SysAdmin

Magazine

netwrix

№

29

IT Horror Stories

Halloween edition

SysAdmin
Magazine

№ 29 October ‘17

SysAdmin Magazine is a free source of knowledge for IT Pros who are eager to keep a tight grip on network security and do the job faster.

The Sysadmin Magazine team
sysadmin.magazine@netwrix.com

Contents

Pierre Hellfire Dehombreux

Director of IT at Whiteriver Unified School District

Ransomware Survivor: 6 Tips to Prevent Ransomware Attacks

My name is Pierre and I am an IT director at Whiteriver School District in Arizona, U.S. I am a recent ransomware survivor, and I'd like to share my story and the lessons I learned with you.

Who We Are

Whiteriver School District comprises three elementary, one high and one general school. Our IT infrastructure is very dynamic. Every year, new children enroll and graduates leave. Teachers and other personnel are coming and going, too — the turnover is really high here. This lifecycle results in a never-ending stream of changes in our IT environment, which my small team of three has to control. We must constantly add and remove users, take care of our backups, make sure nobody touches sensitive files they're not supposed to access, maintain a clean environment, and so on. We never get bored at school!

How We Detected an Anomaly

My teammates and I routinely review reports on file activity delivered by Netwrix Auditor, just to make sure there is nothing anomalous going on. We actively use our file shares to store a very large amount of information, including highly sensitive data — from attendance records to personal student information. Everyone working in the district needs access to some of this data, so we have to keep it safe. If we lost some of the files, the nurse might not be able to retrieve a student's health records or find the emergency contact information if something bad happened. We know that any anomaly — such as somebody trying to modify many files at once — is a warning bell that something might be wrong.

> **We saw that one of the file share activity summaries, which is typically 20–30 pages long, reached 100 pages**

One day in October, right after fall break, we saw that one of the file share activity summaries, which is typically 20–30 pages long, reached 100 pages. We immediately noticed a huge number of failed file modifications: A user was trying to modify hundreds of files in one of our most critical shares.

The report showed the user account name, so we didn't have to be a Sherlock to find the user in our Active Directory, along with the building and the room she sat in.

Resolving the Ransomware Problem in 5 minutes

What happened next? I rushed to the room where that user works and saw one of our teachers in tears. "I got an email, clicked on the attachment, and now all my files are encrypted," she cried.

She needed those files to prepare an expense report for the State of Arizona, which finances her vocational program. Without the files that had been encrypted, our school would have had to close the program and pay back all the money given for it — around $60,000 — as well as a large fine from the Arizona Auditor General. Just one click on a malicious email, and the whole school district was facing a pretty big financial hit.

I came to her computer and saw a pop-up window with a message from the attackers demanding a ransom for the decryption key. Honestly, I just laughed at it. All I had to do was disable the compromised account and restore the encrypted files from the offline backup. It took us not more than five minutes to recover from the ransomware attack and give our teacher back her peace of mind.

Lessons Learned: Make Good Anti-Ransomware Habits Stick

I cannot say that my life changed that day, but our approach to securing the data was certainly borne out by these events. I would be happy to share some basic rules that we established in our IT department that enabled us to beat that ransomware and that help us minimize the risk of ransomware damage in the future:

1. Gain visibility into your IT environment

We were able to track down this issue in minutes because we have visibility into what is happening in our IT environment, including activity across file shares. With deep visibility, you can quickly figure out if something illicit like crypto intrusion is happening in your shares.

2. Follow the least-privilege principle

It is essential to make sure that all file permissions are set up properly. In our case, ransomware managed to encrypt only a limited amount of data — just the files that one teacher had rights to modify

because they were directly related to her job. The files she had read-only access to were safe; the malware was unable to modify them.

3. Regularly test users' permissions

Because proper file permissions are of vital importance, it is essential to test them: Regularly log as a user and try to delete stuff or change files, as if you were a bad guy. Do the same after applying patches. I cannot count how many times I have downloaded a software upgrade and all the permissions were changed. One day, improper permissions could cost you a fortune.

4. Take regular backups and limit access to them

Because proper file permissions are of vital importance, it is essential to test them: Regularly log as a user and try to delete stuff or change files, as if you were a bad guy. Do the same after applying patches. I cannot count how many times I have downloaded a software upgrade and all the permissions were changed. One day, improper permissions could cost you a fortune.

5. Set your spam filter

After what happened with the teacher, we experienced another ransomware attack coming from an email. Fortunately, it was stopped in time, thanks to properly configured spam email filter rules that hinder the delivery of potentially harmful documents.

However, one user who received the email did not take the filter seriously enough. She circumvented it by forwarding the email from her Spam folder to her personal email account, and then opened it on her laptop. As a result, all her personal files got encrypted. In her defense, the email seemed to be coming from a U.S. federal agency, so I can see why she did not trust the filter.

6. Raise awareness and encourage employees to notify about the problem

Finally, you should make your employees and colleagues understand that it never hurts to ask for help and admit their mistakes. The faster they report on the problem, the faster you can respond, and the less tears they shed.

These simple tips will help you mitigate the risk of ransomware jeopardizing the security of your IT ecosystem and stay on the lookout for the next attack. Therefore, I advise all IT pros to take care of establishing healthy habits before ransomware takes care of them.

