VLI HAWAII 2019
ROCHDALE + PARAGON

CYBERCRIMES: TOP THREATS FOR 2019

Sherri Davidoff, Founder & CEO

LMG Security

sherri@lmgsecurity.com 406-830-3165 x 102

Objectives:

1. Understand the threats and vulnerabilities that lead to cybersecurity breaches.
2. Learn about the "hacker economy" and how criminals monetize data.
3. Learn strategies for protecting both your organization and members from attacks.
4. Know the 9 Building Blocks of an effective cybersecurity program.

Protect Yourself Against Banking Trojans

www.LMGsecurity.com

Hackers steal millions of dollars and confidential documents every day. Typically, the attackers send a phishing email to staff. When a victim clicks on the link, the computer is infected with a "banking Trojan" virus that monitors activity and captures your online banking passwords and other financial information.

What can Banking Trojans Do?

Modern banking Trojans are sophisticated commercial software utilities. Attackers can:

- **Steal your banking password** as you type it into a bank's login page
- **Capture payment card information** and other financial data as you type it into a web page
- Copy any passwords that you have **stored in your web browser**
- **Remotely login to your computer** and manually rifle through your files
- **Search your computer** for financial data and steal your data
- Scan your organization's network and **spread to other computers**

Banking Trojans spread quickly! Once a computer in your organization is infected, the malware can take over your entire network in a matter of hours.

How Can You Defend Against Banking Trojans?

- **Think Before You Click** – Make sure all employees receive regular training to defend against phishing.
- **Deploy Effective Antivirus** Install antivirus software on ALL computers. Use it, and keep it up-to-date. Check at least monthly to make sure it is running properly on all systems.
- **Limit Privileges** - Limit what staff can do on their desktop. Make sure they cannot change the system configuration or install any software without prior approval.
- **Protect Against Spam** - Make sure all spam filters are working and kept up-to-date.
- **Update Your Software** - Keep your software up-to-date with the latest patches at all times. Software updates include new security 'fixes' that can save you money and hassles.
- **Segment Your Network** – Separate systems on your network so that a high-risk workstation is less likely to infect an important server.
- **Backup** - Backup your data. Test your backups. Store a copy securely off site. Repeat.

If You Suspect a Banking Trojan…

- **Act Quickly** - If you suspect that a computer has been infected, don't wait! Act right away.
- **Quarantine Infected Computers** – Unplug the network cable immediately to stop the spread.
- **Don't Stomp on the Crime Scene** - You may need to "rule out" a data breach. Don't run antivirus or reformat the computer until a trained forensics professional has examined the system. Keep a copy of the malware if you find it, so that forensic analysts can examine it if needed.
- **Call a Forensics Professional** –Involve a professional forensics examiner right away to ensure that the right evidence is preserved. This can save you a lot of time and money in the long run.
- **Plan Your Response**- Develop your response plan before you get hit with an infection. Banking Trojans are an epidemic. Be prepared.

Questions? www.LMGsecurity.com | info@LMGsecurity.com | Twitter: @LMGsecurity

Business Email Compromise – Prevention and Response

www.LMGsecurity.com

Email account break-ins seem to happen as often as the common cold— and yet they can lead to large financial losses, reputational damage, and more. In this handout, we'll discuss how criminals break into email accounts, and what you can do to protect yourself and your organization.

Why Do Criminals Hack Your Email Account?

- **Your Data is Worth $$** - Business email accounts are potential gold mines. Your emails contain valuable data, such as Social Security Numbers, passwords, credit-card numbers, and other details that can be sold for money on the dark web. In some cases, criminals copy entire accounts of correspondence, which can later be used for ransom or political gain.
- **Criminals Use Email for Financial Fraud** - Often, criminals hack into a business email account in order to commit financial fraud. For example, a criminal might break into an email account and then immediately search searches for data that could easily be monetized (such as invoices or wire transfer instructions). Next, the criminal creates a fake invoice or wire transfer notification to redirect the funds, and then waits for the money to arrive. Sophisticated criminals add mail filtering rules that lengthen the time to discovery.
- **Your Contacts Become the Next Victims** - Once criminals break into an email account, they often made a point of targeting related accounts, such as co-workers, clients, or anyone listed as a contact.

How Do Criminals Get Access?

In recent years, email has moved to the cloud, enabling users (and criminals) to access email from anywhere in the world. Here are three ways that criminals get access to your email:

1. **Infect Your Computer** – Criminals infect your computer by enticing you to click on a link or open a malicious attachment. When you do, your computer may be infected with malware that monitors your keystrokes or steals your login information when you submit a web form.
2. **Phishing Web Site** – Criminals may set up fake web sites that look just like your email provider, bank or other common web service. Then, they trick you into visiting the web site, using phishing emails or other methods. When you type your password into the fake web site, they capture it and use it to login to your accounts.
3. **The Dark Web** – There have been so many data breaches that billions of passwords are available for sale on the dark web. If your password was stolen in the past, it may be sold on the dark web to others who will use it to login to your accounts.

Email Hacks Can Be Data Breaches

In addition to financial fraud, extortion, reputational damage and more, an email account break-in may "count" as a data breach. If an attacker had access to confidential information, you may be required to notify the data subjects and report a breach under state or federal law, depending on the contents of your email.

Protect Your Accounts

You can protect your email (and other data online) using strong passwords and login security. First, here are a few important terms to know:

Authentication - A method for verifying a person's identity. For example, I might tell my computer that I am "sdavidoff," and I prove my identity by typing in a *password.*

There are three different ways that you can verify that you are who you say you are:

- *Something you know* (for example, a password).
- *Something you have* (for example, a key).
- *Something you are* (for example, a fingerprint).

Two-factor Authentication - Verifying a person's identity using two methods combined.

