Five things you need to know about CryptoLocker

1 CRYPTOLOCKER: A BRIEF HISTORY IN CYBERCRIME

Ransomware attacks have been occurring for more than a decade, but it's been in the last few years that we've seen large-scale attacks. Computer security experts have theorized that the rise in this type of attack is due to its higher rate of success versus other cybercrimes that have become more difficult. Plus, these days, the software for ransomware is cheap and readily available—perpetrators need only malicious intent to carry out an attack. No coding required!

Once infected with ransomware, victims have two choices: either pay the ransom or permanently lose access to their files. The malware used to encrypt files can be difficult to defend against, and the encryption in most cases can't be broken.

Ransomware has become attractive to criminals, because they know that many individuals and companies have incomplete data backups—or no backup at all—and, thus, are likely to pay the ransom to recover their files. The criminals have generally kept their ransom demands low, opting for figures that were: a) likely to be paid; and b) not likely to be investigated by law enforcement.

Once a user has opened a file infected with CryptoLocker, the ransomware encrypts files on the user's system and demands payment, within a set timeframe, in order to unlock the files.

Many have paid the ransom; even the FBI, in some instances, advised companies to "just pay the ransom." Unfortunately, paying the attackers off is a strategy that encourages the expansion of such extortion schemes. Furthermore, there's no guarantee that the files will be decrypted once the ransom has been paid.

In 2014, CryptoLocker malware was largely neutralized by Operation Tovar, an international collaboration of security companies and law enforcement, that successfully shut down the command and control centers and the GameOver Zeus botnets that drove the ransomware.

However, the scourge of ransomware is far from over. CryptoLocker, as a result of its success, spawned a slew of copycats. According to the Cyber Threat Alliance, they promise to wreak havoc in 2016.

2 A NEW GENERATION OF RANSOMWARE

CryptoLocker's demise in 2014 gave way to a worthy successor in CryptoWall, which has since evolved into one of the nastiest and most successful strains of ransomware.

CryptoWall has been known to arrive via email attachments, exploit kits, and drive-by downloads, which occur when a user unintentionally downloads a virus or malware (usually due to an outdated browser or OS). Recently, a new campaign involving multiple signed CryptoWall 3.0 samples has appeared in files being downloaded from MediaFire, a popular file sharing and hosting service.

CryptoWall is already bringing the pain

In its 2015 report on the CryptoWall 3 (CW3) threat, the Cyber Threat Alliance presented these alarming findings:

- 4,046 malware samples
- 839 command and control URLs
- Five second-tier IP addresses used for command and control
- 49 campaign code identifiers
- 406,887 attempted infections of CW3

In February 2016, a new version of ransomware arrived on the scene. Known as Locky, it follows the same model of using asymmetric (public key) encryption to lock user documents and demand ransom for the decryption key. Experts have suggested that Locky is likely to become one of the most active and lucrative malware strains. Like previous strains, its delivery vector has been primarily spam email attachments that are responsible for downloading the Locky payload.

Locky was responsible for the February 2016 breach at Hollywood Presbyterian Medical Center, which paid a ransom that amounted to about $17,000. Ultimately, it was a small price to pay for the hospital to regain access to its electronic medical records and restore employees' ability to communicate electronically.

RANSOMWARE IS COMING AFTER BUSINESS AND IT'S GOING TO BE EXPENSIVE

According to Michael Sutton, CISO at Zscaler™, ransomware has hit a sweet spot. Users have been begrudgingly paying expensive but not excessive ransoms in exchange for the return of their precious data.

But the success of these campaigns, largely targeted at individuals, has made the perpetrators set their sights on business, where the money is sure to be better. Newly discovered variants of ransomware are focused on Linux, which is especially troubling, as it's more likely to impact the websites and code repositories of enterprises, which tend to be very willing to pay up rather than risk losing critical intellectual property.

As ransomware becomes more corporate focused, it's unlikely that infected enterprises will get away with paying consumer rates. The criminals behind the ransomware campaigns are savvy and once they realize that they've locked up source code and financial documents that haven't been properly backed up, you can expect ransoms to skyrocket…and be paid.

3 WHY MOST AV AND MALWARE PROTECTIONS AREN'T ENOUGH

CryptoWall remains a potent threat to enterprises and individual users alike. Traditional antivirus (AV) applications struggle against this and many other strains of ransomware, as once the infection is successful, there is very little AV vendors can do, even by adding signatures reactively.

A multilayered security approach is required to counter the ransomware threat, as no single product can be relied upon to provide adequate protection.