Jeff Melnick
Bloodthirsty
IT Security Expert, Blogger

Top 3 Ways Departing Employees Steal Your Data

Cybercrime keeps evolving, but one thing stays the same: The biggest security threats are often not outside your company, but inside. The problem isn't limited to large organizations; in fact, small and mid-sized businesses fall victim to employee data theft even more often, though these breaches are less likely to make the headlines.

No IT pro wants to be the one to tell the CEO or CIO that an employee has stolen critical data on the way out. The first step in preventing such theft is understanding why and how people are stealing data before or after they depart from their organizations. This blog post reveals what industry research has discovered about the motives behind this data theft and explores the top three threats that insiders pose to your sensitive data.

What are the motives?

Why do people to take a risk and steal from their employers? According to the 2017 Verizon Data Breach Investigations Report (DBIR), the primary motive is financial gain, which accounted for 60% of breaches in 2016. This is not a surprise. Personally identifiable information (PII) is extremely valuable on the black market, and stolen intellectual property (trade secrets, sales projections, marketing plans and so on) can be worth billions of dollars to competitors. Less frequent motives for data theft are cyber espionage for career development, revenge, whistleblowing and stealing data for fun — but, of course, these motives can also have a strong financial component.

What happens to those who underestimate the risk of employee data theft?

How exactly does data theft play out based on these different motivations? Here are three case studies that illustrate the process, and the consequences for the victim organizations.

Case #1

Data theft for financial gain and career development

Rogue employee jeopardizes the future of Uber's self-driving car strategy (2017)

Here's how quickly a dream can turn into a nightmare. Uber is one of the most successful and well-known companies in the world. To advance its goal of developing self-driving cars, it acquired a startup called Otto, which was developing a technology Uber needed, and hired its all-star team, including Otto's founder, Anthony Lewandowski. Uber seems well on its way to dominance in the hot new area of autonomous vehicles.

A year later, Uber's lesser known competitor, Waymo, sued Uber for trade secret theft.

> **A developer stole 14,000 confidential technical documents, blueprints, and other files and used that intellectual property to found his startup**

According to Waymo, Lewandowski stole some 14,000 confidential technical documents, blueprints, design files and other files as he was leaving Waymo and used that intellectual property to found his startup, which was later acquired by Uber. **Now Uber is in a very tough position.** It may face criminal prosecution not only for using stolen technology in the production of its self-driving vehicles, but also of actively covering up the trade secret theft.

The case is under investigation and the trial has been postponed to December 2017, but both companies are already involved in a series of intense public hearings. This certainly doesn't look good for Uber, especially considering the fact that the company is facing another federal investigation for allegedly violating the U.S. Computing Fraud and Abuse Act (CFAA).

It's too early to predict how the battle between Uber and Waymo will end, but stakes are already high: Companies are fighting for the right to develop a technology that may be as significant for the industry as the invention of the automobile itself.

Case #2

Deliberate data theft or damage

A plastic surgery drama in Beverly Hills (2017)

It would be horrifying to discover that photos and videos of your plastic surgery have been posted on the internet — especially if you're a celebrity whose face can be readily identified by millions of viewers. But that's exactly what happened to patients of famous Beverly Hills plastic surgeon Dr. Zain Kadri.

In 2016, Kadri hired an employee who worked first as a driver and translator, and then moved on to data entry and answering phone calls. She either quit or was fired in 2017 after being accused of embezzling from the company.

> **An employee with privileged rights used her corporate smartphone to take pictures of patients' medical records and credit card information**

But apparently she misused her insider privileges in other ways. According to a statement from Kadri's practice, she also used her corporate smartphone to take pictures of patients' medical records and credit card information — and also took inappropriate photographs and videos of patients before and during surgery.

The case is still under investigation; however, Kadri believes that the primary motive here is revenge. At least some of the videos and photos were made public on Snapchat and Instagram — a strategy that **could draw ire towards Dr. Kadri from his celebrity clientele and hurt his practice**. So far, there is no evidence that the employee was financially motivated or hired by a competitor.

Case #3

Human mistakes or negligence

FDIC faces a series of data breaches due to employee mistakes (2016)

It would be horrifying to discover that photos and videos of your plastic surgery have been posted on the internet — especially if you're a celebrity whose face can be readily identified by millions of viewers. But that's exactly what happened to patients of famous Beverly Hills plastic surgeon Dr. Zain Kadri.

In 2016, Kadri hired an employee who worked first as a driver and translator, and then moved on to data entry and answering phone calls. She either quit or was fired in 2017 after being accused of embezzling from the company.

In February 2016, an employee at the U.S. Federal Deposit Insurance Corporation (FDIC) was leaving her job. On her last day at work, she downloaded her personal files from her work computer to a USB drive and took it home. Three day later, the FDIC's data protection software detected that 44,000 customer records, including PII, had been accidentally taken along with her personal data. The FDIC promptly contacted the ex-employee and asked her to return the device and sign an affidavit stating she did not use or share the information.

> **The FDIC had already experienced at least 5 security incidents, with departing employees accidentally transferring company data to personal storage devices**

This case wouldn't be so worrisome if the FDIC hadn't already experienced at least five similar security incidents, with departing employees accidentally transferring company data to personal storage devices — including highly sensitive data like loan and banking information. Unlike the February 2016 incident, not all the earlier breaches were immediately handled and reported by FDIC, which led to a series of hearings and fines from regulatory bodies.

