Innovations

LEARNING SERIES

FOUNDATION EDITION

Lessons Learned: Recovering from Ransomware

Inside the Guide

- Ransomware's growth in variety as well as volume
- Do you know where your ransomware vulnerabilities are?
- How to ensure your business survives a ransomware attack

ActualTech Media | rubrik

Lessons Learned: Recovering from Ransomware

TABLE OF CONTENTS

ActualTech Media

6650 Rivers Ave Ste 105 #22489 | North Charleston, SC 29406-4829

www.actualtechmedia.com

Publisher's Acknowledgements

EDITORIAL DIRECTOR
Keith Ward

DIRECTOR OF CONTENT DELIVERY
Wendy Hernandez

CREATIVE DIRECTOR
Olivia Thomson

SENIOR DIRECTOR OF CONTENT
Katie Mohr

PARTNER AND VP OF CONTENT
James Green

WITH SPECIAL CONTRIBUTIONS FROM RUBRIK
Arushi Jain, Principal Product Marketing Manager
Damani Norman, Managing Technical Product Manager
James Knott, Senior Engagement Manager
Jonathan Hemming, Technical Director, Customer Success

Introduction: The Rise of Ransomware Attacks

As enterprises adopt data-driven business models to increase agility, data has become a more lucrative target for cybercriminals. Even with robust defense mechanisms in place, ransomware attacks continue to increase, successfully encrypting the data of many organizations. In the first half of 2020, there were approximately 2.5 million new ransomware attacks according to the November 2020 *McAfee Labs Threat Report*. Similarly, SafetyDetectives found that 54% of medium and large organizations in the United States and 57% in the United Kingdom were affected by ransomware attacks in the last year (see **Figure 1**). Ransomware attacks targeting health care and medical research facilities also exploded as cybercriminals sought to profit from the COVID-19 pandemic. Schools and universities attempting to provide remote learning opportunities for their students were similarly targeted.

THE 101

A Staggering Statistic

According to the U.S. Department of Health and Human Services Fall 2019 OCR Cybersecurity Newsletter, the FBI estimates that cybercriminals will earn over $1 billion in ransom.

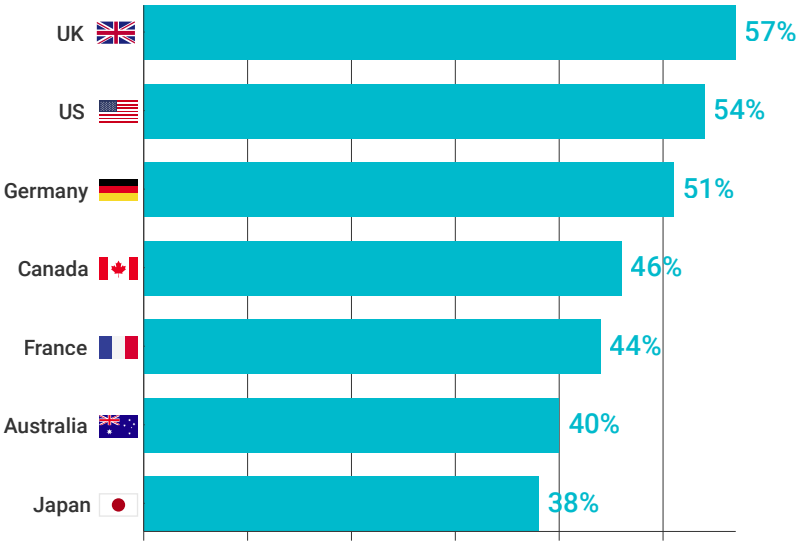

Figure 1: The percentage of organizations that reported ransomware attacks in the last year in each country (Source: SafetyDetectives)

The U.S. Cybersecurity and Infrastructure Security Agency's (CISA) ransomware site US-CERT defines ransomware as:

a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website.

Types of Ransomware Attacks

The idea behind ransomware attacks is relatively simple: deny authorized users access to critical data, most commonly by encrypting their files, then demand a ransom payment (typically in cryptocurrency, such as Bitcoin). In the past, initial ransomware demands were relatively small—typically tens of thousands of dollars—but quickly increased if the victim delayed payment, to encourage victims to pay the ransom. However, the increasing success of ransomware attacks pushed demands to hundreds of thousands or even several million dollars.