A combination of solutions, including Intrusion Prevention Systems (IPS), antivirus, sandboxing, web filtering, IP reputation scoring, and anti-spam services, can significantly reduce a network's vulnerability to CryptoWall and other advanced threats. SSL inspection of traffic is critical, as the use of SSL increasing dramatically and will soon represent the majority of all web traffic. Furthermore, assailants are hiding malicious content in SSL-encrypted messages.

> "SSL is expected to consume 60 percent of all web traffic by the end of 2016."
>
> – NSS Labs

A multilayered approach relies on the various individual protections performing in conjunction with one another. For example, web filtering solutions can block access to CryptoWall C2 sites, and intrusion prevention systems can interrupt delivery of CyptoWall payloads, while antivirus and sandbox can detect and block CryptoWall infection. Known as the "kill-chain methodology," these advanced security solutions work together to close down various vectors for infection.

Some of these solutions, particularly antivirus, are fairly ubiquitous. But ransomware is constantly changing, and variants are sailing past AV and other legacy security solutions. As a result, more advanced solutions—especially multilayered solutions— should be considered an imperative in today's world.

Traditional security appliances are not keeping up with today's threats

60%	40%	54%
of the top 100 sites have malware – *Gartner*	of Internet traffic crosses CDNs and goes uninspected – *Virtual Networking Index, Cisco*	advanced threats hide behind SSL – *ThreatLabz Research, Zscaler*

Inspecting all traffic is critical, but it can require up to 8X more security appliances

A NEW STYLE OF ATTACK: PAY NOW OR PAY MORE LATER

In March 2016, Zscaler detected and blocked a new ransomware family, called Maktub Locker. Upon detonating the malware in the lab, we found that it launches a fake rich-text format (RTF) document as it encrypts user files in the background. When it's finished encrypting the files, Maktub will display a time-sensitive ransom note. The ransom payment starts at 1.4 bitcoins to get the decryption key. But if the ransom isn't paid within 72 hours, the ransom goes up to 3.9 bitcoins.

> "Expect ransomware to become increasingly corporate focused in 2016 and, as it does, enterprises won't get away with paying consumer rates."
>
> **Jay Chaudhry**, *CEO, Zscaler "What cyber trends to expect in 2016," CSO Online, Dec. 2015*

4 HOW TO PROTECT YOUR DATA AND USERS RIGHT NOW

With the threat of ransomware attacks, it is paramount to have backup and redundancy systems in place to ensure your data is secure and available at all times. Cloud backup systems are increasingly recommended for safe, offsite storage.

Because ransomware relies on a user to become an unwilling accomplice in the crime, your best defense is to have well-trained users who understand the threat and are aware of the ways to avoid infection. Some of the best practices include:

- Users should ensure that the operating system, device firmware, and applications—especially antivirus and web browsers—on their systems are up to date.
- Users need to be trained on phishing techniques, for example, always paying attention to the name of the person sending an email message. They should be warned against trusting unknown senders or unsolicited messages, especially if they contain links or attachments.
- Users should also pay attention to the file type of any attachments they receive. Files that are ".zip" should be red flagged, along with other uncommon file types like ".scr," which was used by CryptoWall.
- All of the most popular web browsers offer features that automatically block plug-ins like Java, Flash, and Silverlight until the user chooses to activate them individually. Ensure that these protections are on, and that users only activate plug-ins from trusted sources.

5 YOUR BEST PROTECTION AGAINST RANSOMWARE IS IN THE CLOUD

The people creating ransomware are good at creating email messages that look like the real thing. They often appear to be legitimate senders from trusted sources. Cybercriminals know that if they can get to the user, they have a good chance of accomplishing their mission. Now, with such schemes targeting business, it's important that you implement multilayered protection that can block malicious files and sandbox suspicious traffic. Furthermore, your system should prevent malware from being downloaded in the event that a message is able to get past your other protections.

Hackers use a combination of methods, frequently in tandem, to do just that. That's why, with Zscaler, traffic is examined by eight different security engines in real time, allowing you to quickly discover coordinated attacks and block them before they get into your network.

Zscaler inspects all traffic—including SSL

Many (most!) organizations don't inspect SSL traffic, because it is so compute intensive. They would have to buy many more appliances to handle the load—up to eight times as many—and that's just not feasible most of the time. But Zscaler was built to handle encrypted traffic at a global cloud scale, so the issue of SSL becomes a non-issue. Zscaler inspects every byte of traffic in real time, including encrypted traffic, so threats have nowhere to hide.

With **inbound** traffic, Zscaler looks for viruses, adware, spyware, malicious Javascript, malformed files, and anything else that can disrupt your systems and networks.

With **outbound** traffic, Zscaler watches for malicious URL requests, cross-site scripting, and botnet traffic going to command and control centers (which is how ransomware takes control of your data). If the ransomware can't reach its C&C servers, it can't find and encrypt your data.

