cloudticity

Ransomware Detection: Strategies for Identification and Response

POSTED May 23, 2024 | Author Josh Ray, tagged in ransomware

For healthcare organizations, ransomware continues to be a major threat. Attackers know that if they can hold patient data hostage and disrupt critical services, they might successfully pressure organizations into paying large ransoms.

How can your organization prevent attacks and minimize the damage when ransomware hits? Implementing effective ransomware detection tools and strategies can help you find infections early and stop their spread before they do serious damage.

What Is Ransomware and How Does It Work?

Most healthcare organizations are familiar with the general concept of ransomware today. But understanding more precisely what it is and how it works is an essential first step in improving detection.

Definition of ransomware and its malicious intent

Ransomware is malicious software—or “malware”—designed to encrypt sensitive data or lock authorized users out of essential systems. Attackers demand a ransom in exchange for providing a decryption key or restoring access to systems. In recent years, attackers have increasingly added threats to exert greater pressure on victims: They often threaten to steal and sell data or to attack partner organizations.

Common delivery methods

Many ransomware attacks begin with phishing. Attackers send emails or text messages to employees, trying to trick them into clicking on a link to a spoofed website. If employees enter login credentials, attackers can steal those credentials and gain access to the enterprise network, where they can implant the ransomware.

Alternatively, attackers might try to get employees to download ransomware disguised as legitimate email attachments. Or they might inject malicious scripts into websites, forcing a download of software when the employee visits the site. In both cases, ransomware then spreads from an individual device to the enterprise network.

Attackers sometimes succeed in infecting networks with less inadvertent assistance from employees. They might launch network intrusion attacks or otherwise exploit network vulnerabilities.

Encryption process and locking access to systems

Once the ransomware reaches its target, it begins encrypting files and replacing the originals with the encrypted versions. When they are able to, many attackers also attempt to encrypt backup copies of files.

“Locker” ransomware locks users out of systems instead of encrypting files. This type of ransomware could change a password or PIN, or modify the master boot record. Users might see a lock screen and ransom note, and have no way to access the system. If the attackers set a new, randomly generated password or PIN, it might be impossible to recover data on the system.

The Importance of Early Ransomware Detection

The earlier you can detect ransomware, the better chance you have to contain the threat and prevent large-scale disruptions.

Prevent further spread to and within the network

In some cases, ransomware initially infects an individual employee’s system. If you can detect ransomware on a single desktop, laptop, or mobile device, you can quickly disconnect the system from the network or shut it down.

Once ransomware infects a network system, you still have an opportunity to mitigate potential damage. If you have implemented role-based access controls, for example, you might be able to stop an attacker from using stolen credentials to access repositories with sensitive data. Similarly, network segmentation can help restrict lateral movement of ransomware through your environment.

Minimize data loss and system downtime

Early detection can minimize data loss and system downtime by limiting the infection to fewer, less-mission-critical systems. Ransomware might reach a shared collaborative workspace, for example, but be unable to access the database where you store patient information. Or you might be able to halt its progress before it disables a patient portal. Though you might lose some productivity or need to take some systems offline, you can continue essential operations.

Avoid costly ransom payments

Importantly, early detection can help you avoid having to pay costly ransoms. Attackers that reach your most sensitive data and mission-critical systems might demand millions of dollars to restore your access. And given the urgency of resuming normal operations, you might be tempted to pay. If you can spot and stop ransomware before it encrypts files or locks you out of systems, you can eliminate one of the largest potential costs of the attack.

Signs of a Ransomware Infection

How do you detect a ransomware infection? Though there are multiple ransomware variants in circulation at any given moment, many of them display similar signs in individual computers and network environments.

Unusual system behavior

On individual systems, unusual behavior could be a sign of a ransomware infection. Users might experience slow performance, software crashes, operating system freezes, or rapidly decreasing storage space. They might notice that their usual web browser has a new toolbar or that URLs are redirecting to odd pages. And they also might have trouble logging into cloud-based apps.

At the network level, administrators might first observe a spike in phishing emails across the company or numerous attempts to access network resources. Once infection has occurred, they might see attempts to disable access directories or domain controllers. Data backup activity could increase rapidly if the backup system tries to back up newly encrypted files.

Inability to access files or applications

As the ransomware encrypts files, users will lose access to them. They might notice that file names have new extensions and then be unable to open or use them. It's possible that users won't be able to find the files at all if attackers move them.

When attackers employ locker ransomware, team members might find that their passwords no longer work. Or they might be greeted with a ransom note as they first start up their computers.

