VERITAS

Ransomware Resiliency: The Risks Associated with an Attack and the Reward of Recovery Planning

An overview of the history of ransomware, its potential impact and best practices to protect IT systems.

Veritas™ White Paper | March 2020

Contents

EXECUTIVE SUMMARY

Ransomware attacks are on the rise. According to Cybersecurity Ventures, ransomware will cost organizations across the globe over $20 billion by 2021, with general cybercrime expected to make a $6 trillion impact—estimates including costs associated with restoring data and infrastructure as well as the often-hidden expenses of mitigating the social damage of an attack.

Ransomware is the fastest-growing global malware threat and one that often catastrophically impacts an organization, accounting for the majority of extortion-based events and causing billions of dollars in losses for organizations around the world today. It has the potential to disrupt all organizations using computing infrastructure—whether on-premises, managed by a third-party, virtual or in the cloud.

Typical attack vectors include email phishing schemes, malvertising and unabated vulnerabilities. Once ransomware gains access to an organization, it can spread and corrupt data across networked systems. The data at risk can include daily transactional information and operating systems, system configurations and even backup and cloud-based data. When systems are infected and storage encrypted as a result of ransomware, enterprises have the choice to pay the ransom, hoping their data will be preserved, or recover and rebuild. Either situation is fraught with risk because access to data is never guaranteed and there is the potential to be retargeted by cybercriminals. According to a survey by CyberEdge Group, of the 38.7 percent of respondents who agree to pay a ransom, less than half were able to recover files using the tools provided.

Fortunately, properly protected and secured backup systems can be used to restore data and infrastructure to a known good state prior to a ransomware event. Those of us at Veritas have supported this recovery approach with numerous NetBackup™ customers, including one hit by DoppelPaymer, a crypto-locker ransomware. The organization's administrator indicated all tapes inside the library had been erased, but in collaboration with Veritas Support, the on-site IT team was able to recover data and infrastructure from protected backups. Although the solution proved successful, it would have been less tumultuous if the organization had a tested, reliable ransomware recovery plan in concert with ongoing information security risk assessments.

INTRODUCTION

The concept of ransomware was first introduced at an international AIDS medical conference in 1989 and was known as the "AIDS Trojan," distributed to attendees by way of 20,000 5.25-inch floppy disks. Participants' computers were infected, although the virus lay dormant for 89 reboots of the computer; on the 90th reboot, a warning indicated files had been encrypted and payment was required to unlock the systems. Today, ransomware is much more pernicious, with prominent economic and social costs.

And the effects of ransomware go beyond data loss. The Vanderbilt University Owen Graduate School of Management shows these data breaches can cause injury and even death. A recent study by the school demonstrated a striking impact to hospitals in particular, showing 36 fatalities per 10,000 heart attacks that could have been prevented had systems not been infected. In a critical care unit, it can take an additional 2.7 minutes for suspected heart attack victims to receive an EKG. Those additional 2.7 minutes coupled with the necessary rerouting of patients shows ransomware presents life-threatening consequences. In England, the WannaCry attacked against the National Health Service (NHS) forced the cancellation of thousands of appointments and operations across five regional hospitals. It required almost a year to fully assess the damage the attack caused to systems and individual health costs.

THE ECONOMICS OF RANSOMWARE

A leading objective of cybercriminals is to profit from infected systems. The profit they make largely depends on the willingness of those attacked to pay the ransom—a decision often guided by several factors:

1. The severity of the breach, including the number and value of impacted applications or files.
2. The length of time the malware has been active in the environment.
3. The efficiency of the backup and security teams to roll back to the point of the breach.
4. The ability to get the decryption codes to successfully regain access to data.

Additionally, it's important to understand the economics of ransomware and the perpetrator's motivation to target a particular enterprise, which can be represented that the maximum amount a particular victim is willing to pay to recover files is defined by (vi) the willingness of person (i), to pay. For example, an organization that values files at $10,000 and trusts the criminals would have a vi = 10,000, while an organization valuing files at $20,000 with low confidence in the return of the encryption key or with confidence in a recovery by backup or file sanitation may have a vi = 0. The profit then be summarized as $N=\Sigma\ Ni=1\ (pi-c)1i-F$, where N is the number of people attacked, pi is the ransom asked of the organization I, c is the cost of dealing with any ransom money, 1i is an indicator variable that takes value 1 if pi ⩽ vi and 0 otherwise and F is the fixed cost of operating the malware.

Ransomware criminals look for targets of least resistance with the greatest return on investment (ROI). This formula makes it clear—: iIf the vi = 0, there is little economic value to pursue an attack given the limited ROI of an organization with strong cybersecurity and a hardened backup environment.

