RANSOMWARE: ALL LOCKED UP AND NO PLACE TO GO

KASPERSKY lab

What is ransomware?

Ransomware is a type of malware that attempts to extort money from a computer user by infecting or taking control of a victim's machine or the files or documents stored on it. Typically, the ransomware will either lock the computer to prevent normal usage or encrypt the documents and files to prevent access to the saved data.

- Prevents you from accessing Windows and other devices.
- Encrypts files so you can't use them.
- Stops certain apps from running.

48.3% The number of users attacked by encryption ransomware increased by 48.3% in 2015.[1]

WHY DOES RANSOMWARE WORK SO WELL?

Ransomware is the digital version of extortion. It's as simple as that. It uses age-old tactics to carry out a modern day crime, but the elements behind it are as old as human criminal activity itself.

It all starts by playing on the basic human emotions of fear and embarrassment.

A person gets an ominous message that they have somehow violated internet protocol by visiting inappropriate or illegal sites and must pay a fine. Their files are encrypted and if they don't pay up, they will lose their files. Sometimes, they are even threatened with having the files published on the internet. It sounds real. It looks real. And contacting law enforcement or security teams could be embarrassing or worse. So, they pay up.

Or an employee receives an email from a trusted friend or work colleague. They are told to download the attached invoice, not knowing that the friend's email has been hacked and the attachment is an executable file that has been designed to lock up the whole system. Contacting the IT department before opening an email is unlikely, so employees are often easily tricked into this scenario.

THE MOTIVE

As with any crime, it's natural to want to know the motive behind these attacks. In the case of ransomware, it's about money. Sometimes cybercriminals have complex motives for their actions—whether it is to embarrass an individual or organization or attack them for political reasons. But with ransomware, it is simply a very lucrative way for cybercriminals to make money.

Victims paid a total of over $24 million in some 2,453 reported ransomware attacks.

In 2015, victims paid a total of over $24 million in some 2,453 reported ransomware attacks, according to a report from the FBI Internet Crime Complaint Center.[2] CryptoLocker, one type of ransomware that has infected tens of thousands of machines, rakes in $30 million every 100 days, according to a Dell SecureWorks report. According to a survey conducted by Interdisciplinary Research Centre in Cyber Security at the University of Kent, more than 40% of CryptoLocker victims agreed to pay.[3] It's no wonder, then, that cybercriminals see ransomware as a business opportunity and look to exploit it.

PAYMENTS

The average payment for ransomware is around $300, as of 2015, whereas for businesses, it seems to be around $10,000.[4] The goal with most ransomware attacks is to make the number low enough that replacing the computer would be more costly. With businesses, it is a constant test to see what the market will bear. Most ransomware payments are demanded in bitcoin, which is a currency that is harder to trace.

Clearly, ransomware has all the elements of a perfect digital crime. It has a low cost of entry. It's successful. It's hard to trace. And it won't be going away anytime soon.

[1] The Kaspersky Lab Security Bulletin Overall Statistics Report for 2015
[2] Ransomware: Putting Companies Between a Rock and a Hard Place
[3] The ransomware epidemic: why you should be more concerned
[4] The ICIT Ransomware Report

753,684 Ransomware was detected on 753,684 computers in 2015[5]

HOW DOES RANSOMWARE WORK?

Ransomware is a unique kind of cybercrime. Unlike hackers who attempt to steal data, ransomware criminals only attempt to **prevent access to data**. Because of this, businesses come to a grinding halt when hit by ransomware—and they don't easily forget the experience. They may not have to pay a massive sum of money, but the residual costs, the reputational damage, the harm to their brand and the aggravation all serve to leave a lasting mark on the collective memory of any company hit by ransomware.

When ransomware hits, it usually walks through a number of typical steps.

1. Installs when the user opens a file, usually via email, IM, social network or by visiting a malicious site.
2. Generates a pop-up window, web page or email warning from what looks like an official authority.
3. Encrypts the user's files with an AES-256, a randomly generated one-time key.
4. Creates an individual encryption key for each file.

The first instinct many victims have is to try to unlock the data by decoding the encryption key. This is a losing battle. In 2008, Kaspersky Lab researchers actually cracked a 660-bit RSA key used by the GPCode Trojan. But soon its authors upgraded the key to 1,024-bits, making it practically impossible to decrypt.

