THREAT INTELLIGENCE SPOTLIGHT

Code Grey: Building Cyber Resilience for Healthcare Delivery Organizations

eSENTIRE
Threat Response Unit

Introduction

Healthcare Delivery Organizations (HDOs), including hospitals, clinics, and private practices, store valuable information and deliver essential services – two attributes that make them appealing targets to threat actors looking to steal patients' medical records and deploy debilitating ransomware that disrupts critical patient care. In addition, HDOs rely on a multitude of digital information sharing processes with the government, other healthcare providers, and ultimately, with their patients.

Unfortunately, the IT environment within an HDO is typically made up of a mix of IoT devices, legacy systems, and a diverse range of applications and software. This makes it even easier for threat actors with minimal technical expertise to use ransomware-as-a-service models to deploy ransomware attacks.

Plus, healthcare staff are focused on their mission critical goal of patient care and generally only have a basic security awareness of cyber threats, making it easy for threat actors to target them with carefully crafted phishing messages and bypass traditional security controls.

As a result, HDOs operate under the constant threat of costly and disruptive cyberattacks. In fact, according to **IBM's Cost of a Data Breach Report 2023**, the healthcare industry has reported the highest costs out of all industries for the 13th year in a row. **Healthcare data breach costs have increased 53.3% since 2020 to an average of $10.93 million USD.**

As the organized cybercrime ecosystem continues to evolve, the combination of motive, means, and opportunity—plus easy access to already-developed tools to execute attacks—has led cybercriminals to relentlessly target HDOs, resulting in an ever-increasing volume of attacks and a range of costly consequences.

Unlike many other industries, patient lives are literally at stake when HDO operations are disrupted by cyberattacks. Disruption of service including emergency care & clinical care, rescheduled surgeries, delayed outpatient care and postponed preventative checkups, all have operational and the potential for human costs.

In this report, we'll explore the cyber threats against healthcare providers, why healthcare is a prime target for cybercrime operators and how healthcare organizations can manage their risk to reduce the likelihood and severity of cybersecurity incidents.

As investment in cybersecurity is committed, it must be elevated to a board-level issue and discussed alongside other business imperatives including growth, continuity planning, and risk and governance, with regular metrics and reporting showing progress toward business outcomes.

Motive, Means, and Opportunity: Why Cybercriminals Target HDOs

Given how effective and lucrative it is to conduct cyberattacks against healthcare organizations, it's no surprise that threat actors are targeting healthcare providers with increased frequency.

Moreover, cybercriminals aren't undertaking much risk when attacking HDOs – despite some high-profile law enforcement operations, ransomware gangs are rarely fully prosecuted. The reasons for this are well documented and include the cross-border nature of the crime as well as the indifference of the governments of the countries from which most attacks originate.

At the same time, the rewards of a successful attack are high, especially when threat actors introduce multiple revenue streams by combining ransomware with stealing and selling valuable patient information.

Disabling systems and services, and making crucial information unavailable, continues to generate impressive returns for ransomware operators. Attackers routinely use double- and triple-extortion tactics to compel the victim to pay to recover access to systems and to prevent the publication of PHI/PII (and the possible regulatory fines that may result).

Whether the victim pays the ransom or not, the attacker may still sell stolen data in cybercrime marketplaces:

- **Financial information** is used to compromise bank accounts and commit wire transfer frauds.
- **Employee information** can be used for identity theft, to commit fraud, and to engage in longer, more complex operations like business email compromise (BEC) and highly targeted phishing scams.
- **Patient information** can be used to blackmail individuals—PHI is regarded as being much more valuable than credit card information, with each record worth anywhere from **$10 to $1,000 USD**.

Additionally, intellectual property, confidential, proprietary data, or other sensitive business information can also motivate attackers, especially when an institution has a strong research function.

Rise of the ‘as-a-service’ business models

Ransomware attacks used to be opportunistic attacks used to extort victims for transactional payments so while ransomware attacks aren’t a new threat, cybercriminals are leveraging this attack vector in new and unique ways. Today, we are seeing sophisticated, coordinated state-sponsored adversaries target high-value victims and cripple their operations with the increasing use of the ‘as-a-service’ business models.

Ransomware gangs are increasingly relying on Ransomware-as-a-Service and Malware-as-a-Service models for easy financial gain since it lowers the barrier to entry for unskilled cybercriminals to cause chaos and create instability.

