Ransomware Realities: It is When Not If You are Attacked

by DCIG President and Founder, Jerome M Wendt

Ransomware attacks have escalated to the point that over 50 percent of US businesses reported an attack in the past twelve months. Continuing changes in ransomware's attack methods make it a matter of when, not if, organizations experience an attack. While concerning, best practices exist that organizations can implement to detect, stop, and recover from an attack. Using a combination of cybersecurity software, object-based network storage, and backup software, organizations can keep ransomware at bay.

NASUNI

COMPANY

Nasuni Corporation
One Marina Park Drive
6th Floor
Boston, MA 02210
(857) 444-8500

www.nasuni.com

INDUSTRY

Information Technology

RANSOMWARE REALITIES

- The FBI logged over 450,000 cybersecurity complaints and reported over $3.5 billion in losses in 2019
- Over 50% of US businesses may have reported a ransomware attack in the last twelve months
- Construction, governmental, and manufacturing organizations are the top three targets of ransomware attacks

RANSOMWARE ATTACK METHODS

- Delete or encrypt backup copies rendering them useless for recovery
- Leave the first 8KB of file data unencrypted to avoid detection
- Schedule ransomware attack to occur on all servers at the same time during off-hours

MITIGATING RANSOMWARE'S THREAT

- Implement cybersecurity software
- Store data on object-based network storage
- Back up your data

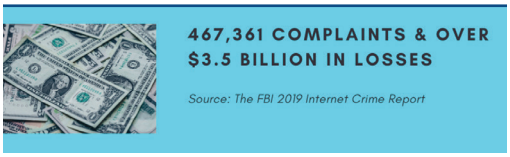
Ransomware represents one of the primary threats every size organization currently faces. The latest surveys reveal the percentage of businesses experiencing ransomware attacks may be higher than anyone initially thought. These statistics suggest it is a matter of when, not if, your organization experiences a ransomware attack.

Ransomware Realities

Frequently when a major ransomware attack occurs and an organization goes offline, it makes headlines. Further, the larger and more recognizable the organization's name, the more likely an attack on it garners national attention. In 2020 alone, ransomware attacks on Communications and Power Industries, Garmin, and Travelex, among many others, help illustrate this trend.

However, the spotlight put on these specific ransomware attacks may overshadow the breadth of them currently occurring on US businesses. Consider these recent statistics on ransomware:

- ***In 2019 the FBI logged over 450,000 complaints and reported over $3.5 billion in losses related to cybersecurity attacks.[1]*** While the FBI attributes only a portion of these complaints and losses to ransomware, they illustrate the impact hackers already have on businesses.



- ***Over 50 percent of US businesses reported a ransomware attack in the last twelve months.[2]*** The Safety Detectives surveyed over 1,000 IT professionals with over half of these individuals reporting a ransomware attack in the past twelve months.

- ***Construction, government, and manufacturing are the top three targets of hackers.[3]*** Hackers target these three types of organizations about 40 percent of the time for one simple reason: they are the most likely to pay.

Entry Points and Attack Methods

Stopping and repelling ransomware attacks requires organizations to understand how it enters their organization and then attacks.

Email

Email represents the primary method though which ransomware enters an organization. Though most organizations deploy some combination of access controls, antivirus software, firewalls, and spam filters, email messages containing ransomware still slip through.

These email messages typically come through as phishing schemes. These emails originate from what the reader perceives as an authoritative source. The email may appear to come from a

"Statistics suggest it is a matter of when, not if, your organization experiences a ransomware attack."

1. https://pdf.ic3.gov/2019_IC3Report.pdf. Referenced 10/2/2020.
2. https://www.safetydetectives.com/blog/ransomware-statistics/. Referenced 10/2/2020.
3. Ibid.

well-known bank, a government agency, or even as an alert from a technology company. Disguised this way, readers fail to discern the email's true sender and click on a link contained it.

Alternatively, an email message may contain personal or sensitive information of the user to whom it is addressed. Upon receiving and reading this email, and unaware of the sender's intent, the user clicks on a link. In both cases, clicking on the link embedded in the email message launches the ransomware.

Attack Methods

Once launched, ransomware may attack an organization in any of number of ways. While many strains of ransomware encrypt data immediately, hackers have become more sophisticated in their attack methods. They recognize more organizations know they can recover from an attack by restoring from backups. To improve their odds of getting an organization to pay a ransom, here are some new tactics they employ:

- ***Delete or encrypt backups.*** Many backup software solutions store backup copies on corporate network file servers. These locations make a tempting first target for hackers. The ransomware first looks for and then deletes or encrypts these backup copies before encrypting production data. In this way, organizations cannot use backups to recover.
- ***Leave the first 8KB of file data unencrypted.*** Many organizations use antivirus software to detect, alert, and quarantine infected files. However, some antivirus software stops scanning the file if it determines the first 8KB of data in a file is unencrypted. Some strains of ransomware take this into account in their attacks. They do not encrypt files smaller than 8KB while also leaving the first 8KB of larger files unencrypted. Taking this approach, ransomware can spread undetected more quickly within organizations.
- ***Coordinated detonation time.*** Rather than starting to encrypt immediately, the ransomware embeds its code on as many servers as possible. Then, at a predetermined time, the ransomware on all the infected servers launches at once. This makes it more difficult for organizations to quarantine the ransomware. Further, the attack may occur during off hours, such as overnight or on a weekend.

Mitigating Ransomware's Threat

Despite these and other methods ransomware uses to enter organizations and hold them hostage, organizations can mitigate ransomware's threat. These three methods provide an effective means to help prevent ransomware's entry into organizations and recover quickly should it get in.

1. ***Implement cybersecurity software.*** The adage, "an ounce of prevention is worth a pound of cure," applies here. Stopping ransomware before it ever gets a hold remains a much better approach than recovering from it. Cybersecurity software may take many forms, to include access controls, antivirus software, firewalls, and security incident and event management (SIEM) software. While many organizations may have these solutions in place, they must remain diligent in their maintenance and upkeep of them.

> ***"Hackers recognize more organizations know they can recover from an attack using backups so they employ more sophisticated attack methods."***

2. ***Store data on ~~object~~ storage.*** Ransomware increasingly first targets data stores on network attached storage (NAS) devices since they often host backups. Additionally, many organizations store critical business data on NAS devices to facilitate data sharing and employee productivity. Using object storage with NAS interfaces facilitates secure data storage and faster recoveries should a ransomware attack occur. Some solutions, such as Nasuni's File Service Platform, offer cloud storage, data immutability, instant recoveries, and snapshot features. This combination of technologies ensures that organizations have copies of unencrypted, unaffected data that they can quickly restore.
3. ***Back up data residing locally on PCs, laptops, and servers.*** Many applications and individuals keep data on local storage on their PCs, laptops, and servers. Backing up this data protects potentially valuable corporate data and intellectual property. Also, some backup software scans backups for latent forms of ransomware which offers organizations another means to check for ransomware attacks.

Organizations will likely never eliminate the threat that ransomware presents to them. It evolves quickly and hackers stand to make a lot of money by extracting ransoms from organizations. However, these three methods provide organizations a practical means to keep ransomware at bay. Simultaneously, they offer them with a high degree of confidence they can recover should a ransomware strike occur. ■