NETSPI™

The Complete Guide to Healthcare Ransomware Attacks

Ransomware is top-of-mind for the healthcare industry today as attacks become more sophisticated. When infected with ransomware, healthcare organizations and networks lose access to their systems and/or data and the cybercriminals demand a ransom in exchange for restoring access.

The impact can be detrimental, leaving hospitals without access to electronic health records, waiting days for lab results, and having no choice but to cancel or reschedule appointments, among other disruptions to patient care.

One in four companies worldwide pay the ransom to regain access to their files and this number increases to 61% in healthcare – the highest percentage across all industries. However, paying up does not always pay off. The likelihood of getting all your data back after paying is slim, with only 2% of ransomware victims in the healthcare space reporting getting all their data back.

To stop ransomware attacks, collectively we need to cut off the cybercriminal's source of income – that means not paying the ransom and understanding the alternative steps to take to prevent and respond to a ransomware attack – and how to improve your ransomware detections to address the threat proactively.

In this guide to healthcare ransomware attacks, explore:

1. How ransomware works
2. Why healthcare is a top target for ransomware attacks
3. Ransomware trends and families
4. Checklists for ransomware detection and prevention

Ransomware Trends, Targets, and Families

Before arming your organization with the right security protocols and tools to prevent a ransomware attack, it is important to understand the ransomware ecosystem. This includes the latest trends, understanding who a prime target is, and which of the 400+ ransomware families healthcare organizations should watch.

- The ransomware-as-a-service (RaaS) model is on the rise. With RaaS, attackers do not write the malware, they purchase and spread it. Commissions are paid to the developers for the use of the malware.
- The number of ransomware attacks on hospitals and health systems more than doubled between 2016 and 2021.[1]
- With COVID, remote worker entry points are being targeted much more, including remote desktop, employee access gateways, and VPN access portals.
- Only about one in five healthcare organizations that were impacted reported being able to restore data from backups.[1]
- Email phishing, admin interfaces, and exploits are common entry points, and drive-by downloads (malvertising, force download, or exploit browser) are becoming more popular.
- Many threat actors that deploy ransomware attempt to disable backup/recovery capabilities, so victims are forced to pay if they want access to their systems and data.
- Emsisoft reported that 200 government, education, and healthcare entities were targeted by ransomware in 2022.
- Once ransomware is deployed, IBM X-Force estimates 70% of victims are paying ransoms.
- Ransom demands are increasing exponentially. We are now seeing ransom demands of more than $40 million.
- IBM Security's X-Force data shows that 20 percent of compromised organizations have paid ransoms of more than $40,000, and 25 percent have paid between $20,000 and $40,000.

[1] https://www.healthcareitnews.com/news/half-ransomware-attacks-have-disrupted-healthcare-delivery-jama-report-finds

NETSPI

Why is Healthcare a Top Target for Ransomware?

Attackers consider many variables when choosing which organizations to target with ransomware. Healthcare organizations in particular are a top target because they cannot afford downtime, as they rely on their systems to provide patient care, and are therefore more likely to pay the ransom faster. The public health pandemic in recent years has only further increased the criticality of avoiding system downtime.

Another reason healthcare is a prime target is that the industry is a gold mine for sensitive data, including social security numbers, payment information, birth certificates, addresses, and more. Breaches of such data is a major HIPAA compliance violation that can lead to heavy fines and potentially have a direct, negative impact on patients if their data is leaked.

Ransomware Families to Watch:

Ransomware Family	RaaS Support	Initial Access	Healthcare Advisory
Venus	No	2022-Present	https://www.hhs.gov/sites/default/files/venus-ransomware-analyst-note.pdf
ALPHV/BlackCat	Yes	2021-Present	https://www.aha.org/2022-12-12-hc3-tlp-clear-analyst-note-blackcat-aka-alphv-december-12-2022
Hive	Yes	2019-Present	https://www.ic3.gov/Media/News/2021/210825.pdf
LockBit	Yes	2019-Present	https://www.hhs.gov/sites/default/files/lockbit-3-analyst-note.pdf
Conti	Yes	2019-Present	https://attack.mitre.org/software/S0575/
DoppelPaymer	Yes	2019-Present	https://www.ic3.gov/Media/News/2020/201215-1.pdf

NETSPI

How Ransomware Works:

Step 1: Getting in

Adversaries can get into a network in numerous ways. Here are four vectors used to gain initial access:

1. Phishing links and attachments.
2. Using weak or default credentials to log into single factor remote management interfaces and desktop platforms such as Citrix, Remote Desktop, and VPN access points.
3. Exploitation of common security vulnerabilities, including SQL injection, broken authentication, broken access control, and insufficient logging and monitoring.
4. Unintentional download and execution of malware through obfuscation and/or social engineering techniques (drive-by downloads, malvertising, forced download, or browser exploits).

