CLEARDATA™

RANSOMWARE

Response & Recovery Guide

A ClearDATA eBook

RANSOMWARE
Response & Recovery Guide

An eBook designed to address healthcare's unique challenges when a ransomware attack occurs

11 SECONDS

passes between each new ransomware attack

Read the Story

2 DEATHS

have been attributed to ransomware attacks

Read the Story

238

healthcare data breaches were reported in the first half of 2021, more than any other industry

Read the Story

If your organization creates, processes, transmits, or stores protected health information (PHI), **you are a prime target for ransomware**. Hackers continue to prey on healthcare and its vast amount of data.

The potential harm to patients, operational damage, threat to human life, and astounding recovery costs can be catastrophic to any healthcare organization that experiences a ransomware attack. In the most severe scenarios, an attack can effectively bring down the hospital's entire system. This type of disruption causes healthcare providers to cancel scheduled surgeries, ambulances to reroute to other emergency rooms and/or transfer critical patients to another facility or provider mid-treatment. Often, clinicians must shift to a pen-and-paper method if they are able to provide care, significantly adding to the total cost of incident recovery.

IN THIS E-BOOK

1. Why Healthcare Is Targeted More Than Other Industries
2. How to Plan for a Ransomware Attack
3. Responding to and Recovering from an Attack
4. Conclusion

INCREASING THREATS

Ransomware attacks against the healthcare industry are reaching crisis levels, and only increasing with data liquidity and the digital front door. During the brief period from July to September 2021, we observed more emerging and malicious ransomware:

- Millions of connection attempts from known malicious hosts, including the Egregor, Ryuk, and Conti ransomware families.
- Hundreds of thousands of attempts to exploit known vulnerabilities in customer cloud environments.
- Sysrv-hello cryptojacking botnets which continue to be highly active, targeting exposed Jenkins servers.
- Hundreds of thousands of brute force attempts against SSH and RDP.

Why Healthcare Is Targeted More Than Other Industries

There are plenty of reasons healthcare is highly sought after by bad actors. For starters, one healthcare record is valued as much as $1,000, whereas on the dark web the values are typically $5 for credit card numbers and $1 for social security numbers. However, the reason healthcare is such a target is much more complex than just the value of an electronic health record. For example:

Healthcare Operates on Outdated and Vulnerable Systems

Most healthcare providers use outdated IT infrastructure. It is estimated that more than half of medical devices operate on legacy systems and many healthcare organizations use outdated operating systems that can no longer be patched, such as Microsoft Windows 7 and Windows Server 2008.

Consumerization, Data Liquidity, and Lack of Data Inventories

Healthcare consumerization greatly accelerated during the pandemic and is not slowing down. The demand for data liquidity - or health data flow and access - is increasing at an exponential pace. Key drivers are virtual care, the acceleration of interoperability standards, the realities of the digital front door, and the rise of new retail health providers.

In this complex setting, one of the first things a privacy officer attempts is creating a map of the sensitive data they are charged with protecting. Now a petabyte problem, this effort quickly becomes futile as data sprawl expands beyond the boundaries of the providers' systems. In both structured and unstructured formats, the data journey takes on a life of its own as it traverses healthcare treatment, payment, and operations activities.

In addition to unpredictable data flow, the journey to the cloud compounds the issue with complexities such as automated scalability. Quickly the privacy officer is left with limited information about the data lifecycle, including where it flows and who or what has access.

Disruption in Healthcare

Healthcare data shared at the right time with the right users saves lives. Disrupt that flow and patient safety becomes an issue where death can occur. This was case in a ransomware attack in 2020 that crippled a German hospital, resulting in a death after the hospital redirected the ambulance more than 20 miles. Most recently, a lawsuit surfaced from a U.S. ransomware attack in 2019 that contributed to the death of a baby several months later. The attack made critical information and technology unavailable during the child's birth, causing significant complications. ***We know ransomware is a patient safety issue, and unfortunately, so do cybercriminals.***

Because the cybercriminal's mission is to generate cash, they want their money fast, with certainty and consistency. In addition to being vulnerable, the healthcare sector is motivated to recover from an attack as quickly as possible. But due to antiquated IT systems, many healthcare organizations cannot recover well or at all. So, criminals attack healthcare organizations believing they will receive payments more quickly than other industries.

Lack of Cybersecurity Awareness and Training

Hospitals in the past have not focused on cybersecurity in general, but rather focused more on general HIPAA compliance, ensuring that employees meet the federal requirements for protecting patient privacy.

How to Plan for a Ransomware Attack

Both **prevention** and **response** rely upon people, process, and technology. It's critical that your organization plans for an attack rather than just to prevent it. Preparation can help minimize the damage of a successful ransomware attack.

