Technology Report

DCIG

Six Ransomware Attack Vectors that Backup Solutions Can Help Protect Against

By DCIG CEO and Lead Data Protection Analyst, Jerome Wendt

Six Ransomware Attack Vectors that Backup Solutions Help Protect Against

Quest

COMPANY
Quest Software, Inc.
4 Polaris Way
Aliso Viejo, CA 92656
(800) 306-9329
quest.com/qorestor

INDUSTRY
Information Technology

FOUNDED
1987

The Impetus behind Ransomware's Constant Evolution

Every day the news around ransomware attacks only seems to worsen with no organization immune to them. Historically, cybercriminals targeted hospitals, government agencies, and schools as they typically had less sophisticated IT infrastructures and cyber defenses. However, cybercriminals also discovered these organizations often only had access to limited funds to pay their ransom demands.

Seeking larger paydays, cybercriminals have begun more aggressively attacking enterprise organizations. Already in 2023, publicly traded companies such as CommScope, Dole, and Western Digital have experienced ransomware attacks.

Further, these cybercriminals no longer only encrypt data in these enterprises before demanding a ransom. In these three examples, ransomware exfiltrated sensitive data threat out of each enterprise's respective systems. The cybercriminals then threatened to release the data unless the company paid a ransom.

The severity of these ransomware attacks comes despite organizations having implemented more stringent cyber security measures. Unfortunately for organizations, cybercriminals have learned the following lessons from their past "successes" and failed attempts.

- Their victims will pay if they have no choice, potentially even more than the media reports.
- Many organizations use backups to restore data and recover from ransomware attacks.
- Data they exfiltrate and threaten to release may more likely result in a ransom payment.

Cyber Criminals Get More Sophisticated

Having learned these lessons, cybercriminals have grown more sophisticated to better prepare themselves to attack larger enterprises. They recognize that while enterprises may have better cyber defenses, they may also pay higher ransoms. This has led to cybercriminals taking steps to initiate more attacks while also avoiding detection by corporate cyber defenses. To do so, cybercriminals often employ one or more of the following three strategies:

1. ***Ransomware as-a-service (RaaS).*** Some experienced cybercriminals with viable ransomware have put their code up for sale. They now license their code to "affiliates" who use the cybercriminal's code to initiate ransomware attacks. The original creator of the code uses these affiliates to initiate a greater number of attacks. The creator may also provide technical support and management consoles to assist its affiliates with their attacks. The affiliates then share some percentage of the ransom with the creator in addition to paying a licensing fee.[1]
2. ***Create variants of successful families of ransomware code.*** Once cybercriminals develop an effective ransomware strain, they want to continue using it. This becomes difficult as antivirus software and firewalls learn how to detect it. To avoid detection, cybercriminals modify their code. For example, some utilize open-source components in their code to make it appear legitimate to antivirus software. Others re-code their software in another programming language to avoid detection.[2]

When cybercriminals disband, they take their ransomware with them, reform as a new entity, and resume their ransomware attacks.

3. ***Cybercriminals disappear and then re-appear as a new entity.*** Once law enforcement agencies and cybersecurity software recognize the ransomware used by certain cybercriminals, the cybercriminals disband. However, this disappearing act does not mean the cybercriminals exited the ransomware business. Instead, they take their ransomware with them, reform as a new entity, and resume their ransomware attacks. Their new identity makes it more difficult to identify, trace, and stop their attacks.

While cybercriminals may have evolved, they continue to use six of the following techniques to carry out ransomware attacks. Understanding these six attack vectors used by ransomware helps enterprises identify the type of attack occurring. It can also help them deploy an appropriate backup solution that protects itself and its backups from these attacks while positioning organizations to recover.

