# COULD YOUR BUSINESS SURVIVE A CRYPTOR?

*Learn how to guard against crypto-ransomware*

www.kaspersky.com/business
#SecureBiz

# A practical guide to cryptor attacks

## The damage they do to businesses and how to avoid infection

- What is ransomware?
- What's the damage?
- Even higher costs for businesses
- There are more cryptor attacks than ever before
- How a cryptor attacks
- What they attack
- Today's cryptors are more dangerous
- Covering their tracks
- How to protect your business
- Get award-winning security

## What is ransomware?

**The days of simple malware – developed by amateurs that were just looking to make mischief – 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.

## What's the damage?

**Cryptor attacks affect both consumers and businesses.**

Whereas consumers are typically faced with ransom demands of $300 to $500, cybercriminals fully understand how valuable data can be for a business… so the ransom charges can be much higher.

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 criminal may simply have had no intention of ever enabling decryption. Instead, they just take the victims' money.

According to a survey conducted by the University of Kent's Interdisciplinary Research Center in Cyber Security, in February 2014, **over 40%** of CryptoLocker victims agreed to pay the ransom.

"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

## Even higher costs for businesses

**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.**

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

... and even putting the entire business in jeopardy.

Imagine losing access to all 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?

It's clear that every business has to do all it can to avoid becoming another victim of a cryptor attack.

If your business is attacked, beware of 'false remedies' – that may be promoted on the Internet – as these may only add to your problems:

1

**Often, they don't work – but just take more money from the victim**

2

**Some can even download additional malware onto the victim's network**

# There are more cryptor attacks than ever before

**Because it's relatively inexpensive to develop and launch a cryptor – and a single item of crypto-malware can generate massive revenue – the volume of attacks is increasing.**

Here are just a few examples of recent cryptors:

**CoinVault** – uses 256-bit AES to encrypt victims' files

**CryptoLocker** – has infected tens of thousands of machines and generated $ millions for criminals

**CryptoWall** – often doubles the ransom demand, if payment is not made within the initial time period

**TorLocker** – encrypts data and uses the Tor network to contact the criminals that launched the attack

**In the first six months of 2015, the number of crypto-attacks equalled the volume experienced in the whole of 2014.**

Source: Kaspersky Security Network

Despite the increase in ransomware attacks, a recent survey found that only **40%** of companies consider ransomware to be a serious danger.

Obviously, this attitude can lead to security weaknesses that can be exploited by cybercriminals.

Source: Kaspersky Lab Global IT Risks Survey 2015

## How a cryptor attacks

**In common with most other types of malware, there are many ways in which a cryptor can find its way onto computers and other devices.**

However, two of the most common ways are:

- **Phishing spam**: where the victim receives an email that contains an infected attachment or includes a link to a phishing website.
- **Water holing**: whereby visiting a legitimate website that is popular with a specific type of user or job role – such as an accountancy forum or a business advice site – can result in the employee's device becoming infected. In these cases of 'Drive-By' infection, the website will have already been infected with malware that is ready to exploit vulnerabilities on visitors' devices.

## What they attack

It's worth remembering that a cryptor can attack a wide range of devices, including:

- PCs
- Mac computers
- Android tablets and smartphones
- Virtual desktop infrastructure (VDI)

Furthermore, if the device being attacked is also attached to a network drive – that enables sharing of corporate files – the shared files are also likely to be encrypted by the cryptor… regardless of which operating system the file server is running under.

Unfortunately, whatever device is being attacked, administrator rights are not required for most of the malicious actions that cryptors perform.

## Today's cryptors are more dangerous

**When the first cryptors were unleashed, it was often possible to reverse their effects.**

Sometimes the decryption key was actually hidden within the infected device – so remediation was just a matter of finding the key and then using it to unlock the data. For some other attacks, security experts could reverse-engineer the malware and find ways to decrypt the data.

However, today's cybercriminals are no longer making basic errors. They're also using much more complex techniques that can be extremely difficult to reverse-engineer – and, even in cases where reverse engineering is possible, it's unlikely that the decryption key will be present on the attacked device.

