COULD YOUR BUSINESS SURVIVE A CRYPTOR?

Learn how to guard against crypto-ransomware

usa.kaspersky.com/business-security

WHAT IS RANSOMWARE?

The days of simple malware developed by mischief-seeking amateurs are long gone. Organized crime lies behind much of today's malware. And the focus is on making money.

As its name suggests, ransomware is a specific type of malware that tries to extract a ransom payment in exchange for unblocking access to an asset that belongs to the victim.

In the case of crypto-ransomware–or cryptors–the 'kidnapped' assets are the files and data that are stored on the infected device. The cryptor encrypts the victim's data into an unreadable form, and the data can only be decrypted by using the necessary decryption key. But that key is only released by the criminal after the victim has paid the ransom demand.

A cryptor will often display a dialogue box that states the encryption has been carried out as a result of an illegal act by the victim. Often the message will claim to be from the police or FBI.

CRYPTOR ATTACKS: DOING DAMAGE TO BOTH CONSUMERS AND BUSINESSES

Whereas consumers are typically faced with average ransom demands of $300, cybercriminals demand much higher ransom charges for businesses where data is a highly valuable commodity.

If one of your devices is infected, the attacker will normally give you 48 to 72 hours to pay the ransom. If you don't pay within the deadline, the price for decryption is likely to increase. After a second deadline passes and the payment is still not made, it's likely that the decryption key will be deleted. At that point it may be impossible to recover your files in a readable form.

Even if you do pay the ransom, there's no guarantee your data will be unencrypted. Some cryptors contain software bugs that may cause them to malfunction–so the decryption process fails. In other cases, the ransomware variant simply does not have decryption functionality. Instead, the criminals simply intend to take the victims' money.

42% of SMB representatives say they consider cryptomalware to be one of the most serious threats that their organization could face.[1]

> "A modern cryptor will often perform a number of additional actions that prevent the recovery of encrypted data–including deleting or encrypting Shadow Copies used for storing System Restore Points and regular Windows backups."
>
> – **Andrey Pozhogin**, Cybersecurity Expert, Kaspersky Lab

KASPERSKY LAB SOLUTION

System Watcher, our crypto-malware countermeasure subsystem that negates the consequences of crypto-attacks by making local, protected backup copies of user data files as soon as they are opened by a suspicious program

[1] Corporate IT Security Risks Special Report Series 2016, The Cost of Cryptomalware: SMBS at Gunpoint

HIGH COSTS FOR BUSINESSES: WHY THE RANSOM PAYMENT IS JUST THE BEGINNING

Despite criminals often demanding bigger payments from business victims, the ransom may only represent a small portion of the overall costs to the business. The inconvenience of the attack can result in much larger financial losses.

Imagine losing access to all of your sales records, customer files, accounting data, product information and design data. How would your business cope? And if it could cope, how much revenue would you lose while your team is trying to get everything back on track?

In today's 'information age', any temporary loss of data can totally disrupt business-critical processes, leading to:

- Lost sales
- Reduced productivity
- Significant costs for system recovery

However, the permanent loss of data can have much more severe consequences:

- Permanently damaging the company's competitive position
- Reducing sales revenues over the long term
- Preventing ongoing access to intellectual property and design data

This can put the entire business in jeopardy.

TOP TIP

If your business is attacked, beware of false remedies promoted on the internet. These may only add to your problems.

1. Often, they don't work and just take more money from the victim.
2. Some "remedies" can even download additional malware onto the victim's network.

THERE ARE MORE CRYPTOR ATTACKS THAN EVER BEFORE

Here are just a few examples of recent cryptors:

CryptoLocker is spread via infected email attachments. It encrypts files and then locks them with a randomly generated one-time key. In order to unlock your files, you need to pay the cybercriminals in bitcoin by a stated deadline. It is estimated that CryptoLocker rakes in $30 million every 100 days, according to a Dell SecureWorks report.

Locky is spread primarily via spam with attachments enticing users to enable macros in Word documents that download the malware onto machines.

Cerber is crypto-ransomware that includes a feature where the infected machine will speak to the victim.

CryptXXX has tainted thousands of sites built on both Joomla! and WordPress content management systems

Only 37% of companies consider ransomware a serious danger.[2]

Obviously, this attitude is a security weakness that can be exploited by cybercriminals.

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

HOW A CRYPTOR ATTACKS

Drive-by downloads happen when someone visits a web site that has already been infected with malware. Often, the site is a legitimate site that is popular with a specific type of job role and can be easily targeted by cybercriminals. They will design and use exploit kits to identify software vulnerabilities in the user's PC. The exploit kit then communicates with the PC and loads malicious code onto their computer. Often, this happens without the person ever knowing that they have visited a compromised site and uploaded malicious software.

Emails with malicious attachments are a common way for cybercriminals to infiltrate any organization. A person receives an email that looks innocent enough--a tax notice, a contract or an invoice. When they open the attachment to investigate further, they unwittingly hit the start button on malicious code. The victim can still use the computer, but they cannot access the encrypted files.

In general, cryptomalware operates by preventing access to files instead of stealing them. In order to get access back, victims are instructed to pay up in bitcoin before a specified deadline. If the victim does not comply, files might be permanently deleted. It's an insidious demand that victimizes many companies before they can protect themselves.

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

TO PAY OR NOT TO PAY?

