IT Pro™
WINDOWS®

THE ESSENTIAL GUIDE TO:

RANSOMWARE:

Detecting Threats and Protecting Your Data

By: Bill Kleyman,
Cloud, Virtualization and
Data Center Architect

SPONSORED BY
VEEAM

The security threat matrix for the modern IT environment is evolving. Why? There are more users, a lot more data and new technologies that are capable of carrying information over vast, widely-distributed ecosystems. In fact, a recent Cisco Service Provider report shows that global IP traffic has increased fivefold over the past five years, and will increase threefold over the next five years. By the end of 2016, annual global IP traffic will pass the zettabyte (1000 exabytes) threshold, and will reach 2 zettabytes per year by 2019.

All of this has created new targets for the proverbial bad guys. Although digital technologies have enhanced the way we conduct everyday business; these same technologies create new risks as they are deployed into the modern IT environment. The prognosis worsens when cutting-edge security technologies are deployed into an aging data and IT management model.

So, throughout this emerging threat matrix – we see new types of powerful advanced persistent threats (APTs).

Today, ransomware is one of the biggest cyber threats in 2016, according to McAfee Labs and Trend Micro. To avoid becoming a victim, you need to take action now to protect your computer systems. Waiting could cost you money, hassle, and negative publicity.

Today, ransomware is one of the biggest cyber threats in 2016. To avoid becoming a victim, you need to take action now to protect your computer systems. Waiting could cost you money, hassle, and negative publicity.

But before we dive in – let's ask one simple question: *What's your data worth?* According to Cisco, the current market around cybercrime actually ranges between $450B and 1T per year. Further estimates expect this number to increase. So how much is your data actually worth? Consider this:

- *Social Security Number:* $1
- *DDoS as a Service:* About $7/hour
- *Medical Records:* >$50
- *Credit Card Data:* $0.25 – $60
- *Bank Account Info:* >$1000 (Depending on the type of account and balance)
- *Mobile Malware:* $150
- *Malware Development:* $2500 (commercial malware)
- *Spam:* $50 for about 500k emails (depending on number of emails and destination)
- *Custom Exploits:* $100k – $300k
- *Facebook Account:* $1 for an account with at least 15 friends

These numbers give us a perspective of how much hackers can make off of your data. But what does it actually cost a business to experience a data breach or loss of vital information? New findings from Juniper Research suggests that the rapid digitization of consumers' lives and enterprise records will increase the cost of data breaches to $2.1 trillion globally by 2019, increasing to almost four times the estimated cost of breaches in 2015. Furthermore, the average cost of a data breach in 2020 will exceed $150 million, as more business infrastructure gets connected.

As you take all of this in – there is good news. Threats like ransomware can be dealt with; very efficiently in many cases. However, to fight ransomware – you need to understand what it is, where it came from, and the kinds of risks you face as an organization. In this **essential guide on ransomware** – you'll learn:

- The Ransomware Story: History, types of ransomware, future impacts
- Risks to the corporation and what every systems administrator should consider when securing their data.
- Precautions, best practices, and how to fight ransomware

Moving forward – your data will become even more valuable. And, as more information becomes distributed between data centers and cloud – the bad guys will be taking aim at weak systems and your critical data repositories.

The Ransomware Story: History, Types of Ransomware, and Future Impacts

A Brief History

Attacks seeking access to data or other valuable systems aren't anything new. What is new, however, is that data being held for ransom. The very first, recorded iteration of a ransomware virus was created by Harvard-trained Joseph L. Popp in 1989. Called the AIDS Trojan, some 20,000 infected diskettes were distributed to the World Health Organization's international AIDS conference attendees. The Trojan's main weapon was symmetric cryptography. However, it didn't take very long for decryption tools to recover the file names, but this effort set in motion over **almost three decades of ransomware attacks**.

Fast forward to the past 10-12 years. Between 2005 and 2006, we began to see ransomware attacks going after data points within other countries. These were created by Russian organized criminals, and aimed largely victims within the country of Russia, as well as neighboring countries like Belarus, Ukraine, and Kazakhstan.

