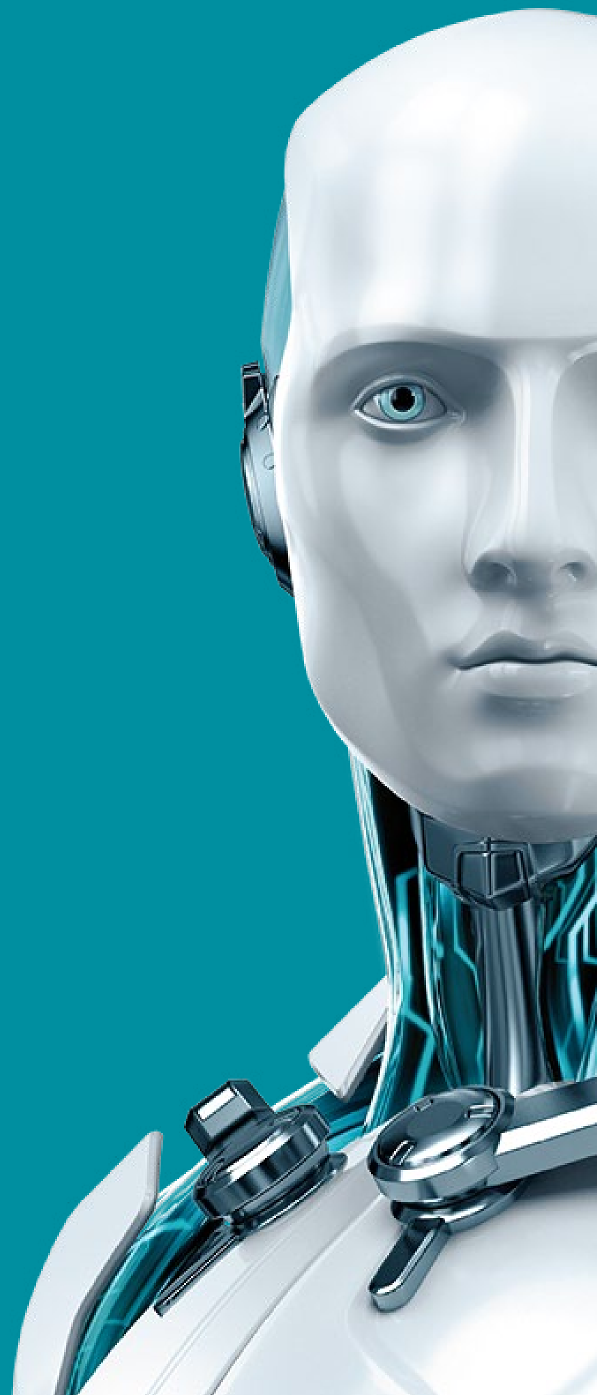
ENJOY SAFER TECHNOLOGY™

RANSOMWARE

How to keep your business safe from extortion malware



Contents

2 Ransomware prevention

4 Keep your company desktops safe

7 What if my company desktop is already infected?

8 Don’t forget about company Android devices

9 What if my company Android device has already been infected?

10 Last but not least: Should I pay a ransom?

Executive summary

Ransomware is malware that can lock a device or encrypt its contents in order to extort money from the owner in return for restoring access to those resources. This kind of malware can also have a built-in timer with a payment deadline that must be met, otherwise the price for unlocking the data and hardware will grow – or the information and the device will ultimately be rendered permanently inaccessible.

Among the well-known examples of ransomware affecting desktop computers are Reveton, CryptoLocker, CryptoWall and TeslaCrypt; and on mobile platforms Simplocker and LockerPin.

Analyses by ESET show that ransomware has emerged as a very popular form of malware for cybercriminals, and that incidences of its use have been rising for many years, targeting both privately owned as well as business devices. Windows and Android are currently the most commonly targeted operating systems, but recent research shows that even Linux and OS X are not exempt from ransomware.

To help companies mitigate the risks of ransomware infection, this white paper documents frequently used attack vectors, offers guidance on how to effectively protect company devices and their contents, and describes the available options when devices or files have already been taken hostage.