Just how hard is it to break through? By looking closely at the math, security experts determined that it would take approximately 7×10^{40} times longer than the age of the universe to exhaust half of the keyspace of a AES-256 key.[6] In short, don't bother.

[5] The Kaspersky Lab Security Bulletin Overall Statistics Report for 2015
[6] Time and energy required to brute-force a AES-256 encryption key

10 new families of ransomware emerged in 2015, according to Kaspersky Lab findings.

TYPES OF RANSOMWARE

People are often confused by the different types of ransomware and how they work. There are really only three categories of ransomware, though different variants under each of these categories appear as cybercriminals look to become more efficient.

Encryption or Crypto-Ransomware

- Encrypts personal files, such as documents, spreadsheets, pictures, videos.
- The victim can use the computer to do anything except access the encrypted files.
- Files are deleted once they are encrypted and generally there is a text file in the same folder as the now-inaccessible files with instructions for payment.
- Crypto-ransomware often includes a time limit, after which the decryption key may or may not be permanently deleted if the victim does not pay the ransom on time.
- A lock screen may appear, but not all variants show one.

Lockscreen Ransomware

- Locks the screen and demands payment.
- Presents a full screen image that blocks all other windows.
- This type is called WinLocker ransomware.
- No personal files are encrypted.

Master Boot Record Ransomware (MBR)

- The Master Boot Record (MBR) is a section of the computer's hard drive that allows the operating system to boot up.
- MBR ransomware changes the computer's MBR so the normal boot process is interrupted.
- A ransom demand is displayed on screen instead.

Because people do not think well under time limits, the deadline element of crypto-ransomware makes it a popular choice among cybercriminals. Lockscreen ransomware is still developed but is less popular, though some security experts feel that it could experience a resurgence with the emergence of the Internet of Things (IoT). How much would you pay to unlock your refrigerator, your wearable personal devices or even your house?

50,000 In 2015, Kaspersky Lab detected crypto-lockers on more than 50,000 corporate computers.

BLASTING THE MYTHS ABOUT BUSINESSES AND RANSOMWARE.

There are a lot of misconceptions about ransomware and how it affects businesses. Many corporate leaders don't understand the scale of the problem and how quickly new capabilities are evolving even on a weekly basis.

Myth #1

Businesses are less of a target than individuals.

How big a threat is ransomware for businesses? Very big, and it's only going to increase. The small payments made by individuals pale in comparison to what cybercriminals can get out of large businesses who simply cannot operate without getting their systems back up and running. As we noted earlier, the ransom market price for businesses is many thousands of dollars, while it is only in the hundreds of dollars for individuals. Cybercriminals know this and recognize a big business opportunity from bigger ransom payouts.

Myth #2

Small- and medium-sized businesses are less of a target than large enterprises.

Cybercriminals do not care if you are a large or small business. They are simply looking to impact as many users as possible to reap the largest financial gain. In that respect, ransomware is a volume business. Some businesses will pay. Some will not pay. Cybercriminals don't care. With a wide enough net, they can generate a lot of cash.

At Kaspersky Lab, our analysts expect to see a shift from the "spray and prey" type of attacks that focus on high-volume in hopes of hitting a few targets successfully to more targeted attacks that specifically go after an organization for the type of sensitive data that they can steal and sell. If you think this kind of targeted ransomware attack is only limited to large enterprises, think again. More and more cybercriminals are looking for two-for-one attacks where they can hack into a smaller business to get at the larger enterprise for which they are a vendor. The long and short of it is this: **Every size business can be a target, and no business is immune.**

Myth #3

It's not that big a threat.

Only 37% of companies consider ransomware a serious danger.[7] This means that most companies have their guard down, and cybercriminals know it. Crime of any kind thrives on complacency, and ransomware is no different. With the knowledge throughout your organization that this can happen, your entire organization should be on alert and aware of the growing threat of ransomware.

[7] The ransomware epidemic: why you should be more concerned

20% of encryption ransomware was found in the corporate sector in 2015, according to Kaspersky Lab data.

TO PAY OR NOT TO PAY?

