defective or counterfeit medical materials to enter hospitals. Such disruptions can slow down vaccine production, delay drug approvals, or introduce contaminated medical products into healthcare systems.



Nutergia.com Database - Leaked, Download!
by 888 - Tuesday February 4, 2025 at 02:57 PM

[Mod] 888

Kingpin

MODERATOR

Posts:	533
Threads:	111
Joined:	Aug 2023
Reputation:	3,653

View All

02-04-2025, 02:57 PM #1

Hello BreachForums Community,

Today I have uploaded Nutergia.com Database for you to download, thanks for reading and enjoy!

Nutergia Laboratory is a manufacturer of healthcare products and nutritional supplements such as vitamins and lactic ferments.

In February 2025, Nutergia Laboratory suffered a data breach which led to the exposure of 15,864 customers.

Breached by @[Mod] 888

The Compromised Data Includes:
ID, Title, First Name, Last Name, Email Address, Date of Registration, Source, Pro Account, Number of Orders, Newsletter Subscriber, Country, Province, Zip Code and City.

Sample:

```
ID Civilité Prénom Nom Email Date inscription Source Compte pro Nombre de commandes Abonné newsletter Pays Province Code postal Ville
```

[redacted]

Figure 9: The post shares a database of healthcare products and nutritional supplements developer

Ransomware Attack Forces UMC Health System to Divert Some Patients

October 2024, **Bleeping Computer**

Mitigations to Reduce Risk

- **Vendor Security Agreements:** Ensure that contracts with third-party vendors outline clear cybersecurity responsibilities, including data protection, breach notification timelines, and compliance with industry standards like HIPAA and GDPR.
- **Monitor Vendor Access:** Limit third-party access to healthcare systems and sensitive data using the principle of least privilege. Restrict access based on the specific needs of each supplier, and periodically review their access levels.
- **Continuous Monitoring of Third-Party Systems:** Utilize tools to monitor and assess the security posture of third-party vendors and any connected systems, APIs, or cloud-based platforms.
- **Patch and Update Software Regularly:** Ensure that all healthcare software systems (e.g., EHR, billing systems, and hospital management software) are up to date and patched regularly to mitigate known vulnerabilities.
- **Secure API Integrations:** Review and secure all third-party APIs used by healthcare software providers. This includes implementing strong authentication, encryption, and API security protocols to reduce the risk of exploitation through API vulnerabilities.
- **Use Secure Software Development Practices:** Encourage vendors to implement secure coding practices, conduct regular code reviews, and utilize vulnerability scanning tools to detect security flaws in their software.
- **Adopt Zero-Trust Architecture:** Apply a zero-trust model within healthcare systems to ensure that no device or user, even within the network, is trusted by default. This approach minimizes the impact of any potential supply chain compromise.

Complex Web of Compliance

The Threat

The healthcare industry is undergoing a rapid digital transformation, with the increasing use of EHRs, telehealth, and connected medical devices.

While these advancements offer numerous benefits, they also expose healthcare organizations to a growing array of cybersecurity threats. For cybersecurity professionals working in this sector, understanding the complex web of compliance and regulatory requirements is paramount to safeguarding patient data, ensuring patient safety, and maintaining the integrity of healthcare operations.

What Trustwave Is Seeing

International Healthcare Cybersecurity Standards

Beyond national regulations, several international standards provide valuable guidance for healthcare cybersecurity professionals. These standards offer frameworks and best practices that can be adapted to various regulatory environments and help organizations establish a strong security foundation.

ISO 27001

ISO/IEC 27001 is a globally recognized standard that provides a framework for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). It helps organizations manage information security risks and protect sensitive data, including patient information. ISO 27001 emphasizes a risk-based approach, requiring organizations to identify, assess, and treat information security risks. It also promotes a culture of continuous improvement, ensuring that security measures are regularly reviewed and updated to address evolving threats.

