EMC²

PREVENTING A RANSOMWARE DISASTER

Ransomware is not just another cyberattack; it can quickly proliferate through shared folders.

ABSTRACT

Ransomware is a threat to businesses that already costs millions of dollars each year, and unfortunately grows more sophisticated. Fortunately, Mozy and Spanning by EMC can help you to protect endpoint and SaaS application data with easy-to-deploy, efficient, and cloud-based backup solutions.

June 2016

To learn more about how you can prevent a ransomware disaster with endpoint data protection, visit Mozy. For more information about protecting your SaaS data, visit Spanning.

Part Number H15174

TABLE OF CONTENTS

INTRODUCTION

Ransomware is a threat that already costs millions of dollars for businesses each year and unfortunately grows more sophisticated. Using a variety of attacks, including targeted emails and infected websites, criminals can inject malware into your network, which then holds your data or other systems hostage until you pay a ransom. It's very difficult to block every ransomware attack, so many experts, including the FBI, advise organizations to have a layered defense with protected backups to enable a fast recovery. Organizations following this advice often focus on key internal systems and forget about their endpoints—desktops and laptops—and SaaS applications, which contain data that is critical for employees to function. Fortunately, Mozy and Spanning by EMC can help you to better protect your data with easy-to-deploy, efficient, and cloud-based backup solutions.

THE RISE OF RANSOMWARE

The first known ransomware was Trojan.Gpcoder, which was discovered in 2005 and affected Windows operating systems. More than 10 years later, there is little doubt that ransomware is on the rise. In fact, new ransomware growth increased by 58 percent for the second quarter of 2015, according to a recent McAfee Labs Threat Report.[1] There is no compelling reason to believe that the threat of this type of malware will not continue to increase dramatically. The reason is simple: "Ransomware is easy to develop, simple to execute, and does a very good job of compelling victims to pay to regain access to their precious files or systems."[2]

A recent analysis summary by Recorded Future noted dramatic increases of ransomware infections in Europe when compared to just a year ago.[3] Although ransomware knows no geographical boundaries, the top six countries affected by this type of malware are the United States, Japan, United Kingdom, Italy, Germany, and Russia.[4] Consider the following ransomware attack that occurred earlier this year.

Cyberterrorists hijacked a large U.S. medical center's computer system, thereby preventing access to the hospital's data by encrypting it. Initially, hackers demanded $3.6 million in return for releasing the data. Although the attackers later decreased their demands to 40 bitcoins (worth US$17,000) in exchange for a decryption key, they had made a point to the world: patient data and medical records are not safe from hackers. After all, if this Los Angeles hospital's information could be held for ransom, why couldn't another's? Which is, in fact, the reality: any type of organization, including medical, government, education, industry, etc. can be the target of a ransomware extortion plot.

WHAT IS RANSOMWARE AND HOW DOES IT SPREAD?

Ransomware is not just another cyberattack; it can quickly proliferate through shared folders, affecting both those within and outside the infected organization. Ransomware either locks the computer (locker ransomware) or encrypts the user's files (crypto ransomware) and then demands that the user pay a specified amount of money—usually a digital payment such as Bitcoin as was the case for the Los Angeles medical center—in exchange for a decryption key that unlocks the computer or files.

Ransomware gains access to a computer system by way of a network's weakest link, which is typically a user's email or social networking site. Once a user clicks on a malicious link or opens an infected attachment, the malware spreads throughout the system. Once opened, fake PDF files, fabricated FedEx and UPS notices, and fraudulent financial institution correspondence that are infected with malware can quickly bypass an organization's network security and spread beyond the local system through network drives and other endpoints tied to file sync and share tools such as Microsoft OneDrive, Google Drive, and Dropbox.

According to the United States Computer Emergency Readiness Team (US-CERT), cybercriminals who use ransomware are so effective because they instill fear and panic into their victims, in part by displaying intimidating messages such as "Your computer was used to visit websites with illegal content. To unlock your computer, you must pay a $100 fine."[5] But ransomware has gained wide adoption among cybercriminals for other reasons as well: the ease by which it is created and deployed.