Six Ransomware Attack Vectors and Symptoms

Attack Vector	Ransomware Strain(s)	First Detected	Attack Symptom(s)	Best Backup Defense(s)
1. Email/social media	Ryuk (1st one) Used by most strains	2018	• Encrypts mounted devices & remote hosts	• Air gapped backups. • Immutable storage. • Instant restores.
2. Antivirus Software	REvil/Sodinokibi	2019	• Antivirus software compromised and used in the attack.	• Air gapped backups. • Immutable storage. • Instant restores.
3. Critical Server Processes	DoppelPaymer	2020	• Terminates server services and processes. • Inability to log into server. • Changes user password. • Data leaks.	• Air gapped backups. • Encrypted backups. • Immutable storage. • Instant restores. • MFA for backup login.
4. Critical Server Processes	Dharma	2018	• Usernames and passwords used in attacks. • Obtained on the dark web. • Obtained using software tools. • Targets Windows RDP TCP port 3389. • Encrypts files.	• Air gapped storage. • Immutable storage. • MFA for backup login.
5. Unpatched Servers	SamSam	2015/2016	• Targets Windows RDP TCP port 3389. • Encrypts files.	• Air gapped backups. • Encrypted backups. • Immutable storage. • Instant restores. • MFA for backup login.
6. Endpoint Devices	EKANS	2020	• Spear phishing. • RDP ports. • Antivirus processes disabled. • ICS processes and services disabled. • Local and networked-attached data encrypted.	• Air gapped backups. • Encrypted backups. • Immutable storage. • Instant restores. • MFA for backup login.

Source: DCIG

Six Ransomware Attack Vectors

Ransomware has existed in some form for more than 20 years. Unfortunately, that history means little for organizations hoping to learn from those early versions to stop today's attacks. Many of ransomware's most dangerous strains began to emerge in 2018.

Contributing to ransomware's rise has been its use of ever more insidious ways to enter organizations and initiate attacks. Here are six attack vectors that ransomware employs either to enter organizations or targets right after entering an organization as part of its attack.

Ryuk was the first ransomware strain to use email as an attack vector within organizations with most other ransomware strains now employing this method to enter organizations before carrying out attacks.

Attack Vector #1: Email/Social Media

Email and social media outlets such as Facebook, LinkedIn, and others remain the predominant ways that ransomware enters many organizations. Whether email or social media, they resemble one another in how they seek to access organizations. Both enter through Internet ports that organizations keep open to permit their staff to access Web resources, social media sites, and send emails.

Cybercriminals often use spam emails that contain attachments or phishing links to lure unsuspecting recipients to click on them. They also use similar techniques on social media sites by using the email and instant messaging features available on them.

The ransomware strain Ryuk was the first one to use email as an attack vector within organizations. However, most other ransomware strains now employ this method to enter organizations before carrying out attacks.

While using email and social media to enter organizations continues, ransomware's behavior once it begins the attack has changed. Cybercriminals may specifically tune their ransomware code to target enterprise environments and even specific enterprises. Once it begins an attack inside an enterprise, ransomware may carry out all types of nefarious actions. In the case of Ryuk, it begins to encrypt mounted devices and remote hosts.[3]

Attack Vector #2: Antivirus Software

Like the first attack vector, ransomware strains that target antivirus software also first enter organizations using phishing emails. However, once executed inside the organization, the ransomware begins its attack by attempting to compromise its antivirus software.

First detected in April 2019, REvil and Sodinokibi represent two strains of ransomware that target antivirus software. These strains first access organizations by sending out phishing emails that have notoriously low detection rates among antivirus software.

Once executed, this ransomware attempts to gain control of the machine on which it is running by obtaining the highest possible user privileges. It then attempts to detect and compromise the organization's existing antivirus software. While it attempts to compromise any antivirus software, only attacks on Ahnlab's antivirus software have been successful to date.

Once they compromise the antivirus software, the ransomware uses the antivirus software to spread inside the organization. It encrypts files on the target machine with these strains primarily attacking small and midsize businesses (SMBs) in Asia and Europe.[4]

Up to 80 percent of organizations who previously experienced a ransomware attack get attacked again.

Attack Vector #3: Critical Server Processes

Ransomware strains such as DoppelPaymer that target critical servers in enterprises surfaced in 2020. These strains again enter using spam emails that contain phishing links or attachments with malicious code.

They begin their attack by first terminating processes running on critical application servers. The attack might shut down the server's backup, database, email, and security processes. This prevents someone or some process from logging in and shutting the server down to stop the ransomware attack.