One challenge for law enforcement when it comes to ransomware is the emergence of cryptocurrency. The cryptocurrency Bitcoin has played a fundamental role in the proliferation of ransomware, allowing easy money transfers with limited traceability. These characteristics provide cybercriminals with a powerful tool to profit from their crimes, using Bitcoin to defeat the known control measures to trace, track and stop payment. Bitcoin is currently the most popular cryptocurrency, but there is a continuous stream of new options, some of which claim to provide full anonymity and untraceability, making law enforcement efforts to follow the flux of money almost impossible.

THE FIVE PHASES OF RANSOMWARE ENCRYPTION

There are generally considered to be five phases of ransomware encryption, from the breach or Infection (Phase 1) of a cooperate environment to User Notification/Settlement and Remediation (Phase 5). Hospitals are given a slightly different set of phases as they are unduly prone to ransomware.

Phase 1 – Infection: Initial entry into the system by means of spam email, phishing attack or an exploit kit—readily available on the Dark Web. During this phase, the vulnerabilities of systems and users are exploited. Lapses in user awareness and training as well as failures to follow corporate security policies provide the ransomware entrance into the computing infrastructure.

Phase 2 – Delivery: Persistence mechanisms are established. These mechanisms alter registry keys to protect the ransomware, hiding it and permitting self-restart even after a system shutdown. This phase enables the ransomware to encrypt files at a later date without requiring additional actions on the part of the user or ransomware command-and-control center.

Phase 3 – Backup Attack: This is a self-defense mechanism for the ransomware to ensure its effectiveness and to facilitate payment. CryptoLocker and Locky, two ransomware variants, execute commands to remove all shadow copies from infected systems. Other variants search for folders holding backup files and remove them.

Phase 4 – Encryption: During this step, encryption keys are established on the local system. Early forms of ransomware included the encryption keys as part of the application, making it easy for security teams to identify the key and unencrypt information. Today, encryption keys are not supplied with the application, and the time to recover files varies based on computing infrastructure characteristics such as file size, network characteristics and number of connected devices.

Phase 5 – User Notification/Settlement and Remediation: The ransomware notifies the user of infection, demands payment and presents instructions for payment. Generally, the user is given a timeframe for payment, with escalating penalties/ransom for not paying. After the ransom is paid, the ransomware frequently attempts to remove evidence of its presence that may be identified by forensic investigators.

With the AIDS Trojan, the encryption algorithm was primitive and security professionals were able to remediate the ransomware quickly. Over time, ransomware has become more sophisticated, with improved coding techniques including a combination of shared-secret traditional encryption using fast algorithms, such as the Triple Data Encryption Algorithm and Advanced Encryption Standards, along with a public-key system that encrypts the encryption key so it cannot be found. This methodology has two basic paths:

1. Using a command-and-control system to provide the public key to use to encrypt the shared-secret encryption key.

2. Embedding the public key into the application itself.

In the former case, the encryption cannot be truly secured (for example, by encrypting the shared-secret encryption key) until the system can connect with the command-and-control center, whereas in the latter case, all attacked systems will share the same public key. Once the private key is provided to users who have paid the ransom, the private key can then be shared for others attacked similarly. In fact, investigators have discovered that the system is tagged with a unique identifier given to the user for payment of the ransom.

DEFINING BACKUP RECOVERY BEST PRACTICES FOR YOUR ORGANIZATION

Having a reliable backup and recovery solution is the most vital step toward building a reliable ransomware prevention plan. Today, companies often rely on several backup paradigms, including traditional backup as well as replication and continuous data protection (CDP). Each of these methods is valuable for creating copies of data, and in the case of replication, moving copies to local or remote storage—a notable benefit in the effort to create distance, or air gap, between backup data and the organization's network.

However, each backup paradigm has pros and cons that organizations must consider when developing a ransomware recovery plan. With replication, data is often replicated in real time, reproducing the ransomware virus as part of the process. By defining frequency, timing and storage parameters for replication guided by the goal of protecting data in the case of an attack, organizations can ensure a dependable, network-disconnected version of backup data exists.

CDP supports point-in-time and version-based file recovery by taking periodic or timed snapshots, giving organizations the ability to roll back to a time prior to the ransomware attack. CDP has the disadvantage of using significant disk space due to the number of managed snapshots, although it may be a small price to pay for ready ransomware recovery.

Organizations also benefit from setting standards for a recovery point objective (RPO) and recovery time objective (RTO). RPO defines a company's loss tolerance, or the amount of data that can be lost before significant harm is done to the business. The objective is expressed as a time measurement from the loss event to the most recent preceding backup. RTO refers to how much time an application can be down without causing significant damage to the business. Some applications can be down for days without significant consequences, but many cannot. Both metrics play an important role in developing a baseline from which an organization can build a ransomware recovery plan that addresses the needs of the business while remaining attentive to its IT realities.

