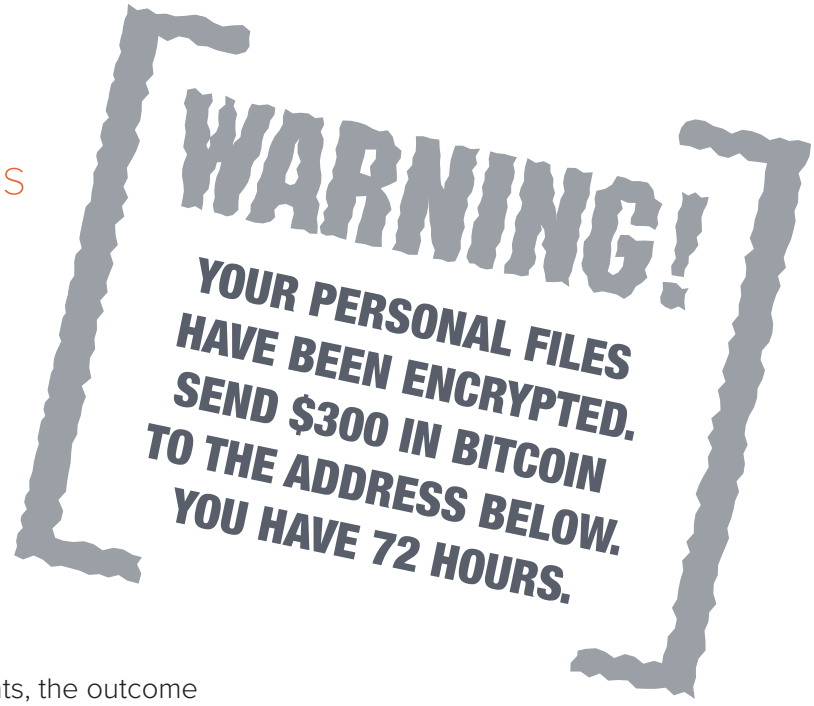
CODE42

Reeling in Ransomware

Data Protection for You and Your Users



Hundreds of thousands of computer users have seen this unfortunate message pop up on their screens. >>

Since the first appearance of cryptoviral extortion in 1989, ransomware has grown into a prolific, global money-making machine. For the average hacker, the return on investment for a successful ransomware ploy is 1425%.[1]

Whether hackers use CryptoLocker, CryptoWall, CTB-Locker, TorrentLocker or one of the many variants, the outcome is the same. Users have no choice but to pay the ransom—unless they have endpoint backup in place. Even with the best tech resources, decrypting the algorithm used to lock files without the key would require several lifetimes.

Ransomware is unique among malware strains because it is particularly malicious and profoundly personal.

When it appears, it produces a visceral reaction in its victims—not unlike the emotion a crime of robbery or burglary evokes. The feelings of violation and loss assure profitability for the hacker because in most cases, victims will do whatever it takes to return their lives to normal.

In the past five years, hackers have reached a new level of crime powered by encryption technology sophistication, pervasive digital habits and security illiteracy.[2]

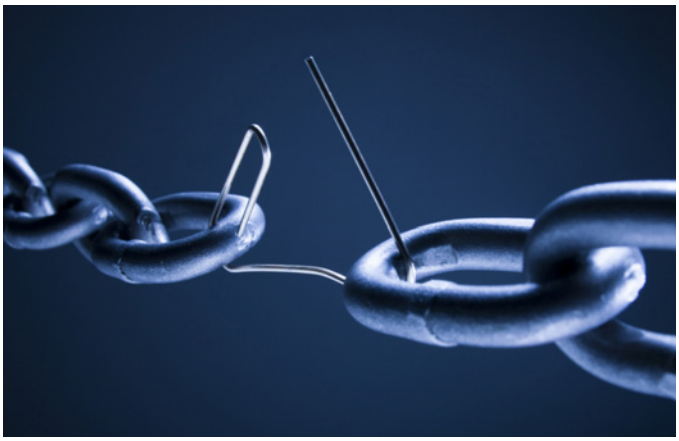
260,000

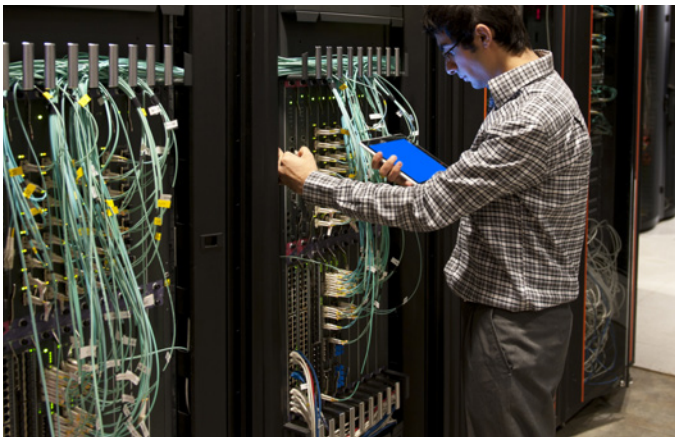
The Department of Justice (DOJ) estimates that, since it's inception in 2013, the CryptoLocker virus has compromised more than **260,000** computers worldwide.[3]