Key elements of ISO 27001 include:

- **ISMS Framework:** Establishing a systematic approach to managing information security, including policies, procedures, and controls.
- **Risk Evaluation:** Conducting thorough risk assessments to identify potential threats and vulnerabilities.
- **Control Selection and Implementation:** Implementing appropriate controls to mitigate identified risks, drawing from a comprehensive set of controls outlined in Annex A of the standard.
- **Monitoring and Review:** Regularly monitoring and reviewing the ISMS to ensure its effectiveness and identify areas for improvement.

IEC 62443

IEC 62443 is a series of standards that address security for operational technology in automation and control systems, including those used in healthcare. It provides a framework for assessing and mitigating cybersecurity risks in industrial environments, with a focus on the security lifecycle of systems and components. IEC 62443 emphasizes a holistic approach to security, considering all aspects of the system, from design and development to implementation and maintenance.

Key concepts in IEC 62443 include:

- **Security by Design:** Incorporating security considerations into the design process of industrial automation and control systems.
- **Defense-in-Depth:** Implementing multiple layers of security controls to protect against a variety of threats.
- **Risk Assessment:** Conducting thorough risk assessments to identify and evaluate potential threats and vulnerabilities.
- **Zones and Conduits:** Segmenting industrial networks into zones with varying security levels and establishing secure conduits for communication between zones.
- **Security Levels:** Defining different security levels based on the potential impact of a security breach.

EU's NIS2 Directive

The EU's NIS2 Directive is a significant piece of legislation that aims to enhance cybersecurity across critical infrastructure sectors, including healthcare. It mandates enhanced risk management and incident reporting obligations for organizations operating in these sectors to protect against cyberattacks and ensure the continuity of essential services. The NIS2 Directive emphasizes a risk-based approach, requiring organizations to implement appropriate security measures proportionate to the risks they face. It also promotes a culture of cybersecurity awareness and encourages information sharing among stakeholders.

Cyberattack at French Hospital Exposes Health Data of 750,000 Patients

November 2024, **Bleeping Computer**

Medical Device Regulation in the UK

Navigating medical device regulations in the UK involves understanding the role of the Medicines and Healthcare products Regulatory Agency (MHRA) and the shift from CE marking to UKCA marking.

- The MHRA is the governing body responsible for ensuring medical devices meet safety and performance standards. Registration with the MHRA is mandatory for placing medical devices on the UK market.
- The UKCA (UK Conformity Assessed) mark is the UK's equivalent to the EU's CE mark. It signifies that a device complies with UK Medical Device Regulations.

HIPAA 2.0: Strengthening Cybersecurity in US Healthcare

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a cornerstone of healthcare data protection in the United States. In January 2025, the US Department of Health and Human Services (HHS) proposed significant updates to the HIPAA Security Rule, often referred to as "HIPAA 2.0," to address the evolving cybersecurity landscape and enhance protections for electronic protected health information (ePHI). These attacks endanger patients by exposing vulnerabilities in our healthcare system, degrading patient trust, disrupting patient care, and diverting resources.

Key Changes in HIPAA 2.0

The proposed changes in HIPAA 2.0 aim to strengthen security standards and improve compliance by:

- **Removing the distinction between "required" and "addressable" implementation specifications:** Previously, some security measures were considered "addressable," allowing organizations flexibility in their implementation. HIPAA 2.0 makes all implementation specifications mandatory unless an exception applies, ensuring a consistent level of security across the industry.
- **Enhancing risk analysis requirements:** HIPAA 2.0 mandates more detailed risk analyses, including a review of technology asset inventories, network maps, and the identification of all reasonably anticipated threats and vulnerabilities.
- **Strengthening incident response and contingency planning:** The updated rule requires written incident response plans, procedures for restoring critical systems within 72 hours, and analysis of the criticality of different systems to prioritize restoration efforts.
- **Mandating new security controls:** HIPAA 2.0 requires encryption of ePHI at rest and in transit, MFA, network segmentation, and regular vulnerability scanning and penetration testing.
- **Increasing accountability for business associates:** Business associates are now required to verify technical safeguards annually, provide written certifications of compliance, and notify covered entities within 24 hours of activating contingency plans.