Password managers:
A smart way to remember strong passwords is to not remember them at all! A password manager is secure software that stores your passwords in an encrypted vault on your computer, or in the cloud.

Here are some video tutorials for setting up and using password managers and two-factor authentication:

https://www.LMGsecurity.com/passwords

Tips for Strong Passwords and Login Security

DO:

1. **Use Two-Factor Authentication!** It's easy to set up with many providers, such as Office365 and Google.
2. **Pick Strong Passwords** - Choose a password that is long- at least 14 characters or more. Use a *passphrase* (a sentence fragment, song lyrics, etc.) to help you remember it.
3. **Use a Password Manager Program** to store your passwords securely, so you don't have to remember them all. Popular options include LastPass and KeePass.

DON'T

1. **DON'T Share Your Password** with anyone-- not friends, co-workers, vendors, or even IT staff.
2. **DON'T Re-use Important Passwords.** Avoid using the same password for multiple different websites or services. Never re-use personal passwords for work, or vice versa.
3. **DON'T Write Your Password Down on Paper**, unless it's secured in a locked location.
4. **DON'T Store Passwords in Files on Your Computer**, such as Word documents or spreadsheets. Instead, use a secure password manager.

What Should You Do If Your Email Gets Hacked?

- Reset your password.
- If possible, activate two-factor authentication.
- Place a legal hold on any mailboxes that you suspect may have been compromised, to preserve all emails. That way you can conduct an inventory and evaluate any data that may have been exposed.
- Preserve logs immediately. Export and make copies of any logs that might show who logged into your email account, where they logged in from, or what they did. This can potentially help you narrow down the scope of what may have been compromised. In many cases, mail providers delete logs after a certain number of days (ie. 30 days), so it's critical to capture logs immediately, and not wait.

Questions? www.LMGsecurity.com | info@LMGsecurity.com | Twitter: @LMGsecurity

Ransomware

Prevention and Response

by Sherri Davidoff, CEO, LMG Security

www.LMGsecurity.com

"Ransomware" has become an epidemic. Organizations of all kinds – from financial institutions to corporate and non-profit clients – are held hostage by ransomware, the malicious software that encrypts your data until you pay a hefty fee. All it takes is one person clicking on a link, and all of your shared files could be locked up for good.

The risk is huge. How can you reduce your risk of a ransomware incident in today's complex environments, and how should you respond if you fall victim? Here is an FAQ that will help you understand how ransomware works, and how you can minimize your risk before—and after—a ransomware infection.

We will answer the following questions in this FAQ:

1. What does ransomware do, and how does it work?

"Ransomware" is malicious software that attackers use to encrypt the data on your computer. When you get infected with *ransomware*, all the data on your computer gets locked up (encrypted)—and only the attacker has the key. The ransomware may also encrypt files on any network shares your have attached. It can crawl through an entire organization, encrypting files. It can even encrypt files you have in the cloud, such as DropBox or OneDrive.

Typically, the attacker will demand payment. Once your files are encrypted, you'll see a ransom note--sometimes on your desktop, sometimes as a popup. The ransomware note will usually tell you that your files are encrypted, and you won't get the decryption key unless you pay up. The criminals hold

you hostage. If you're lucky, when you pay the attacker, he or she will decrypt your data for you. In some cases, the attacker will only decrypt *some* of your precious data, and try to extort *more* money out of you to decrypt the rest.

What does it actually look like when ransomware encrypts all the files on an employee workstation… and then moves on to encrypt your company's file share, and even cloud-based documents? LMG Security released a video that shows an unsuspecting employee, "Dan D," clicking on a link and getting infected with the "Jigsaw" ransomware.[2]

The video begins by showing "Dan" clicking on a link in a phishing email:

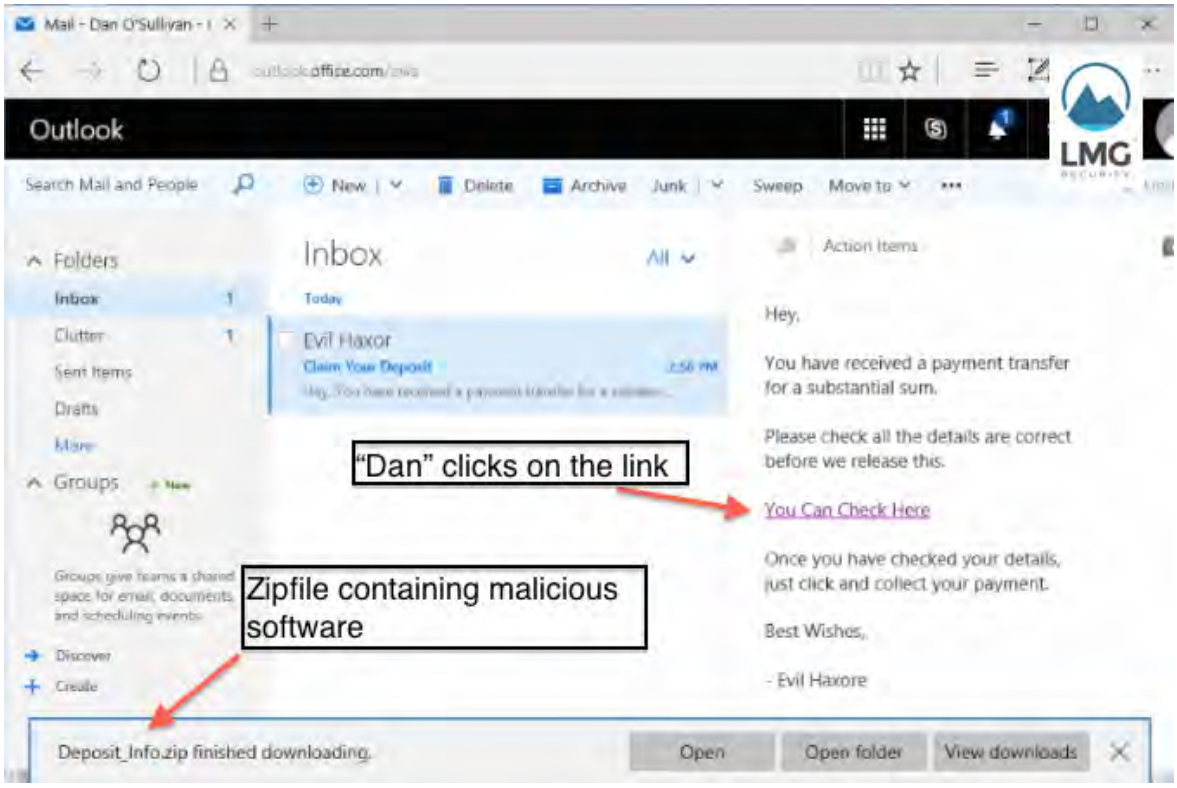


Figure 1: Staff member "Dan D" clicks on a link in a phishing email from "Evil Haxor".

As soon as he clicks, the zipfile downloads automatically. Next, "Dan" extracts and opens the Deposits file, thinking that it's a legitimate document. The ransomware installs itself and produces a pop-up with a registration message and confirmation code. Slowly, the files on the desktop start to change, as Jigsaw locks them up one by one.

[2]Davidoff, Sherri. "Watch Ransomware Wreak Havoc in the Cloud," 7/2016, http://lmgsecurity.com/blog/2016/07/19/watch-ransomware-encrypt-company-file-share-cloud-storage.

Figure 2: "Jigsaw" ransomware locks up files on the desktop.

The Jigsaw ransomware then goes on to **lock up the company's network file share** (the Y drive)!

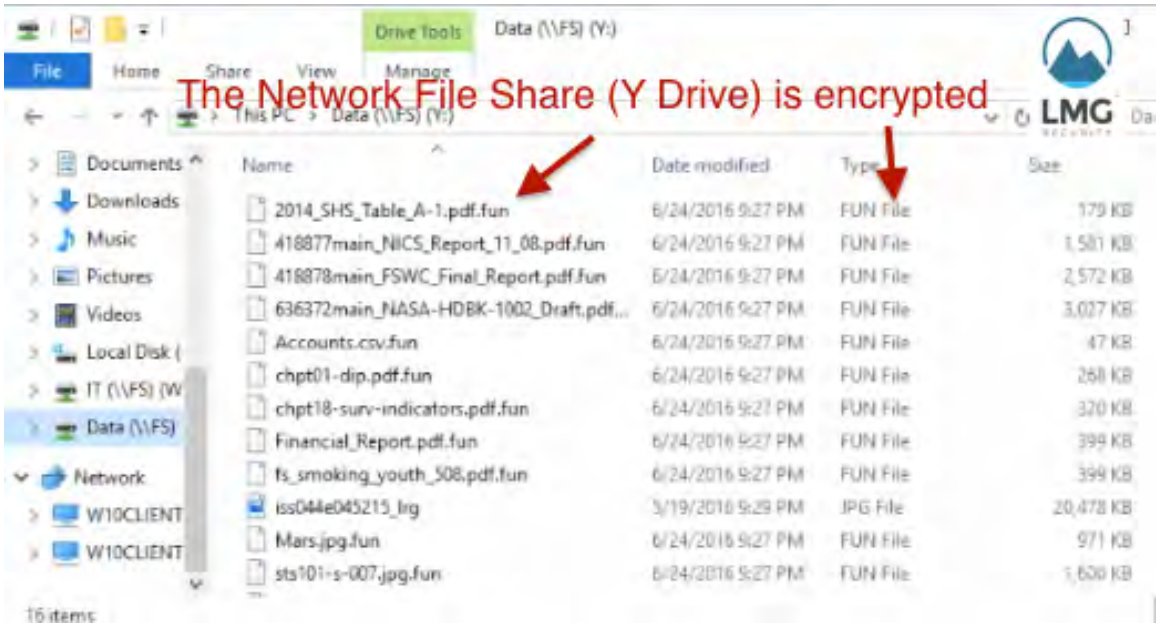


Figure 3: Jigsaw encrypts files in the network storage folder (Y drive).

The ransomware even locks up the cloud file repository, hosted in OneDrive.

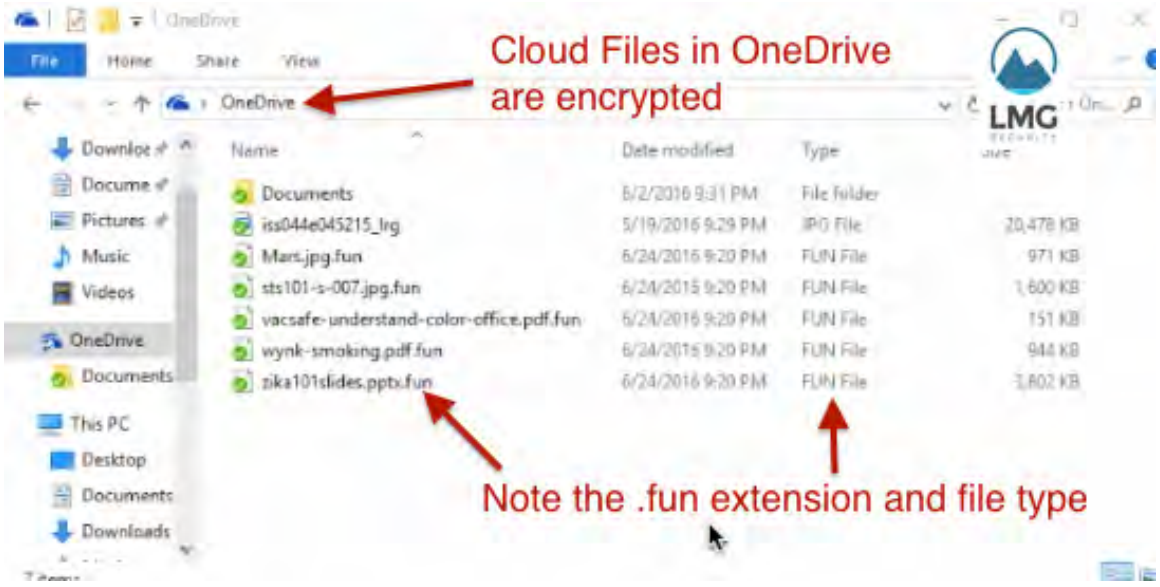


Figure 4: Even cloud-based files in OneDrive are encrypted.