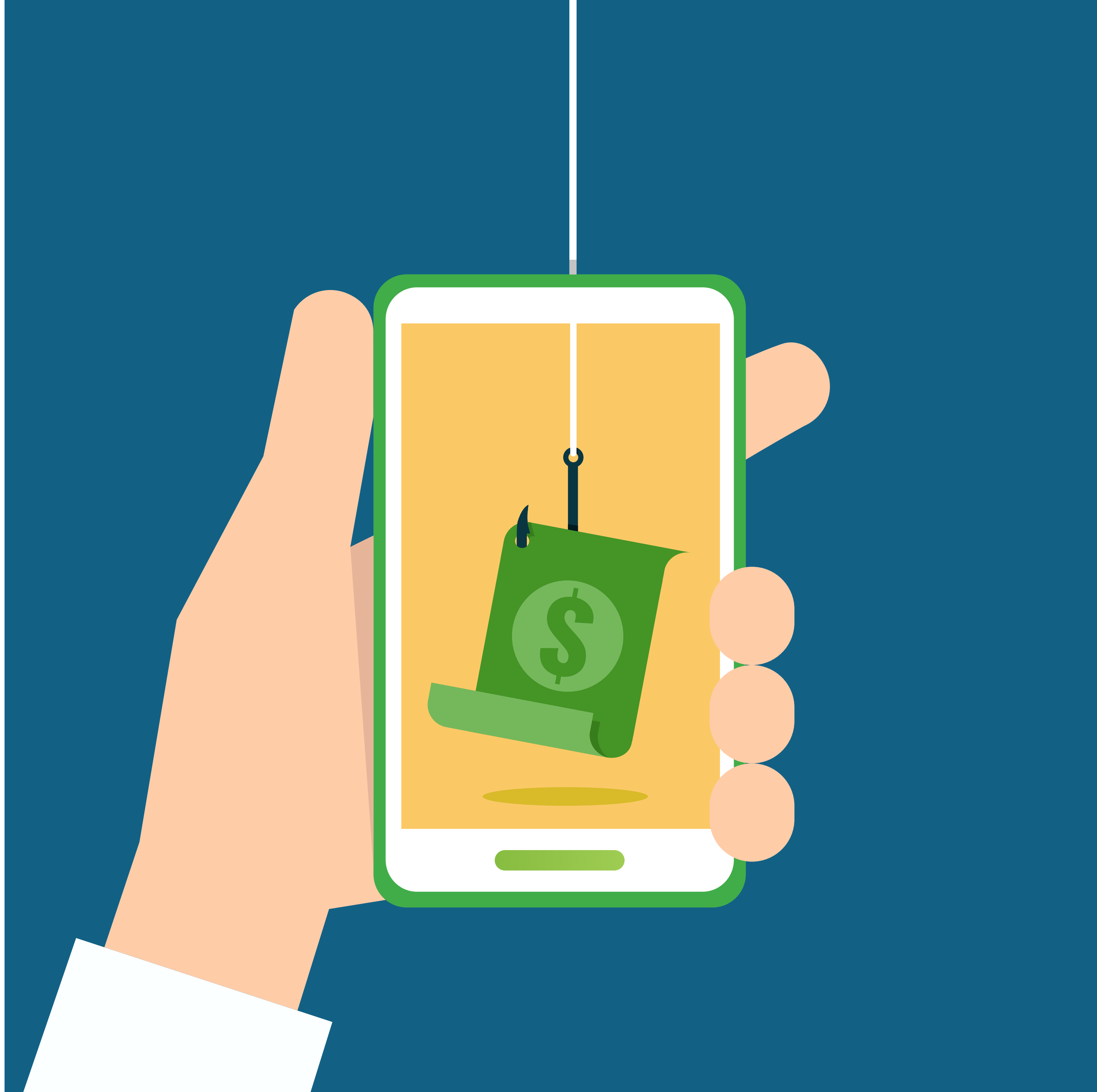
That is the question. Paying the ransom is a bad practice for several reasons:

1. **There is no guarantee that you'll get the decryption key.** There are many cases where the cybercriminals do not actually have access to the key that decrypts the data. Ransomware is now readily available on the black market, so many take leaked sources of ransomware, modify the payment information and launch it through their own distribution channels. They never had the key in the first place, but it should come as no surprise to you that criminals sometimes lie.