Once this ransomware takes control of the system, it does NOT immediately encrypt the data. Instead, it scans the systems looking for high-value or sensitive data to steal. This may include social security numbers, credit cards, or password files. The ransomware copies and exfiltrates the data outside the organization to a site hosted by the cybercriminals.

Only after it exfiltrates sensitive data does it begin to encrypt data on local and network drives. Then, in the last stage of the attack, it changes user passwords before demanding a ransom.[5]

Attack Vector #4: Usernames and Passwords

The sensitive data that other ransomware strains harvest from organizations may have found a cybercriminal buyer. Crysis, Dharma, and Phobos each represent ransomware strains that utilize usernames and passwords in their attacks.

Dharma specifically capitalizes on usernames and passwords as it attempts to enter organizations through TCP Port 3389. The Microsoft Windows operating system's Remote Desktop Protocol (RDP) uses this TCP port to grant remote users access to Windows systems.

Cybercriminals may obtain usernames and passwords in a couple of ways. It may use available software tools that identify usernames and passwords. It may also obtain them on the dark web from other cybercriminals who have harvested usernames and passwords in their earlier attacks. This may help explain why up to 80 percent of organizations who previously experienced a ransomware attack get attacked again.[6]

Once cybercriminals obtain usernames and passwords, Dharma uses them to attack organizations. It enters the organization using RDP, accesses a Windows server, and attempts to compromise it with a username and password.

Once active inside the organization, it steals data and files. It also scans for other computers on the network it can access and compromise. Once it completes these tasks, it encrypts files on the computer before it freezes out users. It then shuts the computer down and reboots it to deny use access.[7]

Attack Vector #5: Unpatched Servers

First detected in late 2015 and early 2016, SamSam enters organizations in the same manner as Dharma. It uses Windows RDP in conjunction with usernames and password to access and gain control of Windows servers.

Once logged in, SamSam exploits known vulnerabilities in the Windows operating system that are unpatched to compromise them. After it compromises a server, SamSam uses the host to access corporate networks and infect other hosts. It continues to propagate inside the corporate network and access other Windows hosts using RDP. As part of its attacks, it encrypts files on each server it compromises.

Organizations have more endpoints than ever in their environment that remain poorly secured or unsecured. If compromised, ransomware may use these endpoints as a gateway into organizations.

Attack Vector #6: Endpoint Devices

Today organizations have more endpoints than ever in their environment that remain poorly secured or unsecured. While enterprises have made significant strides to secure their desktops and laptops, many others remain unsecure. Specifically, cell phones, tablets, and Internet-enabled devices such as sensors may become compromised. Once compromised, ransomware may use these endpoints as a gateway into organizations.

EKANS (snake spelled backwards) ransomware distinguishes from other ransomware strains. First detected in 2020, it seeks out and stops antivirus and Industrial Control System (ICS) processes and services. Once disabled, it deletes shadow copies to prevent possible restores. It then encrypts data attached to the device or data it can access over the network. This strain specifically targets energy, healthcare, manufacturing, transportation, and other industries that use ICS software and devices.[8]

The Inevitability of a Ransomware Attack

These six attack vectors represent only some of the ones that criminal justice and cybersecurity firms openly discuss. Other attack vectors may exist that remain yet undetected or which these agencies have only begun to disclose.

For instance, in 2021, security researchers detected a new strain of ransomware. This specific strain attacks and encrypts Linux systems and has been active since at least March 2022.

This constant evolution of existing ransomware strains coupled by the introduction of new ones creates a dilemma for organizations. Ideally, they want to prevent a ransomware attack as opposed to having to recover from one.

Unfortunately, this ideal becomes nearly impossible to achieve as ransomware changes quickly with new strains constantly emerging. Further, individuals within organizations make mistakes or may add endpoint devices at any time that compromise corporate security. This makes it unlikely that any organization's IT environment is ever completely immune from a ransomware attack.