Moreover, threat actors are also forming specialized cybercrime gangs to perform different stages of an attack and provide Initial Access-as-a-Service. This allows other cybercriminals to simply purchase this access to deploy ransomware by executing orchestrated campaigns and automated attacks to break into your IT environment, establishing a persistent presence, and performing reconnaissance. Then, using the intelligence gathered, they calculate a market value for the access and sell it on a cybercrime marketplace.

Unfortunately, it can take months, and even years, for businesses to recover from the effects of a ransomware attack. In fact, the threat of ransomware doesn’t end when you recover your IT systems and data from backups. While your team may be able to prevent a ransomware attack, it’s unrealistic to think you can stop every attempt via preventative methods alone.

Shifting to a cloud strategy

Within the past two years, there has been a significant technology advances designed to improve the overall quality of healthcare delivery within the industry that have accelerated cloud adoption.

From the increasing reliance on telemedicine to the use of augmented reality for remote collaboration and training, healthcare business leaders are pursuing cloud-based strategies that allow for greater efficiency, flexibility, and scalability while balancing resource and budget constraints.

However, shifting to the cloud also comes with its own set of challenges. Cloud misconfigurations, lack of complete visibility, and the unaccounted use of cloud platforms can expose the sensitive PII and PHI stored within your cloud, or hybrid, environment to threat actors. In turn, this places your HDO at risk for non-compliance with legal and regulatory requirements, and the financial repercussions that result.

In addition, given the lack of skilled cybersecurity workers, it’s incredibly difficult to find the in-house expertise needed to build, optimize, and manage your cloud environments securely without continuous manual monitoring.

A complex, expansive threat surface

As the leading edge moves forward and the trailing edge lags, the threat surface expands, creating opportunities for attackers. HDOs simultaneously exist at the forefront of innovation and in the past so the effort required to attack a healthcare provider is relatively low.

New equipment and software are regularly introduced, while records are digitized, and cloud migrations create hybrid enterprise environments. All HDOs use an Electronic Medical Record (EMR) system as the hub of clinical practice. These systems track patient data, pharmaceutical dosages, treatments, etc. Healthcare IoT devices and management systems feed the EMR, which is accessed from nursing stations and physician offices, and can automatically alert medical staff when a patient's condition requires immediate care.

At the same time, legacy systems often remain in operation and in many cases, these systems are embedded in critical applications and devices, and cannot be updated. Some have not been restarted in years for fear of system failure.

Further complicating matters, shadow IT—tools, technologies, or applications that are in use but not officially sanctioned—is an ever-present problem that has likely increased due to the COVID-related expansion of remote work. Lastly, patch management is a challenging and operationally intensive activity, so most organizations fall behind, especially since patching is not an option for legacy systems.

While most HDOs have many traditional defenses and security measures in place (e.g., antivirus, firewall, logging, user access controls, network monitoring, IDS/IPS, MFA), few have next-generation antivirus, endpoint detection and response (EDR) and other modern solutions to safeguard against today's threats. One consequence noted by **HIMSS** is that "healthcare cybersecurity professionals often lack visibility into remote endpoints. This is especially true with home computers and personal devices."

As a result, diligent patching, risk assessments and layered defenses become essential elements of the defensive strategy.

Undertrained staff

Most of the devastating cyberattacks begin with a phishing email and while it's common practice to scapegoat employees for their mistakes, or to act like phishing lures are easy to spot, the reality is that cybercriminals are extremely skilled at disguising their lures.

Threat actors are routinely using social engineering tactics such as email thread hijacking, in which the threat actor inserts their malicious emails within legitimate email threads obtained by exfiltrating the mailboxes from compromised hosts. Since the email was formerly part of a legitimate conversation, it is much less likely to arouse suspicion. This tactic has been observed on several occasions to deliver information stealing malware like **Qakbot**.

In addition, the rise of Generative AI technologies also means that non-native English-speaking cybercriminals are using tools like ChatGPT to remove language barriers and craft highly convincing emails that can manipulate users into believing the email is legitimate. Unfortunately, healthcare staff are focused on their mission critical goal of patient care and generally only have a basic security awareness of cyber threats, making it easy for threat actors to target them with carefully crafted phishing messages and bypass traditional perimeter controls.

While cybersecurity awareness doesn't remove the need for policies that prevent malware execution, vulnerability management programs, threat detection technologies, or experts who can quickly respond to eliminate critical cyber threats, it does contribute to a much stronger cybersecurity posture. Therefore, it's imperative that your HDO adopts a culture in which everyone recognizes that they have a role to play as part of the greater cybersecurity program.