People

Human error continues to be one of the top causes of breaches, and in healthcare, it accounts for nearly one third of breaches. Here are a few tips to reduce incidents caused by an insider.

- Train your workforce to be more aware of phishing, safe browsing, irregular system activity, social engineering, remote working, and working in public places.
- Learn from others ransomware attacks. There are several resources available through organizations such as Cybersecurity & Infrastructure Security Agency (CISA), MITRE ATT&CK, FBI: InfraGard, the SANS Institute, (ISC)2 and many others.
- Conduct disaster recovery tests on a frequent, regular basis.
- Know how to quickly report an incident with as much specific information as possible.
- Have an incident response plan in place. Create runbooks, share it among executives, and practice your incident response plan.

Process

Process is vital to arming yourself against ransomware attacks. Here are some tips on processes to put into place to tighten your security.

- Maintain offline, encrypted backups. Regularly test them.
- Retain back up hardware.
- Ensure the availability of application source code or executable code and store it with backups, escrowed, or other air-gapped means.
- Regularly scan for vulnerabilities and remediate findings.
- Properly configure and harden devices.
- Disable or block Server Message Block (SMB) protocol outbound and remove or disable outdated versions of SMB.
- Regularly patch and update software & operating systems.
- Establish baseline system behavior patterns.
- Enforce strong password security.
- Use multi-factor authentication.
- Whitelist applications.
- Restrict access where it is not necessary and don't forget to immediately revoke access when an employee leaves the organization.
- Label assets that have sensitive data.
- Know and manage your data lifecycle.

Technology

Again, outdated technology, operating systems, and servers that are overly abundant in healthcare make it easy for a bad actor to find an entry point into your network. Here are a few tips on how to improve your security posture with the use of technology regardless of what operating systems and servers you are using.

- Tune your Security Information and Event Monitoring System (SIEM) to watch for known Indicators of Compromise (IOCs) with automation if possible.
- Deploy and use VPN for remote connectivity to hide your IP address. Ensure VPN servers are hardened, maintained, and regularly patched.
- Segment your network.
- Use endpoint protection to prevent malware and detect malicious activity.
- Harden email to avoid being a victim of a phishing scheme.
- Use ad blockers and block script executions.
- Display file extensions to help you identify ransomware variants when responding to an attack.
- Ensure devices automatically go offline in case of a threat.
- Deploy edge and host-based firewalls.

Responding to & Recovering from a Ransomware attack

First, take a deep breath and try to stay cool, calm, and collected. Time is of the essence and being prepared is essential. Responding to a ransomware attack is different than responding to other cyberattacks and preparation with the right e approach is key to a successful recovery. Here are some tips to ease the pain when a ransomware attack happens.

Isolate — As soon as humanly possible, isolate the infected system by disconnecting it from the network.

Identify — Determine the type of ransomware and the scope of the infection. Identify which systems are affected. Be sure to take copious notes about the issues that you noticed, when it occurred, what systems were you using, and what were you doing at the time you detected the abnormalities.

Contact — Immediately report the attack to your helpdesk team. They should be trained to escalate the issue to the incident response team. Bring the CISO in during early stages of the investigation and communicate with leadership per procedure. Communicate with internal and external legal counsel per procedure, including discussions of compliance, risk exposure, liability, law enforcement contact, etc. Also, communicate with internal users, customers, cyber insurance providers, and security and IT vendors. Consider notifying and involving law enforcement when the time is right.

Contain & Remove — Find the infection vector and contain it as quickly as possible. Quarantines (logical, physical, or both) prevent spread from infected systems to critical systems and data. Quarantines should be comprehensive – include cloud/SaaS access, single-sign-on, system access to enterprise resource planning (ERP), or other business tools, etc.

Analyze — Determine the scope of the infection and assess its impact. Determine the impact to confidentiality, integrity, and availability of data, and how it will affect your business and customers. Assess how sensitive the data is (e.g., is the data PII or PHI). Use this information to prioritize and motivate the appropriate response resources.

Eradicate & Remediate — Restore infected systems and from known-clean backups. Confirm endpoint protection and patches are up to date. Deploy custom signatures to endpoint protection and network security tools based on the discovered indicator of compromise.

Recover — Launch business continuity/disaster recovery plan(s): e.g., consider migration to alternate operating locations, fail-over sites, or backup systems. Check backups for indicators of compromise and consider partial recovery and backup integrity testing. Also, find and try known decryptors for the variant(s) discovered using resources like the No More Ransom! Project's Decryption Tools page.

Conclusion

Ransomware is going to continuously evolve and become more sophisticated and prolific. The consequences are costly, and more importantly, in healthcare it is a threat to patient safety. Now is the time to prepare your organization for when, not if, an attack occurs.

View our detailed whitepaper with specific recommendations to respond and recover from a ransomware attack.