Impact on Healthcare Organizations

These changes have significant implications for healthcare organizations, demanding a proactive and comprehensive approach to cybersecurity. Some key impacts include:

- **Increased compliance costs:** Implementing the new security measures, such as encryption, MFA, and network segmentation, will require investments in technology and employee training.
- **Operational disruptions:** Organizations may need to redesign workflows and update legacy systems to comply with the new rules.
- **Enhanced protection against cyberattacks:** The stricter security standards will reduce the likelihood of data breaches and improve overall cybersecurity posture.
- **Improved patient trust:** Demonstrating a commitment to cybersecurity can enhance patient trust and confidence in the organization's ability to protect their data.

HIPAA 2.0 represents a significant shift in the healthcare cybersecurity landscape. While the increased requirements may pose challenges for some organizations, they also present an opportunity to improve security posture, align with modern security practices, and enhance patient trust.

Other Relevant US Healthcare Cybersecurity Regulations

In addition to HIPAA, several other US regulations and frameworks are relevant to healthcare cybersecurity professionals:

- **HITECH Act:** The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 strengthened HIPAA's privacy and security provisions, extended its reach to business associates, and introduced stricter penalties for violations. It also incentivized the adoption and meaningful use of EHRs to improve healthcare quality and efficiency.
- **NIST Cybersecurity Framework:** The NIST Cybersecurity Framework provides a voluntary set of standards, guidelines, and best practices to help organizations manage and reduce cybersecurity risks. It is widely adopted across various industries, including healthcare, and aligns with HIPAA's Security Rule.
- **Healthcare Cybersecurity Act of 2022:** This Act requires the Department of HHS to undertake activities to improve the cybersecurity of the healthcare and public health sector, including coordinating with CISA to provide resources and training to healthcare organizations.
- **FDA's Role in Medical Device Cybersecurity:** The Food and Drug Administration (FDA) plays a crucial role in regulating the cybersecurity of medical devices. It provides guidance to manufacturers on cybersecurity considerations for medical devices and requires that devices meet specific cybersecurity guidelines to ensure patient safety and device functionality.
- **HITRUST Framework:** HITRUST provides a certifiable framework, the CSF, that consolidates security and privacy regulations, enabling organizations to demonstrate robust risk management and compliance. It's a widely recognized standard, particularly in healthcare, signifying strong information protection practices.

UK Healthcare Cybersecurity Regulations

In the UK, healthcare cybersecurity professionals must navigate a framework of regulations and standards to ensure the protection of patient data and the secure operation of healthcare systems:

- **Data Protection Act 2018:** This Act incorporates GDPR into UK law, setting strict rules for processing personal data, including health information. It emphasizes accountability, requiring organizations to demonstrate compliance with data protection principles. The Act brings together four regimes of data protection law, ensuring comprehensive coverage of various data processing activities.

- **NHS Data Security and Protection Toolkit:** This online self-assessment tool allows organizations to measure their performance against the National Data Guardian's 10 data security standards. It is mandatory for all organizations that handle NHS patient data, ensuring consistent security practices across the healthcare sector.

- **NIS2 Directive:** While the UK is not implementing the NIS2 directive, it is working on its own proposals to amend the existing NIS regulations to address the evolving cybersecurity landscape and ensure the security of essential services, including healthcare.

Australian Healthcare Cybersecurity Regulations

Australia has a robust regulatory framework for protecting healthcare data and ensuring the privacy of individuals:

- **My Health Records Act 2012:** This Act established a national system for sharing health information electronically, with provisions for security and privacy. It outlines requirements for access controls, data breach notifications, and the use of My Health Record data. Importantly, participation in the My Health Record system is voluntary for individuals.

- **Australian Privacy Principles:** These principles, enshrined in the Privacy Act 1988, govern the handling of personal information, including health information, by Australian government agencies and private sector organizations. They cover aspects such as collection, use, disclosure, and security of personal information. The Principles include specific requirements for health information security, such as limitations on collection, use, and disclosure, and the implementation of reasonable security safeguards to protect personal information from misuse, interference, loss, and unauthorized access.

Threat Actor Techniques by Attack Stage

Data breaches and compromises come in many forms but often follow a similar pattern. Attackers gain access, escalate privileges, establish a foothold, steal or destroy data, and then vanish. Trustwave SpiderLabs analyzed data from across our clients to understand the path that threat actors take within the healthcare industry and the techniques they deploy at each stage.