THE HUMAN USER

Humans are the weakest link in your network—and hackers know it.

Hackers know that the easiest way to circumvent your anti-virus software, firewalls and other protective measures is through your employees. Ransomware is designed to take advantage of users' trust in content delivered online. Using trickery and market-tested emotional cues, hackers can turn the most cool-headed user into a distraught victim.





DIFFERING POINTS OF VIEW

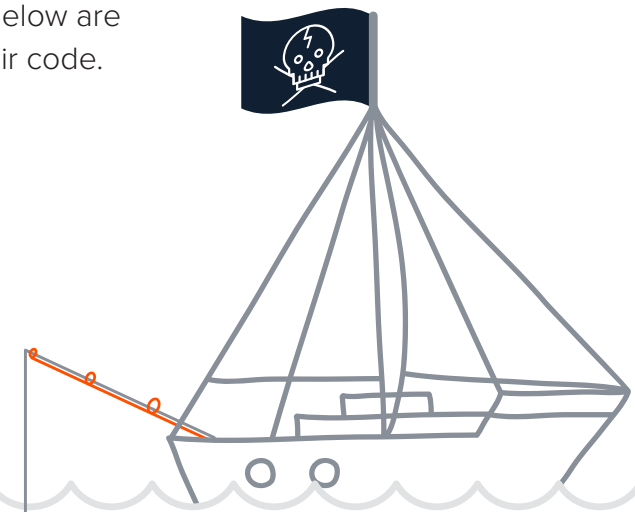
While IT professionals value network security, users value productivity. With customers to serve, meetings to prepare for and deadlines to meet, users consider security to be IT's problem not theirs.[4] Hackers capitalize on the (mistaken) belief that IT will protect them despite their behaviors online.

Human error was responsible for 95% of successful security hacks in 2013.[5]

THE ART OF THE PHISH

Four Ways Ransomware Worms its Way Into Our Lives.

Planting ransomware in the enterprise organization requires a "personal" connection inside the organization. Below are four ways that ransomware authors propagate their code.



The Phishy Download

Phishing, or presenting a human user with a questionable file to download, is one of the most common method of ransomware distribution. Masquerading as something the user wants or trusts, a baited link is placed in an ad on a shady website or inside an email attachment. When the user clicks the link, the malware goes to work encrypting the user's files.

The Leaky Program

Computer software that has not been updated properly can provide hackers with an easy access point in a user's system. Hackers have also been known to hide malware in fake updates for popular programs like Flash Player.

The Flashy Flash Drive

Removable storage devices such as USBs can also be used to spread ransomware—in fact, the first occurrence of ransomware was distributed via floppy disk. Well-known vulnerabilities like BadUSB in USB peripherals have shown how easy it is for malware authors to infect computers.[6]

The Bad App-le

Malware authors infect computers by embedding malicious code in seemingly innocuous and useful applications. Browser toolbars, key generator tools, third party executable (.exe) files, messaging applications, torrent sites and other peer-to-peer file sharing sites have all been used successfully by criminals to spread malware.

THE BUSINESS OF PUSHING THE RIGHT BUTTONS

The amount of research, design and social engineering that goes into a ransomware attack is unprecedented in the field of malware. Ransomware developers have been known to use A/B testing to pinpoint the perfect combination of images, text and flow in an attack to create irrefutable fakes that practically guarantee a ransom payout. No one is safe: even police departments around the U.S. have admitted to being victims of ransomware attacks.

Ransomware designers use tools like A/B testing, to identify the most convincing delivery mechanisms and highest “open rates” in order to reap the greatest payouts.[7]

Stages of Emotional Manipulation

Trust

Data “kidnappers” take advantage of users’ trust by disguising their exploits with digital imagery from trustworthy companies, government agencies or software brands.

Surprise

The ransom note appears onscreen after the files have been encrypted. Trojan strains lie in wait for a set period before beginning to encrypt to obscure receipt time and origin. Often a user doesn’t know how he or she was infected.