Suddenly, a ransom note pops up! “You have 24 hours to pay 150 USD in Bitcoins to get the decryption key.”

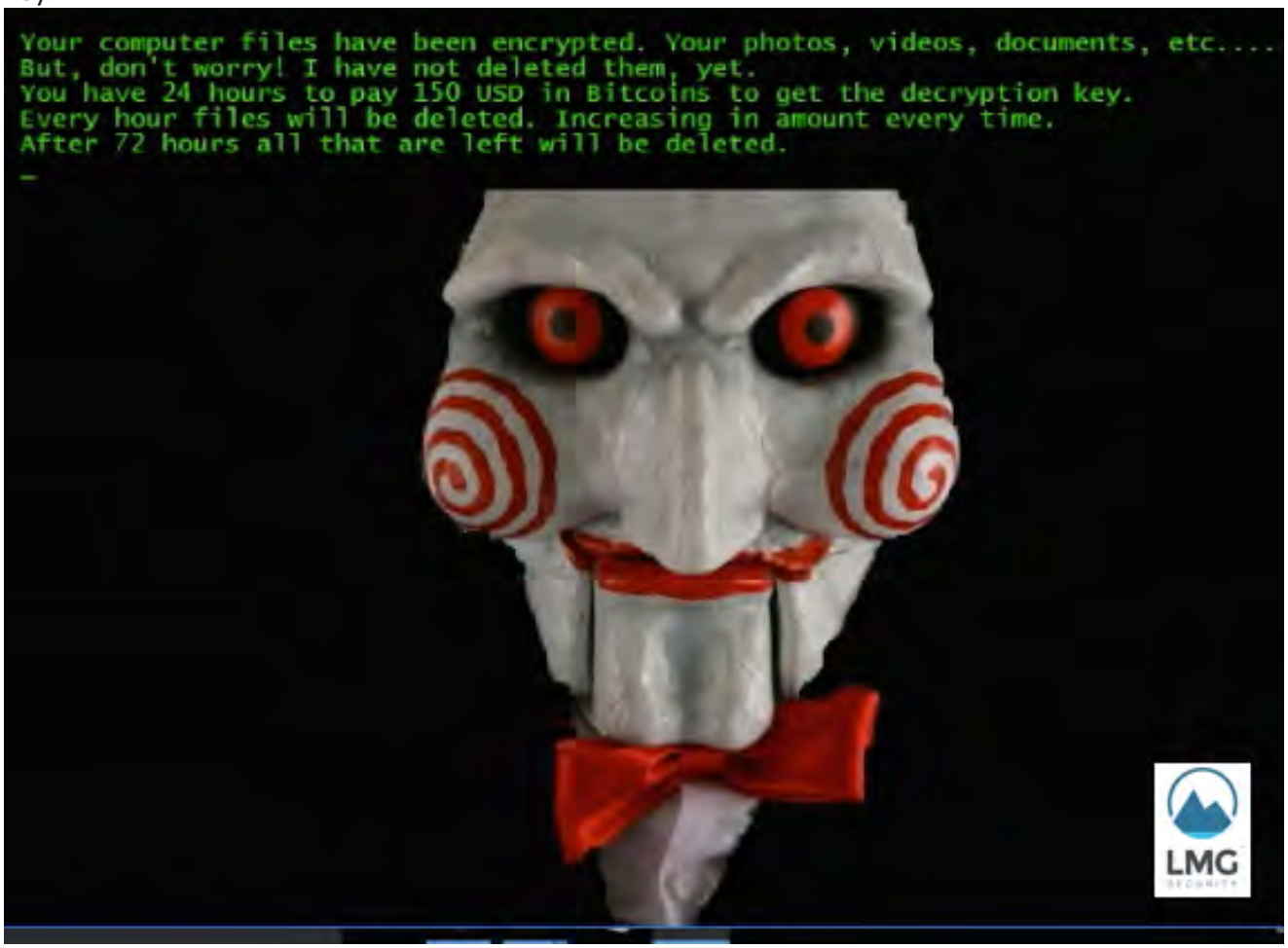


Figure 5: A ransom note pops up!

A countdown timer starts, at 60 hours:

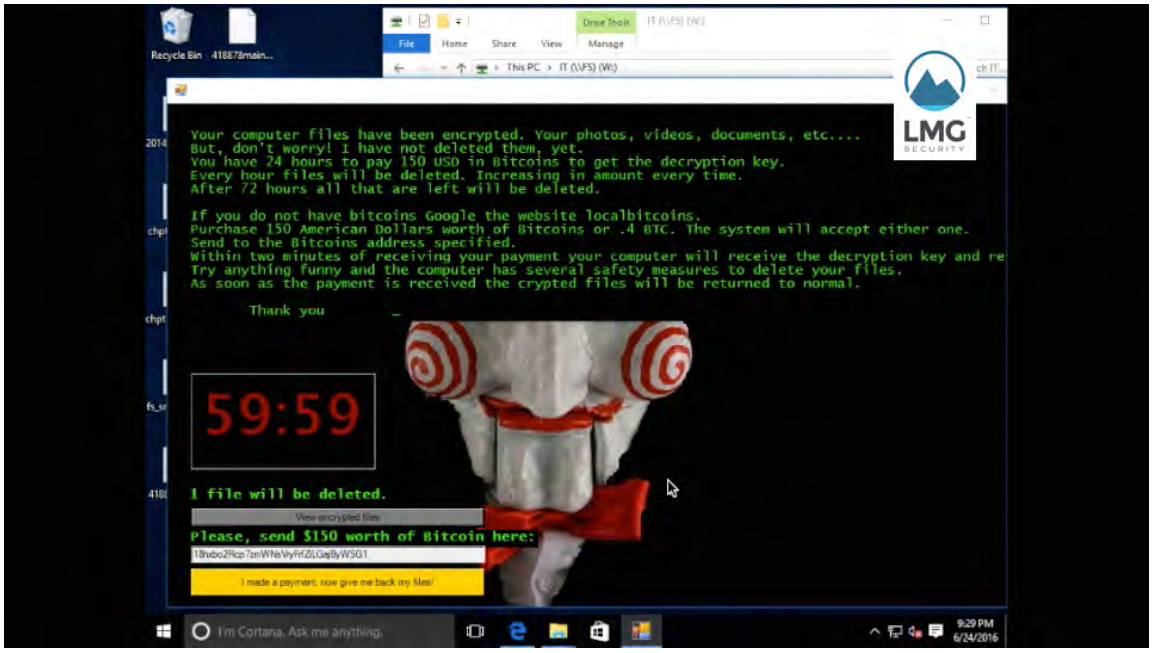


Figure 6: A countdown timer starts.

Every hour files will be deleted," says the ransom note. "After 72 hours all that is left will be deleted." Here's a screenshot showing files on the network share that have been deleted, according to Jigsaw:

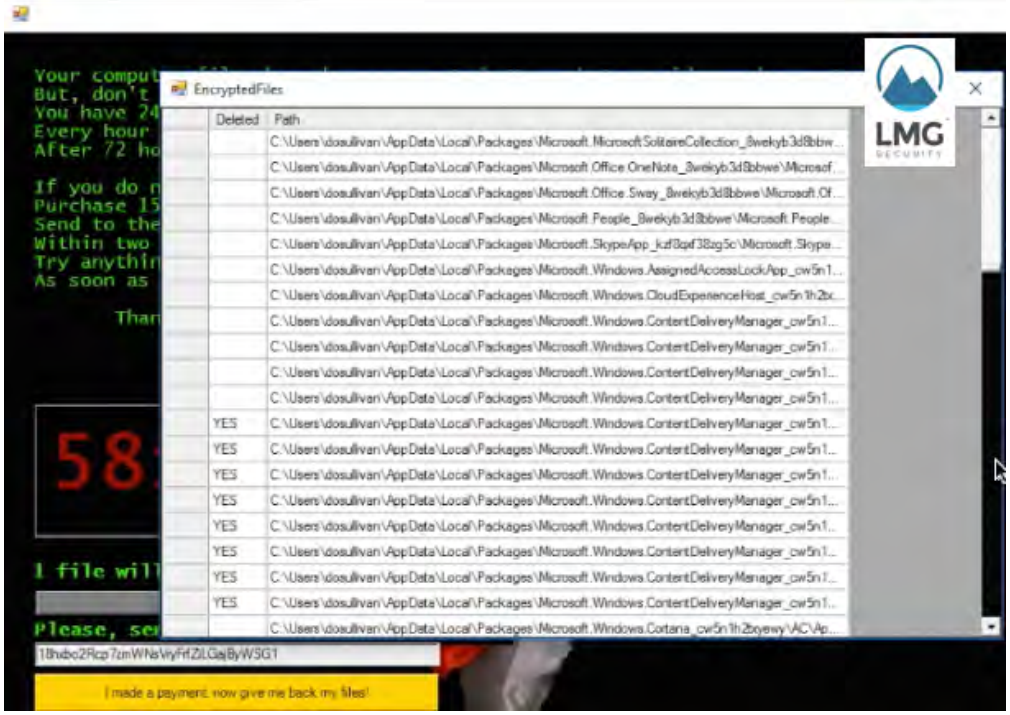


Figure 7: "Every hour files will be deleted."

2. What happens if I don't pay the ransom?

That depends! Typically, one of three things will happen:

A) Your files won't get decrypted.

B) The ransom will go up over time.

C) Files will be deleted over time. For example, in the "Jigsaw" example that we saw, files were deleted every hour until the victim paid the ransom.

3. Should I pay the ransom, and if so, how do I do that?

There has been a lot of debate about whether or not to pay the ransom. In 2015 the FBI said to pay the ransom.[3] "To be honest, we often advise people just to pay the ransom," said Joseph Bonavolanta of the FBI, speaking at the Cyber Security Summit in Boston.[4]

Certainly that's what cybersecurity professional see happen in the majority of cases where businesses get hacked and they don't have good backups. For many organizations, paying the ransom—commonly $200-$2,000[5]-- is far less costly than legitimate recovery attempts, or the impact of permanently losing files that may not be available via backups. At LMG, we keep a stockpile of BitCoins now, and if your legal counsel tells us to pay a ransom on your behalf, you can reach out to us and we will take care of the ransom payment for you.

As of September 2016, the FBI issued a public service announcement stating that:[6]

"The FBI does not support paying a ransom to the adversary. Paying a ransom does not guarantee the victim will regain access to their data; in fact, some individuals or organizations are never provided with decryption keys after paying a ransom. Paying a ransom emboldens the adversary to target other victims for profit, and could provide incentive for other criminals to engage in similar illicit activities for financial gain. While the FBI does not support paying a ransom, it recognizes executives, when faced with inoperability issues, will evaluate all options to protect their shareholders, employees, and customers."