Initial Access Techniques

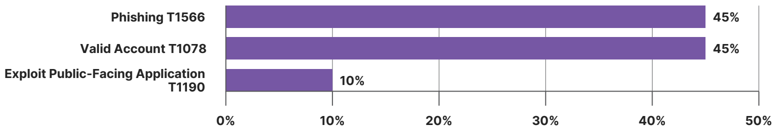


Figure 10: Initial access techniques used by attackers of healthcare entities

Initial access vectors used in healthcare attacks were split between phishing (45%) and exploit attempts against web applications (45%). Most of the phishing attempts were generic and leveraged social engineering with links to external websites.

Exploit Public-Facing Applications

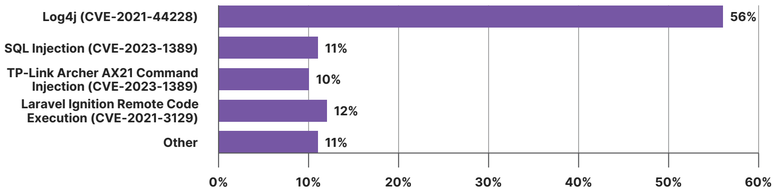


Figure 11: Public-facing applications exploited in the healthcare sector

Exploit procedures observed in the initial access attempts against web applications were mostly Log4j CVE-2021-44228 – accounting for 56% of the observed cases, and SQL Injection and CVE-2023-1389 – TP-Link Archer AX21 Command Injection (CVE-2023-1389) – accounting for 11% and 10% of the cases respectively.

Execution Techniques

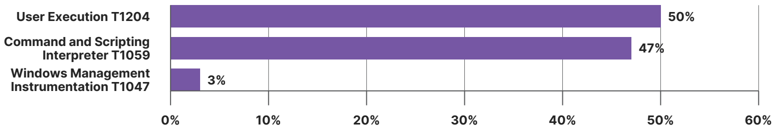


Figure 12: Execution techniques used by attackers of healthcare entities

Execution techniques observed in the healthcare security incidents mostly involved user execution of malicious files and links (50%), followed by malicious uses of PowerShell scripts and commands (47%). Some commands were found to be a result of Mimikatz hacktool execution.

Persistence Techniques

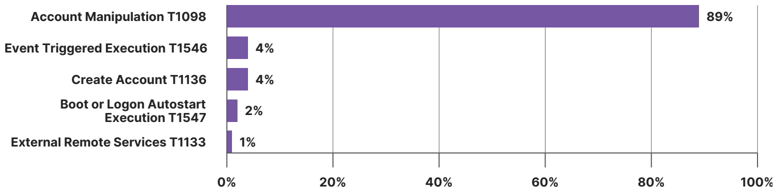


Figure 13: Persistence techniques used by attackers of healthcare entities

The persistence techniques observed relied mostly on account manipulation (89%), but also other techniques such as account creation, (4%) and event-triggered execution (4%).

Account manipulation involves modifying existing accounts to either maintain access or escalate privileges. For example, an attacker might change account permissions or add their credentials to an existing user account to retain access. Account creation refers to the creation of new user accounts by attackers. Threat groups use these new accounts to maintain access or to disguise their activities as legitimate users.

Defense Evasion Techniques

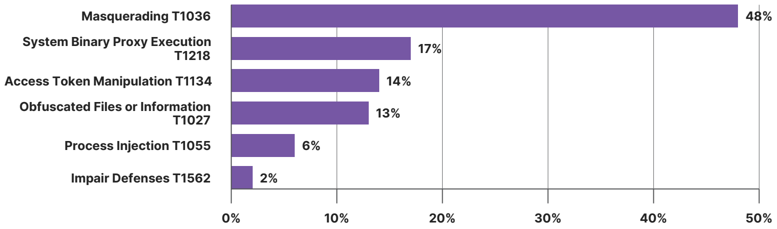


Figure 14: Defense evasion techniques used by attackers of healthcare entities

Defense evasion techniques observed in healthcare security incidents mostly utilized masquerading (48%), using process names such as explorer.exe, srvany.exe, taskmgr.exe and chrome.exe, and system binary proxy execution using rundll32 and curl.exe to download and execute external payloads.