The gist of ransomware is simple: if you don't pay the ransom, you forfeit access to your computer and the data that's on it. And you further forfeit access for others to shared documents and data, compounding the impact exponentially. Unfortunately, victims who

[1] McAfee Labs Threat Report, page 33, Intel Security Group, August 2015.
[2] Ransomware a Favorite of Cybercriminals, Matthew Rosenquist, McAfee Blog Central; September 1, 2015.
[3] Locking Up Europe With Ransomware: Origination, Targeting, and Payment, Recorded Future, Inc., 2016.
[4] The evolution of ransomware, Version 1, page 5; Kevin Savage, Peter Coogan, Hon Lau; Symantec; August 6, 2015.
[5] Ransomware and Recent Variants, United States Computer Emergency Readiness Team; March 31, 2016.

pay the ransom might still not get their files back. The harsh reality is that the attacker might not supply the decryption keys. In fact, a recent survey found that of those victims of ransomware who paid the ransom, only 71 percent had their files restored.[6]

REALITY OF RANSOMWARE

The results of a 2015 Infosecurity Europe survey published by ESET revealed that 84 percent of respondents believed that their companies would be seriously damaged if infected by ransomware. Nearly a third of them (31 percent) admitted that they would be forced to pay the perpetrators in order to get their decrypted data back.[7]

Businesses know that it's very difficult to protect against every threat, but ransomware is particularly challenging. For example, "CryptoWall, the current leader in ransomware, is highly sophisticated and uses unbreakable encryption. If you have no current backups you are toast…," according to Stu Sjouwerman, author and anti-spyware expert.[8]

Crypto ransomware, such as CryptoWall, accounts for the majority of all ransomware, according to the latest Internet Security Threat Report. "Never before in the history of human kind have people across the world been subjected to extortion on a massive scale as they are today."[9] The number of crypto ransomware types amounted to 362,000 in 2015 (up 35 percent from the previous year) and averaged 992 per day.[10]

Although you and your data might not fall victim to CryptoWall, there are literally millions of new malware variants added each year. There were 431 million variants added in 2015, up 36 percent from the previous year.[11] Effectively defending against ransomware requires not only threat detection and prevention, but a backup and recovery strategy. Failing to do so can result in significant costs. Consider that recent research found that 36 per cent of participants of global public and private organisations surveyed have suffered unplanned system downtime and/or data loss due to an external or internal security breach. The estimated average cost to each of those organisations experiencing system downtime in the last 12 months is £385,000. Even more significant is the estimated cost to organisations that have experienced data loss in the last 12 months—£635,000. Clearly, your data needs to be protected—and you need to be confident in the readiness of your protection.[12]

WHAT CAN BE DONE?

Data that's key to an organization's daily operations or that's subject to regulatory compliance must always be protected. Hackers don't necessarily care who the information belongs to; they will do their best to exploit any weakness in the IT infrastructure to steal, damage, or hold for ransom an organization's data. Like most criminals, cybercriminals are opportunists who seek out easy targets. Are you an easy target? For starters, consider these questions:

- Are your employees aware of the risks of unsolicited emails?
- Are your firewalls and mail filters always up to date?
- Are you using expired antivirus software?
- Are you syncing data from endpoints up to cloud-based file sync share systems?

It is important to note that common backup solutions such as a USB drive or network-attached storage device (NAS) are not reliable methods for backing up and safeguarding your data. Ransomware typically spreads throughout an organization's entire file system, including an attached drive or network share, encrypting both production data and backup data.

The most reliable form of protection organizations can leverage to safeguard their data is backup. The more your backup supports fast, easy restore to the pre-infection state, the less likely you will be to suffer a massive failure of business continuity. When looking for a backup solution, what should you evaluate to ensure that your data is protected? Consider the following:

- Is the backup off site (away from your primary site)?
- Can you verify that the backups are happening?