2. **The ransomware is not your only problem.** If paying the ransom is your only option, then it's a pretty good indication that you didn't have a good disaster recovery plan in place. And if you don't have a good disaster recovery plan in place, then you certainly won't be able to properly remediate from the attack and fully clean your infrastructure from infection. This means more potential data lock-ups, costly breaches and other cyber disasters. Getting the decryption key will not solve all of your problems.

3. **Break the cycle.** If you pay the ransom, you will be perpetuating a vicious cycle. The ransom will be reinvested by cybercriminals in producing other ransomware tools that will become an even bigger problem in the future for your organization and for others. If there's no profit to be made, cybercriminals will not put more money into developing ransomware.

Prevention is truly worth a pound of ransomware cure. Prepare your company for the inevitability of cyberattacks—ransomware or otherwise—and you won't have to face the difficult decision about whether or not to take money out of your budget to recover from an attack.



WHAT DO WE RECOMMEND?

Now that we've told you what not to do, let's take a look at what you should do to prevent ransomware and mitigate the effects of an attack.

Here are **10 simple tips** to protect your data from ransomware.

1. **Back up your files regularly.** The only way to ensure that you can immediately handle a ransomware attack is to implement a regular backup schedule so that your company can get access to the files it needs without dealing with the cybercriminals. Your backup should have certain restrictions, such as read/write permissions without an opportunity to modify or delete the files.

2. **Check your backups.** There are times when something can damage your files. Be sure to check regularly that your backups are in good shape.

3. **Protect against phishing attacks.** Cybercriminals often distribute fake email messages that look like an official message from a vendor or bank, luring a user to click on a malicious link and download malware. Teach employees that they must never open attachments from an unknown sender or even suspicious attachments from a friend in case they have been hacked.

4. **Trust no one.** Or rather, trust but verify. Malicious links can be sent by your friends or your colleagues whose accounts have been hacked. Let employees know that if they receive something out of the ordinary from a friend, they should call that person directly to verify that they sent it and find out if their accounts have been compromised.

5. **Enable 'Show file extensions' option in the Windows settings.** This will make it much easier to distinguish potentially malicious files. Because Trojans are programs, employees should be warned to stay away from file extensions like "exe", "vbs" and "scr." Scammers could use several extensions to masquerade a malicious file as a video, photo, or a document.

6. **Regularly update your operating system.** Cybercriminals tend to exploit vulnerabilities in software to compromise systems. With Kaspersky Lab's automated Vulnerability Assessment and Patch Management tools, you can rest assured that your system will be scanned and that patches will be distributed regularly in order to keep your system updated.

7. **Use a robust antivirus program to protect your system from ransomware.** Our Kaspersky Lab products employ a multi-layered system of defense that checks malware from many different angles to ensure that it does not corrupt your system.

But if ransomware hits…

8. **Cut off your internet connection immediately.** If you discover ransomware, shut off your internet connection right away. If the ransomware did not manage to erase the encryption key from the computers in question, then there is still a chance you can restore your files.

9. **Don't pay the ransom.** If your files become encrypted, we do not recommend paying the ransom unless instant access to some of your files is critical. Each payment made helps the criminals to prosper and thrive to go on to build new strains of ransomware.

10. **Try to identify the malware.** If you are hit by ransomware, try to find out the name of the malware. Older versions of ransomware used to be less advanced, so if it is an earlier version, you may be able to restore the files. Moreover, cybersecurity experts, including Kaspersky Lab experts, collaborate with law enforcement to provide file restoration tools online and, hopefully, detain the adversaries. Some victims are able to decrypt the files without having to pay the ransom. To check whether that's possible, visit kaspersky.com

HOW DO KASPERSKY LAB'S PRODUCTS PROTECT AGAINST RANSOMWARE?

While there are many things you and your users can do to prevent ransomware from infiltrating your organization, implementing a multi-layered security solution is still the best defense against these sorts of attacks. Kaspersky Lab's products secure your organization through layer after layer of countermeasures that ensure that you are protected.

Our technology uses a range of sophisticated behavioral technologies to discern suspicious patterns, block malicious activities and roll back any harmful actions, including malicious file encryption.