Zscaler doesn't just send alerts when there's suspicious traffic. It automatically blocks identified zero-day attacks as well as inbound malware, outbound botnet communications from infected devices, and outbound data exfiltration.

Zscaler protects all users, in any location, on any device

Zscaler's integrated security functions, including threat intelligence, botnet detection, and cloud sandboxing, work together in real time, providing comprehensive protection. And we bring that protection to all your users, on all their various personal and company-owned devices, on or off the network.

Attackers target the most vulnerable parts of your infrastructure, and they know that many organizations have critical gaps in their protection of remote offices, road warriors, mobile devices, and Internet-connected things. Zscaler, because it's in the cloud, protects all of your users and all of your systems, wherever on the planet they happen to be. A user on a mobile device on a public Wi-Fi connection gets the very same protection as a user hardwired into the headquarters network.

Cloud intelligence benefits all users

The massive, global Zscaler cloud security platform handles 160B transactions at peak periods. Suspicious objects are automatically executed and monitored in a controlled sandbox, and any malicious behaviors, including zero-day threats, are recorded, analyzed, and blocked. Best of all, if a threat is discovered for any one of our 15+ million users, it is blocked for all Zscaler users.

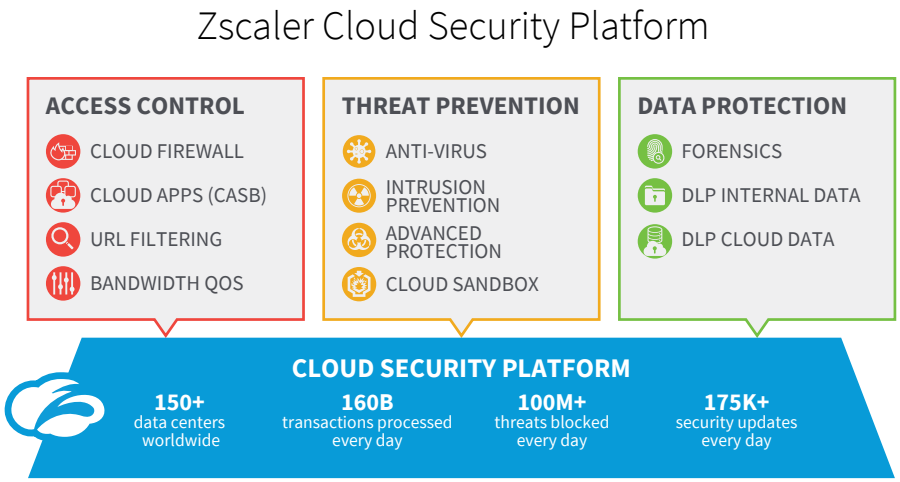
The Zscaler Platform

Zscaler ensures that more than 15 million employees at thousands of enterprise and government organizations worldwide are protected against cyberattacks and data breaches, while staying fully compliant with corporate and regulatory policies. Zscaler's award-winning cloud security platform delivers a safe and productive Internet experience for every user, from any device, and from any location.

Zscaler effectively moves security into the Internet backbone, operating in more than 150+ data centers around the world and enabling organizations to fully leverage the promise of cloud and mobile computing with unparalleled and uncompromising protection and performance.

Learn more

The best way to protect yourself and the users on your network is by learning about the threat, where you're vulnerable, and how to close any security gaps in your current infrastructure. By taking the Zscaler Security Preview, you can learn, in just a few minutes, where such gaps may exist. The test is safe, free, confidential, and informative. **www.zscaler.com/security-preview**



> Ransomware is less about technological sophistication and more about exploitation of the human element. Simply, it is a digital spin on a centuries-old criminal tactic.

– **Institute for Critical Infrastructure Technology**

ADDITIONAL RESOURCES

CYBER THREAT ALLIANCE
"Lucrative Ransomware Attacks: Analysis of the CryptoWall Version 3 Threat" November 2015
http://cyberthreatalliance.org/cryptowall-report.pdf

INSTITUTE FOR CRITICAL INFRASTRUCTURE TECHNOLOGY
"The ICIT Ransomware Report" 2016
http://icitech.org/wp-content/uploads/2016/03/ICIT-Brief-The-Ransomware-Report2.pdf

US-CERT United State Computer Emergency Readiness Team
https://www.us-cert.gov/ncas/alerts/TA14-295A

ZSCALER THREATLABZ
https://www.zscaler.com/blogs/research

CONTACT US

Zscaler, Inc.
110 Rose Orchard Way
San Jose, CA 95134, USA
+1 408.533.0288
+1 866.902.7811

www.zscaler.com

FOLLOW US

facebook.com/zscaler
linkedin.com/company/zscaler
twitter.com/zscaler
youtube.com/zscaler
blog.zscaler.com