The majority of cryptors now also generate a unique decryption key for each attacked device – so, even if you gain access to one decryption key, it won't help you to decrypt files on any other devices.

These techniques – plus increasingly sophisticated encryption schemes, including:

- **Combined RSA / AES method** that allows high data encryption speed – using the AES algorithm – and later encrypts the AES key with the powerful RSA algorithm
- **Elliptic curves algorithms** that enable even deeper levels of encryption while retaining the speed

… now make it virtually impossible to decrypt the data.

## Covering their tracks

The cybercriminals that launch cryptors are also devoting more resourses to frustrating the efforts of law enforcement agencies – so it's getting harder to track down and close modern crypto-operations:

- Payment is typically requested in Bitcoin or other digital currencies – so the payment trail is not easy to trace
- Use of anonymizing mechanisms – such as the Tor network – make it virtually impossible to trace the location of the criminals

# How to protect your business

**When it comes to dealing with the risk of a cryptor attack, you have two choices:**

**1. Hope you're not attacked – but, with the increasing number of cryptors, that's not really a viable option!**

**OR**

**2. Follow some easily applied rules to help keep your data – and your business operations – safe.**

*Educate your users*
People are often the most vulnerable element in any business. Teach your employees about IT security basics, including:

- Awareness of phishing and spear-phishing risks
- The security implications of opening any email attachment that looks suspicious – even if, at first sight, it appears to be from a trusted source

*Regularly back up data and verify the restorability of your backups*
Almost all businesses will already have data back up policies. However, it's essential that you backup your data onto an offline backup subsystem – instead of just copying files to another 'live' system on your corporate network… otherwise a cryptor will be able to encrypt your backup files.

Establish a 'back up and disconnect' policy – so you're not just copying data onto a permanently connected file server.

*Protect all devices and systems*
Because cryptors don't just attack PCs, you'll also need to ensure your security software can protect your Mac computers, virtual machines and Android mobile devices.

It's also worth ensuring you have sufficient protection installed on your email system.

*Deploy and maintain security software*
As with all malware prevention, your watchword should be 'update early – and update often'… so you:

- **Update all applications and operating systems** – to eliminate newly discovered vulnerabilities
- **Update the security application and its anti-malware database** – to ensure you benefit from the latest protection

Try to select a security solution that includes tools that let you:

- **Manage the use of the Internet** – for example, according to job role
- **Control access to corporate data** – again, according to job or department
- **Manage the launch of programs** – using Application Control technologies that help you block or permit programs

> "Cybercriminals are becoming more and more skilled at developing ransomware that can operate without being noticed, and they have many tools and techniques at their disposal to ensure that the ransomware isn't discovered by the victim."
>
> Andrey Pozhogin, Cybersecurity Expert, Kaspersky Lab

# Get award-winning security

**Kaspersky Endpoint Security for Business delivers multi-layered security – to help defend your business against known, unknown and advanced threats… including cryptors.**

**We deliver updates – for our security agent and anti-malware database – much more frequently than most other security vendors can achieve. In addition, Kaspersky Endpoint Security for Business includes proactive, heuristic and behavioral techniques as well as cloud-assisted technologies – for an extremely rapid response to new threats.**

**Many of our products also offer a whole host of additional security tools and technologies.[1]**

*System Watcher[2] including Crypto-Malware Countermeasures technology*
System Watcher monitors the behavior of all programs running on your systems – and compares each program's behavior with models of typical malware behavior.

If any suspicious behavior is detected, System Watcher will automatically quarantine the program. Because System Watcher keeps a dynamic log of the operating system, registry and more, it helps enable the roll back of malicious actions that were implemented before the malware was identified.

In addition, System Watcher constantly monitors access to some types of files – including Microsoft Office documents – and temporarily stores copies if any of these files are accessed. If System Watcher detects that it was a suspicious process – such as a cryptor – that was accessing the files, the temporary 'backups' can be used to revert the files to their unencrypted form. Although the temporary backups generated by System Watcher are not intended as a replacement for running a full data backup strategy, they can be valuable in helping you to guard against the effects of a cryptor attack.

Working in conjunction with System Watcher, Application Privilege Control also enables administrators to limit the critical system resources that applications are permitted to access – including low-level disk access to the disk.