In 2006, (before the term 'ransomware was even used) one of these ransomware variants - called *TROJ_CRYZIP.A* - was discovered. For the most part, it went after machines running Windows 98, ME, NT, 2000, XP, and Server 2003. Once downloaded and executed, it would identify files with a certain file-type, and move them to a password-protected ZIP folder, having deleted the originals. For the victim to recover their files, they would have to transfer a payment to an E-Gold (precursor to modern BitCoin) account.

In 2012, Trend Micro discovered a new type of ransomware variant: TROJ_RANSOM.AQB. Growing more dangerous and sophisticated, the method of infection was to replace the Master Boot Record (MBR) of Windows with its unique malicious code. When the computer booted up, the user would see a ransom message written in Russian, demanding payment. When paid, the victim would get a code, which would allow them to restore their computer to normal.

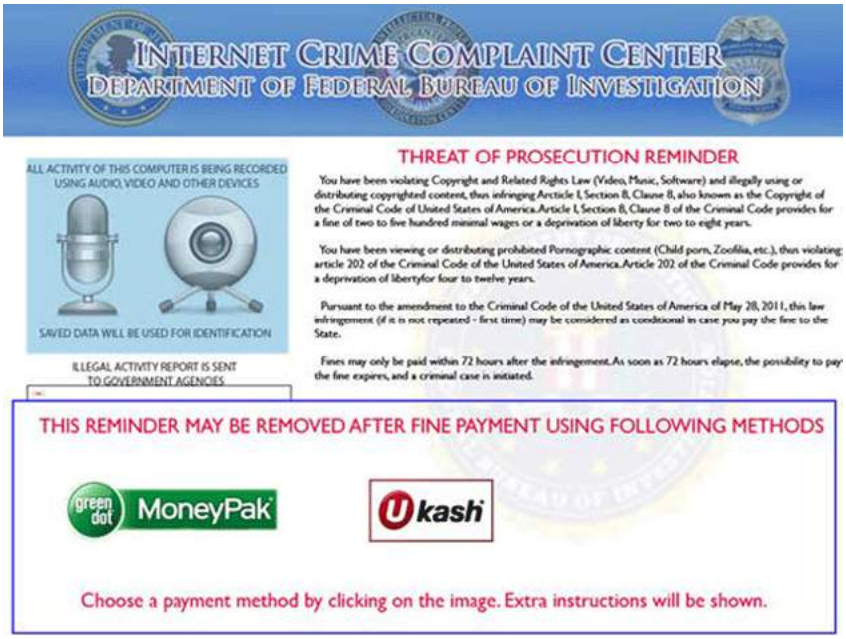
Now, there are even more ways to get ransom out of the victim or the victim organization. Attackers can use Vouchers, BitCoins, Paysafecard, MoneyPak, UKash, CashU, and MoneXy to demand payment. All of this makes it easier to collect and easier for the victim to pay. However, just like with any monetary crime – the more victims pay, the more attacks we will be seeing. *So, whatever you do – avoid paying that ransom; if you can.*

Moving into the end of the 2000s and into the start of the 2010 decade, ransomware grew even more sophisticated and began to be realized as a real-world international security threat.

Types of Ransomware Attacks

There are two basic types of ransomware in circulation. The most common type today is crypto ransomware, which aims to encrypt personal data and files. The other, known as locker ransomware, is designed to lock the computer, preventing victims from using it.

1. **Locker ransomware** (computer locker): Denies access to the computer or device.
    a. This type of ransomware would impersonate law enforcement in order to extract ransoms. They would accuse the victim of being involved with a crime — ranging from mere copyright infringement, to illicit pornography — and say that their computer is under investigation, and has been locked. For example, Reveton fraudulently claims to be from a legitimate law enforcement authority and prevents users from accessing their infected machine, demanding that a 'fine' must be paid to restore normal access. Although this type of ransomware can be more easily removed via common security methods – it would go to great lengths to disguise itself as legitimate to gain payment.



2. **Crypto ransomware** (data locker): Prevents access to files or data. Crypto ransomware doesn't necessarily have to use encryption to stop users from accessing their data, but the vast majority of it does.
    a. **CryptoLocker:** This was the first, big, crypto-ransomware to impact the industry. It uses a near-unbreakable encryption to lock down user's files, folder, and data repositories. Here's the scary part - even if the malware was removed, the data and files remain encrypted and locked. CryptoLocker relies on social engineering techniques to trick the would-be targets into running it. More specifically, the victim receives an email with a password-protected ZIP file purporting to be from a logistics company, for example. As soon as the victim runs it, the Trojan goes memory resident on the computer.