INCREASING RANSOMWARE RESILIENCY WITH VERITAS NETBACKUP

NetBackup inhibits the potential devastation caused by a ransomware attack and supports the ready, reliable recovery of data. Even when cybercriminals have targeted backup software and appliances, NetBackup enables users to restore a valid copy of data from a known point in time to months or even years in the past, depending on configuration and retention rate.

With NetBackup, the organization can use incremental backups to identify a sudden, unexpected increase in the change rate, which can indicate an undetected ransomware attack. As ransomware begins to encrypt data on a host system and over the network, it is modifying those files. NetBackup tracks backup metadata over time, and this data can be mined and compared to historical patterns to support the early flagging of a ransomware attack—even notifying backup and security administrators of the shift.

Here's how your organization can use NetBackup to build a robust ransomware recovery plan:

1. **Secure physical access to the production NetBackup server and/or Appliance**—Physical security of the backup server is the first line of defense in protecting backups. Limit physical access to the backup server environment, and when possible, segregate your backup environment from your production environment.

2. **Harden and protect the NetBackup Master servers**—Severely limit access to the NetBackup Master servers. Implement security and organization-driven encryption to provide protection for NetBackup operations on NetBackup Master servers, media servers and attached clients.

3. **Secure communications pathways and ports**—Veritas recommends using the default port number settings for NetBackup services and Internet service ports. It also may be necessary to implement IPsec rules such as blocking backup client connections with an unauthorized server and incoming connections to the backup server from an unauthorized client to reduce the likelihood of data access by ransomware via a client server.

4. **Protect and secure client nodes**—Secure client nodes and subject them to regular security audits and scans. On critical systems, audits should include a review of the logs, the size of files and the incremental change rate.

5. **Manage security patches and alerts**—Veritas developed NetBackup software and NetBackup Appliances with security as a primary engineering requirement. We test each element of the Appliance, including its Linux operating system and the core NetBackup application, for vulnerabilities using industry standards and advanced security products. These measures minimize exposure to unauthorized access and resulting data loss or theft.

   We verify each new version of NetBackup and NetBackup Appliance software and hardware for vulnerabilities before release. Depending on the severity of issues found, Veritas releases a patch or provides a fix in a scheduled release. To reduce the risk of unknown threats, Veritas regularly updates the third-party packages and modules in the product as part of regular maintenance release cycles.

6. **Test your disaster recovery plan**—Disaster recovery testing is required to secure a backup environment. To confirm ransomware readiness, it's important to routinely test failover in the event of a disaster and/or security breach as well as restores.

7. **Recover from data spillage**—Data spillage is the transfer of classified or sensitive information to unaccredited or unauthorized systems, individuals, applications or media such as the transfer of encrypted financial records to an unauthorized email client. Data spills are becoming more common because the trend toward increased information sharing has weakened access controls. When data spills are combined with low end-user security awareness, unmanageable networks and poorly implemented data policies, organizations lay a ready inroad for ransomware. It's important to manage NetBackup role-based access to harden the NetBackup Master server and protect the data it accesses.

8. **Perform frequent security audits, reviews and training**—It's difficult to overestimate the value of frequent audits and security training. Ransomware generally infects corporate environments through human activity, often spread through phishing emails or drive-by downloads that can occur when a user visits an infected website. Ongoing employee training and frequent systems auditing help to mitigate the risk of ransomware attacks.

9. **Ensure critical systems protection for the backup server**—All Veritas Appliances have critical systems protection, providing security from installation of unauthorized executables.

CONCLUSION

Ransomware presents a serious threat to today's data-driven organizations, with potentially severe economic and social consequences. Although some may consider backup and recovery to be the last line of defense against ransomware, it's perhaps better framed as a meaningful part of proactive strategic planning. A reliable, tested backup and recovery strategy will minimize the risks to your business and its systems and provide the confidence you need to thrive in the face of a ransomware attack, ensuring data availability and business continuity.

ABOUT VERITAS

Veritas Technologies is a global leader in data protection and availability. Over 50,000 enterprises—including 87 percent of the Fortune Global 500—rely on us to abstract IT complexity and simplify data management. The Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas Enterprise Data Services Platform supports more than 800 different data sources, over 100 different operating systems, more than 1,400 storage targets, and more than 60 different cloud platforms. Learn more at www.veritas.com. Follow us on Twitter at @veritastechllc.

2625 Augustine Drive, Santa Clara, CA 95054
+1 (866) 837 4827
www.veritas.com

For specific country offices and contact numbers, please visit our website.
www.veritas.com/company/contact

VERITAS

V1004 07/20