---

[3] Ragan, Steve. "The FBI isn't wrong; sometimes you will have to pay the ransom," CSO from IDG, 10/27/2015. http://www.csoonline.com/article/2998163/disaster-recovery/the-fbi-isnt-wrong-sometimes-you-will-have-to-pay-the-ransom.html. Retrieved Feb 26, 2017.

[4] Roberts, Paul. "FBI's Advice on Ransomware? Just Pay the Ransom." SecurityLedger, October 22, 2015. https://securityledger.com/2015/10/fbis-advice-on-cryptolocker-just-pay-the-ransom/. Retrieved Feb 26, 2017.

[5] *CryptoWall Ransomware*, Dell SecureWorks Counter Threat Unit, Aug 27, 2014. http://www.secureworks.com/cyber-threat-intelligence/threats/cryptowall-ransomware/. Retrieved by Sherri Davidoff on January 10, 2016.

[6] Alert Number I-091516-PSA. "Ransomware Victims Urged to Report Infections to Federal Law Enforcement." https://www.ic3.gov/media/2016/160915.aspx

In addition, the FBI "urged" victims to report ransomware cases to the Internet Crime Complaint Center, at www.IC3.gov. "Knowing more about victims and their experiences with ransomware will help the FBI to determine who is behind the attacks and how they are identifying or targeting victims."

As of late 2016, you have another option: There is now a new type of ransomware called "Popcorn Time." If you don't want to pay the ransom, you can infect other people instead. They give you a referral link, and if two other people get infected and pay the ransom because of you, you get your decryption key for free.[7] We certainly do not recommend that you do this (and it's probably illegal), but nonetheless, it is an interesting development.

4. How much money do criminals make using ransomware?

Ransomware is often perpetrated by organized crime groups, who approach it as a lucrative commercial enterprise. They are licensing hacking software in the cloud called "exploit kits." The organized crime groups pay a monthly fee-- $3,500-7,000/month is typical-- to use exploit kits in the cloud, which have lots of nice features and make it very easy to infect your computer.[8]

In 2015, the Cisco Talos research team was able to get access to an "Angler" exploit kit infrastructure. The adversary was able to set up 147 Angler servers in the course of a month, and each server had a lifespan of a single day. In that one day of activity, each server was used to compromise 3,600 people's computers. That meant the adversary compromised approximately 529,000 computers each month.

Approximately 62% of the time, the Angler exploit kit was used to install ransomware on the infected computer (approximately 2,232 ransomware installations a month for this particular adversary).

What were they installing the other 38% of the time? Whatever they wanted. Maybe programs that steal your files or your password.

The average ransom demand was $300. According to the US Cert, 2.9% of users actually pay the ransom. Doing the math, that means **this adversary was generating approximately $2,854,505 per month, or over $34 million per year!**[9]

What were they installing the other 38% of the time? Whatever they wanted. Maybe programs that steal your files or your password.

CNBC reported: "Ransomware is on track to be a $1 billion business in 2016."[10] The revenue for criminals is only likely to increase.

---

[7] Newman, Lily Hay. "Devious Ransomware Frees You if you Infect Two Other People." https://www.wired.com/2016/12/popcorn-time-ransomware/. Retrieved Feb 26, 2017.

[8] Olenick, Doug. "Neutrino rental price doubles as Nuclear and Angler disappear." June 28, 2016. SC Magazine. https://www.scmagazine.com/neutrino-rental-price-doubles-as-nuclear-and-angler-disappear/article/529304. Retrieved Feb 26, 2017.

[9] Biasini, Nick et al. "Threat Spotlight; Cisco Talos Thwarts Access to Massive International Exploit Kit Generating $60M Annually from Ransomware Alone," Oct 6, 2015. http://www.talosintelligence.com/angler-exposed/. Retrieved February 26, 2017.

5. What should I do if I think my computer is infected with ransomware?

Time is of the essence!

- ✓ Pull the network cable out, or if your computer is connected wirelessly, find some way to get it off the wireless network. Immediately disconnect any USB drives. Remember, the ransomware will crawl through your system encrypting files. You want to stop it from locking up files on any shared drives, or backup drives that you have attached to your system.
- ✓ Call IT. They may want you to pull your computer's plug out of the wall (or pull out the battery if it is a laptop). The not-so-nice shutdown is important. If you try to shut your computer down nicely by pressing a button, sometimes the ransomware can tell and it might not actually shut down.
- ✓ Figure out quickly what was encrypted, what the extent of the damage was. If you have backups for that data, GREAT! This really underscores the importance of taking regular backups, every single day, automatically.

  If you can't restore from backups, check to see if the ransomware you got is known to be broken. There are certain kinds of ransomware where we know how to break the encryption. For example, Kaspersky has released a tool that will decrypt files if you're infected with certain strains of CryptXXX ransomware.
- ✓ If all else fails, you may have to pay the ransom. If you're going to do it, do it quickly before the price goes up.
- ✓ If there's a chance you have sensitive or regulated data on any computer that was encrypted (such as personal information, Social Security Numbers, health care information, or other sensitive data, talk to legal counsel immediately for guidance on whether or not you are required to notify any parties involved.
- ✓ Finally, consider reporting the ransomware attack to the FBI. They are tracking these cases. Either contact your local field office, or go to the Internet Crime Complaint Center at www.ic3.gov.

[10] Taylor, Harriet. "Ransomware spiked 6,000% in 2016 and most victims paid the hackers, IBM finds," CNBC, Dec 14, 2016. http://www.cnbc.com/2016/12/13/ransomware-spiked-6000-in-2016-and-most-victims-paid-the-hackers-ibm-finds.html. Retrieved Feb 26, 2017.

6. How can I prevent ransomware from happening in my office?

An ounce of prevention is worth a pound of cure. To effectively prevent ransomware, use a combination of training and technical countermeasures.