DEEP DIVE

Ransomware Comes in Many Forms

Ransomware comes in many forms and via a number of attack vectors, including:

- **Encryption ransomware:** Encrypts personal files, folders, and shared network storage. The targeted files are deleted once they've been encrypted, and users generally encounter a text file with ransom payment instruction in the same folder as the newly inaccessible files.
- **Network-attached storage (NAS) ransomware:** Encrypts and/or deletes files on a NAS system including home directories, virtual machine (VM) hypervisor backups, shadow volumes, and backup files.

- **Lock screen ransomware:** Locks the user's computer screen and demands payment, but no personal files are encrypted. Recovery from lock screen ransomware is relatively easy and involves booting into safe mode and removing the lock screen with anti-malware recovery tools.
- **Hardware locker:** Changes the computer's master boot record (MBR) so that the normal boot process is interrupted, preventing the operating system from properly starting. Recovery requires either fixing the MBR or restoring data to a new system.
- **Application/web server encryption:** Encrypts files and web servers through application vulnerabilities. On web servers, the index.php or index.html files are replaced with ransom instructions. Recovery requires finding the infected files and restoring them to their previous state.
- **Ransomware as a Service (RaaS):** Widely available on the Dark Web, RaaS enables practically anyone to attack an organization with ransomware that manages all aspects of the attack including delivery, infection, encryption, payment collection, and decryption—all for a small licensing fee or commission.
- **Data Exfiltration:** Reads critical data from the attacked systems and copies it to the attacker. This ransomware attack is often combined with other attacks which lock up the critical data.

Advanced ransomware is now targeting backups, modifying them or completely wiping them out, compromising the last line of defense and maximizing chances of ransom payout.

Best Practices for Ransomware Recovery

Despite the FBI and other cybersecurity agencies strongly advising against victims paying a ransom to recover their data, more than a quarter of all victims do pay the ransom, according to recent reports by CrowdStrike and Sophos. However, there are no money-back guarantees, and according to Sophos, victims that pay a ransom actually double their cost of dealing with a ransomware attack, from approximately $730,000 to $1.4 million.

The following best practices will help you plan for, identify, and successfully remediate a ransomware attack if your organization is targeted (see **Figure 2**).

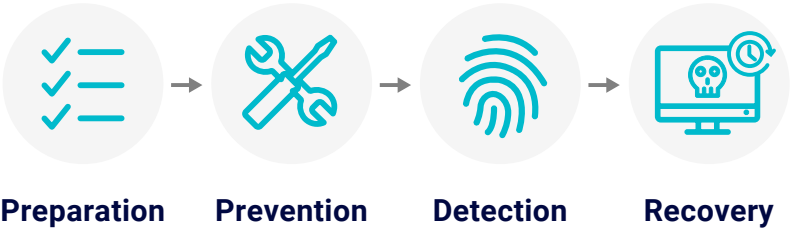

Figure 2: Ransomware defense includes preparation, prevention, detection, and response and recovery best practices

PREPARATION

Taking the time to prepare for a ransomware attack is key to successfully recovering from one. Some best practices include:

- **Build a plan:** Begin by developing a ransomware response and recovery plan and a supporting playbook. The plan and playbook should be reviewed and updated periodically and stored in a secure manner that can't be attacked by ransomware (such as a printed copy).
- **Identify stakeholders and response team members:** You need to identify key stakeholders across management, IT, system/application teams, and others, as well as specify who will be responsible for executing and managing the incident response and recovery plan. Ensure everyone understands their individual responsibilities and how to execute their assigned activities in the recovery plan.
- **Create a communications plan:** Timely, accurate, and thorough internal communication within an affected organization is critical. Identify methods of communication that will be available during a ransomware attack. Corporate email and phone systems may be impacted and unavailable. Provide alternate means of communicating both internally and with outside vendors, law enforcement agencies, customers, and the general public.
- **Prioritize systems based on business criticality:** Identify the criticality of each system and its data to the business. Knowing which systems in the business need attention first and how they interact with other business systems will facilitate a smooth and orderly recovery. Based on

each system's criticality level, document a recovery plan that identifies which systems will be recovered in what order.