Fear

Ransomware instills real fear in victims’ hearts. And it’s a fear that is not entirely unwarranted—their files are gone for good if they don’t pay.

Shame

In ransomware attacks, we tend to blame the victim. “You” visited the wrong site. “You” trusted the wrong message. “You” should have been more careful. As a result, shame is inherent in every ransomware attack.

Intimidation

Ransomers employ timed pop-up messages and ticking countdown clocks—reminding victims that they better pay before it’s too late.

Relief

It is in the kidnapper’s best interest to make sure his victims get their files back so that word gets around that recovery is guaranteed if the ransom is paid. Some strains of ransomware even have a customer service chat feature to help victims through the payment process.

THE MANY FACES OF RANSOMWARE

Ransomware has taken many forms, including CryptoLocker, CryptoWall, TorrentLocker and CTB-Locker. The world of ransomware is a diverse jungle of threats all stemming from one common source: Dr. Joseph L. Popp. In 1989, Popp was turned down for a job at the World Health Organization. In response, he wrote the first “cyber extortion” program, which targeted AIDS research facilities affiliated with the WHO.

THE EVOLUTION OF RANSOMWARE

1989

The AIDS Trojan is Born.

Delivery: Floppy disks masquerading as acquired immune deficiency syndrome (AIDS) education software are distributed via the U.S. Postal Service.
Target: AIDS research facilities outside of the U.S. affiliated with the World Health Organization (WHO).
Cryptography: Notably weak and easily reversible symmetric encryption algorithm.
Ransom: After a set amount of time, a note delivered by post instructed users to turn on their printers, which printed a ransom demanding $189. Payments were sent to a P.O. box in Panama.
Notoriety: A truly senseless and vengeful attack. Cyber extortion is born.

2005/ 2006

Viruses Like Trojan.Cryzip and Trojan.Archiveus Leverage Password Protected Archive and Zip Files.

Delivery: Apps posed as spyware removal tools and computer performance enhancement tools.
Target: Mostly Windows users.
Cryptography: Weak and easily reversible—often symmetric encryption algorithms.
Ransom: $30–$90 for a "software license." Archiveus had victims buy medication from online URLs (which the attackers earned commission on).
Notoriety: As people found fixes for the weakly-encrypted malware, many versions of these fake tools were released, each slightly improving on the last. Criminals realize that the ransomware game is worth pursuing (even if they aren't that great at cryptography).

2008/ 2009

Faux Antivirus Software Proves Lame Extortion Route.

Delivery: Apps posed as fake antivirus programs.
Target: Mostly Windows users.
Cryptography: None.
Ransom: $40–$100 paid to fix fake problems.
Notoriety: These scams didn't make much money, as many users chose to ignore the "problems" their antivirus software was reporting.

2011/ 2012

Russian Variants Like Trojan.Ransom Begin Era of Locker Malware.

Delivery: Pornography websites. In 2012, apps begin to mimic law enforcement notices and Windows error messages.
Target: Begins with Russian users. By 2012, ransomware is a large-scale global problem.
Cryptography: None. Computers are "locked" by the software, and "unlocked" when payment is made.
Ransom: As low as $12, using mobile payments and electronic cash vouchers.
Notoriety: Ransomware moves from reporting fake problems to causing very real ones. Social engineering and scare tactics begin. Lower, easier payments prove fruitful, as more users are more likely to pay—ransomware becomes an operation of scale.

2015

CryptoLocker is Born; Cryptocurrency Enters the Field.

Delivery: Spam campaigns and USB drives are introduced; older methods used as well.
Target: Mostly personal computers, enterprises begin to be targeted as well.
Cryptography: The authors leveraged the existing cryptography tools in the operating systems they were targeting to use AES to encrypt the user's files and RSA encryption to encrypt the AES key. The AES/RSA combo proves to be nearly unbeatable.
Ransom: Huge variations in ransom prices arise, as entire companies and government agencies are hit. Bitcoin payments begin.
Notoriety: CryptoLocker renders both the computer and its files unusable. If users don't have backups, they are forced to pay the ransom or lose their files entirely. Special enterprise-aimed variants like Cryptofortress and Ransomweb begin to encrypt files on shared network resources, websites and servers.

KEEPING RANSOMWARE AT BAY

While ransomware has no cure, there are things an enterprise can do to limit its exposure to infection. Employing defensive strategies like anti-virus programs, firewalls, SPAM blockers and user education initiatives help mitigate, address and prevent ransomware attacks in your enterprise organization.