Presence of ransom notes or messages

A ransom note is a clear sign of a ransomware attack. Attackers using locker ransomware might display that note front and center when someone logs into an individual system. Or IT administrators might discover notes among files within an infected system. Some attackers might otherwise send emails or text messages notifying victims of the attack and providing ransom payment instructions.

Signature-Based Ransomware Detection

IT or security teams might first become aware of ransomware when an intrusion detection system (IDS), web application firewall (WAF), anti-virus solution, or another tool detects the signature of malicious code.

Identifying known ransomware signatures or patterns

Signature-based detection tools scan files or network traffic and try to match what they see with known viruses, malware, or patterns. When suspected malware is detected, the tool can quarantine it—blocking it from spreading—and then alert administrators.

Regularly updating signature databases

Signature-based tools rely on continuously updated databases of known signatures. Those databases should be updated by external security experts or tool vendors as soon as new ransomware variants are discovered. Without the latest known signatures, new variants can evade detection.

Behavior-Based Ransomware Detection

While signature-based methods require a library of known digital fingerprints, behavior-based ransomware detection identifies atypical behaviors.

Monitoring system activities and file access patterns

Behavior-based tools—such as user behavior analytics (UBA) or user and entity behavior analytics (UEBA) tools—monitor system activities, file access patterns, and user activities to establish a baseline of normal, typical behaviors. These tools might find, for example, that particular users generally log into certain applications from the same location every day, between the same hours.

Identifying suspicious behaviors

Once typical behavior is understood, these tools can identify atypical behaviors. For example, a tool might see that one user's credentials are being employed to login from a new location, in the middle of the night. It might also detect rapid encryption of files or a spike in network traffic that suggests someone is downloading files to an external system. The tool can then alert administrators and begin an automated response, which might include requiring multi-factor authentication (MFA) or stopping downloads.

Machine learning and heuristic analysis techniques

Behavior-based detection tools can use machine learning and heuristic analysis capabilities to enhance its detection capabilities. Machine learning enables the tool to quickly identify new patterns that might be suspicious. Heuristic analysis examines code, looking for something suspicious in software that is not yet known to be malware.

Network Traffic Anomaly Detection

Network traffic anomaly detection is a form of behavior-based detection that focuses on network traffic.

Establishing baseline network traffic patterns

Network anomaly detection tools first set the baseline for typical behavior. For example, users might usually transfer no more than 10 GB of data during certain hours of the day. Backup systems might normally transfer larger amounts after work hours, sending data to a backup location.

Identifying suspicious data transfers or other atypical activity

A network anomaly detection tool might use machine learning to detect deviations from typical patterns. For example, it might spot large data transfers to an atypical remote location, which could signal an attacker is trying to steal data. Or it could identify an unusual amount of traffic coming into remote desktop protocol (RDP) or server message block (SMB) ports. Strange outgoing traffic might indicate that ransomware is contacting an external command-and-control server.

Incident Response and Recovery

Detecting ransomware is only part of the battle. To combat infections, your organization needs to have a plan in place for incident response and recovery.

Contain the infection by isolating systems and devices

The first step in incident response is to contain the infection. Isolate systems by severing the connection between them and the rest of the network, shutting systems down if necessary. Without a conduit to the network, ransomware will be unable to harm your sensitive data and critical systems.

Restoring data from backups

Even if the ransomware has reached its target destination, you might be able to avoid major disruptions. If your organization has continuously backed up data—and that backup data has not also been infected—you could restore the backup data to clean systems. Failing over to redundant systems would be even better: You could avoid service disruptions while you disinfect and wipe clean infected systems.

Reporting Ransomware Attacks

Healthcare organizations and other businesses might be reluctant to admit they were victims of a cyberattack. After all, this type of publicity could steer away customers or patients. Still, there are legal obligations to report attacks. Moreover, reporting can help law enforcement agencies catch criminals, enable other organizations to better prepare for attacks, and help governments better understand the severity of threats.

Reporting incidents to relevant authorities

If you are attacked, you need to report the incident to law enforcement and regulatory authorities. Healthcare organizations that are subject to HIPAA rules and experience a breach of patient data must **report the incident** to the U.S. Department of Health and Human Services (HHS).

Your organization will also need to notify customers or patients whose data might have been exposed. Then you'll need to offer identity protection services to those individuals for a time after the event.

Gathering evidence and documenting the attack

As your teams respond to and recover from an attack, gather all evidence that could be useful in a law enforcement investigation. Document the source and pathway of the attack, the number of infected devices, the variant used (if you can determine it), the number of files affected, and the systems targeted. Collect the ransom note, messages from attackers, and any files that could be used as signatures that identify the attackers.