    The Trojan gets run when the user opens the attached ZIP file, by entering the **password included** in the message, and attempts to open the PDF it contains. CryptoLocker takes advantage of Windows' default behavior of hiding the extension from file names to disguise the real .EXE extension of the malicious file.

    Ultimately, this puts an immense pressure on the victim to pay. In fact, security researchers have uncovered that a group of cybercriminals or an individual involved in a widespread ransomware delivery operation has earned over $120m (189,813 Bitcoins) in just 6 months. The group still holds $94m in Bitcoin wallets, with the rest likely spent on amassing botnets, servers, other cyber tools and personal costs.

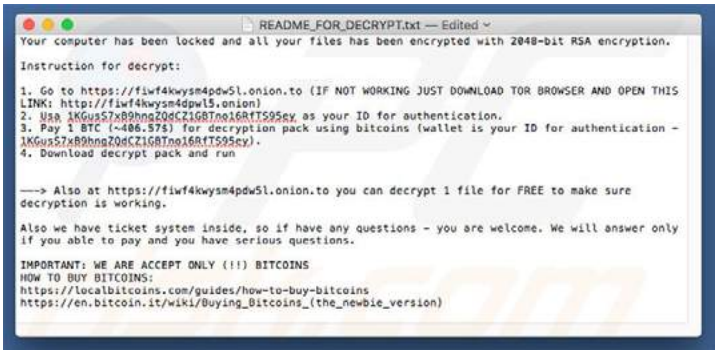
b. **CrypJoker:** A new form of ransomware called CrypJoker was discovered in January 2016. It uses the AES-256 algorithm to encrypt victims' files and then demands a ransom for their release. CrypJoker affects computers running Microsoft Windows operating systems. Although CrypJoker is not widely distributed at this time, security experts have started warning people about it. Besides using a strong encryption method, it targets 30 different types of files and deletes any shadow copies of them.

   The CrypJoker attack usually starts with a phishing email that tries to get the recipients to open a CrypJoker installer disguised as a PDF file. If the email recipients open that file, the installer downloads or generates the executables needed to carry out the attack. CrypJoker then scans the computer drives, looking for 30 different types of files, including PDF files, text files, Microsoft Word and Excel files, and image files (e.g., JPG, PNG). After encrypting those files, it appends ".crjoker" to their file extensions. For example, a file named "BusinessForecasts.docx" would become "BusinessForecasts.docx.crjoker".

Remember, these types of ransomware attacks may also perform other malicious acts, all intended to make victims pay up. For instance, it deletes any shadow copies made by Windows' Volume Shadow Copy Service so that the victims' files cannot be recovered. Or, it'll terminate several processes so that victims cannot run Windows Task Manager or the registry editor.

As a result, victims have only two options to get their files back: **recover them from a backup or give into the attackers' demands.** Even if the victims do pay the ransom, there is no guarantee the attackers will provide the decryption key and decoder needed to decrypt the files.

It doesn't stop there. Already there have been other variants. Onion, for example uses the Tor network to avoid detection. Others, like KeRanger, specifically target Mac users and their files. Detected in March 2016, it is believed to be the first fully functional ransomware seen on the OS X platform.



The Future of Ransomware

McAfee Labs security researchers noted in their quarterly report that ransomware attacks have grown over 128% "year over year". Additionally, researchers observed that ransomware attacks targeting hospitals have also spiked recently. Such is the propensity and profitability of ransomware that developers have even taken to showing off the functions and abilities of codes on underground forums.

You're going to see even more ransomware attacks in the very near future. The darkest corners of the web are showing us that ransomware is a selling tool which can now we "white-labeled" and even rebranded by a would-be attacker. Basically, a malicious entity can buy ransomware, customize it slightly, make it their own, and go after a target.

You're going to see even more ransomware attacks in the very near future. The darkest corners of the web are showing us that ransomware is a selling tool which can now we "white-labeled" and even rebranded by a would-be attacker. Basically, a malicious entity can buy ransomware, customize it slightly, make it their own, and go after a target.