Although the FDIC seems to have taken to heart the need to report security incidents promptly, the management team should really ask two key questions: First, how long will it be before the organization finally updates its security policies and makes sure that employees follow basic cybersecurity rules? And second, **were all of these breaches truly unintentional?**

A ticking bomb: Who's next?

All the cases above have one thing in common: It took less time for ex-employees to obtain sensitive data than for organizations to detect and investigate the incident. Indeed, stealing an employer's data doesn't take long — you need only a couple of minutes to copy sensitive files to your personal device. But detecting a malicious insider in your company's network can be challenging; the DBIR found that data theft can take months or years to discover.

The simple fact is, you can't get inside the head of employees and know whether they are planning to resign and whether they plan to take your critical data with them when they go. Therefore, you need to treat every employee as a ticking bomb who can cause a security horror story. Specifically, you must take proactive steps to prevent data theft and have strategies in place to detect cases you can't prevent. Unfortunately, the 2017 Netwrix IT Risks Survey revealed that most of organizations still have only partial visibility into what users are doing in their IT environments — which makes these goals difficult to achieve.

Ben Brumm

Tarantula

IT Software Consultant, Database Specialist

4 Things You Should Never Store in Your Database

Databases are mainly used to support various business-critical applications. They can store many kinds of data. However, there are some things you should never keep in a database.

These basic database security techniques will help protect your data:

1. Unsecured Credentials

This is probably an obvious point, but it's not a good idea to store plain text passwords in your database.

If a hacker gets access to the data in this table, he or she has a list of all passwords for all users. These passwords are in plain, readable text, which can be used to log in to the system as though the hacker were that user. This might not seem like a big deal: If the hacker has already accessed the system, why would he or she need a login? The problem is, people often use the same password for many accounts. If a hacker has user names and passwords, he or she can use that information on other sites. So, how do you get around this issue? Encrypt the password before storing it. This process is often called "hashing" and can also be combined with "salting."

Hashing involves applying an algorithm to an entered password, which encrypts it. It can then be stored in the database. To check against this password, the system can perform the same hashing process against whatever value the user has entered and can check the output against the stored hashed value previously entered (the correct password). Many programming languages have a built-in functionality to perform this for you. Long story short, don't store plain text passwords in a database.

2. Duplicate Data

Storing duplicate data in your database is not a good idea. It occupies more space in your database, which can be a considerable amount if you have

a large database. Also, it can cause problems when you need to update the data, as you need to update it in several places. The only exception to this is when you're creating a data warehouse. These kinds of databases are optimized for fast querying, rather than updating, and usually contain duplicate data.

One of the advantages of using a relational database to store data is the ability to store data in multiple tables, with each table representing an entity, which is then linked to each other. This is referred to as "normalization". It allows you to have a single table for each entity, and use ID numbers (or other key values) to link between tables.

This means it's easier to update data if you ever need to make changes to some values. It also saves space, and can often improve performance when making changes to the data.

3. Files Such as Images

Databases allow you to store files within tables in the database, such as images.

Now, while you can create tables and columns to store files (such as Oracle's BLOB data type), it doesn't mean you should. Storing a file in a database table means you need to use database logic (and possible application logic) to access the file. This increases the size of your database and degrades its performance. It also makes backups and data corruption harder to deal with. A better approach to storing files and images is to use the file servers. That's what they're made for. Doing so allows for faster file access, easier file metadata access, and easier backup and restore functionality.

4. Credit Card Data

Finally, you shouldn't store credit card information in your database unless you absolutely need to. This includes credit card owner names, numbers, CVV numbers, and expiration dates. There is far too much risk involved. If a hacker gets access to credit card data from your system, it has a big impact on your company and your customers. You also need to be externally audited to make sure you comply with strict standards—namely PCI DSS—if you store credit card numbers. This creates more trouble for your IT department and means additional expenses. A better approach is to use an existing solution, such as Authorize.net or PayPal. These organizations have already developed the software, proved their compliance, and many other companies already use and trust these companies. It's better to avoid storing credit card data at all. Doing so is not worth the risk, and other companies do it better.

[Infographics]

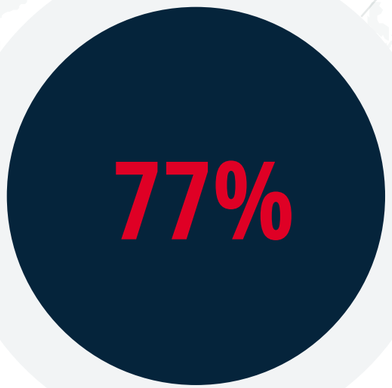
Top Cybersecurity Risks in Education

Netwrix conducted its 2017 IT Risks Survey to learn more about the security, compliance and operational issues that bother organizations worldwide. As part of the survey, we've gathered feedback from IT specialists working for educational institutions to find out about their IT security practices, pain points, experiences and plans. Let's look at our findings.

