RANSOMWARE: FREQUENTLY ASKED QUESTIONS

SECTION 1: RANSOMWARE OVERVIEW

What is ransomware?

Ransomware is a form of malicious software designed to either block access to a computer system or encrypt a user's files or other data. The cybercriminal then demands a ransom (usually in the form of virtual currency, such as Bitcoin, which is difficult to track), at which point the perpetrator might (there is no guarantee!) provide instructions that explain how to regain access to their system and files. Ransomware is often aimed at individuals; however, businesses—including enterprises—have become targets as well.

Why should I be concerned about ransomware?

Ransomware is a growing threat; in fact, there are literally millions of new malware variants each year. You must have a plan in place to combat this form of cybercrime.

How does ransomware propagate?

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. More often than not, criminals will target informed users through phishing emails and dubious web links. Once a user clicks on a malicious link or opens an infected attachment, the malware spreads throughout the system. Once opened, files that are infected with malware can quickly bypass an organization's network security. The malware may also reside within files on end-user machines. If those files are synced or stored in a collaboration platform where other users can access them, the malware can also spread from machine to machine.

How is ransomware detected?

A ransomware attack usually goes undetected until after the malware has infected the system. Often, a message appears on the user's computer screen informing them that their computer has been locked and/or that their files are encrypted.

What can I do to protect myself from ransomware?

You can utilize whitelisting, filtering, quarantining, antivirus, and system scans in an attempt to prevent ransomware. However, criminals are resourceful and persistent; all it takes is one click to become infected. The best way to protect yourself from ransomware is to have a reliable backup that can return your files uninfected. Backups should be frequent and reliable to ensure you can recover data to a point in time prior to the attack.

Why is sync not a good backup method?

Sync is not backup. All changes executed on the source file, including ransomware, get quickly synchronized to the cloud and all other users who have access to the file. Additionally, sync services that offer versioning or trash bins require the user to select individual files to restore one at a time as opposed to an entire point-in-time snapshot, whereas a backup service allows specific files or all files from a specific date to be restored with a few clicks. Thus, a sync service provides convenient access to files, but a backup service provides a much more comprehensive restore experience in the event of disaster. Additionally, a sync service can unintentionally serve as a vehicle for propagating malware across multiple computers and devices.

SECTION 2: RANSOMWARE AND MOZY

How is Mozy data protected from a ransomware attack?

Mozy customer data is stored in the EMC cloud, which is isolated from the customer's environment. Additionally, the EMC cloud is a non-executing environment, which means that programs, including viruses, cannot execute or "run" in the cloud and cannot infect files stored there.

What's the process to restore uninfected data with Mozy?

Once you have identified all of the affected users, eradicated the malware, and isolated when the infection occurred, you can restore data from a particular backup that was completed prior to the infection.

What if my Mozy backup includes the malware?

The Mozy cloud is a non-executing environment, which means that programs, including viruses, cannot execute or run in the cloud and cannot infect files stored there. Additionally, 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. This is sometimes referred to as a rollback.

SECTION 3: RANSOMWARE AND SPANNING

How can data in Google Drive or OneDrive for Business become infected with ransomware?

Most organizations that leverage Google Drive or OneDrive for business deploy synchronization services on their end-user endpoints (laptops), so they can easily access, edit, and then synchronize file changes back to the cloud and down to all other users who have shared access to the files. When ransomware attacks an endpoint, such as a laptop, files that are encrypted by the ransomware are synchronized to the cloud and propagate to other users in your organization, or worse, partners or customers outside of your organization.

How is data in Spanning Backup protected from a ransomware attack?

Customer data stored in Spanning Backup is isolated from the customer's environment. All data is stored in Spanning's SSAE SOC 2 compliant cloud environment and is isolated in a non-executing environment, which means that programs, including viruses and malware, cannot execute and infect files stored there.

What is the process for restoring uninfected data with Spanning?

Once you have identified all of the affected users, eradicated the malware, and isolated when the infection occurred, you can restore data directly back into Office 365 or Google Apps from any of the point-in-time backups in Spanning Backup. Once the data is restored, it can then be synchronized back down to the endpoints. Additionally, organizations could choose to suspend sync services while the infection is still present and only allow users to edit documents in the cloud services like Google Docs and Office 365's online versions of Word, Excel, and PowerPoint.

CONTACT US

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

EMC², EMC, the EMC logo, Mozy, and Spanning are registered trademarks or trademarks of EMC Corporation in the United States and other countries. © Copyright 2016 EMC Corporation. All rights reserved. Published in the USA. 06/16, Handout, H15180.

EMC believes the information in this document is accurate as of its publication date. The information is subject to change without notice.