There is certainly a surging tide of ransomware attacks – it's critical to be ready for this and protect your data.

Risks to the corporation and what every systems administrator should consider when securing their data.

February 5, 2016, started out like any other day for the doctors, nurses, and other staff members at the Hollywood Presbyterian Medical Center in Los Angeles, California. But by the end of the day, many of them could no longer access or update patients' medical records. Nor could they send or receive emails. When the hospital's IT department investigated, it found that the computer systems were infected with ransomware.

The ransomware had encrypted the hospital's files, paralyzing its computer systems. The hackers de-

manded 40 bitcoins (about $17,000) to get the decryption key. *The hospital paid the ransom*. "The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key," explained president and CEO Allen Stefanek in a statement released by the hospital. After the hospital regained control of its computer systems on February 15, the IT staff, with the help of outside computer experts, removed the malware.

The Hollywood Presbyterian Medical Center is not the only hospital to come under attack. Two hospitals in Germany also reported being ransomware victims. The Lukas Hospital in Neuss was attacked on February 10, 2016. Two days later, Klinikum Arnsberg was targeted. Although the ransomware had encrypted some files at each hospital, neither one paid the ransom.

While the Hollywood Presbyterian Medical Center, Lukas Hospital, and Klinikum Arnsberg reported their attacks, most organizations attempt to hide them, according to Bob Shaker, director of strategic operations for Symantec's Cyber Readiness and Response group. He knows about hundreds of ransomware attacks in a variety of industries that have been kept secret.

Shaker and other security experts fear that the successful attack on the Hollywood Presbyterian Medical Center will encourage more organizations to pay the ransom if infected by ransomware.

NOTE: Remember, paying off the attackers isn't always the right answer. If more organizations systematically pay, ***this, in turn, will lead to hackers launching even more attacks.*** If you're in such a position – remember to always contact your federal and/or local authorities so they can document the attack and, in some circumstances, provide detailed courses of action.

What Every Systems Administrator Should Know

First of all – know that your data is extremely valuable. And, it's important to remember that the bad guys are continuously trying to find ways to get into your systems. As a systems administrator, there are several key factors to be aware of to secure your environment against a ransomware attack:

1. *Where is your data? Is it secure?* With so much more data being stored, administrators might actually lose a repository or file archive. Run deep analysis around your ecosystem. Know where all of your data points reside and which servers or systems support the data. Lock down all points of entry and ensure that your network is secure as well.

2. *When was your last backup – did you test it?* Yes, you have a back-up solution. And, yes – you didn't get any errors on your last backup run. But when was the last time you tested it? When was the last time you recovered a file, or an entire directory? What about database systems and email servers? Testing is an integral part of securing your data and keeping it safe.

3. *Are your end-points secure and segmented?* With the influx of BYOD and remote users – how are you securing data which is onsite or located remotely on user's computers? Most of all – how are you backing this up and ensuring the backups are safe? It's so critical to utilize technologies which help segment user files from corporate files – especially when working with BYOD initiatives. Furthermore, controlling the information once it hits the server is critical as well.

4. *How well are you protecting your network?* Your network is the lifeblood of data and information flow. Proper segmentation is critical to mitigate risk and ensure proper data security.

5. *How are you controlling access?* ACLs are a great way to control access into key systems. Furthermore, you can lock down who has access into data that has already been backed up. This ensures clean data copies and allows you recover if there is an incident.

Finally, systems administrators must have clear dialogues with their users. Remember, ransomware uses social engineering and very dangerous techniques to fool the user into downloading malicious content. Too often, it's the error of the user or a simply flaw in data control which leads to a major ransomware incident.

Precautions, best practices, and fighting ransomware

"Take action now, or pay later." Given these attack vectors, one way to help prevent ransomware is to use anti-malware software and utilizing good data protection methodologies. It can help guard against known ransomware ploys and other kinds of malware threats.

Taking advantage of the popup blocker functionality in web browsers is another way to help guard against ransomware. Popups sometimes contain malware or lead to malicious websites.

