Precautions To Take Against Ransomware

NEWMIND

CONTENTS

There's a malware threat online, maybe lurking in your inbox or spam folder, called Ransomware. It's been around for a while, but recent months have seen it gaining traction, under different names you may have heard, such as Cryptolocker, Cryptowall, and TeslaCrypt.

WHAT IS RANSOMWARE?

One of the ways that Ransomware makes its way to end users is through a well-crafted email with an attachment. The attachment is malicious and when you click to download it, the ransomware encrypts (locks) certain types of files (.docx, .pdf, .jpg, etc) stored on local and mounted network drives, such as a server shared drive at the office. It then displays a message which offers to decrypt the data if a payment is made by a certain deadline—and threatens to lock the data permanently if the deadline passes.

Although the malware itself can quickly be removed, the encrypted files stay encrypted, in a way that researchers consider infeasible to break. Some victims claim that paying the ransom did not always lead to the files being decrypted. The current advice is to not pay the bad guys, and to recover as much data as possible on your own.

A big challenge with the newer versions of ransomware is that they get around email spam filters, most antivirus solutions, and most firewalls. So what's your best defense right now?

> As a user, you should very careful when clicking links, and the files you download through email! For any IT support reading this, your number one priority will be to get a solid backup system in place.

Ready to learn more? Call today.

(877) 230-5284

or email info@newmindgroup.com

WHO IS IT AFFECTING?

The top 3 countries being targeted with ransomware attacks are the US, Canada, and Italy, though attackers are targeting any and all users they can reach with their malware. In 2015, victims paid an average ransom of $300 per infected device, and globally ransomware attacks amounted to $325 million in damages.

Ransomware attackers are targeting anyone vulnerable enough to become infected, but the groups running the highest risk are organizations lacking sophisticated IT security, such as small businesses and public institutions. These organizations have data that they can't afford to lose (such as government records), and a low-security network for the ransomware to spread through after the first victim is hit.

RANSOMWARE-AS-A-SERVICE

Ransomware-as-a-service (RAAS) refers to a number of Ransomware variations which are packaged into a kit easy enough for an amateur to use. This means that anyone who can find and purchase a RAAS kit can begin attacking victims on their own, leading to a much higher volume of ransomware attackers in 2016.

COMMON FORMS OF RANSOMWARE

This list was originally published in the article "6 New Ransomware Threats to Look Out For in 2016"

CERBER

Cerber is contracted by opening a downloaded file from a questionable email or website. It targets Windows users, but only those located outside Russia or the former Soviet Union (otherwise Cerber deactivates without harming files). Cerber is very common and known to be linked with RAAS attackers.

Solution:

There is no current solution for Cerber outside of prevention and data backup.

CRYPTOLOCKER

Cryptolocker is contracted by opening a downloaded file (with a disguised file extension) from a questionable email or website. Once the downloaded file is opened, Cryptolocker saves itself to a folder in the user's profile, and adds a key to the registry to make sure it runs every time the computer starts up.

Solution:

There is no current solution for Cryptolocker outside of prevention and data backup, but disabling hidden file extensions in Windows will also help recognize this type of attack.

CRYPTOWALL

Cryptowall is very similar to Cryptolocker—contracted by opening a downloaded file (with a disguised file extension) from a questionable email or website. Once the downloaded file is opened, it saves itself to a folder in the user's profile, and adds a key to the registry to make sure it runs every time the computer starts up. It encrypts files with particular extensions on the computer and creates additional files with instructions on how to obtain the decryption key

Solution:

There is no current solution for Cryptowall outside of prevention and data backup, but disabling hidden file extensions in Windows will also help recognize this type of attack.

CRYPTXXX 3.0

Cryptxxx 3.0 is contracted by opening a downloaded file from a questionable email or website. It targets Windows users, and it comes packaged with a module that steals credentials, so that they can draw money from your account even if you refuse to pay the ransom.

Solution:

There is no current solution for Cryptxxx outside of prevention and data backup, but it is known that Adobe Flash and Adobe Reader are popular entry points, so remember to keep your software patched and up to date.

DOGSPECTUS

Dogspectus is Android ransomware automatically installed from an infected website (no user input required). It only affects Android systems older than version 5, but instead of encrypting data for a ransom, it merely locks the user out until a ransom is paid.

Solution:

There is no current solution for Dogspectus outside of prevention and data backup.