- **Store backups in a secure location:** Determine where backup copies will be stored, both locally and/or offsite. Local copies must be stored on an immutable (unchangeable) storage platform. This ensures that your backup data cannot be encrypted or modified in the event of a ransomware attack so that you will be able to recover quickly (see **Figure 3**). Remote copies of the data will be required if your plan calls for recovery at an alternate site. Special attention should be given to how data is stored offsite. Data stored in offsite archives is subject to attack by ransomware because the storage platforms on which the backups are stored might not be immutable. Moreover, restoring from offsite backups can be complex and very time-consuming. Cloud archives can also be externally accessed if not properly secured. If archival locations will be relied upon to recover from ransomware attacks, appropriate steps should be taken to secure those locations.

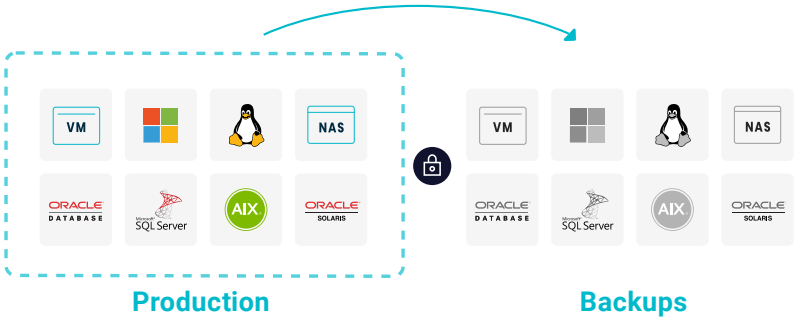

Figure 3: Immutable platforms prevent ransomware attacks from accessing or encrypting online backup systems and data

- **Test recovery plans regularly:** Periodically test data recovery to be prepared for an actual incident. Without testing, there can be no assurance that the recovery plan will work when an attack happens. Testing also provides the experience and confidence to response and recovery team members that an attack can be quickly and successfully remediated. Tests should be as realistic as possible without disrupting business operations and conducted at both planned and unplanned intervals. One purpose of testing is to be prepared for the unexpected.

Despite the FBI and other cybersecurity agencies strongly advising against victims paying a ransom to recover their data, more than a quarter of all victims do pay the ransom, according to recent reports by CrowdStrike and Sophos.

PREVENTION

Ransomware prevention best practices include end-user awareness training to help users recognize malicious links and attachments in email, as well as malicious websites that deliver ransomware. Spam and phishing emails, weak passwords, and malicious websites are the most common methods of ransomware infections (see **Figure 4**). This training should be interactive and engaging, similar to the

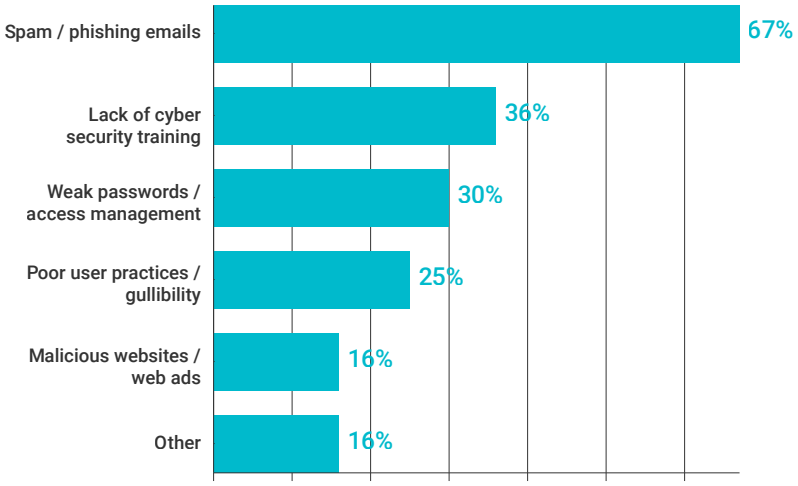

Figure 4: Most common methods of ransomware infections in North America (based on MSPs reporting attacks on organizations) (Source: SafetyDetectives)

anti-phishing training that many organizations provide today. Additional prevention measures include updating and patching your operating systems and applications, enabling link and attachment filtering in email (like Safe Links and Safe Attachments in Office 365), and ensuring anti-malware software is installed and current on all your endpoints.