From Phishing to Ransomware: Understanding the Healthcare Threat Landscape

Before threat actors can exfiltrate data or deploy ransomware, they must first gain Initial Access into the environment, perform certain Intrusion Actions (i.e., the intermediary steps prior to launching the attack), and execute the Actions on Objective.

As seen in Figure 1, modern threats typically employ a multi-stage approach:

1. A highly automated attack arsenal gains initial access into an IT environment and performs initial reconnaissance. The tactics, techniques, and procedures (TTPs) employed are adept at bypassing perimeter defenses by exploiting both human behavior and unpatched vulnerabilities.
2. Later, a human operator takes over ("hands-on-keyboard") to evade more complex defenses, establish persistence, find critical systems, exfiltrate data, detonate ransomware and perform additional detail work.

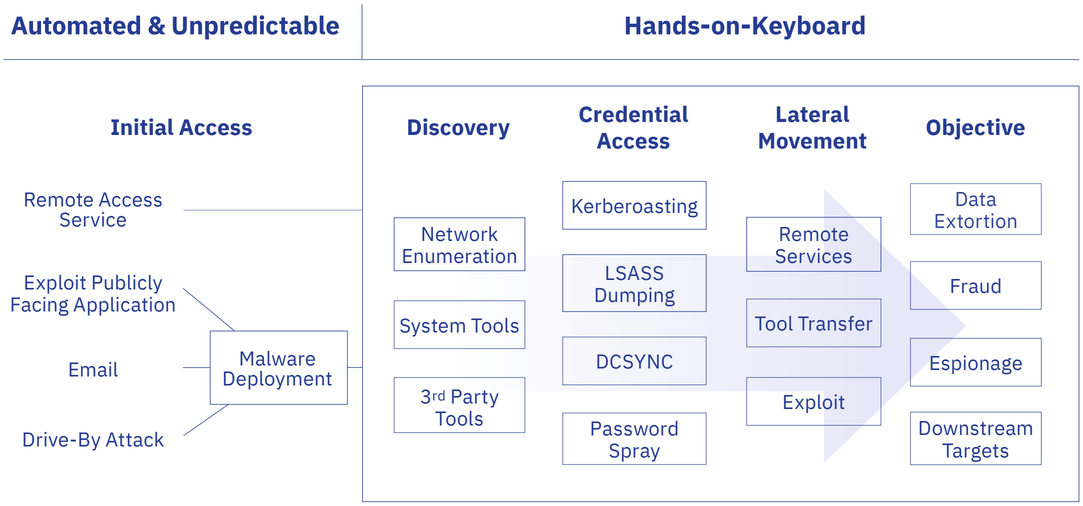


Figure 1 High-level view of the common attack paths

Each stage has its own techniques and actions, and cybercriminals have developed specialized tools, skillsets and working relationships to increase attack efficiency.

Therefore, defending against an attack also means being able to disrupt every stage of the attack workflow.

Reading the warning signs

Today's threat actors are adept at bypassing traditional defenses like firewalls and antivirus systems, often remaining undetected within the environment for days or weeks before 'detonating' ransomware or disabling services.

However, in most attacks, some preparatory work is required before the threat actor can pursue their ultimate objectives, which creates a window of opportunity for skilled cybersecurity practitioners to intervene. **After all, detecting and responding to an attack before it causes a business-disrupting event often comes down to recognizing the subtle signs of an attacker's presence within the environment.**

Over the last 12 months, eSentire TRU detected and responded to more than 45 incidents across our healthcare customers. The most common initial access vectors we observed (Figure 2) in these incidents are:

- **Browsers (62%):** These threats are encountered when employees browse the web. For example, GootLoader employs search engine optimization (SEO) poisoning to hijack search results when employees look for domain-specific forms and template. Solarmarker uses the same approach but doesn't seem to have targeted legal firms as much or as successfully as has GootLoader. Socgholish leverages compromised websites and uses false "out-of-date browser" alerts to trick users into executing the malware, while AsyncRAT largely relies upon HTML smuggling to execute malicious code.

- **Email (25%):** These threats arrive in email inboxes disguised as typical business communications with subjects like "Invoice" and "Signature Required." To bypass email filters, these malware strains often wrap malicious documents (e.g., Word or Excel files that use macros to execute malicious commands) and other files (e.g., LNK, ISO) in a password-protected .zip archive. Additionally, to increase the chances of a user unwittingly aiding the attacker, several malware strains (e.g., Qakbot) are known to hijack and replay older email threads, sometimes from known business partners.