In addition, you need to educate employees about the importance of avoiding any websites marked as potential security threats by their web browsers or anti-malware software.

You also need to educate employees about how to spot phishing or spear phishing emails. Let them know what they should and should not do:

- They should not open any email attachments that are not expected. If the email is from someone they know, have them check with that person first before opening the attachment.
- They should not click any links embedded in emails sent from unknown sources. Even if they know the person who sent the email, have them check the link (hover their cursor over the link to see the address of the website) before clicking it.

To help prevent a ransomware attack, you can take several measures:

- Do not open any email attachments that you are not expecting. If the email is from someone you know, check with that person first before opening the attachment.
- Do not click any links embedded in emails sent from unknown sources. Even if you know the person who sent the email, check the link before clicking it. Hover your cursor over the link to see the address of the website that you will be taken to. If the website address seems suspicious, perform an online search to see if it is associated with any cybercrimes.
- Use anti-malware software.
- **Back up your files regularly.** Although this will not prevent a ransomware attack, it can mitigate the effects of one.

Employing the 3-2-1 Backup Rule to Fight Ransomware

Let's assume that you walk into your office, early on a Monday, to find some of your critical data folders locked down, and encrypted with a ransomware attack.

At this point there are two outcomes to the administrator:

- You begin to sweat and prepare yourself for the impending headaches.
- You begin the recovery process, go make yourself a cup of coffee, file a report, and get on with the day. You remain calm and confident that your users, given that you did everything right, might not even know anything was out of place.

Of course, everyone would want the latter outcome. And, the reality is that you can protect yourself against ransomware and intelligently secure your most critical data points.

The 3-2-1 Backup Rule:

- You must have at least **three** copies of your corporate data.
- Those copies must be stored on at least **two** different types of media.
- At least **one** must remain offsite.

In working with backup solutions and even data security – the 3-2-1 rule will effectively secure your data from any kind of ransomware attack. You can leverage powerful replication methodologies to store your data remotely and very efficiently. In creating and specifying your SLAs, you can create your own recovery objectives to ensure your data is available when you need it.

Most of all – an effective backup plan *will* allow you to recover user data, server data, information within a storage environment, and much more. You're basically creating a backup solution that will work across any user workload; and one that will be able to rollback quickly (across a number of backup iterations) to restore data in the event of an attack.

Securing Your Environment

There are powerful ways to protect your existing ecosystem from being a victim of a ransomware attack. A lot of it starts with some very basic infrastructure and security best practices. Consider the following:

- Attacks often come in the form of attachments or even modified files being sent it. Make sure you have good policies around productivity applications. For example, disabling macros so that advanced code can't be executed on a host machine. Also, new types of end-point protection as well as end-point protection and response technologies can spot anomalies and changes in file headers which look strange. These types of precautions and tools can help stop ransomware from getting in.
- Ensure that ALL of your systems are up to date; and test out your updates! Patching, updates, security updates, password control, and even firmware upgrades are all critical in keeping your environment safe. From there – ensure your systems have proper segmentation as needed. This can be done at the network, storage, and even compute layer. All of this helps limit and even mitigate the impacts of a potential ransomware attacak.
- Remember, it's not enough to have the best software and hardware available to fight ransomware. You absolutely have to educate the end-user. Security education and user interaction best practices must

be taught not just once – but throughout an associate's employment at the organization. Teaching them security once won't cut it. Technology evolves, business change, and threats get more advanced. An educated user may very well think twice before clicking on something or downloading a file when they know (and clearly understand) the dangers of ransomware.

Final Thoughts and Conclusion

Ransomware is one of the biggest cyber threats in 2016, according to McAfee Labs and Trend Micro. And, this threat, seemingly, isn't going anywhere. Remember, the value of your data will only continue to increase. And, there will be more targets and more bad guys trying to get to your users and your data. You simply can't afford a breach in today's IT-dependent business model. Most of all – a ransomware incident could cost you the loss of your critical, and sensitive data points. With that in mind - *Take Action Now, So You DON'T Have To Pay Later.*


VEEAM
AVAILABILITY
for the Always-On Enterprise™
ANNOUNCING
NEW Veeam Availability Suite 9.5
Availability for the Always-On-Enterprise
go.veeam.com/v9-5