Ransomware: This Threat Will Stop Your Business & Hold You Hostage

Don’t be a Victim!! NSA has Your Answer!

By: Brian Weaver/VP, Cloud & Managed Services - NSA
Ransomware: This Threat Will Stop Your Business & Hold You Hostage
Don’t be a Victim!! NSA has Your Answer!

By: Brian Weaver/VP, Cloud & Managed Services - NSA

Ransomware has emerged as a major threat to individuals and businesses alike. Ransomware, a type of malware that encrypts data on infected systems, has become a way for cyber criminals to cash in at your expense. When the malware is run, it locks your files and demands a “ransom” payment to release them so you can use your computer again.

Ransomware is Spreading Like the Flu

Unless you’ve been living under a rock, you are probably well aware that ransomware is a hot topic in the news these days. Organizations of all types and sizes have been impacted, but small
businesses can be particularly vulnerable to attacks. And ransomware is on the rise. In a recent study conducted by security software vendor McAfee Labs, researchers identified more than 4 million samples of ransomware in Q2 of 2015, including 1.2 million new samples. That compares with fewer than 1.5 million total samples in Q3 of 2013 (400,000 new). Ransomware is like the flu virus: it’s difficult to protect against it because it’s constantly evolving and distributed in a variety of ways. In fact, new estimates from the FBI show that costs from ransomware have reached an all-time high. Cyber-criminals collected $209 million in the first 3 months of 2016 by extorting businesses and institutions to unlock computer servers. At that rate, ransomware is on pace to be a $1 billion a year crime this year. Even worse, this estimate may be very low, as the FBI told CNN that few companies actually report the losses, concerned about the negative publicity. If you look at the chart below, you can see how quickly new ransomware is spreading:

**How Ransomware is Spread**

Spam is the most common method for distributing ransomware. It is generally spread using some
form of social engineering; victims are tricked into downloading an e-mail attachment or clicking a link. Fake email messages might appear to be a note from a friend or colleague asking a user to check out an attached file, for example. Or, email might come from a trusted institution (such as a bank) asking you to perform a routine task. Sometimes, ransomware uses scare tactics such as claiming that the computer has been used for illegal activities to coerce victims. Once the user takes action, the malware installs itself on the system and begins encrypting files.

*It can happen in the blink of an eye with a single click.*

Another common method for spreading ransomware is a software package known as an exploit kit. These packages are designed to identify vulnerabilities and exploit them to install ransomware. In this type of attack, hackers install code on a legitimate website that redirects computer users to a malicious site.
Unlike the spam method, sometimes this approach requires no additional actions from the victim. This is referred to as a “drive-by download” attack.

How to Protect Yourself Against Ransomware

While mid-sized businesses aren’t specifically targeted in ransomware campaigns, they may be more likely to suffer an attack. Frequently, small business IT teams are stretched thin and, in some cases, rely on outdated technology due to budgetary constraints. This is the perfect storm for ransomware vulnerability. But there are ways you can protect your business against ransomware attacks. Security software is essential, however, you can’t rely on it alone.

A proper ransomware protection strategy requires a three-pronged approach, comprising of education, security and backup:

1) **Education**: It is critical that your staff understands what ransomware is and the threats that it poses. Provide your team with specific examples of suspicious emails with clear instructions on what
to do if they encounter a potential ransomware lure (i.e. don’t open attachments. If you see something, say something, etc.). Conduct bi-annual formal training and new employee training to inform staff about these risks and keep them top of mind.

2) Security: Antivirus software should be considered essential for any business to protect against ransomware and other risks. Ensure your security software is up to date, as well, in order to protect against newly identified threats. Keep all business applications patched and updated in order to minimize vulnerabilities. Some antivirus software products offer ransomware-specific functionality. Sophos, for example, offers technology that monitors systems to detect malicious activities such as file extension or registry changes. If ransomware is detected, the software has the ability to block it and alert users. However, because ransomware is constantly evolving, even the best security software can be breached. This is why it is absolutely crucial to have a second layer of defense to ensure recovery in case malware strikes – Backup & Restore!!!

3) Backup: Modern total data protection solutions, take snapshot-based, incremental backups as frequently as every five minutes to create a series of recovery points. If your business suffers a ransomware attack, this technology allows you to roll-back your data to a point-in-time before the corruption occurred. When it comes to ransomware, the benefit of this is two-fold. First, you don’t need to pay the ransom to get your data back. Second, since you are restoring to a point-in-time before the ransomware infected your systems, you can be certain everything is clean and the malware cannot be triggered again.
Common Types of Ransomware

**Cryptolocker:** Started in 2013, distributed via exploit kits and spam. Losses to business in the millions.

**Cryptowall:** First appeared in early 2014, copies itself to Microsoft temp folder and begins encoding files. When encryption is complete, displays ransom message.

**CTB-locker:** actually “outsource” the infection process to partners for a share of the ransom profits. Copies itself to the Microsoft temp directory and uses Elliptic Curve Cryptography (ECC) – impacting more files than Crypto-locker.

**Locky:** Spread using spam, typically in the form of an email message disguised as an invoice. When opened, the invoice is scrambled and victim is instructed to enable macros to read the document. When macros are enabled, Locky begins encrypting a large array of file types. Bitcoin ransom is demanded once encryption is completed.

**TelsaCrypt:** One of the newer forms of ransomware, attacking Adobe vulnerabilities. Once through, it is distributed via the Angler exploit kit. Once encryption is complete, ransom is paid via Bitcoin, PaySafeCard or Ukash.

**Torrentlocker:** distributed via spam or email, and in addition to encoding files, also collects email addresses form victims address book to spread malware beyond initially infected computer network. This malware also deletes Microsoft Volume Shadow Copies to prevent restores using Windows recovery tools.

**Jigsaw:** One outrageous newer example is Jigsaw Ransomware. Once infected, you get a message stating “Your computer files have been encrypted. Your photos, videos, documents, etc.. But don’t worry! I have not deleted them, yet. You have 24 hours to pay $150 USD in Bitcoins to get the decryption key. Every hour files will be deleted, increasing in amount over time. After 72 hours all that are left will be deleted.”
NSA’s Instant Virtualization: Protects Against Ransomware and Eliminates Downtime

Additionally, some data protection products today (like those from NSA) allow users to run applications from image-based backups of virtual machines. This capability is commonly referred to as “recovery-in-place” or “instant recovery.” This technology can be useful for recovering from a ransomware attack as well, because it allows you to continue operations while your primary systems are being restored and with little to no downtime. NSA’s version of this business-saving technology is called Instant Virtualization, which virtualizes systems either locally or remotely in a secure cloud within seconds. This solution ensures businesses stay up-and-running when disaster strikes!

To find out more about NSA’s online backup & restore, please contact:

Brian Weaver, Vice President of Cloud Services at NSA Professional Services: 516.240.6020 ext. 114 or email bweaver@nsacom.com.