To Pay or Not to Pay: Ethical and Legal Considerations

When organizations are attacked, they face a difficult decision about whether or not to pay the ransom. Paying the ransom is often the fastest way to restore access to data and systems—and consequently, many healthcare organizations do pay. Still, there are multiple risks and legal implications to consider.

Potential risks of paying the ransom

The high cost of the ransom—which could amount to millions of dollars—is one good reason to refuse payment. But there are important risks you should consider if you are contemplating paying. For example, paying the ransom does not guarantee that you will actually recover data or regain access to systems. Cybercriminals have little incentive to help you once you've given them what they want.

There are also ethical considerations. Paying a ransom rewards criminal behavior. As more organizations give in to attackers' demands, more criminals will launch attacks.

Legal implications and regulations surrounding ransom payments

Many governments and law enforcement agencies discourage the payment of ransoms. The International Counter Ransomware Initiative—which includes members from 48 countries, the European Union, and Interpol—released a joint policy statement saying that governments should not pay ransomware extortion demands. The United States **signed** the statement. Still, the statement does not exclude companies from paying, and the U.S. federal government has not banned companies from paying.

Organizations do, however, have a legal responsibility to protect sensitive data. If attackers steal and sell patient data, for example, a healthcare organization would be subject to regulatory fines and could also face lawsuits.

Preventive Measures and Best Practices

In addition to developing an incident response plan, healthcare organizations and other businesses should implement preventive measures and best practices to reduce the odds of successful attacks.

Implementing regular backups and data recovery strategies

Data backup and recovery strategies are critical for defeating ransomware attacks and quickly resuming normal operations. If you can maintain a complete, up-to-date copy of data—in an environment that cannot be reached by attackers—you can dramatically reduce the need to pay ransom. If attackers encrypt your primary database or data storage environment, you can restore clean data to uninfected systems and get back to business.

Keeping software and security solutions up to date

Cybercriminals are continuously searching for vulnerabilities in operating systems, applications, and security solutions. Keeping all software up to date can help you avoid being a victim. Make sure you reach all systems with updates and patches: A single unpatched system could enable an attacker to access your network.

Employee awareness and training on cybersecurity threats

Employees are often the inadvertent vector for attacks. Educating them on how to identify phishing attempts and ransomware infections can help you detect and defeat attacks early. They should know what to look for and who to contact if they experience anything suspicious. At the same time, they should be aware of how important early detection is to avoiding devastating consequences for your organization and your customers.

Emerging Trends and Future Challenges

Cybercriminals continue to develop new schemes and incorporate new tactics into their attacks. To prevent large-scale incidents, you need to stay up to date on the latest trends.

Evolution of ransomware tactics and techniques

Artificial intelligence (AI) will likely play a key role in future ransomware attacks. Attackers are already using generative AI to write better phishing emails. In the future, they might integrate AI into ransomware to evade detection methods in real time.

Meanwhile, attackers have also employed Ransomware-as-a-Service offerings to launch new malware variants without having to write any code themselves. The separation of ransomware development from attacking has contributed to the proliferation of attacks in recent years.

Advancements in detection and mitigation technologies

Fortunately, emerging technologies, such as AI and machine learning, are also available to cybersecurity solution vendors and consultants. Behavior analysis tools are already using machine learning to identify suspicious patterns. In the near future, these technologies could analyze greater volumes of available data to identify new trends faster. AI could also play a role in automated responses to attacks.

Sharing information and collaborating with partners

Your organization is not alone in facing the threat of ransomware. Sharing information about cybersecurity tools, best practices, and incidents can help all organizations prevent attacks and mitigate damage.

In many cases, healthcare organizations will also benefit from partnering with external cybersecurity consultants and managed service providers. These organizations can draw on threat intelligence, deep expertise, and client experiences to help you develop customized plans, implement the right tools and best practices, and then carry out your incident response if an attack occurs. You can optimize your defenses while keeping your teams focused on strategic goals.

How Cloudticity Can Help

Cloudticity has been managing and securing healthcare data in the public cloud since 2011 and we've never had a breach. With our **ransomware protection services**, part of our **managed security services**, we can help you implement a ransomware detection and response strategy, while taking much of the security burden off of your team.

Ready to learn more about ransomware detection? Cloudticity can help. Cloudticity can help. Reach out today for a **free consultation**.

TAGGED: ransomware

COMMENTS (0)

SUBSCRIBE TO BLOG

« Previous Post

Back To Blog

Next Post »

Connect With Us
1301 Spring St, Ste 25i
Seattle, WA 98104

855.980.2144

contact now

f in X

HIPAA/HITRUST

HIPAA

HITRUST

Managed Cloud

AWS Services

Azure Services

Google Cloud Services

Security Services