While preventing a ransomware attack always trumps recovering from one, organizations must assume an attack will eventually succeed. They can never be 100 percent confident they have plugged all their cybersecurity holes. Even if they theoretically have, cybercriminals may gain access to usernames and passwords that may negate existing cybersecurity countermeasures.

These reasons highlight why organizations should select a backup solution that possesses two primary characteristics. First, it must protect itself and its data from the ransomware attack. Second, it must offer features that position organizations to restore data and recover applications.

Backup Solution Enhancements that Counter Ransomware's Attack Vectors

In response to the new threats that ransomware poses, providers have made multiple enhancements to their backup solutions. These include offering new features that specifically protect the backup solution and backups from ransomware attacks. They also offer more options that organizations may use to quickly restore data and recover applications.

To secure backups against ransomware attacks, backup solutions have embraced the use of immutability on storage devices.

Secure Storage

To first secure backups against ransomware attacks, backup solutions have embraced the use of immutability on storage devices. This shows up in multiple ways. For instance, many organizations want to use cloud object storage available from cloud providers to store their backups.

Many cloud storage offerings now support an object lock feature to store backups in an immutable format. More on-premises object-based storage devices also support this object lock functionality. Additionally, some storage devices with NAS interfaces also offer data immutability features. Regardless of which of these storage devices that organizations use, they all prevent ransomware from changing, deleting, or encrypting backups.

Storing backups on air gapped media such as tape also serves as an effective counter measure to ransomware attacks. While organizations need to thoughtfully use tape, it does create an air gap that protects backups from ransomware attacks.

To address some of tape's drawbacks, specifically slow retrieval times, some disk storage devices offer a logical air gap feature. This feature makes data stored on disk on the device essentially invisible on the network. Only the right software can detect the logically air gapped backups stored on these storage devices.

Finally, organizations should consider encrypting backups whether they store them on standard storage devices or in an immutable format. Stored in either of these two formats, ransomware can read the data and exfiltrate copies of it. Encrypting backups mitigate the possibility of cybercriminals being able to understand the data stored in them.

Authenticating Backup Solution Logins

Some ransomware strains now attempt to log in and access the backup software. Once logged in, the ransomware may perform any number of tasks. It may delete or encrypt existing backups. It may reschedule or stop backup jobs. It may reconfigure the backup software to send backups to cloud storage managed by the cybercriminal.

Backup solutions offer some options to protect itself from this unauthorized access. Backup solutions often now support multifactor authentication (MFA). The first time, or potentially every time, a user logs into the backup solution, the user must enter a second code to complete the login.

Due to the critical nature of the data kept in backups, some backup solutions go even further. For instance, an administrator may want to change a backup schedule or delete a backup. To verify this request, the backup solution may require a second backup administrator to authorize this change.

Restores and Recoveries

Ransomware attacks may occur at anytime and anywhere within organizations. This makes it almost impossible to predict the scope of its impact. However, the data it encrypts and systems it compromises does impact the speed and scope of data restoration and application recoveries.

To assist on this front, backup solutions offer more restore and recovery options. Many support storing data on multiple media types that have various performance character-

istics. In this way, organizations may quickly restore data.

In some cases, organizations cannot wait to restore data to production systems. They need to resume production while the data still resides on the backup systems. To accommodate this requirement, more backup solutions offer instant restore functionality. This functionality ranges from permitting access to files residing on backup storage media to running applications hosted on it. Backup solutions may even permit live migrations of recovered production applications from the backup to the production environment.

More backup solutions offer instant restore functionality. This functionality ranges from permitting access to files residing on backup storage media to running applications hosted on it.

NetVault Plus's Specific Countermeasures to Ransomware's Attack Vectors

NetVault Plus provides the specific countermeasures that organizations need to address today's multiple ransomware attack vectors. NetVault Plus first secures backups and itself from ransomware in multiple ways. NetVault Plus offers air-gapped backups to tape, immutable backups, an immutable backup recycle bin, data encryption, a proprietary storage protocol, multi-factor authentication, and a cyber-resistant Linux-based hosting option.