Credential Access Techniques

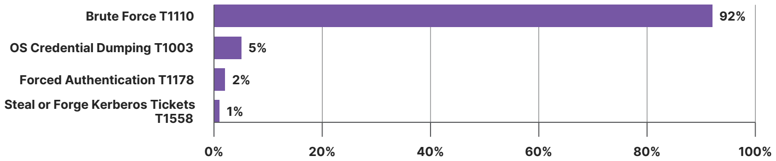


Figure 15: Credential access techniques used by attackers of healthcare entities

Credential access techniques observed in the attacks relied mostly on brute-force attempts and generic brute-force attacks (92%). We also observed OS credential dumping attempts (5%) using ComSvcs and Mimikatz and forced authentication attempts (2%).

Lateral Movement Techniques

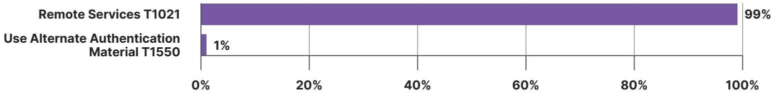


Figure 16: Lateral movement techniques used by attackers of healthcare entities

To move laterally within healthcare organizations, attackers relied almost exclusively on Remote Services (99%), specifically Remote Desktop Protocol (RDP).

Conclusion & Key Takeaways

Conclusion

The healthcare sector is facing an evolving and alarming landscape of cyber threats, underscoring the importance of robust cybersecurity practices to safeguard not just data, but human lives. With the rapid expansion of digital tools such as telehealth, IoMT devices, and cloud-based systems, healthcare organizations are increasingly vulnerable to a variety of cyberattacks, including ransomware, data breaches, and supply chain compromises. These threats have the potential to cause disruptions that can delay critical treatments, compromise patient records, and even jeopardize patient safety.

Despite these risks, many healthcare organizations are still grappling with outdated security practices, inadequate authentication measures, and insufficient staff training. To address these challenges, the healthcare sector must prioritize proactive cybersecurity strategies that integrate strengthened access controls, device security, vendor management, and employee training. A robust cybersecurity posture will not only help mitigate financial losses but also ensure the resilience of healthcare systems and the protection of patient safety in this digital age.

Ultimately, cybersecurity in healthcare is no longer just a technical issue—it is a critical component of patient care. By investing in comprehensive security measures and fostering a culture of vigilance, healthcare organizations can better safeguard their networks, protect sensitive data, and ensure that technological advancements enhance rather than endanger the well-being of patients.

Key Takeaways:

1. **Emerging Cyber Threats:** The healthcare sector faces growing cyber threats, including ransomware attacks, data breaches, and supply chain compromises. These attacks can disrupt medical services and put patient safety at risk.

2. **Impact on Patient Care:** Cyberattacks in healthcare can directly harm patients by delaying treatments, compromising medical devices, and disrupting critical healthcare operations, which can lead to life-threatening consequences.

3. **Need for Stronger Cybersecurity Measures:** Many healthcare organizations are vulnerable due to outdated cybersecurity practices, weak authentication, and insufficient staff training. Implementing multi-factor authentication, zero-trust models, and regular cybersecurity audits are essential steps to enhance security.

4. **Vendor and Supply Chain Risks:** Cybercriminals increasingly target third-party vendors and suppliers. Healthcare organizations must strengthen their security frameworks to protect data shared with external partners.

5. **Comprehensive Security Approach:** A robust cybersecurity strategy should include endpoint protection, IoMT device security, staff training, dark web monitoring, and a well-defined incident response and recovery plan.

6. **Patient Safety as a Priority:** Cybersecurity is not just an IT concern but a patient safety imperative. Healthcare organizations must treat securing their networks and data as a top priority to safeguard patient lives and preserve trust in the healthcare system.

By taking proactive and strategic action, healthcare organizations can significantly reduce their risk exposure and build a more resilient, secure environment for both healthcare professionals and patients.

Trustwave®