---

[6] Crypto-Ransomware: Survey of IT Experts, page 16, Jeffrey Henning, Researchscape International; February 4, 2016.
[7] UK Companies Commonly Held Hostage by Hackers, Urban Schrott, ESET Ireland; June 29, 2015.
[8] Ransomware victims: Just pay up, grin, and bear it, says the FBI, The Register; October 27, 2015.
[9] Internet Security Threat Report, Volume 21, page 58, Symantec, April 2016.
[10] Ibid., page 8.
[11] Ibid.
[12] EMC Global Data Protection Index, independent research by Vanson Bourne, March–April 2016.

- Can you verify that data can be restored to its original state?
- How quickly can you restore data that's taken hostage?

Having a viable backup and recovery plan is not just a sound operational practice, it is often required by law or regulation, depending on your organization's industry or type:

- HIPAA requires healthcare organizations to have and periodically test a viable data backup and disaster recovery plan for their electronic protected health information.[13]
- Two financing and banking enforcement arms, the OCIE and FFIEC, have made cybersecurity—including the ability to recover from incidents—a key part of their enforcement and audit priorities.[14]
- The SEC has reminded public companies of their need for adequate cyber controls, which include backup and recovery functions, and responsibility to disclose material cybersecurity risks. In today's world, certainly the inability to recover from an increasingly common threat such as ransomware could rise to the level of disclosure.[15]

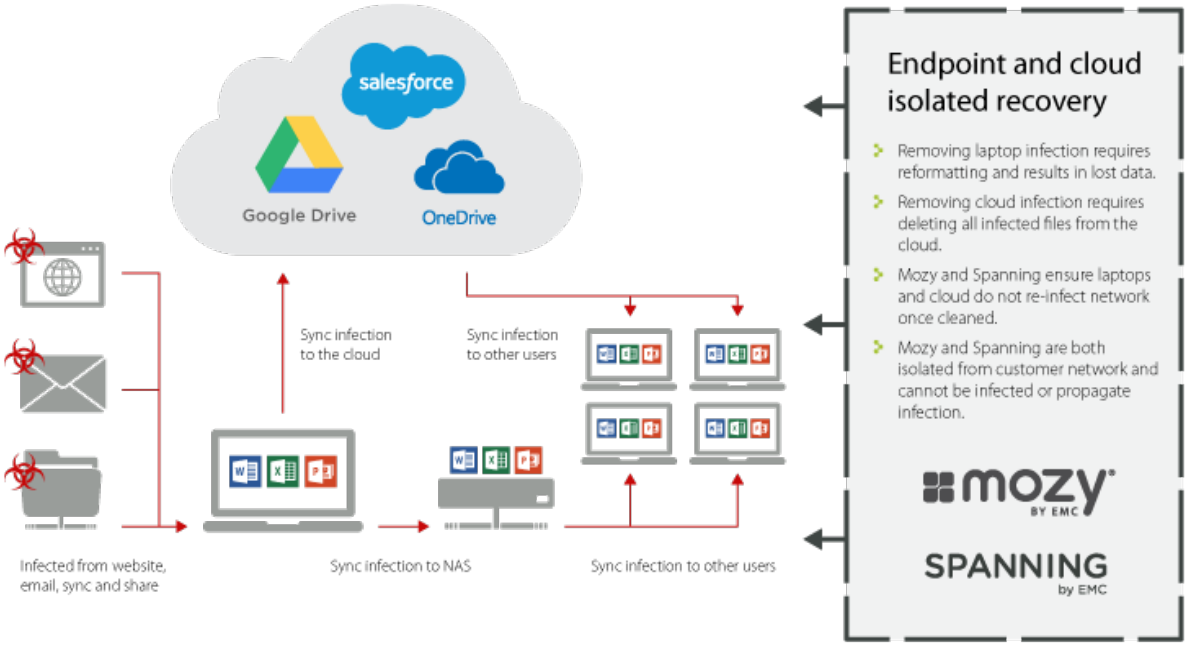
In the event of hardware failure, theft, virus attack (including a ransomware extortion plot!), accidental deletion, or natural or man-made disaster, if you have the right backup and recovery solutions in place, you can ensure that your data will be available and can be restored to its original state, and that your organization is compliant with applicable regulations.

