Ransomware preparedness and recovery guide

By Jim Flynne, Vice President of Operations, Carbonite

Ransomware has proven to be phenomenally effective at producing a fortune in ransom payments for its nefarious authors. It's been estimated that cybercrime cost the global economy $445 billion in 2016—and ransomware was the primary driver. The astonishing "success" of ransomware makes one thing certain: It's only a matter of time before the next form of malicious ransomware strikes. There are steps you can take to prevent an attack, and a few ways to get your data back if your systems become infected. The first step is knowing what ransomware is and how it extracts payments from victims.

Ransomware overview

Ransomware is a type of malware that prevents users from accessing their data until they pay a ransom. Most ransomware viruses are triggered by clicking a link in an email or opening an attachment. When combined with phishing techniques, these emails may seem like normal correspondence from a business partner.

Recent forms of ransomware

Ransomware in its various forms has been around since 1989, and it shows no signs of slowing down. The problem has gotten worse in recent years due to the popularity of mobile devices and anonymous payment methods, like Bitcoin, which make it easier for cybercriminals to cover their tracks and evade law enforcement.

How to prepare for a ransomware attack

It's important to warn employees about clicking on suspicious attachments, but they may fail to adhere to the policy or simply be fooled by a well-targeted phishing attack. Additionally, while firewall protection and security software are crucial components in a ransomware-prevention strategy, they won't guarantee protection. When prevention methods fail, the best way to regain access to your data is by having a backup plan in place.

Since the latest version of your files may be affected by the virus, a backup solution with a versioning feature is necessary. It allows you to roll back to a specific date before your systems were infected. Although ransomware will eventually make itself known to you, the virus can take hours or days while it spreads and encrypts your files before sending you the ransom message. On shared drives, this is a huge problem when suddenly, not only are your files unusable, but creating new ones results in more infected files. The only

Common types of ransomware

CryptoLocker—summer 2013

- Infected over 250,000 computers
- Generated nearly $30 million for cybercriminals in about 100 days
- Shut down in mid-2014 by law enforcement

CryptoWall—November 2013

- Steals potentially valuable data from infected systems

TorrentLocker—August 2014

- Includes components of CryptoLocker and CryptoWall
- Typically distributed via emails that pretend to be shipping notifications, motor vehicle violations, or other corporate or government correspondence

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 infection took place.

This is where the frequency of your backups becomes a key component of your recovery strategy. The more frequently you back up, the more recent your recovery point can be. Having automatic, continuous backups also ensures data protection with minimal human intervention. Depending on the nature of your business, it may be worthwhile to run more frequent, continuous backups.

An added benefit of using a backup plan as part of a prevention strategy is that it also protects you from other common causes of data loss, such as server or disk failure, natural disasters, and human error.

While any data recovery effort costs time and resources, paying a ransom might be an even bigger risk since it doesn't necessarily guarantee you'll get your data back. You're essentially counting on the trustworthiness of thieves to give you the encryption key after they've taken your money. With a complete backup of your data that includes an earlier version of your system before it became infected, you stand a very good chance of recovering most of your data without ever having to pay a ransom.

Five steps to take if your systems become infected

If you have a comprehensive malware-prevention strategy in place and a backup plan is part of it, here are the five steps you should take if your systems become infected:

1. As soon as you're aware of an attack on your computer, file server or network, immediately shut down all file sharing activity.
2. Use your antivirus software to determine where the infection happened. If you can't determine where the infection originated using antivirus software, right click on an infected file to find out the last user or computer to make changes to the file. This will tell you where the infection originated.
3. Assess the extent of the infection and the damage.
4. Remove the virus by deleting all infected files.
5. Use your backup application or dashboard tool to recover clean versions of the infected files.

At Carbonite, we've had thousands of customers tell us they were able to recover successfully after a ransomware attack without having to pay a ransom. Most were able to restore all their data, sometimes in just a half-hour.

Learn more about Carbonite backup and disaster recovery solutions today.

Phone: 800-683-4667
Email: DataProtectionSales@carbonite.com

CryptoFortress—March 2015

- Similar to TorrentLocker in appearance
- Uses 2048-bit RSA-AES encryption

Pacman

- Uses authentic-looking Dropbox links to fool victims
- Initial targets were Danish chiropractors who received phishing emails with the subject line, "possible new patient"

Locky—February 2016

- Spread via Microsoft Word documents, Adobe Flash and Windows Kernal
- Used frequently to target hospitals and health care organizations