TECHNOLOGY OVERVIEW

INTRONIS CLOUD BACKUP & RECOVERY

THE RISE OF CRYPTOLOCKER:

5 Ways to defend against this new class of ransomware

intronis

Introduction

In September 2013, the first few reports of a powerful new strain of malware began trickling in, and it didn't take long for the IT world to dread the name "Cryptolocker." The ransomware variant has quickly become infamous for its sophistication, and ongoing reports have revealed just how profitable it has been for its authors.

Estimates vary, but a thesis by computer security professional Michele Spagnuolo estimated the "take" from Cryptolocker ransoms to be more than $1 million as of late December[1]. The malware's authors have targeted victims indiscriminately, and there have been reports of businesses of all kinds being hit. Even law enforcement isn't immune – CBS news reported that a Massachusetts police department paid $750 to restore access to its files[2].

What does all this mean for managed services providers? As the IT professionals tasked with protecting your clients from cyber threats, Cryptolocker should absolutely be front-of-mind. In this Tech Guide, we'll examine Cryptolocker's roots and method of propagation, and provide steps you can take to keep your clients safe from this dangerous malware.

What is ransomware?

Cryptolocker is a type of ransomware, which Microsoft defines as malicious software that locks a computer and retains control until you pay a certain amount of money. Ransomware can appear in two forms – either by locking your screen with a full-screen image or webpage to prevent you from accessing your PC, or by locking your files with a password so they can't be opened[3].

What is Cryptolocker?

Cryptolocker has been a particularly sophisticated ransomware variant of the password type, wrapping up victims' files and data in several layers of virtually unbreakable encryption before demanding ransoms of several hundred dollars[4].

Security vendors have a number of names for Cryptolocker – Trojan.Ransom, Trojan.Cryptolocker, Win32/Crilock.A. By any name the malware is a serious threat, in part because of its highly organized method of attack.

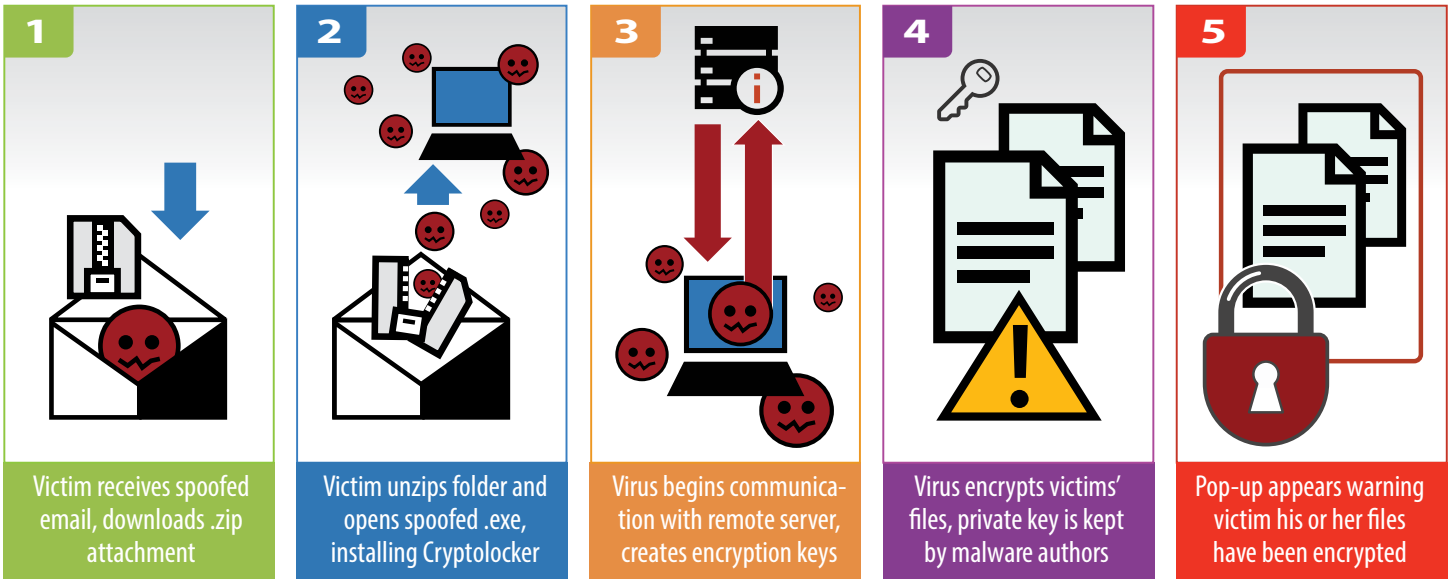
Research from antivirus vendor Bitdefender Labs sheds some light on just how effective Cryptolocker is at propagating, finding that the malware was able to attack more than 12,000 systems in just one week[5].

