Whitepaper: January 2015 Virus Backup Update

Regular data backups:

The only sure way to knock out threats from Crypto-style viruses

One of the biggest data security threats of 2013 – CryptoLocker – has brought the term “ransomware” to new levels of awareness. That’s because CryptoLocker is one of the most infamous examples of a virus that renders data files unusable unless the victim pays for a key to unlock the infected files.

According to recent reports, ransomware attacks grew by 500 percent in 2013, led by CryptoLocker – which first appeared in late summer 2013, and escalated sharply throughout the remainder of the year.

Like many viruses, CryptoLocker is triggered by clicking on a link sent in an email, or by downloading and opening an email attachment. When combined with phishing techniques, some of these emails may seem like a normal, harmless request from a business partner.

The good news is that by mid-2014, law enforcement had shut down the botnet used to distribute the CryptoLocker virus. Two organizations also came up with a Web tool purportedly able to unlock individual encrypted files.

The bad news is that there are CryptoLocker imitations such as CryptoWall and TorrentLocker. So, unfortunately, the threat from this type of virus is very much alive. And with the introduction of anonymous payment systems such as Bitcoin, it’s a pretty sure bet that this type of cyber extortion will continue.

So how do you protect against Crypto-style viruses?

Isn’t it as simple as instructing employees to never click on suspicious attachments or links of unknown origin?

Unfortunately, that method of protection doesn’t work all the time. Employees get careless or don’t adhere to policy, and if the virus is embedded within a well-targeted phishing attack, it’s possible for someone to make a mistake.

So, yes, setting a clear policy regarding suspicious emails, links, and attachments should be your first step – part of your “Plan A” for protection – but it’s hardly foolproof.

Pinning all your hopes on data security vendors being able to spot and remove all phishing attempts or on other specialists being able to devise software to unencrypt ransomware, also falls short of foolproof. Of course you should have firewall protection and security software, but that won’t guarantee complete protection.

Since total immunity from these viruses can’t be counted on, that leaves us with mitigation measures that help an organization with infected files get back to normal.

Regular data backup is the answer. It’s a surefire “Plan B” should efforts to protect against Crypto-style viruses ever fail.

CARBONITE™

ENSURING BUSINESSES ARE ALWAYS IN BUSINESS

It's important that your backup solution has versions that can be rolled back to a specific date. While ransomware will make itself known soon after infection, there may be a lag time of a few hours to a few days before the virus spreads to encrypt most of your files and the ransom message appears.

On shared drives found in businesses, this can be a huge problem if suddenly your files can't be used. And creating new files only creates more infected files. So the only way to get things back to normal is to roll back to a complete, clean set of files that was backed up before the initial entry point of the virus.

There is work and costs involved in rolling back all of your data and bringing everything back up under fresh installs of your system's software and applications, but let's face it, what's the alternative if you aren't backing up?

Paying the cybercriminals might get you a code that will unlock your data, or it might not. After all, these aren't exactly trustworthy individuals you are dealing with. You might hope that the encryption used isn't really all that strong and can be broken, but you can't count on that as a solution. And in the meantime, your data is locked.

So, the most effective mitigation strategy for Crypto-style viruses is to have regular, versioned backups in place.

There's added costs to saving more data more frequently, but depending on the nature of your business, it may be worth the peace of mind and risk reduction to have a more frequent, full data backup.

It also helps to have strong support services to walk you through recovery steps should you ever fall victim to one of these viruses, and to also offer options – like being able to overnight you a clean set of files on disk to speed up file restoration.

The great thing about automatic backup solutions is that they don't just mitigate Crypto-style viruses, they protect you from other causes of data loss, such as server failure, disk failure, or a natural disaster that wipes out your server room. The risk mitigation step here addresses overall systems continuity.

So by all means, set some serious policy about unknown emails and the like, and educate all your employees about nasty threats like Crypto. Just remember, there is a cost to being too draconian with prevention. Your people need to be able to collaborate with business partners without too many hurdles in the way.

Most small to mid-sized businesses (SMBs) can't build a hyper-secure private cloud in which to conduct absolutely all collaboration, and we certainly can't go back to the days of faxes and paper forms.

But, for sure, you can take the necessary protection measures and combine them with regular backups as a sure way to knock back the damage from one of these viruses should your business ever fall victim.

Jim Flynne
Vice President, Operations
Chief Security Officer
Carbonite, Inc.

CARBONITE™

ENSURING BUSINESSES ARE ALWAYS IN BUSINESS