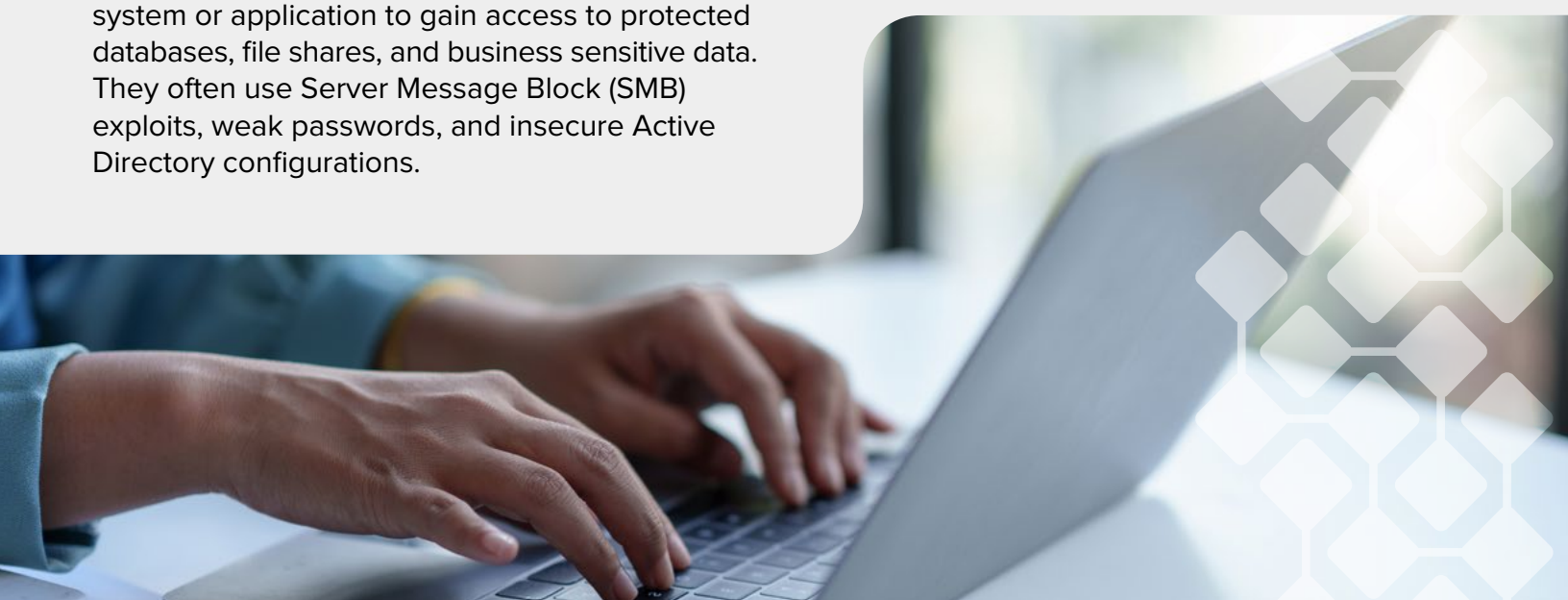
Step 2: Privilege escalation

Once in, adversaries work to exploit bugs, design flaws, or configuration oversights in an operating system or application to gain access to protected databases, file shares, and business sensitive data. They often use Server Message Block (SMB) exploits, weak passwords, and insecure Active Directory configurations.

Step 3: Find and exfiltrate sensitive data

Attackers leverage well known techniques to quickly identify servers that may contain sensitive data and upload the data to systems on the internet. Threat actors often follow this workflow:

1. Perform Active Directory reconnaissance for all domain computers, SQL Servers, and SMB shares.
2. Attempt access to file servers and SQL Servers with privileged accounts.
3. Search for sensitive data patterns across file servers and SQL Server databases.
4. Package data for export (this often includes encrypted and compressing data).
5. Upload data to systems on the internet in one large file or in parts using common protocols such as SMB, Secure Shell (SSH), file transfer (FTP), and HTTP/HTTPS.



Step 4: Ransomware deployment

Now it is time to deploy the ransomware. Ransomware can take many forms, including: locker (uses screen locking to block basic computer functions), wiper (deletes files on a timer), or crypto (encrypts important data and often includes a kill switch to delete data if the ransom is not paid by a specific time). Here are the steps ransomware families often take to deploy the malicious code:

1. Verify the correct platform, language, and time zone.
2. Disable or bypass detective security controls.
3. Remove system restore capabilities.
4. Encrypt files, often targeting specific file types and resulting in central processing unit (CPU) spikes.
5. Overwrite MBR (less common, but growing in popularity).
6. Propagate over SMB to spread through the environment.

Standard File Encryption Process:

1. Hardcoded or generated RSA key pair Generate Advanced Encryption Standard (AES) key.
2. Encrypt files with AES.
3. Encryption AES key with public key.
4. Only a private key can be used to decrypt the AES key required to decrypt the files.