Spam and phishing emails, weak passwords, and malicious websites are the most common methods of ransomware infections

DETECTION

Unfortunately, prevention isn't always possible. The security industry increasingly recognizes that an effective cybersecurity posture requires both prevention and detection/response capabilities. In the event that ransomware thwarts your prevention efforts, you need to have the right processes and tools in place to detect ransomware before it has fully activated. Real-time detection and alerting tools are your first line of defense. These tools should also include monitoring and analysis to ensure the integrity and availability of your last line of defense—your backup data. Some best practices include:

- **Align protection to business commitments:** Ensure all critical systems and data are being protected in a manner that guarantees Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) can be met. Also ensure sufficient data retention in the event a ransomware infection isn't detected for weeks or months.

In the event that ransomware thwarts your prevention efforts, you need to have the right processes and tools in place to detect ransomware before it has fully activated.

Figure 5: Tools that automatically assess an attack's impact and clearly identify which applications and files were encrypted and where they are located enable faster recovery at a granular level that minimizes data loss

- **Identify affected data at a granular level:** Implement tools to identify, at a file or object level, which data has been infected with ransomware (see **Figure 5**). Having this data during an attack will be invaluable in speeding up recovery and preserving uninfected data. Innovations such as machine learning (ML) can be trained to identify trends that exist across all samples of backup data and classify new data by their similarities without requiring human input. This analysis is largely based on file system behavior and content analysis performed on file system metadata. It looks at characteristics like the number of files added, number of files deleted, and so forth, to detect outlier behavior and alert IT and security teams. It can also provide an added layer of intelligence for anomaly detection on your backup data as your last line of defense.

RESPONSE AND RECOVERY

After a ransomware attack has been detected, prompt notification of stakeholders and response team members (including support vendors) will help ensure the right people are engaged and mobilized as quickly as possible. Assessing the scope of the attack and isolating any systems suspected of being infected is the first order of business in an effective response. Have a plan to isolate infected systems so the ransomware can be prevented from spreading further on the network. Also, have a plan to recover infected systems and data that you've isolated from the network. If the ransomware can't be safely neutralized, recovery to new systems on a separate network may be necessary. Additional best practices include:

- **Determine what recovery methods will be used for each type of recovery.** Options like Live Mount for VMware VMs allow systems to be recovered in minutes, but they work by rolling entire systems back to a safe point in time, so uninfected data may be lost. File- and database-level restores for infected data may be a better option. The appropriate method needs to be evaluated ahead of time so it can be quickly selected during an attack.
- **Leverage automation to speed response and minimize human error.** A key factor during recovery is automation as it minimizes the risk of human error. It also speeds up recovery and aids in progress tracking. Your backup and recovery vendor should offer a full set of APIs and SDKs to help automate recovery. These can be integrated with automation tools such as Ansible, Terraform, Puppet,

Chef, PowerShell, and Python. Once a recovery plan and prioritization have been established, automation is the next step in building a robust recovery capability.

Once ransomware has been detected, snapshot expiration should be carefully reviewed to ensure no valid snapshots expire that would affect data recovery. Service-level agreements (SLAs) with near-term retention policies should be extended for at least one year for the duration of the ransomware event. Be sure to make note of the original retention periods so that they can be set back after the ransomware event is over.

Ask your vendor if they can deliver near-zero RTOs for VMs, file shares, and databases and execute instant file recovery without hydration of data.

Before starting the recovery process, it's important to know what type of recovery is required. If the ransomware only infected files on servers or user shares on a NAS, a file-based recovery method can be used. If, however, the ransomware attacked the virtual disk images for a hypervisor or the MBR records of a physical system, a full system recovery may be needed. Best practices for recovery include:

- **General recovery best practices** (these apply to all recovery scenarios):
    - *Recover safely:* Begin recovery operations only after the ransomware has been neutralized. This may

mean that data needs to be recovered in isolation or to new systems. Restoring systems or data before the ransomware has been neutralized may result in the system or data being infected again. If the ransomware can't be isolated and neutralized in a timely manner, the alternative is to recover systems in isolation, where they can't be reinfected.

- *Local isolated recovery:* Often ransomware attacks are so pervasive that recovering to the original locations will result in secondary infections. Recovering to a local environment that is isolated from the infected environment is the best way to avoid a secondary infection. Planning during the Preparation phase (discussed earlier) should include identifying and testing local recovery in an isolated environment.
- *Prioritized recovery:* As planned for in the Prevention phase, recovery will be based on the prioritization of applications and lines of business. Ensure that foundational services required for basic functionality, such as DNS, DHCP, and authentication, are running or restored first. Without these foundational services, the recovered systems may not function properly.