- **Removable Media (13%):** These threats gain access into your environment with the use of removable media devices, such as USB drives and even mobile devices. Adversaries can load hide malware within PDF files or media files that are designed to 'auto-run' when executed.

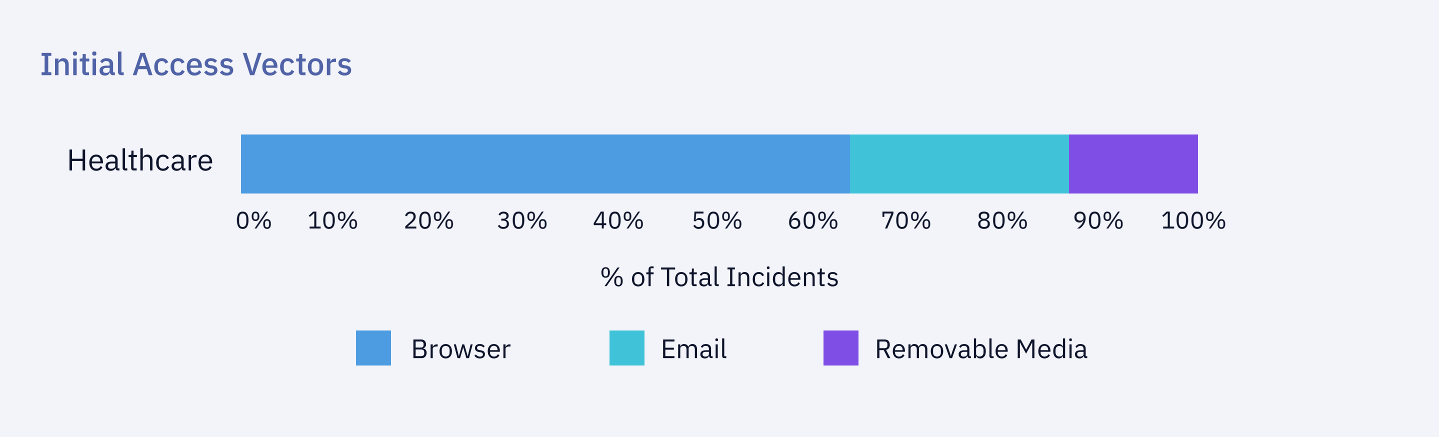


Figure 2 A breakdown of Initial Access tactics observed by TRU targeting eSentire healthcare customers.

Examining intrusion ratios

Overall, in around 70% of these incidents, the attack was stopped at the initial access phase. **However, in nearly 30% of the incidents, the attack had already progressed to the point where a hands-on operator was likely manually executing the intrusion actions.** For example, an infected endpoint may have been weaponized successfully to exploit internal resources.

This finding suggests that healthcare organizations are slower to contain cyberattacks and/or more susceptible to targeted cyberattacks compared to other critical infrastructure industries across our global customer base such as construction, utilities, transportation, and government (Figure 3).

Looking at the ransomware intrusion ratio specifically – that is, only factoring threats known to be associated with ransomware – the data shows a similar finding as that for the overall intrusion ratio.

Out of all the ransomware-related incidents, only about 17% progressed to the intrusion actions or actions-on-objectives stage (Figure 3). In these cases, only the timely threat detection and response actions from our 24/7 SOC Cyber Analysts prevented operational disruption.