NetVault Plus provides a choice of storage targets on which organizations may store their backups. It supports multiple types of disk targets as well as tape and cloud storage from multiple cloud providers. Its support of backup targets includes its own robust software-defined deduplication as well as deduplication appliances from multiple providers.

Using NetVault Plus's software-defined deduplication (also sold separately as Quest QoreStor®), organizations may deduplicate backups and still get fast restores. Quest has internally documented that organizations may restore any deduplicated backup with speeds comparable to using raw disk.

Its speed of restore from deduplicated backups shows up in NetVault Plus's Instant Restore option. Organizations may mount one or more virtual machines (VMs) directly from QoreStor's deduplicated backup repository. Once mounted, VMware's Storage vMotion can perform a live migration of a VM to an existing VMware vSphere datastore.

NetVault Plus has also for some time offered Bare Metal Restore (BMR) for organizations that need to quickly recover applications hosted on physical machines. It also provides continuous data protection (CDP) that takes snapshots as frequently as every hour to minimize data loss.

NetVault Plus's CDP feature can even store snapshots in a deduplicated format. This combination of CDP, deduplication, and instant restore provides short RPOs and fast RTOs for applications and data while controlling storage costs.

To store backups offsite, NetVault Plus can replicate deduplicated data to remote sites and multiple public clouds. Using this feature, organizations can create a 3-2-1 DR and backup strategy. This positions them to recover locally, at a remote site, or with a public cloud provider.

This combination of features positions organizations to use NetVault Plus as an effective countermeasure to ransomware attacks. It protects itself and its backups from ransomware attacks while providing the multiple restore and recovery options that organizations need.

Organizations must have a backup solution in place that positions them to quickly restore their data and recover their applications when their cybersecurity defenses fail.

Backup Solutions a Key Component in Today's Defense Against Ransomware's Multiple Attack Vectors

Any organization that believes it is immune from a ransomware attack does so at its own peril. Ransomware evolves so rapidly that organizations may find it impossible to defend against every type of attack. While organizations should maintain a firm cybersecurity defense, they should prepare for the likelihood these defenses will fail.

If, and when, they do, they have less time than ever to restore their data and recover their applications. This makes it imperative they have a backup solution in place that positions them to perform these actions.

To do so, this backup solution must first protect itself and the backups under its management from the multiple attack vectors used by today's ransomware strains. This minimally requires it to store backups in an immutable format and secure user logins. It should also offer the option to encrypt data to mitigate the impact of data leakage. Finally, it must still provide multiple data restore and application recovery options to quickly get organizations up and operational.

No organization ever wants to experience a ransomware attack. But with so many ransomware strains and mutations in the wild, no organization can ever really feel 100 percent safe. Selecting a backup solution that possesses these backup features positions organizations to withstand ransomware attacks from these various vectors. At the same time, it positions organizations to safely, and quickly, perform restores and recoveries from these attacks. ■

Sources

1. https://encyclopedia.kaspersky.com/glossary/ransomware-as-a-service-raas/. Referenced 4/23/2023.
2. https://www.csoonline.com/article/3617983/5-ways-hackers-hide-their-tracks.html. Referenced 4/23/2023.
3. https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/. Referenced 4/23/2023.
4. https://www.cybereason.com/blog/research/the-sodinokibi-ransomware-attack. Referenced 4/23/2023
5. https://www.trendmicro.com/en_us/research/21/a/an-overview-of-the-doppelpaymer-ransomware.html. Referenced 4/23/2023.
6. https://www.securityweek.com/it-doesnt-pay-pay-study-finds-eighty-percent-ransomware-victims-attacked-again/. Referenced 4/24/2023.
7. https://www.comparitech.com/net-admin/dharma-ransomware/#: Referenced 4/24/2023.
8. https://unit42.paloaltonetworks.com/threat-assessment-ekans-ransomware/. Referenced 4/24/2023.

About DCIG

The Data Center Intelligence Group (DCIG) empowers the IT industry with actionable analysis. DCIG analysts provide informed third-party analysis of various cloud, data protection, and data storage technologies. DCIG independently develops licensed content in the form of TOP 5 Reports and Solution Profiles. More information is available at **www.dcig.com.**