- ✓ Educate staff about the dangers of phishing emails and scams on social media sites. Include phishing in annual training, and conduct regular phishing exercises to train your team not to click on links.
- ✓ Social media sites like Facebook and LinkedIn have also been used to spread ransomware, as well as other types of malicious software.[11] Consider restricting access to social media sites on work computers, and instead encourage staff to use separate, personal devices for appropriate social media communications.
- ✓ If you have servers online that people use to connect remotely from home, make sure all of your account passwords are strong and changed regularly. Strongly consider using two-factor authentication for remote access whenever possible. There has been a recent spike of ransomware incidents where criminals broke into remote access servers using guessed or stolen passwords, and installed malware on corporate servers.
- ✓ Get effective spam-filtering software to block phishing emails consistently.
- ✓ Keep your organization's operating system and application patches up-to-date, so your workstations and servers are as resistant to infection as possible.
- ✓ Use reliable, commercial-grade antivirus software to reduce the risk of infections.
- ✓ Monitor your network (typically using a third-party service) so that suspicious activity is caught early.

[11] Mendelsohn, Tom. "Locky ransomware uses decoy image files to ambush Facebook, LinkedIn accounts" ArsTechnica, Nov. 25, 2016. https://arstechnica.com/security/2016/11/locky-ransomware-decoy-image-files-boobytrap-facebook-linkedin/. Retrieved Feb 26, 2017.

7. How can I limit the damage caused by ransomware if someone does get infected?

A ransomware infection doesn't have to be a major crisis—but it often is, if you're not prepared. There are three things you can do to limit damage in the event that ransomware does worm it's way into your network.

- ✓ Take regular backups of everything important-- and test your backups. Karen Sprenger, COO for LMG Security advises, "Test the backups and the restore process regularly. If you aren't testing, then you don't really have backups."
- ✓ Make sure everyone knows who to call, and what to do if they get infected with ransomware. Set up an easy-to-remember hotline that anyone can call to report ransomware, at any hour. You don't want to wait until the ransomware spreads throughout your whole network before IT figures out the problem. Everyone in your organization needs to recognize the signs and know that time is of the essence, pull that network cable, and call for help quickly.
- ✓ ONLY give people access to folders they really need. One of the reasons that ransomware is SO damaging is because we trust each other. Within your organization, you give people access to lots of files on the network shares.

  The Ponemon Institute did a survey and found that 71% of people have access to files that they really don't need to do their jobs.[12] We used to think that's convenient. Now it's a huge risk.

  Remember, when one person gets infected with ransomware, it will encrypt every file you have access to on your network. Now is the time to go through your organization's file permissions and lock them down, so if one person clicks a link they can't accidently encrypt everything.

[12] Ponemon Institute. "Corporate Data: A Protected Asset or a Ticking Time Bomb?" Ponemon Institute, Dec. 2014. https://info.varonis.com/hs-fs/hub/142972/file-2194864500-pdf/ponemon-data-breach-study.pdf. Retrieved 9 Aug. 2016.

8. How do I recognize whether an email might contain ransomware or other malware?

It can be hard to tell if an email is legitimate, especially if you typically get email from a wide variety of people, such as clients.

Phishing emails are designed to convince you to click on a link or open an attachment. The sender wants you to click right away, without thinking or checking to make sure it's legitimate. To accomplish this, they often appeal to your sense of fear or excitement, hoping to instill a sense of urgency that will trigger you to click without thinking.

Common characteristics of phishing emails include:

- ✓ A "lure," such as a free gift card or a tax refund;
- ✓ A scare tactic, such as an expiration or a threat that a service will be shut down unless you take action;
- ✓ A deadline or other urgent reason that you should take action immediately.

At LMG, we like to say, "Think Before You Click" (a phrase coined by my colleague Mike Wright, who managed cybersecurity for a community bank).

When you receive an email that prompts you to take an action, always take time to think. Ask yourself:

1. Do I even know this person?
2. If so, did I expect to receive this message from this person? [Remember, their email account could have been hacked]
3. Do I really NEED to click on this link? Let's say it looks like it comes from your bank. It's much better to go to your bank's web site and find the link from there, than to click on it in an email.

You can always hover your mouse over a link without clicking on it to see where it really goes. This can be a quick way to verify that an email is suspicious.

If you are not sure if an email is legitimate, as for help from your IT security staff or your organization's point of contact. When in doubt, don't click.

9. Is ransomware considered a data breach?

This is a very important ethical and legal question. The answer, of course, is that it depends on the capabilities of the ransomware and the legal definition of a data breach.

Keep in mind that some ransomware does get installed with information-stealing malware. In 2016, SecurityWeek reported that the CryptXXX ransomware had information-stealing capabilities.[13] When the ransomware is installed, it encrypts all your files and steals user data.

Your computer can also be infected with other types of malicious software, or malware, that is designed to "steal corporate secrets to sell to the highest bidder." For example, researchers reported one malware sample, examined in August 2016, which automatically searches your computer for Word docs, Excel spreadsheet, text files, and upload all of that to a server, without you ever knowing.[14]

Remember, ransomware is typically installed using an "exploit kit." That means before you're infected with the ransomware specifically, a criminal has first gained access to your computer. The criminal could have installed other types of malware on your computer as well.

This is why it is critical to understand exactly what malicious software is on your computer. A huge mistake IT folks make is to clean off your computer and wipe away the malware without saving a copy. That means if someone asks later, you'll never know what it was capable of doing—and under some federal and state laws, if you can't prove information wasn't accessed, you have to assume that it was, and notify all possible affected persons.

It's always smart to save a copy of the malicious software, so that if you need to, you can have a professional analyze it and tell you definitively what it can do.

If you have any sensitive data whatsoever - employee SSNs, payroll data, health information, confidential client files, you name it—then immediately talk to a qualified attorney who specializes in data breach law to determine whether your ransomware infection constituted a breach under state or federal regulations, or as attorney Shane Vannatta points out, "whether you are professionally obligated to alert your clients."