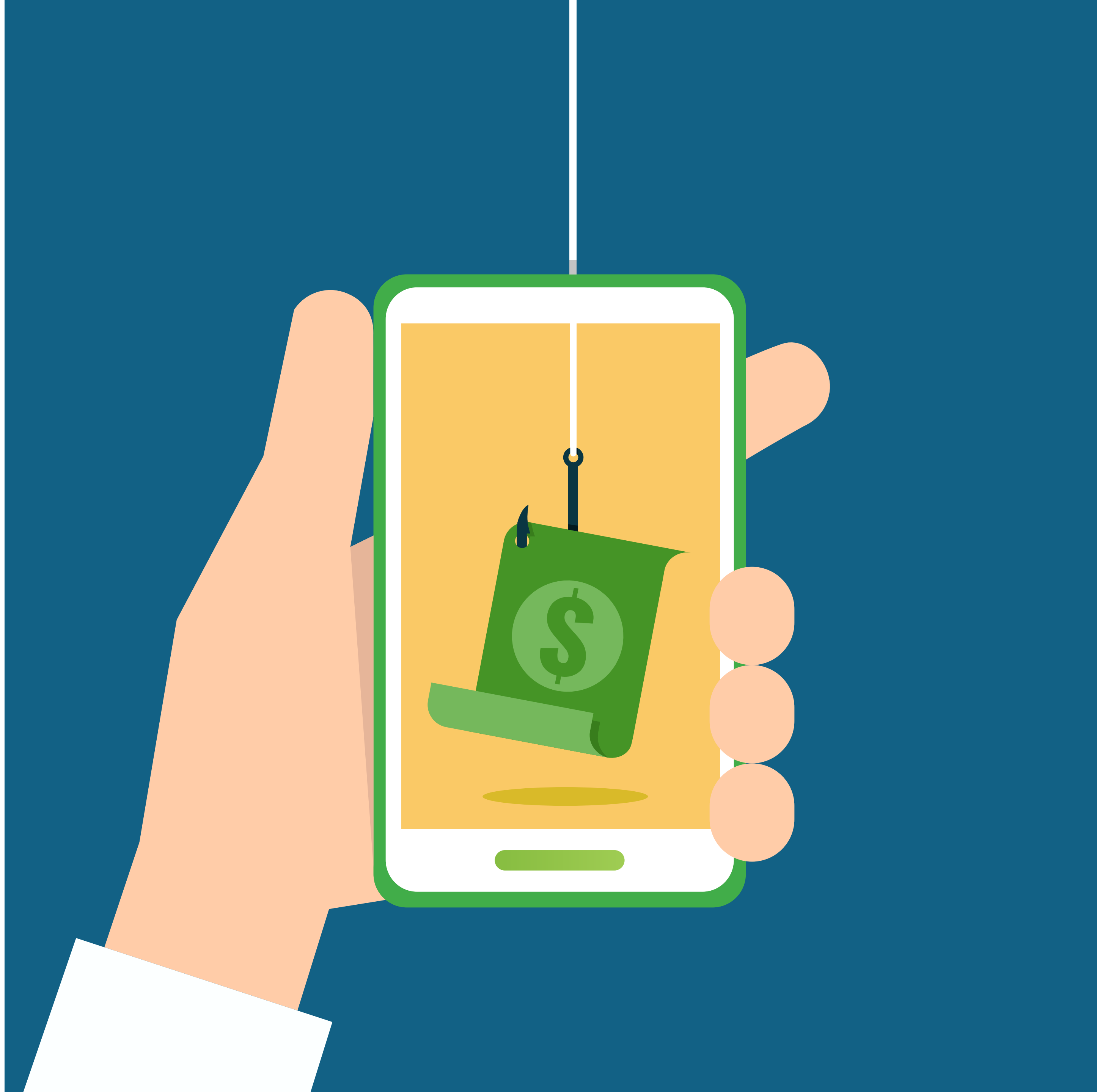
That is the question. Paying the ransom is a bad practice for several reasons:

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.



WHY CYBERCRIMINALS DO IT

It should come as no surprise that the motive behind cryptomalware is money. With the average ransom at $300 and the downtime costs to businesses so high, the balance of power is shifted. Companies desperately want their data back, and $300 seems like a small price to pay relative to the potential loss of files, customer information and business continuity costs. This puts the cybercriminal in the driver's seat—making easy money off of companies' desperation to keep their businesses up and running, even though there is no guarantee that they will give them back all of the data.

According to the Corporate IT Security Risks Survey 2016, the average amount of damage caused by one cryptomalware attack may cost small and medium businesses up to $99,000.

WHAT IT COSTS BUSINESSES

The total amount of damage caused by cryptomalware can be divided into two parts—the ransom and the related losses.

For smaller companies, even a short-term lack of access to corporate data could cause significant losses or completely bring them to a grinding halt. If the organization has not taken appropriate measures to secure its critical information, purchasing a decryption key may be the only way to get back up and running.

Despite the fact that cybercriminals do not guarantee the return of corporate data, 34% of entrepreneurs admitted paying extortionists. According to Kaspersky Lab research, about 67% of SMB representatives have reported complete or partial loss of corporate data due to cryptomalware—underscoring the fact that paying up does not always equal getting back up and running.

As for related losses, business continuity is the first thing to be affected when all work comes to a halt. How long downtime lasts and how quickly you return to normal operations depends largely on the preventative measures of IT staff. Do you have up-to-date backups? Have you updated and patched your software regularly? Are your systems administered correctly? Having the correct procedures in place can mitigate these costs tremendously.

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.

Kaspersky Lab's innovative security products and technologies win more awards than other security vendors' offerings.

In 2015, our products achieved first place in **60 out of 94 independent tests and reviews**

1st *

Kaspersky Lab | 2015
#1 in 60 independent test

* For details, see
usa.kaspersky.com/top3

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