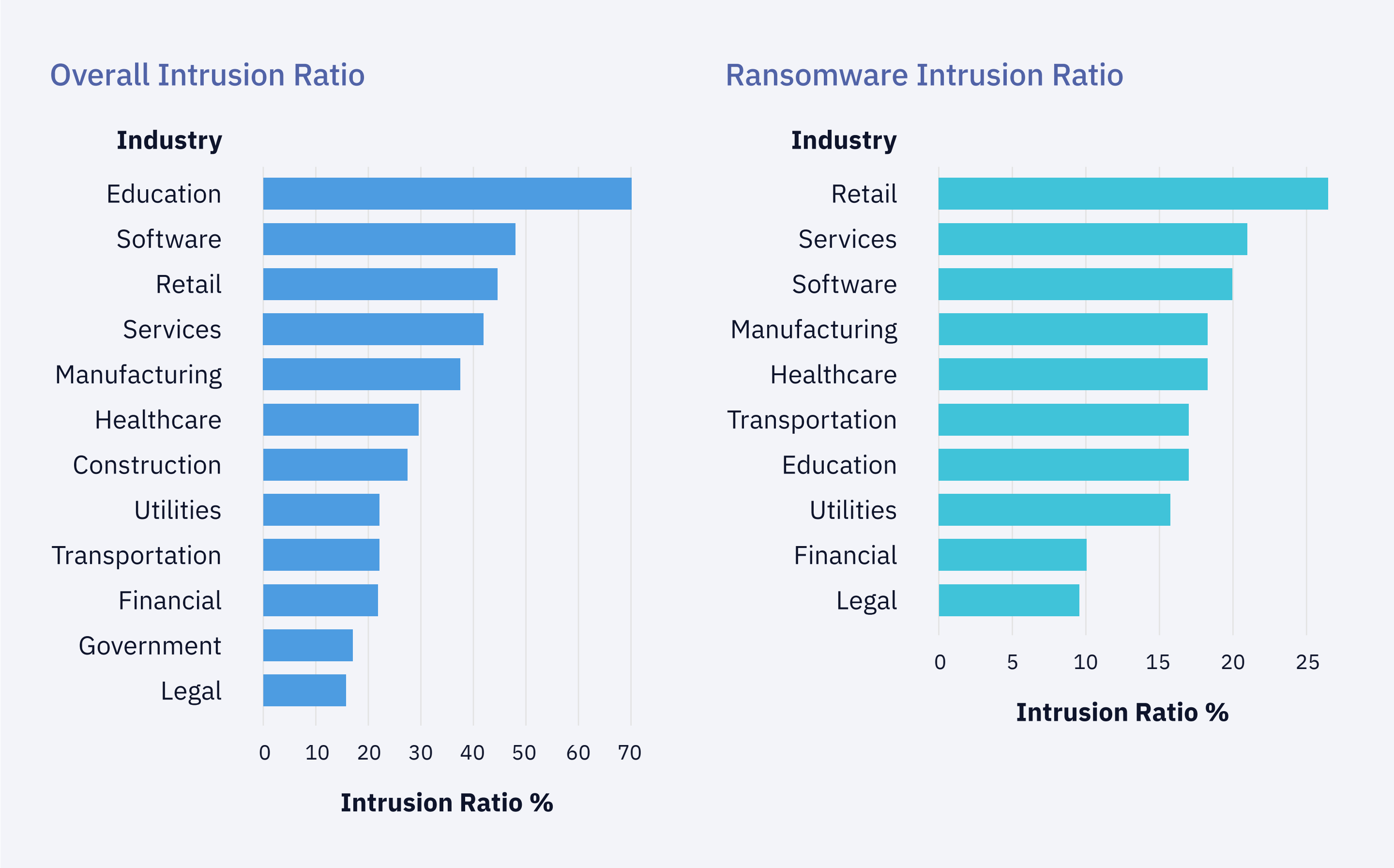


Figure 3 The percentage of attacks that progressed beyond initial access for our healthcare customers in comparison with other industries we protect.

Breaking down the threats

Figure 4 shows the incidents within our HDO customer base in which the attacker successfully bypassed existing client defenses before being detected by our team of 24/7 SOC Cyber Analysts and Threat Response Unit (TRU).