---

[1] "Bitlodine: Extracting Intelligence from the Bitcoin Network," Michele Spagnuolo, December 2013
[2] "Swansea Police Pay Ransom After Computer System Was Hacked," CBS Boston, November 2013
[3] "What is ransomware?," Microsoft, retrieved January 2014
[4] "CryptoLocker Ransomware Information Guide and FAQ," bleepingcomputer.com, October 2013
[5] "Cryptolocker weekly haul? More than 10k victims," Bitdefender Labs, November 2013

Cryptolocker

How it Attacks



Part of what makes Cryptolocker so dangerous is its sophisticated approach. It relies on social engineering to attack and several layers of encryption to hold their files hostage.

It is unknown who is behind Cryptolocker, but experts speculate it may have originated in Eastern Europe or Russia[6]. The National Crime Agency of the United Kingdom says it is investigating organized crime units for potential connections to the virus[7].

How does Cryptolocker attack?

Cryptolocker typically relies on social engineering to infiltrate[8]. Spoofed emails are its best-known tools of attack, although some variants and copycats have been known to attack via drive-by download advertising or peer-to-peer network file sharing[9].

The emails are sent from a spoofed address from a well-known company and include an enticing subject line – "ADP Payroll Alert" or "USPS Missed Package Delivery" are two known examples. The emails will also include.zip files with similarly common names, like "ADP_Invoice_6599263.zip" and "Case_8363954.zip".

Within those .zip folders is a file disguised as a common extension - .docx or .xls. In reality, the .zip contains an .exe, which downloads onto the target computer, adding a key to the Windows Registry so that it can run on startup.

Once downloaded, the malware establishes communication with a command and control server. Cryptolocker relies on a domain generation algorithm and hops between new servers routinely to avoid detection. Once the server connection is established, the malware generates a pair of encryption keys – one public, one private – using the huge RSA-2048 bit encryption algorithm and military-grade 256-bit AES encryption.

---

[6] "Cryptolocker ransomware," Dell SecureWorks Counter Threat Unit, December 2013

[7] "ALERT - Mass ransomware spamming event targeting UK computer users," National Crime Agency, November 2013

[8] Dell SecureWorks

[9] "Cryptolocker 2.0 – new version, or copycat?" welivesecurity.com, December 2013

When crypto-locker hits, victims will see a pop-up message that includes a count-down timer and payment portal (left). Their desk-top background will also be replaced with an image that alerts the user of the infection (right).

The public key is sent back to the target computer and is used to encrypt the victim's files, scanning for popular business file extensions like .docx, .ppt, .xls, .accdb, and many more. The private key is kept back on the Cryptolocker server and is the only tool users can deploy to decrypt these files[10].

Signs of infection

All of that happens in the background, before the user knows he or she has been hit. The first sign of infection is typically a pop-up window, which tells the victim that his or her important files have been encrypted and setting a time limit for payment before the private encryption key is destroyed and the files are lost forever.

This window also includes options for payment. Victims are able to use GreenDot MoneyPaks – a form of anonymous payment available for purchase at any convenience store – or Bitcoins, the popular online currency that enables anonymous money transfer.

Cryptolocker also hijacks the user's desktop background with an image that includes instruc-tions on how to re-download the virus in the event that the payment window has been deleted or removed off the computer. Remember, even removing Cryptolocker from the computer doesn't restore file access, so re-download of the virus may be necessary if victims wish to pay the ransom.

Cryptolocker's authors have also started allowing late payment options, with the ransom amount rising to as high as $8,000 to $9,000 if it is paid late[11].