*Vulnerability Assessment and Patch Management[3]*
Vulnerabilities – or bugs – within any of the applications and operating systems running on your devices can provide entry points for malware attacks… including cryptors.

Our automated Vulnerability Assessment and Patch Management tools can scan your systems, identify known vulnerabilities and help you to distribute the necessary patches and updates – so known security vulnerabilities can be eliminated.

*Automatic Exploit Prevention (AEP)[4]*
Our AEP technology also helps to prevent malware exploiting vulnerabilities within applications and operating systems. It specifically monitors the most frequently targeted applications – including Adobe Reader, Internet Explorer, Microsoft Office and Java – to provide a powerful, additional layer of security.

> Security experts are sometimes able to find a vulnerability within a cryptor – and then exploit the vulnerability to help victims recover their files.
>
> Kaspersky Lab recently partnered with the National High Tech Crime Unit (NHTCU) of the Netherlands Police – to create a repository of decryption keys and a decryption application for victims of CoinVault.

*[1] Security features vary for different types of system / platform. For full details, please see www.kaspersky.com/business*
*[2] System Watcher is available in Kaspersky Endpoint Security for Business (all tiers) and KSV|Light Agent. Windows Workstation Operating Systems only, server platforms are not supported. Not Available for Mac and Android devices.*
*[3] Vulnerability Assessment and Patch Management are included in Kaspersky Total Security for Business, Kaspersky Endpoint Security for Business Advanced and Kaspersky Systems Management.*
*[4] AEP is available in Kaspersky Endpoint Security for Business (all tiers) and KSV|Light Agent. Windows Workstation Operating Systems only, server platforms are not supported. Not Available for Mac and Android devices.*

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

In 2014, our products achieved **first place** in 51 out of 93 independent tests and reviews.

**MOST TESTED.**
**MOST AWARDED.**
**MOST PROTECTIVE.***

***kaspersky.com/top3**

*Application Control and Whitelisting*
Flexible Application Control tools – plus Dynamic Whitelisting – make it easy for you to permit or prevent the launch of programs. In addition to blocking blacklisted programs, you may choose to implement a Default Deny policy for some of your workstations and servers – so that only applications that are on your whitelist are allowed to run… and that means cryptors will automatically be blocked.

*Web Control*
Easy-to-use tools let you set up Internet access policies and monitor Internet usage. You can prohibit, allow or audit users' activities on individual websites or categories of sites, such as social networks, games or gambling sites – so there's less likelihood of users visiting a website that has been infected with a cryptor.

*Anti-phishing*
Our cloud-assisted anti-phishing engine helps to prevent your employees becoming victims of phishing and spear-phishing campaigns that can lead to cryptor infections.

*Email system security*
Kaspersky Security for Mail Server scans incoming, outgoing and stored mail – on Microsoft Exchange, Linux Mail and Lotus Domino mail servers.

Our advanced, cloud-assisted anti-spam engine and anti-phishing engine help you to eliminate distractions and protect against cryptors and other threats.

*Helping you protect all your endpoints[1]…and more*
We have solutions for protecting a wide range of endpoints:

- PCs
- Mac computers
- File servers
- Mobile phones and tablets
- Virtual servers
- Virtual desktop infrastructure (VDI)

… plus security for Internet gateways and collaboration systems.

*1: Security features vary for different types of system / platform. For full details, please see www.kaspersky.com/business*

# GET STARTED NOW
# FREE 30 DAY TRIAL

Discover how our premium security can protect your business from malware and cybercrime with a no-obligation trial.

Visit **kaspersky.com/trials** today to download full product versions and evaluate how successfully they protect your IT infrastructure, endpoints and confidential business data.

**GET YOUR FREE TRIAL NOW**

## JOIN THE CONVERSATION

*#SecureBiz*

Watch us on YouTube

Like us on Facebook

Follow us on Twitter

Join us on LinkedIn

View us on SlideShare

Review our blog

Join us on Threatpost

View us on Securelist

## 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 IT security solutions (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.

**kaspersky.com/business**
**#SecureBiz**