Read Full Report

of educational organizations do not use any software for information security governance

of educational organizations had compliance issues in 2016



of educational organizations consider employees to be the biggest security risk

IT RISKS Education 2017

netwrix

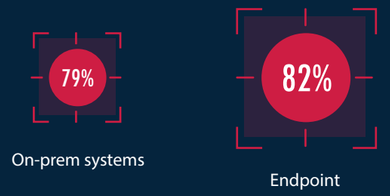
CONTEXT

79% Of organizations do not use any software for information security governance or risk management

77% Of IT operations teams are at least partially responsible for security

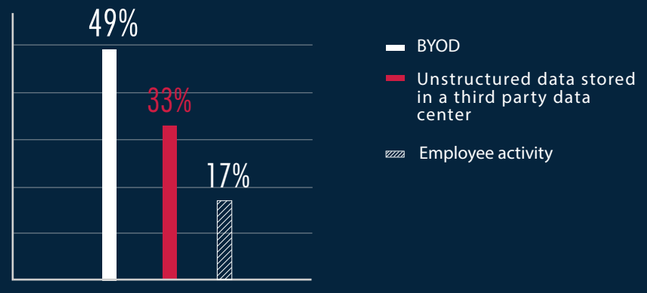
72% Of organizations do not have a separate information security function

MAIN SECURITY FOCUS



On-prem systems | Endpoint | Virtual infrastructure

MOST NEGLECTED AREAS



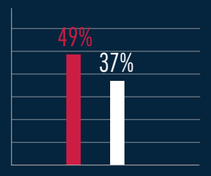
BIGGEST SECURITY RISKS

77% Employees

23% Hackers

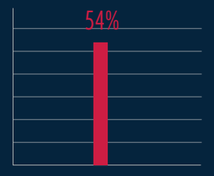
35% of organizations had compliance issues in 2016

MAIN CAUSES OF SECURITY INCIDENTS IN 2016



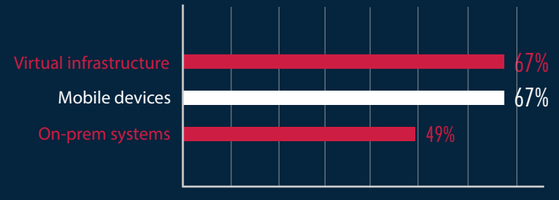
Human errors
Malware

MAIN CAUSES OF SYSTEM DOWNTIME IN 2016



Accidental or incorrect user activity

WHERE VISIBILITY INTO USER ACTIVITY IS MOST NEEDED



ONLY 23% of organizations are well prepared to beat cyber risks

WHY?

54% Lack of time

74% Lack of budget

44% Insufficient participation of senior management

FOCUS OF FUTURE INVESTMENTS

49% Data breach

23% Intellectual property theft

49% Fraud

WHY ORGANIZATIONS NEED VISIBILITY

98% To detect and mitigate human factor (errors, misuse, etc.)

98% To investigate security incidents

95% To maximize system uptime

Ryan Butcher Brooks

Product Evangelist

8 Scariest Ransomware Viruses

The first ransomware infections drew attention in 2013, and they have been steadily on the rise since then. Today, they are one of the most common online threats affecting Internet users and organizations of all sizes. According to the Verizon 2017 Data Breach Investigations Report (DBIR), ransomware was the top malware variety within Crimeware in 2016.

What Is Ransomware and How Does It Work?

Ransomware infection most commonly results in encryption of the data stored in the computer system. However, certain types of ransomware block access to the data without encrypting it or even leak it online for everyone to see. Then, the hackers demand a ransom to return everything to the way it was and give victims their data back. In most cases, the transaction is in bitcoins, wire transfers or premium-rate text messages to protect the anonymity of the attackers and make the payment hard to trace. The ransom amount varies, from $150–$500 for an individual to thousands of dollars for an organization. The worst aspect of ransomware is that a paid ransom does not guarantee that the blocked data will be unlocked by the intruders.

Security experts name four main types of ransomware:

1. Encrypting ransomware
2. Non-encrypting ransomware
3. Leakware
4. Mobile ransomware

Encrypting ransomware

Encrypting ransomware uses an RSA encryption algorithm, which encrypts victims' data files or the entire hard drive and then demands a ransom to unlock the encrypted files. Ransomware became prominent in 2013 with a new version called Cryptolocker. The Cryptolocker was the first to demand a ransom to be paid in bitcoins to get the

decryption key for the encrypted data.

The newest version of crypto-ransomware is website ransomware, which is a crypto-ransomware type of malware that targets websites. It has a limited influence as it attacks and infects the website files and doesn't affect databases. After the attack has happened, the files on the server are inaccessible, and the homepage is defaced with a warning that the website has been held hostage.

Check out our step-by-step guide to learn how to get rid of encrypting ransomware, based on a real example.

Non-encrypting ransomware

Non-encrypting ransomware doesn't encrypt the data files present in the system. Its methods can be different, but the most common types of non-encrypting ransomware are:

- Ransomware that gets into the user's computer system, displays porn images and offers to get rid of this display if the user sends a premium-rate text message. After paying the ransom, the user receives a code that can unlock the machine and stop the porn images from being displayed.

- A ransomware worm that uses the notice of Windows Product Activation to fool computer users. This malware informs users that a system's Windows installation should be reactivated. However, the link always remains unavailable. The user then calls the helpline number written on the notice, which claims to be free. In fact, the call is made to an international number that gets busy for a long period of time. The result is a huge money loss by the victim of the ransomware.