Best practices to protect against Cryptolocker

When it comes to fighting Cryptolocker, the best offense is a good defense. Fortunately for users, many best practices for malware prevention are effective ways to keep computers safe from Cryptol-ocker. MSPs should ahere to the following 5 tips to protect their clients.

---

[10] Bleepingcomputer.com

[11] Dell SecureWorks

Tip #1: Educate users on security best practices

Education is still the best way to avoid infection by Cryptolocker – or any other form of malware or virus. Solution providers should make their business clients aware of popular social engineering methods and tactics so that they don't fall victim to spoofed emails or messages.

It would be particularly helpful if MSPs shared the subject lines, email addresses, and email attachments that are most often associated with social engineering attempts so that end users know to avoid them. You can find a full list of known spoofed email addresses in the Additional Resources section at the conclusion of this guide.

A few best practices to share with your clients:

- Do not open emails from strange or unfamiliar email addresses
- Do not disable or deactivate antivirus or antimalware
- Do not download software from torrent sites – official or direct downloads are preferable
- If you receive an email from a familiar contact that includes an attachment or link, verify separately that the person or organization actually sent you this message

Tip #2: Maintain up-to-date antivirus, antimalware, and operating systems

Most security vendors are working on updates to catch and stop Cryptolocker before it takes hold of your clients' files. If you resell antivirus or antimalware to your customers, be sure that they are running the most recent versions of these products. You may want to contact your vendors to learn more about how they are protecting against Cryptolocker. It's also important to be sure your clients' operating systems are up to date with the latest security patches.

Tip #3: Review your managed email security features

Managed email security software can often scan and detect viruses and spam before they attack. You may also want to consider implementing several additional email security measures. For example, you can block certain file types – including .exe files within .zip folders – from being transmitted via email.

Tip #4: Prevent .exe from running in AppData or LocalAppData folders

Cryptolocker operates within the AppData or LocalAppData folders, so you may be able to prevent the initial malware download from executing by blocking .exe files from running in these folders. This may actually prevent legitimate programs from working correctly. Spotify, for example, runs in AppData. However, you can create exceptions to allow these programs to work correctly.

Tip #5: Back up your data to an offsite location

Offsite backup is a critical component to a Cryptolocker recovery strategy. Webroot says cloud backup is "highly recommended" for mitigation, adding that "offsite backup has long been an essential part of any Disaster Recovery plan." [12]

[12] "Cryptolocker Ransomware and what you need to know" Webroot, December 2013

Why offsite? Because Cryptolocker infections have been known to infect local drives and network shares that are mapped as a drive letter on the infected computer, according to the United States Computer Emergency Readiness Team (US-CERT).[13] That means if you're using these tools as your clients' sole means of backup, there's little chance of recovery.

Below are a few best practices to keep in mind when backing up offsite.

Choose the right offsite backup solution

Not all cloud backup is built the same. When looking for an offsite backup solution, lean toward a solution that provides several benefits:

- The ability to choose cloud-only backup, rather than mandating both local and cloud backups
- Proprietary backup file formats minimize the likelihood that the malware encrypts your backup file
- Military-grade backup encryption in transit and in storage at secure data centers
- User-definable retention and security policies
- Economical archiving and retention capabilities

Keep multiple versions of your protected files

Certain cloud backup offerings provide the advantage of sophisticated version histories, which is a critical component to successful restores. If you only back up a single version of your files, it is possible that your software has backed up an infected file. By saving as many revisions as possible, solution providers have a better chance of restoring to a clean version of their data.

Keep multiple days' worth of files

It's possible to store multiple versions of a single file, all of which were backed up the same day. But it's important to also back up several days' – or even weeks' – worth of files to ensure maximum protection.

This can be especially helpful in the event of a malware infection that goes unnoticed for some time. By retaining clean backups over days, weeks, or months, IT solutions providers give themselves additional safe restore points, raising the likelihood of a successful restore.

3 steps to recover from a Cryptolocker infection

The above tips are all solid preventative measures you can take to avoid an infection, but what happens if Cryptolocker is able to strike? The following 3 steps should be taken immediately after an infection is discovered.

---

[13] "CryptoLocker Ransomware Infections," US-CERT, November 2013

Step 1: Disconnect from your network and stop backing data up immediately

To ensure a successful recovery, US-CERT recommends that victims immediately disconnect the infected computer from wired and wireless networks as soon as they learn of an infection[14].