FANTOM

Fantom is contracted by opening a downloaded file from a questionable email or website. It targets Windows users, and once the file reaches your computer, it opens a window disguised as a Windows Update prompt. If the user approves the prompt, Fantom begins encrypting files, marking them with a .fantom extension, and leaving ransom notes throughout your computer.

Solution:

Currently Fantom has not been cracked, and there is no simple solution outside of prevention and data backup

LOCKY

Locky is contracted through malicious spam email. It targets Windows users, and it's designed to fool many forms of antivirus software.

Solution:

There is no current solution for Locky outside of prevention and data backup, but Trustwave suggests modifying your inbound email policy to block inbound .js attachments and macro-enabled Office documents.

PETYA

Petya is contracted by opening a downloaded file from a questionable email or website. It targets Windows users, and when run, it rewrites the master boot, which prompts a system restart, locking the user out, and delivering a message that files have been encrypted.

Solution:

Thankfully, an Petya has been cracked by a developer who created a decryption password generator.

TESLACRYPT

TeslaCrypt is a now-defunct form of ransomware contracted by opening a downloaded file (with a disguised file extension) from a questionable email or website. TeslaCrypt behaves similarly to Cryptolocker, but it targets game files on the target's computer (extensions like .xxx, .ttt, .micro).

Solution

In late 2015, TeslaCrypt's creators released master keys to unlock victim data, which have been packaged by security experts in a kit called TeslaDecoder.

PROTECT YOURSELF WITH THESE TIPS:

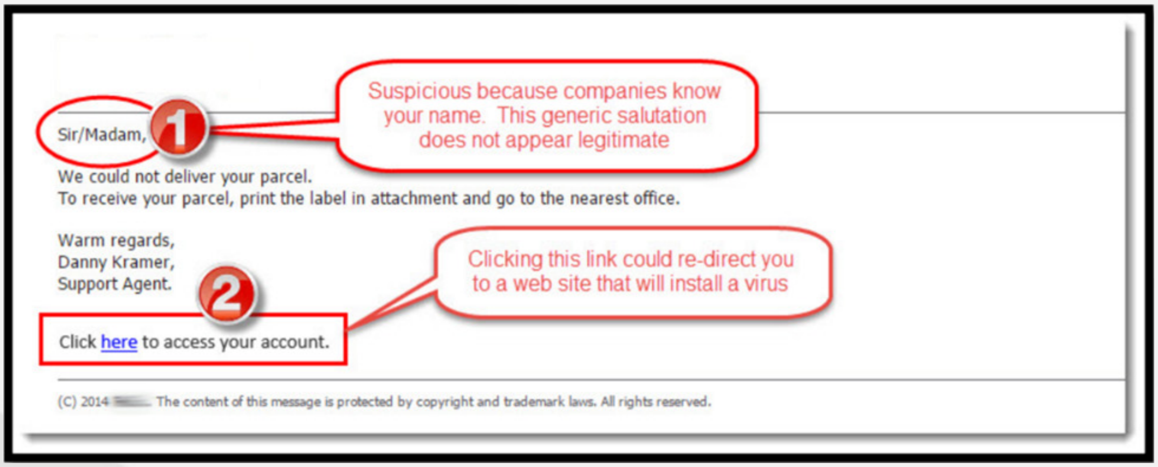
The threat also goes much deeper than the infection of a single user or device—once it begins infecting you, it can very easily spread throughout your entire organization's network, and lock out ***everyone***.

- **Good backup practices.**
  Workstations should save their important files to your organization's server, rather than locally. Ideally, those servers are set to back up at least every night. In some cases, Windows System Restore can be used to recover encrypted files, but the best solution is to keep all your data backed up in the first place, and to back those files up often!

- **Implement an antivirus solution**
  The ideal practice is to work with an antivirus solution that's cloud-managed, and it's important to remember that no single solution will protect you against everything. Coupling your solution with a product like Malwarebytes can cover a lot of what's out there. When looking at antivirus for your organization, here are some things to consider:
  - Easy deployment
  - Fast installation and scanning
  - Low system resource consumption
  - Mobile options for iOS & Android where applicable

- **Modify your inbound email policy**
  Block inbound attachments with .js extensions, as well as macro-enabled Office documents, as these are two popular mediums for infecting users via email attachments.