Leakware

Leakware is a relatively recent form of ransomware. It can be thought of as the opposite of classical ransomware. Leakware doesn't lock users out of their data but threatens to publish stolen information online. Generally, the stolen files contain information that could taint the reputation of the victim. Damage to businesses from leakware can be huge. Therefore, victims usually pay the ransom to save the sensitive data and their reputation. Because it is possible to thwart traditional ransomware by keeping backups or formatting the hard drive, hackers have started to prefer leakware more and more. Threatening to release confidential data to the public is better motivation that just encrypting the data. A typical case of Leakware is shown in one of the episodes of the TV series Black Mirror.

Mobile ransomware

Mobile ransomware is a form of malware that affects mobile devices. It locks your device screen or steals sensitive data and then demands a ransom to unlock it or return the stolen data to the user. The attack begins

with a download of allegedly innocent content or critical services. After the malware is downloaded onto a device, it will show a fake message accusing the victim of a law violation (for instance, using copyrighted files) before encrypting the files and locking the phone. After the ransom is paid, commonly via Bitcoin, the ransomware will send a code to unlock the phone or decrypt the data.

Most Dangerous Ransomware Infections

Encouraged by the profitability of ransomware, criminals have taken this threat to the next level by offering ransomware-as-a-service, which enables anyone, regardless of their skill or coding knowledge, to upgrade to an encrypting ransomware business model. This approach was followed by a variety of experiments regarding how ransomware is delivered and how much it demands. Criminals introduce time limits after which files will be deleted (e.g., Jigsaw, Koolova), ransoms that increase over time (e.g., Cerber) and even options to decrypt files for free if the victims become attackers themselves and infect other people (e.g., Popcorn Time).

These are the nine biggest and most dangerous ransomware threats that made headlines in 2016-2017:

#1 CERBER

Having emerged in late February 2016, Cerber is a ransomware-type malware that encrypts various file types including .jpg, .doc, .raw, .avi, etc. Cerber adds a .cerber extension to each encrypted file. Following successful infiltration, Cerber demands a ransom of $499 in bitcoins to decrypt these files. The payment must fall within the given time frame (seven days), otherwise the ransom amount will double.

Having generated $2.3 million in a year, Cerber is currently one of the top crypto menaces in the world, along with its direct competitor Locky. Cerber is sold mainly on underground Russian forums and deploys the finest Advanced Encryption cryptographic standard. Cerber has spawned four editions with various improvements within the eight months of its operation. Cerber is also offered in the form of ransomware-as-a-service, which allows “affiliates” to distribute the Cerber ransomware in exchange for 40% of each ransom amount paid.

#2 LOCKY

Locky ransomware was discovered in February 2016, and since that time, it has been sent to millions of users worldwide, including 30 million Amazon users attacked in May 2016. The ransomware infection is distributed via spam e-mails that contain JavaScript attachments. The malicious .doc files attached to e-mails (which are allegedly an invoice requiring payment) contain scrambled text, which appears to be macros. When

users enable macro settings in the Word program, an executable file is downloaded, and the user's files are encrypted.

Locky also changes all file names to a unique 16-letter and digit combination with an **.aesir, .thor, .locky, .zepto** or **.odin** file extension. Thus, it becomes virtually impossible to identify the original files. To decrypt the files, victims must pay a ransom of approximately $235–$470 in bitcoins.

#3 KILLDISK

KillDisk is a destructive data-wiping malware that has previously been used to sabotage companies by randomly deleting files from the computers. Once in the network, KillDisk targets any drive, local or network, that the user has access to, which means that infecting one user can shut down a number of others. KillDisk is able to target not only Windows systems but also Linux machines, which is something we don't see every day. KillDisk is possibly the most expensive type of ransomware to date – it asks for around $247,000 in bitcoins. It is important to note that the Linux variant of KillDisk does not store the encryption key anywhere, so even if you pay an extremely large ransom, the criminals cannot just supply you with the decryption key and bring your files back.

#4 PETYA

Discovered in July 2016, Petya was one of the first types of ransomware virus to gain major success by spreading via a ransomware-as-a-service scheme. Petya targets mostly business users. For example, an HR employee receives an e-mail that contains a Dropbox link, which appears to be a person's curriculum vitae. In reality, it is an .exe file that contains a self-extracting executable file, which will later infect the system. Apart from encrypting files, Petya locks the function of the full system and replaces the reboot code of the computer with a malicious reboot code; victims are forced to pay a $400 ransom to regain access to their computers.

> **Popcorn Time turns victims into attackers by giving them an option to pay a ransom or to infect two other people**

#5 POPCORN TIME

Popcorn Time is a type of crypto-ransomware that combines Ponzi schemes, social activism and blackmail. Initially discovered by MalwareHunterTeam in late 2016, the Popcorn Time ransomware has been designed to give the victims a criminal way of getting a free decryption key for their encrypted files and folders. In fact, Popcorn Time turns victims into attackers by giving them an option to pay a ransom or to infect two other people and have them pay the ransom to get a free decryption key.

The Popcorn Time ransomware appends the **.filock**

extension to the encrypted files and is able to encrypt more than 500 file types using AES-256 encryption. Popcorn Time demands a payment of one bitcoin, which now equals $780.