BACKING UP YOUR DATA WITH EMC

You can prevent a ransomware data loss disaster by backing up your valuable data with reputable data protection solutions from EMC.

It starts at the endpoint

Recovering servers doesn't guarantee you've removed the infection from your network because it probably started at the endpoint as illustrated in the following graphic. Data that's backed up by Mozy and Spanning—both from EMC—is isolated from the customer network and cannot be infected or propagate an infection.



[13] HIPAA Security Rule, 45 CFR 164.308(7).
[14] National Exam Program Risk Alert, Volume IV, Issue 8; September 15, 2016.
[15] Emerging SEC guidance and enforcement regarding data privacy and breach disclosures, Joseph D. Masterson, Inside Counsel; June 25, 2015; and Cybersecurity Update: Heightened Concerns, Legal and Regulatory Framework, Enforcement Priorities, and Key Steps to Limit Legal and Business Risks, Paul Weiss; September 30, 2015.

Endpoint data protection from Mozy by EMC

Mozy cloud backup ensures that your important endpoint files and server data cannot be compromised by ransomware. Due to its unique backend technology, Mozy prevents any execution of code within the files that have been backed up. But simple backup in and of itself is not enough to ensure that your files are protected from ransomware.

When a malware infection is involved, restoration of an endpoint or server from a backup works best when you can easily select a moment in time from where to restore. Mozy keeps up to 90 days of file versions, meaning if you have identified the point of infection (user and file) and the time the malware was introduced to the machine, Mozy can restore all of the files for the given user from the point in time just before the malware was introduced. For example, if the malware was introduced on June 2, you can restore files from the June 1 backup.

SaaS data protection from Spanning by EMC

SaaS office productivity platforms such as Google Apps or Microsoft Office 365 are also vulnerable to malware attacks, and Google or Microsoft may not be able to quickly roll back your files to a pre-infected state. Infected endpoint devices can sync with these platforms, and in some cases the malware can automatically proliferate through shared drives and folders, encrypting files shared within your and even outside of your organization.

Spanning Backup fully protects data that is stored and generated in Google Apps and Office 365 and enables you to rapidly recover data from a previous point in time, before the files were encrypted by ransomware.

Backing up and protecting your organization's mission-critical data with Mozy and Spanning backup solutions provides peace of mind, knowing that you can quickly and easily restore your data exactly the way it was at any point in time should a data loss event strike. That means your data is safe, secure, and always available. These solutions ensure that you can respond and recover from an attack, and rapidly restore your data to its original state for business continuity and to meet recovery time and recovery point objectives (RTO and RPO).

CONCLUSION

According to ESET Ireland, ransomware is becoming more aggressive with new capabilities and continuous waves of variants.[16] Although prevention and detection are critical, a regularly updated backup that enables rapid, accurate restores is the last line of defense. "…[T]he use of backup files is an effective way to minimize the impact of ransomware and…implementing computer security best practices is the most effective way to prevent ransomware infections. Individuals or businesses that regularly back up their files on an external server or device can scrub their hard drive to remove the ransomware and restore their files from backup. If all individuals and businesses backed up their files, ransomware would not be a profitable business for cybercriminal actors."[17]

Organizations rely on digitized data more than ever. As such, all organizations—from the smallest business to the largest enterprise—must take the necessary steps to ensure that their data is securely backed up and quickly restorable to its original state.

For more information on how you can prevent a ransomware disaster with endpoint data protection, visit Mozy. And, to learn how to protect your SaaS data, visit Spanning.

---

[16] Jigsaw and how ransomware is becoming more aggressive with new capabilities, Urban Schrott, ESET Ireland; May 4, 2016.
[17] U.S. Department of Justice, Federal Bureau of Investigation, Letter to Senator Ron Wyden, February 8, 2016.