10. How can I see an example of ransomware in action?

Check out LMG's YouTube video of a ransomware infection! Watch as "Jigsaw" holds the fictitious company for ransom and starts the countdown clock. The video is an excellent way to show your friends and colleagues how ransomware works, and what NOT to do. You can watch the video here:

https://youtu.be/Z-htleMYq5E

Feel free to share with your friends and colleagues so that they, too, can recognize the signs of ransomware.

---

[13] "CryptXXX Ransomware Steals Bitcoin, Private Data" SecurityWeek News. April 20, 2016. http://www.securityweek.com/cryptxxx-ransomware-steals-bitcoin-private-data. Retrieved Feb 26, 2017.

[14] Abrams, Lawrence. "New Information Stealing Trojan Steals and Uploads Corporate Files" BleepingComputer, August 12, 2016. http://www.bleepingcomputer.com/news/security/new-information-stealing-trojan-steals-and-uploads-corporate-files Retrieved Feb 26, 2017.

About the Author

Sherri Davidoff is the CEO of LMG Security and the co-author of "Network Forensics: Tracking Hackers Through Cyberspace" (Prentice Hall, 2012). She has sixteen years of experience as a cyber security professional, specializing in digital forensics, penetration testing and security awareness training. Sherri is a speaker for the American Bar Association, and has conducted onsite security training for the Department of Defense, Google, Comcast, Los Alamos National Laboratories, and many other organizations. She is a faculty member at the Pacific Coast Banking School, where she teaches cybersecurity classes. Sherri is a GIAC-certified forensic examiner (GCFA) and penetration tester (GPEN), and holds her degree in Computer Science and Electrical Engineering from MIT.

Questions?

Sherri Davidoff

Web: www.LMGsecurity.com

Phone: 855-LMG-8855

Email: info@LMGsecurity.com

LMG SECURITY

9 BUILDING **BLOCKS**

of an Effective Cybersecurity Program

Cybersecurity management can seem complicated. How do you make sure you've covered all the bases? Whether you're in a small business or large organization, these are the 9 building blocks of every effective cybersecurity program.

1

CHOOSE AND USE A CYBERSECURITY CONTROLS FRAMEWORK

The foundation of your cybersecurity program is your controls framework, which is a checklist for your cybersecurity program. Once you've picked a framework, use it! Conduct controls assessments regularly and track your progress over time.

TEST YOUR SECURITY

Does reality match what's on paper? Conduct technical security testing. This can include penetration tests, vulnerability assessments, web application assessments, social engineering testing, and more.

ASSESS YOUR RISK (OFTEN)

Conduct an information security risk assessment at least annually, to identify your risks and develop a mitigation plan. Use a widely accepted risk assessment and management framework, such as NIST SP 800-30.

TRAIN YOUR STAFF AND CUSTOMERS

Humans are the most critical component of your security infrastructure. Conduct cybersecurity awareness training regularly for all of your employees, IT staff, and (yes!) even your customers.

PREPARE FOR A BREACH

Every day, another company gets hacked and makes the news. Plan ahead! Create formal policies and procedures for cybersecurity incident response. Train your first responders. Conduct tabletop exercises.

LMG Security

Toll-Free:
855-LMG-8855
info@LMGsecurity.com
www.LMGsecurity.com

KEEP TRACK OF YOUR DATA

Identify sensitive information and track where it is stored, processed, and transmitted. Make sure to include mobile devices and USB drives. Decide if staff may access and store data using personal devices.

MAINTAIN POLICIES AND PROCEDURES

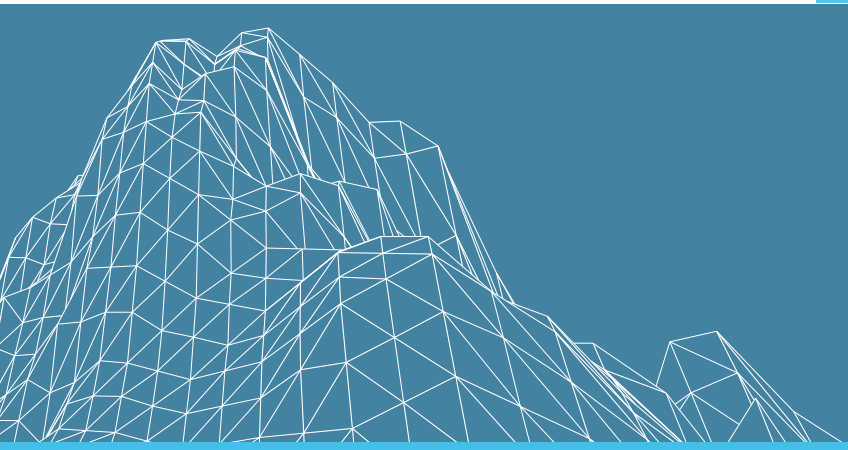
Make sure to document your organization's cybersecurity policies and procedures and follow them. You can purchase policy templates, or have a professional create them for you. Update your policies and procedures routinely.

MONITOR YOUR IT

How do you know if you have a cybersecurity problem? Monitor your IT infrastructure. This includes network monitoring as well as security software installed on desktop, mobile devices and servers. Make sure that you budget for staff or a third party to respond to alerts.

GET INSURANCE

You can't solve information security issues overnight. Transfer risk to a third party by purchasing cybersecurity insurance. Make sure the policy you select covers your highest-risk scenarios. Have an experienced cybersecurity professional review your policy.



We make **nothing** happen.

CYBERSECURITY • COMPLIANCE • FORENSICS • TRAINING

LMG Security

Toll-Free: 855-LMG-8855
info@LMGsecurity.com
www.LMGsecurity.com

LMG SECURITY