> **Koolova's victim has to read two articles about how to protect data against ransomware before the countdown reaches zero**

#6 KOOLOVA

Koolova is perhaps the strangest thing to pop up. This ransomware claims to restore your files for free (just like Popcorn Time). The only difference is that you don't have to infect others to get a free decryption key. Instead, the victim has to read two articles about how to protect himself or herself against ransomware attacks: Google's "Stay safe while browsing" and Bleeping Computer's "Jigsaw Ransomware Decrypted: Will delete your files until you pay the Ransom."

Once the Koolova ransomware infects a machine, it encrypts the files and then displays a warning screen, where the text instructs the victim to open and read two awareness posts before giving a decryption key. It then displays a screen similar to the Jigsaw Ransomware and tells you that if you are too lazy to read two articles before the countdown reaches zero, it will delete the files, which is not a joke, as Koolova actually does delete the files.

#7 SPORA

Spora is a new ransomware that appeared in January 2017. Its most notable features are a solid encryption routine, the ability to work offline and an extremely sophisticated payment site. Spora is distributed via spam e-mails that pretend to be invoices. E-mails come with ZIP attachments, which contain HTA (HTML Application) files. These files contain double extensions such as **PDF.HTA** or **DOC.HTA**. On Windows computers, users only see the first extension and can be easily tricked into opening the malicious files.

Spora does not appear to have weaknesses in its encryption process, and it has a unique pricing model. Full decryption, which includes removal, file restoration and immunity against future versions of ransomware, is approximately $79-$280 in bitcoins. The price varies depending on what option the victims choose: They can choose only one option (either restore files, remove ransomware or receive immunity), or victims can decrypt two files free of charge. Victims have a limited time to pay the ransom, otherwise decryption keys are permanently deleted.

Unlike other ransomware, Spora does not append

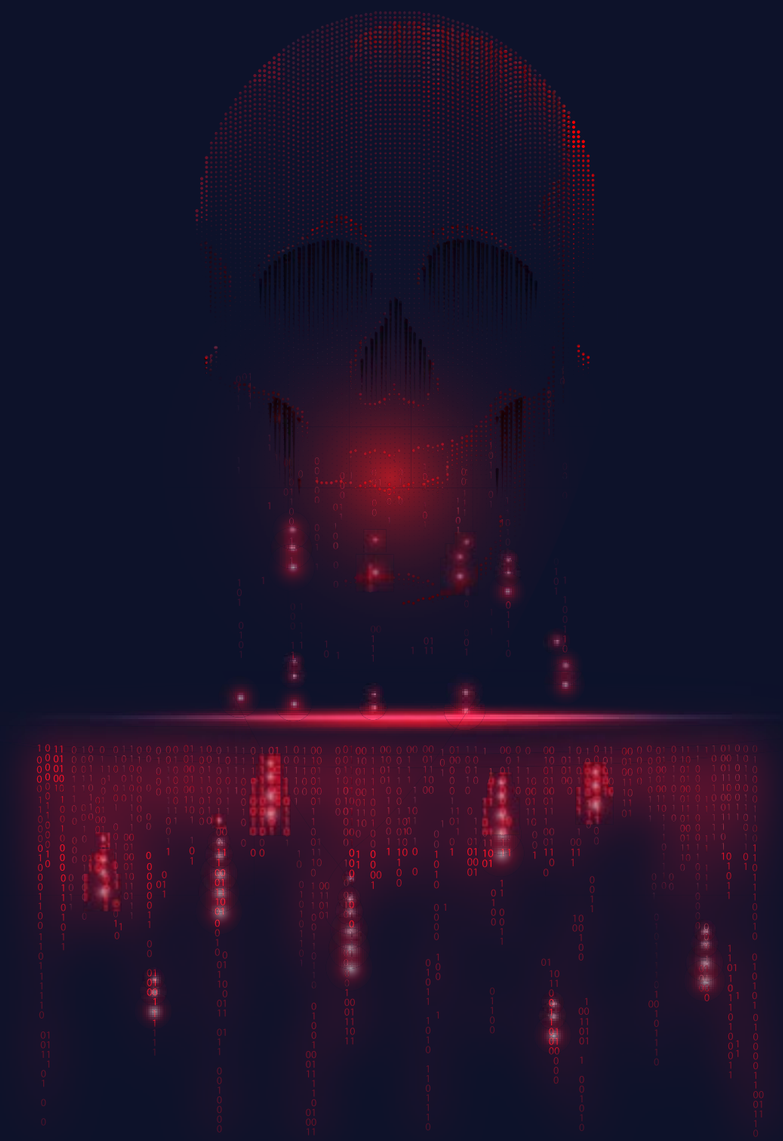
a file extension at the end of encrypted files. To avoid damaging computers to the point that they are inaccessible to users, Spora only encrypts the following types of files: **.xls, .doc, .xlsx, .docx, .rts, .odt, .pdf, .psd, .dwg, .cdr, .cd, .mdb, .lcd, .dbf, .sqlite, .accdb, .jpg, .jpe, .jpeg, .tiff, .zip, .rar, .7z and .backup**.

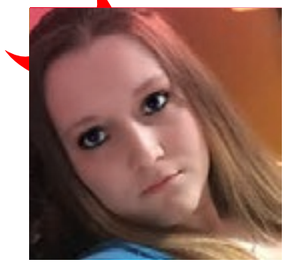
#8 WANNACRY

The latest and probably one of the worst digital disasters to happen in years, WannaCry (also known as WannaCrypt, WannaDecrypt, WCry and WanaCryptOr 2.0) emerged on 12 May, 2017, and has infected over 300,000 computers in 99 countries. The list of organizations affected by this attack includes well-known companies like Renault, LATAM Airlines, Deutsche Bahn, FedEx and UK's National Health Service, as well as government organizations and departments worldwide (e.g., the Ministry of Internal Affairs of the Russian Federation and the Ministry of Foreign Affairs in Romania).