- **File-only recovery best practices** (these apply to scenarios where only files and directories need to be recovered):
  - *Verify the operating system:* Verify that the underlying operating system can be trusted and wasn't compromised by the ransomware attack.

- *Recover to a clean system:* If the original system can't be trusted, recover files to a known good system. This may be a newly built system isolated from the production environment.
- *Identify files for recovery:* Use automated tools to identify which files were infected by the ransomware and recover them.

- **VM and database recovery best practices** (these apply when the VM itself can't be used, which may happen if the NAS storage the VM is running on has been compromised or if the ransomware renders the VM unbootable). Instant recovery capabilities are not common for all providers. A modern data protection solution provider such as Rubrik provides these capabilities, enabling fast and accurate restores:
  - *Restore smaller data sets:* Instant recovery capabilities allow VMs and databases to be mounted directly from storage, saving the time it would take to copy backups back to primary storage before making resources available. Once mounted, VMs can be moved back to primary storage in the background while providing their regular services. Databases can be run until a planned outage can be scheduled to move the databases back to primary storage.
  - *Export directly to primary storage:* Modern data protection solutions include an export function that can be used to recover or copy a VM or database directly to primary storage. Once copied, the VM or database

can be brought back online. This method provides the fastest data transfer performance back to primary storage and is best for recovering many VMs.

- *Mix instant recovery and export:* Instant recovery and export recovery workloads can be mixed, but this should be done with extreme care. Exports will utilize the full resources of the storage cluster to move data back to primary storage. Instant recovery may have to contend with the traffic that's being recovered. This may cause degraded performance in the VMs and databases restored with instant recovery. Mixed workload recovery should be evaluated on a case-by-case basis.

- **Hypervisor manager recovery best practices** (coordinate the recovery of vCenters or other hypervisors with the appropriate support team to ensure a smooth recovery):

  - *vCenter recovery:* Care must be taken if vCenter has to be recovered or when recovering VMs into a new vCenter. Duplication or reuse of the VMware Managed Object ID (MOID) can lead to issues during the recovery of VMs. If vCenter has been compromised, it's better to restore it from backup than to create a new empty vCenter and recover the VMs into that.

  - *Recovery and/or reinstallation of non-vSphere hypervisor managers(s):* When hypervisor managers such as Microsoft's System Center Virtual Machine Manager (SCVMM) or Nutanix Prism are protected using snapshots, contact your backup and recovery vendor for

recovery options. When the hypervisor manager is protected using built-in backup methods, engage the hypervisor vendor as well as your backup and recovery vendor.

Recover Faster and Easier

Ransomware continues to proliferate and is costing companies millions of dollars. Moreover, it has also evolved and become more sophisticated. Ransomware not only blocks access to systems, it also encrypts or deletes active data, including backups on vulnerable systems.

When prevention of a ransomware attack fails, having an immutable backup that can't be deleted or encrypted is crucial for recovery. Being able to intelligently identify and remediate encrypted data makes recovery efforts easier and faster while reducing data loss and downtime.

Rubrik helps organizations recover faster from ransomware attacks with innovative capabilities like Rubrik Instant Recovery, Rubrik Radar for detailed impact analysis and anomaly detection, and Rubrik Sonar for sensitive data discovery. Learn more at https://rubrik.com/ransomware-recovery.

About Rubrik

Rubrik helps enterprises achieve data control to drive business resiliency, cloud mobility, and regulatory compliance. Rubrik bridges the gap between owned, on-premises infrastructure and the cloud by decoupling data from the data center through a software-defined fabric and offering a single management plane for all data, whether on-prem or in the cloud. Comprehensive data management is delivered through instant access, automated orchestration, and enterprise-class data protection and resiliency.

About ActualTech Media

ActualTech Media is a B2B tech marketing company that connects enterprise IT vendors with IT buyers through innovative lead generation programs and compelling custom content services.

ActualTech Media's team speaks to the enterprise IT audience because we've been the enterprise IT audience.

Our leadership team is stacked with former CIOs, IT managers, architects, subject matter experts and marketing professionals that help our clients spend less time explaining what their technology does and more time creating strategies that drive results.

If you're an IT marketer and you'd like your own custom Gorilla Guide® or Innovations Learning Series title for your company, please visit https://www.gorilla.guide/custom-solutions/