- **Make sure users look before clicking**
  Attackers disguise malicious emails to look as legitimate as possible, but a keen eye can spot it. Train your end-users on these cues! Are there spelling or grammar errors? Do the images and messaging match what you're used to seeing from that particular sender? Here's an example of a malicious email:



Sir/Madam,

We could not deliver your parcel.
To receive your parcel, print the label in attachment and go to the nearest office.

Warm regards,
Danny Kramer,
Support Agent.

Click here to access your account.

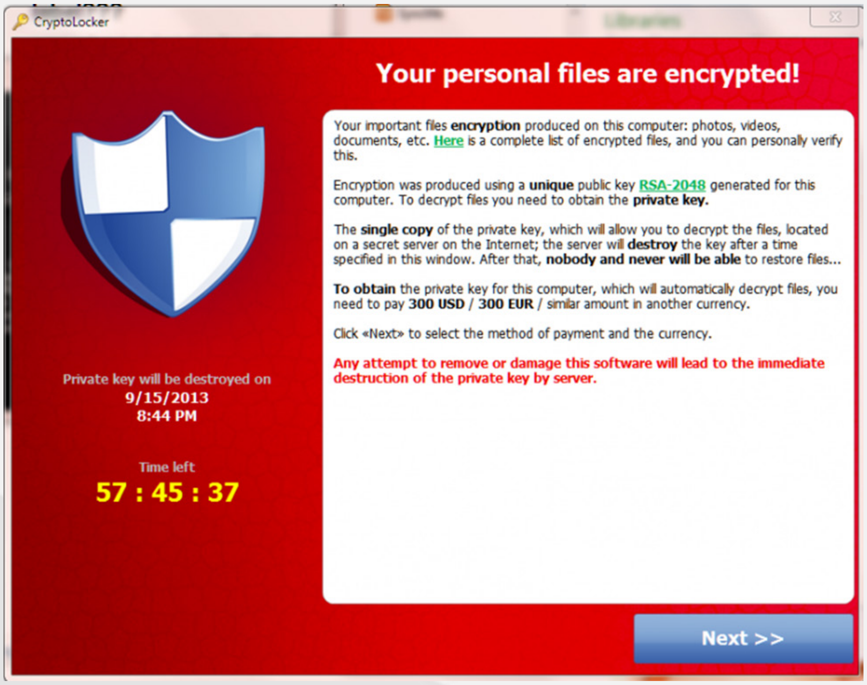
(C) 2014 The content of this message is protected by copyright and trademark laws. All rights reserved.

1
Suspicious because companies know your name. This generic salutation does not appear legitimate
2
Clicking this link could re-direct you to a web site that will install a virus

- **Scan Attachments**
  Files you download as attachments can be concealed as all kinds of file types, such as PDFs, video files, or images. Don't open any file that wasn't either from a trusted source or first scanned by your antivirus solution. Also be aware of attachments large enough that they can't be automatically scanned—one helpful, alternative practice is to avoid sharing attachments within your organization, and sharing files using a tool like Google Drive instead.

HOW TO HANDLE AN INFECTION:

If you think you downloaded an infected file, or you see a popup like this:



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD** / **300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
9/15/2013
8:44 PM

Time left
57 : 45 : 37

Follow these steps:

1. Unplug or disconnect from your network immediately.
   a. If you're connected with an ethernet cable, manually disconnect cable, located on the side or rear of your device.
   b. For wireless connections:
      i. On Windows, navigate to "Settings," "Network & Internet," and under "WiFi," toggle the switch to OFF.
      ii. On Macintosh, click the WiFi symbol on the menu bar (often located in the top right of screen), in the drop-down that appears, select "Turn WiFi Off"

2. Force shut down your computer.
   a. Hold the power key for ~10 seconds to force shut down.

3. Notify your IT support personnel immediately.

Ready to learn more? Call today.

(877) 230-5284

or email info@newmindgroup.com

YOUR NEXT STEP

Since Ransomware first emerged, it has taken on many forms, and it's targeting businesses of all sizes, all around the world. All it takes is one errant user to crack the door for a threat.

Are you practicing the best backup and security for your organization? If you'd like to learn more about the solutions out there, or you'd just like some peace of mind, give Newmind Group a call.

Explore a better security solution for your team.

Newmind Group can assess your security, give you a boost with best practices, and find the best ransomware prevention gear for your team.

Stay ahead of the threats and set a meeting today.

Schedule a Meeting

(877) 230-5284

info@newmindgroup.com