WannaCry uses ETERNALBLUE exploit, a part of the NSA's cyber-arsenal published in April 2017 by the hacker group Shadow Brokers.

WannaCry takes advantage of the vulnerability in Microsoft's implementation of the Server Message Block file-sharing protocol to remotely target computers using unpatched or unsupported versions of Windows, and after that, it infects computers connected to the same network. After encrypting the files, WannaCry gives victims 3 days to pay the ransom of $300 in bitcoins; otherwise, the ransom amount will double, and after 7 days, all the data will be deleted.





Cassie Phillips
Dracula's Bride
Cybersecurity Writer, SecureThoughts.com

4 Steps You Should Take If You Have Been Hacked

A data breach can be a disastrous scenario for a small or medium-size business, and even the largest of corporations can be set back months or spend millions recovering from a hack. Minimizing risk and preventing network hacking from happening in the first place should be one of any company's top priorities, to keep employee and customer data safe and to protect the reputation of the organization.

Unfortunately, not all hacks are preventable, and even the best security systems can be overcome using tricks and methods that hackers haven't tried before. New methods of attacks are researched every day, and despite the best efforts of professionals, they simply might not be enough. Businesses will still get attacked, but there is a proper way to respond. Damage can be minimized in time, and a potential disaster can be turned into a speed bump on the road to business growth.

If your network gets hacked, here are the steps you should take immediately.

Step #1

Find the Source of the Problem and Fix It

Just because a data breach has occurred and a cybersecurity incident has been discovered, it doesn't mean the threat has passed or that your systems are now secure. As soon as humanly possible, your IT professionals (and perhaps a hired expert, depending on the staff working at your business) need to be able to track down the source of the problem. This is less to place blame in the event of human error (which likely was involved), and more to cut off the breach and prevent the exploit from being used again in the future.

Step #2

Perform a Cybersecurity Audit and Keep Inventory

After the immediate issue has been contained, it's

important that businesses take an inventory of their data and perform a "cybersecurity audit." This is a difficult term to precisely apply to all businesses, but your business may want to do the following, if applicable:

- **Review all data throughout the company** and keep track of where files are and where they've been, if possible. Check how services have been used and where the most sensitive information has traveled (and whether those movements have been within company policy). This might be hard to track, but the more information, the better.

- **Check to see if any files are missing.** While this is unlikely as hackers and cybercriminals are far more likely to simply copy files, it is worth noting signs of possible sabotage as well.

- **Determine if any files have been released to the public** or if there is a trail that can determine where the leaked files went. While you might not be able to remove or retrieve them, this will allow you to determine the potential motive and the likely impact of the attacks, allowing you to respond better both now and in the future.

These steps might vary wildly and you might need to add extra steps, but the main point to be made is that you need to investigate the problem extensively and take inventory of the data you have and where it's gone. This information will be invaluable in your efforts to contain the problem.

Step #3

Perform Damage Control

This is another step that is highly dependent on the type of cybersecurity incident that occurred and the type of business you are involved with. There are different problems that can arise when a data breach occurs, and here is how to get ahead of most of them:

- **Get ahead of the problem before it becomes public knowledge,** if your company is involved with the public or has investors. Under no circumstances should a data breach be swept under the rug, as it likely will be discovered, and trying to hide it will only make things much worse for your business. Explain that the problem has been discovered, that it is being managed and that all the necessary steps are being taken so that it will never happen again.

- **Change passwords and verification methods** immediately as both are a measure to reassure employees as well as strengthen security.

- **Take proactive measures** to protect those affected by a breach or identity theft as a means to mend and protect those relationships. Providing credit monitoring services is generally a good start.

- Set aside resources to handle further complications from the problem, perhaps even **set aside IT professional time to answer questions from employees and clients/customers.**

- **Document everything.** It is quite possible legal battles or issues could arise as a result of the data breach, and you will want to make sure everything is in order so that you can make a strong argument in your favor.

- **Get back to the day-to-day routine of the company.** Outside of the following emphasis on training, you will want to keep on-message with your brand, and you will still want to provide spectacular service to maintain your business's credibility. No one wants to see a company in panic.

Step #4

Retrain and Refocus

Once the dust has settled and your business has plans under way to deal with the problem and prevent it from happening again in the foreseeable future, it is a great time to review your cybersecurity protocols in general and to provide efficient training for employees within your organization. It will likely improve the morale of employees, who will feel more confident such a thing will not happen again, and given the threat, they will be more receptive to feedback and training on cybersecurity topics.

You may wish to refine or refocus the training depending on the exact nature of the data breach and the operations of your company, and your business should rely on its cybersecurity or IT professionals for these considerations.

As a leader and a professional, what steps would you add to those above to a data breach response plan? Have you ever experienced a breach, and if so, how did you handle it? Do you have any other thoughts on the subject? Please leave a comment below and tell us what you think.