- **Firewalls and security appliances** will help filter malware before it gains access to the network.
- Adding **SPAM blockers** and filters on users' email accounts will help weed out phishing attempts.
- **Anti-virus tools** help prevent the virus from taking control of your network by identifying questionable programs through periodic systems scans.
- **User education** is an essential part of your defense strategy. When it comes to cybercrime, criminals have a clear target in their crosshairs: the user. Keeping your users out of the crosshairs is not an easy task, but education provides an additional layer of defense.

The following tips may prevent users from biting on phishing attempts. Share this information frequently and you'll be one step closer to eliminating ransomware.

5 Tips to Make Humans Unhackable

1 Throw Password Post-it Notes Away.

Good security precautions require passwords to be longer, more varied and changed more frequently. Password fatigue finds many users writing their passwords on post-it notes for reference. Ditch the post-it and opt for a password manager app. Add a password to your computer or phone and you've got multi-factor security to protect your digital life.

2 Think Before You Click!

Some of the largest high-profile leaks in recent memory all began with employees clicking on email links that were laced with malware. Criminals will use the logos of law enforcement agencies and trusted brands to lure users in. Beware the unexpected attachment! Marketing emails from major brands will never include an attachment. If something seems too good to be true, it probably is.[8] A healthy amount of skepticism when browsing the web and your inbox will go a long way toward keeping you free of ransomware.

3 "S" is for Secure Communication.

URLs that start with HTTPS are more secure than those that start with HTTP. Whenever you need to log in to a site or fill out a form requiring personal information, make sure the site you are on uses HTTPS for secure communication. There are tools available that force web browsers to seek more secure addresses when browsing the Internet.[9]

4 Use a VPN When Doing VIP Work on a Public Connection.

If you find yourself doing lots of important work on public connections—like those offered in coffee shops, airports or hotels—this tip is for you. Use a virtual private network (VPN)–to package your computer's Internet communications together and encrypt them before sending them to your organization's network or another computer on the Internet.

5 Stay Up-to-date.

It's tempting to click "remind me later" when prompted to update your computer software, but it's critical that you make sure that all your security programs, operating systems and other applications are updated frequently. Malware is known to take advantage of vulnerabilities in out-of-date applications.

DEFEATING RANSOMWARE

It's All About Endpoint Backup.

There's only one way to recover from ransomware without paying a ransom once it has infected your network. Having endpoint backup in place allows you to restore the files and get your users back to work.

Harsh Reality:	Silver Lining:	The Solution:
Users are a security vulnerability. Their priorities lie in being productive, not in being secure.	Automation can add a layer of defense against data loss without relying on users remembering to back up their work	Code42 CrashPlan runs unobtrusively on the device, automatically backing up every version of every file, no end-user intervention required.
When a device is infected with ransomware, the encrypted files are nearly impossible to decrypt without paying the ransom.	When backups are available, there's no reason to pay a ransom to recover your files.	Code42's reliable backups mean files are healthy and ready for quick restore—eliminating ransom payments altogether.
Ransomware destroys productivity. At worst, data is lost entirely. At best, the company loses money and employees lose time when forced to recreate important files.	Having versioned backups in place allows IT to pinpoint the best point in time from which to restore files.	Code42's continuous endpoint backup enables IT to quickly and easily restore files to minutes of the infection, disabling the effects of ransomware.

CONCLUSION

Ransomware attacks are painful, but they don't have to result in lost files or ransom payments. The solution to ransomware attacks is clear: deploy automatic, continuous endpoint backup software on every machine in your organization. With Code42 CrashPlan in place, you can restore infected devices in less time, with less IT effort, all while returning users to where they were minutes before their files were maliciously encrypted. You'll find it's an essential, foundational layer to your cybersecurity defense strategy.

Reference links:

1 http://ubm.io/1JChqvd
2 http://bit.ly/1SDCPGV
3 http://1.usa.gov/1MwQj5u
4 http://bit.ly/1jmvYEQ
5 http://bit.ly/1iefEV5
6 http://bit.ly/1s9n5Ob
7 http://symc.ly/1MZJ6dx
8 http://bit.ly/1K7kU3E
9 http://bit.ly/18qiajr

CODE42

WP101504

CORPORATE HEADQUARTERS 1 MAIN STREET #400 | MINNEAPOLIS, MN 55414 | 612.333.4242 | WWW.CODE42.COM

Code42 is a global enterprise SaaS provider of endpoint data protection and security to more than 37,000 organizations, including the most recognized brands in business and education. Our highly secure cloud solutions enable IT and security teams to limit risk, meet data privacy regulations and recover from data loss, no matter the cause.