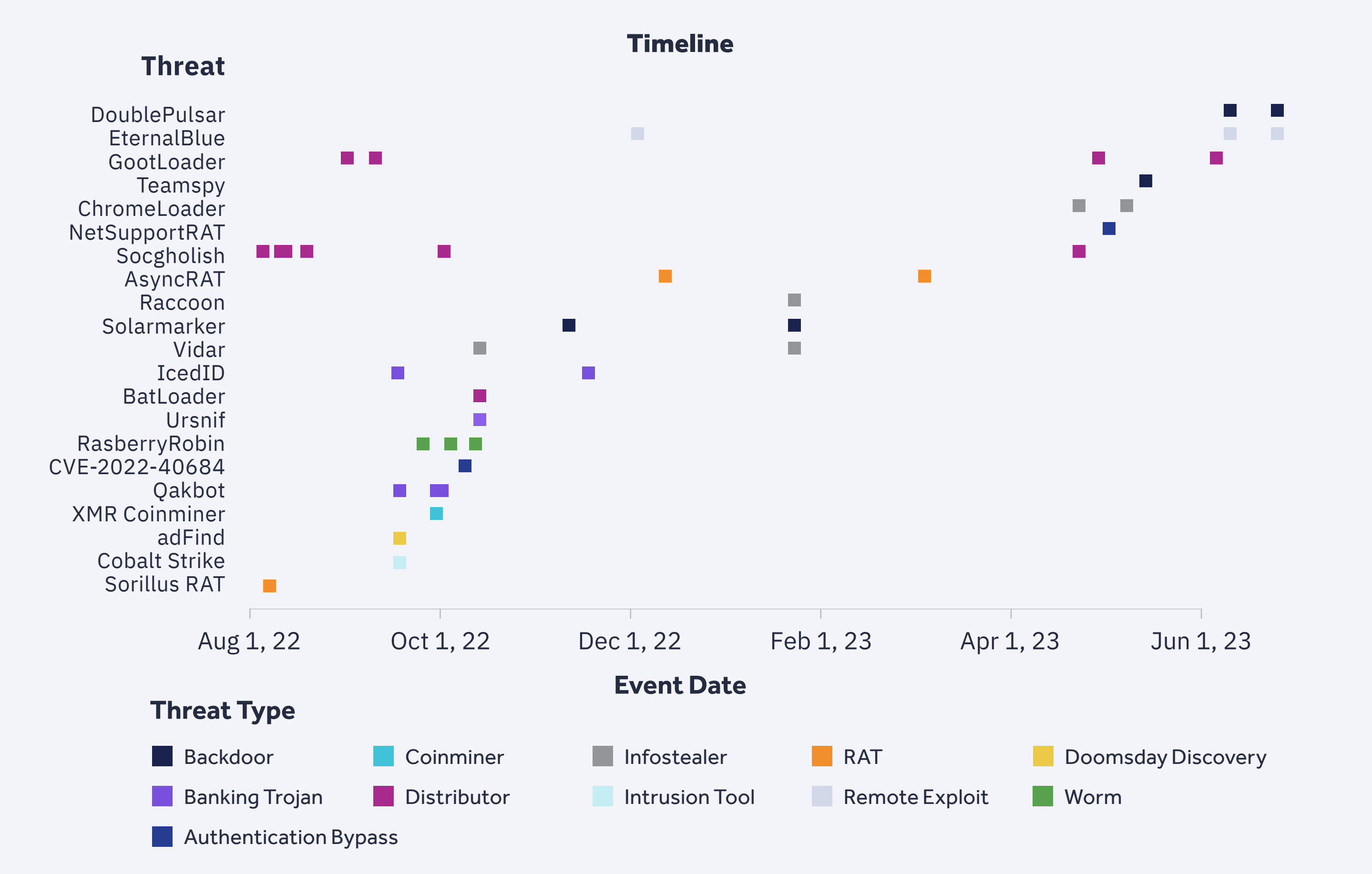


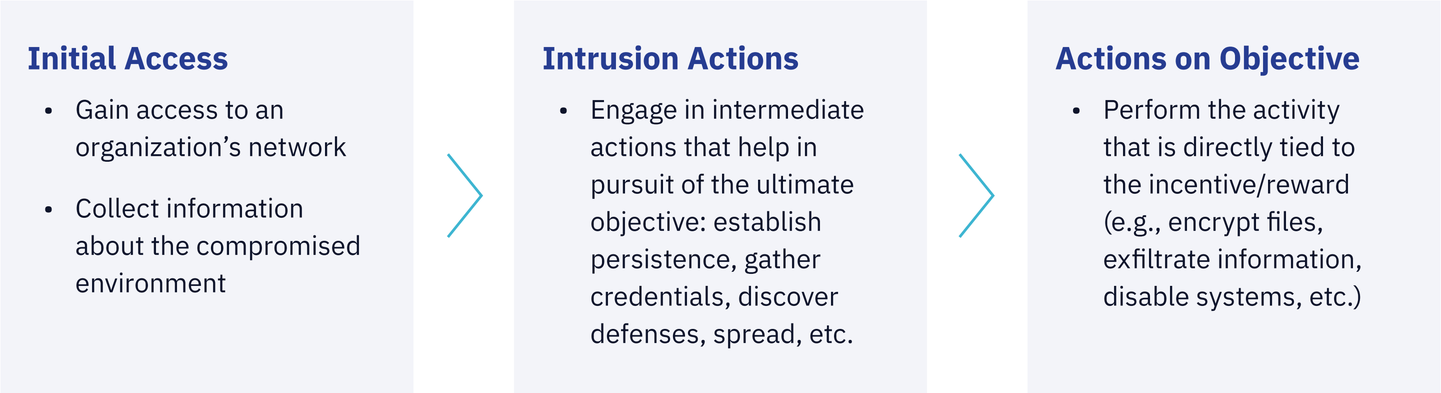
Figure 4 Detecting and responding to threats that bypass existing defenses is crucial to minimizing the impact of incidents