About the Author

Cassie is a cybersecurity writer and blogger who regularly contributes to Secure Thoughts, a website that regularly runs pieces on cybersecurity for businesses and the average person alike. She hopes this information helps you and that you will be able to formulate an improved plan for protecting your business from cyber threats.

Free Tool of the Month

Password Expiration Notifier

Download Free Tool

Freeware tool that helps reduce the time spent on password management by automatically sending Active Directory password expiration notifications to users and their managers.

Report example

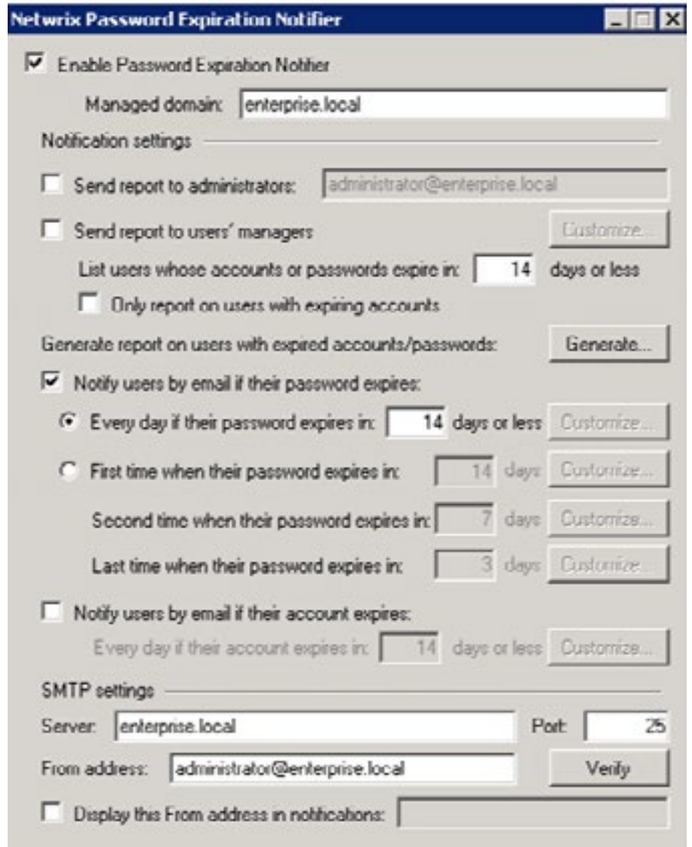
From: IT Helpdesk
To: John Brooks
Subject: Password Expiration Notification
Sent: Sat 4/10/2017 10:07 PM

Hi John,
Your password for account "JBrooks" expires in 14 day(s). Please change the password as soon as possible to prevent further logon problems.

Thank you!

Passwords and/or accounts of the following users are about to expire:

User Name	E-Mail	Expires in
Administrator	Administrator@enterprise.local	0 day(s): password never expires
BBrown	BBrown@enterprise.com	0 day(s): password
LBlack	LBlack@enterprise.com	3 day(s): password
CMorisson	CMorisson@enterprise.com	4 day(s): password
BCliff	BCliff@enterprise.com	4 day(s): password
JBurns	JBurns@enterprise.local	5 day(s): password
JSmith	JSmith@enterprise.local	5 day(s): password
ABons	ABons@enterprise.local	5 day(s): password
LFrinz	LFrinz@enterprise.local	7 day(s): password
GGordian	GGordian@enterprise.local	8 day(s): password
FSamuelson	FSamuelson@enterprise.local	8 day(s): password
TDulton	TDulton@enterprise.local	9 day(s): password
FFranko	FFranko@enterprise.local	12 day(s): password
GGilby	GGilby@enterprise.local	13 day(s): password
FDeiton	FDeiton@enterprise.local	14 day(s): password



How-to for IT Pro

How-to Stay on Top of Permissions Changes to Public Folders in Exchange Online

1. Open Exchange Administrative Console in Internet Explorer > Navigate to “Compliance management” > Choose “Auditing” > Choose “Run the admin audit log report…”

2. Choose a start date and end date Click “Search”. You will see all configuration changes made during the specified time period.

3. Sort the list by cmdlet and find “Add-PublicFolderPermission” Click on it for details.

4. You will see who changed permissions (“User”), which public folder permissions were changed and how (“Parameters”).

Report example

Date:
4/10/2017 4:39:41 AM

User:
J.Carter@enterprise.onmicrosoft.com

Object modified:
finance:\finance

Cmdlet:
Add-PublicFolderClientPermission

Parameters (Parameter:Value)
Members: Identity,AccessRights,User
Identity: \finance, AccessRights: None;ReadItems;CreateItems;
EditOwnedItems;DeleteOwnedItems;EditAllItems;DeleteAllItems;
CreateSubfolders;FolderVisible, User: T.Simpson

[Recorded Webinar]

Expert Explains:

Hacking Your Windows IT Environment

Watch Now

Netwrix Auditor 9.5

netwrix.com/auditor9.5html

Corporate Headquarters:
300 Spectrum Center Drive,
Suite 200 Irvine, CA 92618

Phone: 1-949-407-5125
Toll-free: 888-638-9749
EMEA: +44 (0) 203-318-02

Copyright © Netwrix Corporation. All rights reserved. Netwrix is trademark of Netwrix Corporation and/or one or more of its subsidiaries and may be registered in the U.S. Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are the property of their respective owners.