It's similarly important to discontinue backups to the cloud once a Cryptolocker infiltration has been identified to ensure the software does not overwrite clean backups with the infected files.

Again, this is where storing multiple versions of a file over several days, weeks, or even months can be helpful; because this strategy offers a higher chance of clean restore points.

Step 2: Remove Cryptolocker and clean computers of malicious software

It's important to remember that removing the Cryptolocker virus also removes the payment portal. Effectively, by removing the malware, you forfeit your ability to restore data using the private key held by the malware's authors. This should not be a problem if you have backed up your client's data to a separate offsite location and don't intend to pay the ransom.

Therefore, take steps to remove the virus from your clients' network and hardware by using anti-virus software and malware removers. The Windows blog wintips.org also recommends a number of steps to this process, including running the computer in Safe Mode with Networking, using anti-malware to remove malicious processes and additional threats, and deleting hidden Cryptolocker files that may be lurking[15]. It's worth considering these steps – as well as your own best judgment – when lining out recovery steps post-infection.

Step 3: Restore from your backup

If you follow best practices for backing up your data offsite, you should be able to locate clean versions of your files and restore from there. Unfortunately, if you have not followed these steps, you're left with few alternative options: pay the ransom, or accept that all of your data is gone and start fresh.

Conclusion

Cryptolocker is no lightweight in the area of malware. Its authors have taken great pains to disguise themselves and make it as difficult as possible to recover your clients' data without paying the ransom. It's a threat the IT channel needs to take seriously, because failure to help your managed services client could mean lost business and a tarnished reputation.

Until they are caught or stopped, Cryptolocker's authors will likely continue to exploit victims to make money. But by taking these preventative steps, you can ensure that your own clients don't have to pay the ransom.

[14] US-CERT

[15] "How to remove CryptoLocker Ransomware and Restore your files," wintips.org

intronis

Additional Resources:

- Intronis cryptolocker success story
- Cryptolocker Resource Center
- Cryptolocker webinar replay

Full list of known cryptolocker spoof emails, attachments, and targeted files available at:

- "CryptoLocker Ransomware Information Guide and FAQ," bleepingcomputer.com

Cryptolocker removal guide

- "How to remove CryptoLocker Ransomware and Restore your files," wintips.org

See our 30-minute webinar
Cryptolocker: Should you pay the ransom? CLICK TO VIEW

Sources:

- "Bitlodine: Extracting Intelligence from the Bitcoin Network," Michele Spagnuolo, December 2013
- "Swansea Police Pay Ransom After Computer System Was Hacked," CBS Boston, November 2013
- "What is ransomware?," Microsoft, retrieved January 2014
- "CryptoLocker Ransomware Information Guide and FAQ," bleepingcomputer.com, October 2013
- "Cryptolocker weekly haul? More than 10k victims," Bitdefender Labs, November 2013
- "Cryptolocker ransomware," Dell SecureWorks Counter Threat Unit, December 2013
- "ALERT - Mass ransomware spamming event targeting UK computer users," National Crime Agency, November 2013
- "Cryptolocker 2.0 – new version, or copycat?" welivesecurity.com, December 2013
- "Cryptolocker Ransomware and what you need to know" Webroot, December 2013
- "CryptoLocker Ransomware Infections," US-CERT, November 2013

ABOUT INTRONIS

Intronis provides world-class data protection solutions for Small Businesses, delivered exclusively through the IT channel. The Intronis ECHOplatform securely protects physical and virtual data with native support for physical imaging, VMware, Hyper-V, Exchange, and SQL, all through a re-brandable central management console that integrates with major RMM and PSA tools. Offered with unlimited and fixed-fee storage pricing per SMB account, IT service providers are able to rapidly grow revenue and scale profit. Through Intronis ECHOshare, channel partners can easily expand their IT services portfolio to include tightly integrated business-grade file sync and share. Learn more at www.intronis.com.

On the Web: **www.intronis.com**
Intronis Cloud Backup and Recovery Blog: blog.intronis.com
Social Channels: @IntronisInc | Facebook: intronisonlinebackup | LinkedIn: Intronis