Taking a deeper look at the attacks impacting our healthcare customers, we see that a significant use of malware that leverages browser-based attacks, such as GootLoader, Solarmarker, Socgholish, Batloader, and Chromeloader:

- **GootLoader and Solarmarker** both leverage a social engineering tactic known as search engine optimization (SEO) poisoning, in which users are served malicious results after performing a search on websites like Google or Bing.
  - Gootloader is known to target legal language, often when users are searching for specific contract or agreement templates, while Solarmarker tends to target users looking for technical how-to documents.
- **Socgholish** is a watering hole attack that poisons known or trusted sites. When unsuspecting users visit a poisoned site, their browsing is interrupted with a warning claiming they need to update their browser but are instead served malware.
- **Batloader** often leverages Google Ads to appear in search results for common generative AI technologies like ChatGPT and Midjourney.
- **Chromeloader** is a type of adware that intercepts web traffic and pushes advertisements that deliver malicious ISO files. Once downloaded, it can read the browsing history, manage apps and extensions, manipulate webpage content, and more. It also blocks any attempt to edit Chrome extensions so users can't remove the extension.

GootLoader, Socgholish, and Batloader – all of which are distributor malware – make up 13 of the total 45 incidents impacting our healthcare customers. Distributors specialize in delivering malware into client environments; they often propagate additional malware such as banking trojans, backdoors, and infostealers.

Solarmarker, on the other hand, is a backdoor malware that allow threat actors to remotely send commands, load additional malware or directly access a system, and establish persistence in the compromised environment.



Initial Access

- Gain access to an organization's network
- Collect information about the compromised environment

Intrusion Actions

- Engage in intermediate actions that help in pursuit of the ultimate objective: establish persistence, gather credentials, discover defenses, spread, etc.

Actions on Objective

- Perform the activity that is directly tied to the incentive/reward (e.g., encrypt files, exfiltrate information, disable systems, etc.)

Figure 5 Simplified attack workflow

Given that all four malware are deployed via browser-based attacks, they are used to gain Initial Access into your environment so threat actors can progress to performing Intrusion Actions and then Actions on Objectives to deploy ransomware or other infostealer malware.

Chromeloader, on the other hand, is an infostealer that finds and exfiltrates sensitive data, but is typically configured to target credentials, machine fingerprints, banking information, and more. This malware is typically seen only after threat actors get to the final Actions on Objective stage.

Recommendations to Build Resilience Against Ransomware and Prevent Operational Disruption

A successful ransomware attack or data breach can result in major operational disruption, lasting reputational damage, and significant legal and regulatory repercussions.

The first step in building cyber resilience across healthcare delivery organizations in today's threat environment is to adopt the mindset that your goal isn't just to reduce cyber risk – it's to build real resilience.

This means you must have the capabilities to anticipate, withstand, and recover from the most sophisticated cyber threats.

Although there are no magic-bullet solutions, one essential element is to establish a culture in which cybersecurity is taken seriously — ideally championed by the extended leadership team and carried through the entire organization.

$244,267

Average daily cost of downtime for healthcare delivery organizations

78%

Of data breaches impacting HDOs were from hacking and IT incidents

$10.1M

Average daily cost of downtime for healthcare delivery organizations

To build a strong defensive posture, we recommend implementing specific controls to help prevent common ransomware and malcode execution techniques, improve your ability to respond & recover from a cyberattack, and reduce your overall cyber risk:

1. Identify and audit critical systems and data.
2. Understand your legal, regulatory, supply-chain, and client obligations.
3. Establish cybersecurity policies, procedures, and executive reporting mechanisms.
4. Conduct an annual risk assessment and security readiness exam.
5. Require encryption of stored data (mobile devices, laptops, servers, etc.).
6. Establish mobile and bring-your-own-device (BYOD) rules and controls to enforce strong passwords and limit access to corporate assets.
7. Establish back-up systems and services, and test restoration/recovery procedures. Pay particular attention to domain controllers, as they are prize targets of threat actors.
8. Establish an incident response plan (IRP) and team, and practice fire drills to hone your program.
9. Consider cyber insurance to cover investigation, disruption, lost revenue, and other costs not covered in non-cyber specific policies.
10. Implement a **Phishing and Security Awareness Training (PSAT) program** that educates the employees about the threat landscape.
    - Ensure there are processes in place for employees to browse the web for free examples of templates and contracts, and downloading free software from the official vendor site.
    - Train users to recognize ‘normal’ file extensions from ‘abnormal’ extensions.
    - Encourage your employees to use password managers instead of using the password storage feature provided by web browsers.
    - Stay up to date on the **latest threats and trends** impacting the threat landscape.
11. Always display file extensions for known file types.
12. Leverage Group Policy or PowerShell to enable attack surface reduction rules that prevent scripts downloaded from the internet from firing.
13. Use **Windows Attack Surface Reduction rules** to block JavaScript and VBScript from launching downloaded content.
14. Employ an **Endpoint Detection and Response (EDR)** tool on user workstations to detect and isolate threats before they spread laterally.
15. Implement a **Log Monitoring solution** since VPN logs and domain controller logs can help to track intruder movements from endpoint to endpoint,
    to identify initial access, and to help determine when the attacker has obtained domain administrator privileges.
    - In recent attacks, intruders have been observed registering their own virtual machine in the VPN pool; when attackers do this, their IP cannot be differentiated from other IPs in the VPN pool and VPN logs are required to identify their true IP.

We also recommend extending beyond the fundamentals of a multi-layered cyber defense strategy and adopting a risk-based approach to cybersecurity that includes:

- ✓ **24/7 Managed Detection and Response (MDR)** with multi-signal attack surface coverage, powered by a strong XDR platform foundation and human expertise, to identify, contain, and respond to threats that bypass traditional security controls.
- ✓ **Digital Forensics and Incident Response (DFIR)** expertise through the engagement of an incident response provider on retainer who can support with Security Incident Response Planning, and Emergency Preparedness as well as incident response, remediation, digital forensics investigation, root cause analysis and crime scene reconstruction in the event of a severe incident or breach.
- ✓ **Vulnerability Management program** that includes continuous awareness of the threat landscape, vulnerability scanning to understand which systems are inadvertently exposed, remediation, and additionally, disciplined patch management.
- ✓ **Phishing and Security Awareness Training (PSAT)** for all employees to build a culture of cyber resiliency by leveraging a context-relevant training program and driving organizational behavioral change. This helps take away one of the threat actors' most common attack vectors.

It's clear that cybersecurity needs to be a board-level issue, alongside concerns like business growth, continuity planning and governance, with regular metrics and reporting showing progress toward business outcomes. It should also be regarded as a proactive investment in risk management and harm reduction, rather than a cost.

Ideally, this shift in perception will help to address one of the biggest roadblocks to building cyber resilience within HDOs: small security budgets. It's worth reiterating that these budgets are often static, while the rate of cyberattacks and the cost of their consequences are roughly doubling each year.

Most importantly, HDO leaders must recognize compliance does not equal protection.

Meeting the standards of HIPAA, PIPEDA, PCI, and other regulatory frameworks is related to—but very much separate from—creating a strong security posture.

Ready to get started?

Connect with an eSentire Security Specialist to learn how eSentire Multi-Signal MDR, powered by our XDR Cloud Platform, can help you build a more resilient healthcare organization and prevent disruption.

CONTACT US

IF YOU'RE EXPERIENCING A SECURITY INCIDENT OR BREACH CONTACT US ☎ 1-866-579-2200

eSENTIRE

eSentire, Inc., the Authority in Managed Detection and Response (MDR), protects the critical data and applications of 2000+ organizations in 80+ countries, across 35 industries from known and unknown cyber threats by providing Exposure Management, Managed Detection and Response and Incident Response services designed to build an organization's cyber resilience & prevent business disruption. Founded in 2001, eSentire protects the world's most targeted organizations with 65% of its global base recognized as critical infrastructure, vital to economic health and stability. By combining open XDR platform technology, 24/7 threat hunting, and proven security operations leadership, eSentire's award-winning MDR services and team of experts help organizations anticipate, withstand and recover from cyberattacks. For more information, visit **www.esentire.com** and follow **@eSentire**.