Step 5: Get paid for the decryption key

Often ransomware attackers request the ransom is paid in Bitcoin. Once paid, the likelihood of recovering the money is low. Even when money is returned you're not likely to get all of it back. For example, in 2021 the FBI recovered $2.3 million of the $5 million from the Colonial Pipeline attackers.

Step 6: Extort additional money by threating to publish exfiltrated data

Adversaries exfiltrate sensitive data early in the ransomware deployment process so that, even if a ransom is paid, they can continue to threaten the organization and make more money.

NETSPI

How to Prevent and Detect a Ransomware Attack:

Remember, paying a ransom is a losing game. Invest in security now to avoid paying a ransom later. Leverage the following checklists to proactively prevent ransomware and ensure your ransomware detective controls are working as intended.

Ransomware Prevention Checklist:

- [ ] Continue to build and maintain robust asset management, vulnerability management, patch management, and configuration management programs.
- [ ] Reduce and monitor all internet facing attack surfaces.
- [ ] Enable multi-factor authentication on all internet-facing interfaces.
- [ ] Ensure least privilege is enforced across applications, cloud platforms, systems, and databases.
- [ ] Isolate sensitive networks, systems, and data.
- [ ] Isolate and validate backup and restore capabilities.
- [ ] Perform a comprehensive evaluation of how your preventative and detective controls hold up to TTPs used by real-world ransomware.

Ransomware Detection Checklist:

- [ ] Ensure data sources are available to provide your security operations teams and/or partner with enough information to develop detections for common malicious behavior. This should include file modification events, registry modification events, process creation events, image load events, network connection events, Windows endpoint security event logs, command line event logs, PowerShell event logs, Netflow/Pcap data, and security event data from third party software or devices.
- [ ] Review telemetry flows on a regular basis to ensure they're still functioning as expected. You can't act on the data you can't see.
- [ ] Ensure your security operations team and/or partner have the capability to tune or create new detections. NetSPI found that most endpoint detection and response and security information and event management (SIEM) solutions only identify around 15% of the most common TTPs used by real world attackers out of the box. This is why it is important that you carefully read your MSSP contracts – many organizations are not getting the coverage they thought they were.
- [ ] Identify behavioral choke points to focus detection/prevention effort. Lateral movement is a great starting point as it is a part of almost every ransomware operation.
- [ ] Begin efforts to build custom behavioral detections tuned to your environment, as these typically can't be prepared for in advance by threat actors.
- [ ] Ensure that alert levels trigger response for high-risk behavior associated with high fidelity detections.
- [ ] Deploy or configure monitoring for high-risk command execution related to scheduled tasks, service manipulation, and LOLBAS (living off the land binaries, scripts, and libraries) execution. It's important to monitor these patterns as they can be the result of encrypting files on scale during ransomware attacks.

  Note: This could potentially be done using existing performance monitoring tools.
- [ ] Monitor for the deletion of shadow copies.
- [ ] Monitor for modifications to SafeBoot and similar restore capabilities.
- [ ] Ensure security tool tampering logs are enabled and forwarded to the SIEM.
- [ ] Monitor for high file I/O and CPU utilization on individual systems and the average across the network.

Many governments are discouraging ransomware payments because they naturally fuel a threat actor's ability to conduct future ransomware attacks. However, right now, no one is outright prohibiting direct ransomware payments or ransomware insurance claims. Yet, 93% of healthcare organizations with cyber insurance against ransomware have reported that it's becoming more difficult to secure coverage, with 34% saying it was also more expensive.

If we do not see new regulations restricting ransomware payment, hopefully, we will see governments offering some subsidies to small and medium businesses that can't afford to partner with security firms but may be considered high-risk targets. While we wait for the global cybersecurity community to work toward solutions, Ransomware Resiliency Planning is going to become a priority for everyone. We hope this guide helped provide you with a jump start in the right direction.

For continued reading on the state of ransomware attacks, read:

1. Trends in Ransomware Attacks on U.S. Hospitals, Clinics and Other Health Care Delivery Organizations
2. Sophos The State of Ransomware in Healthcare 2022
3. Red Canary 2022 Threat Detection Report
4. Mandiant M-Trends 2022
5. CrowdStrike® 2022 Global Threat Report
6. Verizon 2022 Data Breach Investigations Report

NetSPI is the leader in enterprise penetration testing and attack surface management. Today, NetSPI offers the most comprehensive suite of offensive security solutions – penetration testing as a service, attack surface management, and breach and attack simulation. Through a combination of technology innovation and human ingenuity NetSPI helps organizations discover, prioritize, and remediate security vulnerabilities. For over 20 years, its global cybersecurity experts have been committed to securing the world's most prominent organizations, including nine of the top 10 U.S. banks, four of the top five leading global cloud providers, four of the five largest healthcare companies, three FAANG companies, seven of the top 10 U.S. retailers & e-commerce companies, and 50 percent of the Fortune® 50. NetSPI is headquartered in Minneapolis, MN, with global offices across the U.S., Canada, the UK, and India.

www.netspi.com