WORKSTATION PROTECTION

Vulnerability Assessment And Patch Management

Vulnerabilities within any of the applications and operating systems running on your devices can provide entry points for ransomware. Our automated Vulnerability Assessment and Patch Management tools scan your systems, identify known vulnerabilities and help you to prioritize and distribute the necessary patches and updates so that known security vulnerabilities can be eliminated.

Anti-Phishing

Because phishing emails are usually the starting point for many ransomware attacks, Kaspersky Lab's anti-phishing technology uses a multi-layered approach to protect against infiltration. First, it checks sites with the product's local anti-phishing databases on the user's device. Next, it checks URLs of sites against Kaspersky's own vast, continually updated database of phishing sites, which are collected through Kaspersky Security Network. When a new malicious URL is detected on the computer, information about this threat is made available from the cloud database within 15-30 seconds of detection. Finally, our heuristic analysis is an intelligence system that looks at dozens of phishing symptoms and compares it with other indications, classifying them based on known modern phishers' methods and the vast Kaspersky Lab database of already detected phishing sites.

Heuristics

Heuristic analysis provides proactive protection from threats that can't be detected using signature databases. Kaspersky Lab's heuristics enable the detection of new malware or unknown modifications to known malware. Static analysis scans code for signs of suspicious patterns associated with malware, while dynamic analysis examines the machine code the file might try to execute.

Default Deny

Increasingly viewed as the most effective security posture to adopt in the face of ever-evolving, advanced threats, Default Deny simply blocks all applications from running on any workstation unless they have been explicitly allowed by the administrator. Since most malware is delivered as an executable file that cannot be found on any whitelist, organizations that adopt this approach can thus prevent any malicious file from executing without really needing to know what those files actually are. Default Deny means all new, file-based malware varieties are automatically blocked, even for targeted attacks.

System Watcher

System Watcher monitors applications and processes activity to discern behavioral patterns, relying on behavioral stream signatures that look at sequencies of actions, rather than just one isolated action. Malicious actions and destructive behavior patterns suggestive of malware are blocked.

Automatic Exploit Prevention (AEP)

As part of System Watcher, this technology specifically targets malware that exploits software vulnerabilities. AEP acts like a safety net, an extra layer of security that complements Kaspersky Lab's other technologies.

Rollback

Our crypto-malware countermeasure subsystem negates the consequences of crypto-attacks by making local, protected backup copies of user data files as soon as they are affected by a suspicious program, returning user data to its original preserved state.

SERVER PROTECTION

Application Launch Control

Application Launch Control prevents unapproved applications from launching and spreading malware right from startup.

Anti-Malware With Kaspersky Security Network Integration

Our anti-malware protection draws on our global network of sensors to anticipate the latest threats, giving our technology a worldwide perspective on evolving threats. This intelligence is then applied to our technology in order to protect your infrastructure before the attack ever reaches your server.

Anti-Cryptor

Our Anti-Cryptor technology monitors the server for signs of corruption, cuts the infected workstation's access to the server for 30 minutes, and alerts administrator to the infection.

TRY KASPERSKY LAB

Discover how Kaspersky Lab's premium security can protect your business from malware and cybercrime with a no-obligation trial. Register today to download full product versions and evaluate how successfully they protect your IT infrastructure, endpoints and confidential business data.

GET YOUR FREE TRIAL TODAY >

JOIN THE CONVERSATION

Watch us on YouTube

Like us on Facebook

Review our blog

Follow us on Twitter

Join us on LinkedIn

Learn more at usa.kaspersky.com/business-security

ABOUT KASPERSKY LAB

Kaspersky Lab is one of the world's fastest-growing cybersecurity companies and the largest that is privately-owned. The company is ranked among the world's top four vendors of security solutions for endpoint users (IDC, 2014). Since 1997, Kaspersky Lab has been an innovator in cybersecurity and provides effective digital security solutions and threat intelligence for large enterprises, SMBs and consumers. Kaspersky Lab is an international company, operating in almost 200 countries and territories across the globe, providing protection for over 400 million users worldwide. Learn more at usa.kaspersky.com.

Contact Kaspersky Lab today to learn more
about Kaspersky Endpoint Security for Business
and our other IT security solutions and services:
usa.kaspersky.com/business-security
(866) 563-3099
corporatesales@kaspersky.com

KASPERSKY lab
THE POWER
OF PROTECTION