Additionally, it provides ESET’s views on the most pressing question that victims of ransomware attack have to answer: “Should I pay what the cybercriminals demand?”

Ransomware prevention

For businesses, the stakes are fairly high. Compared to private users, if a firm loses access to crucial resources it might result in financial loss and/or reputational damage. And as a *recent survey* of nearly 3,000 IT and cybersecurity professionals worldwide showed, as many as one in five organizations has already experienced an incident involving this kind of threat.

Attackers nowadays use encryption that is as strong as that used by banks to protect payments by their clients, making recovery of files and devices more complicated—and in the worst cases, even impossible.

It is therefore cheaper to focus on prevention than to pay for the consequences. If company devices are not protected and employees lack proper training, there is a high risk that in the event of a ransomware infection, valuable data stored on company devices and subsequently on disks connected to them via networks, will be lost forever.

A. Use the latest version of your security software

Install the most recent version of your security software, as many infections occur because outdated solutions remain in place. If you have a valid ESET license, updating to the latest version costs nothing.

If you are still using ESET Endpoint Security versions 3 or 4, we strongly recommend updating to the newest, 6th generation of our business products, which applies the latest technologies specially crafted to improve client protection from malware that uses obfuscation and/or encryption to stay undetected.

Examples of these technologies include **Advanced Memory Scanner**, which looks for suspicious behavior after malware decloaks in the memory, and **Exploit Blocker**, which strengthens protection against targeted attacks and previously unseen vulnerabilities, also known as zero-day vulnerabilities.

B. Keep your security software's virus database up-to-date

New versions of ransomware are released frequently, so it is important that computers and other company devices receive regular virus database updates. Among other precautions, this helps to ensure they are not vulnerable to ransomware infections. ESET products check for updates every hour, provided they detect a valid license and a working Internet connection.

C. Enable the ESET LiveGrid® cloud protection system

Unknown and potentially malicious applications, and other possible threats, are monitored and submitted to the ESET cloud via the ESET LiveGrid Feedback System. The samples collected are subjected to automatic sandboxing and behavioral analysis, which results in the creation of automated signatures if malicious characteristics are confirmed.

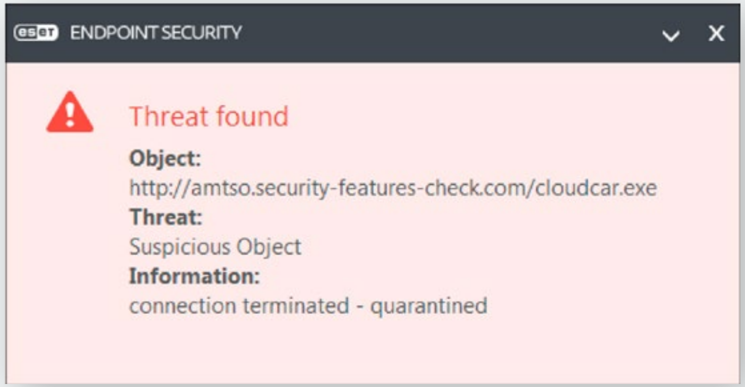
ESET clients learn about these automated detections via the ESET LiveGrid Reputation System in a matter of **minutes**, without the need to wait for the next signature database update. If a process is deemed unsafe – such as deleting a backup – it is immediately blocked. It is important to note that ESET LiveGrid uses only hashes of suspicious files, never their contents, thus respecting the privacy of ESET customers.

IMPORTANT NOTE

It is possible that your company firewall could block ESET Live Grid communications, so you should verify that it is working properly. To do this, please visit the following webpage of the renowned testing organization AMTSO, of which ESET is a member:

http://www.amtso.org/feature-settings-check-cloud-lookups/

Click on the link "Download the CloudCar Testfile" and download the test file "cloudcar.exe". If ESET LiveGrid works properly, the file will open on ESET's servers and, after obtaining the necessary information, will block it. The file will not be downloaded onto your computer and following message will be displayed:



Threat found

Object:
http://amtso.security-features-check.com/cloudcar.exe
Threat:
Suspicious Object
Information:
connection terminated - quarantined

Keep your company desktops safe

To mitigate the risk of data loss and damage to devices commonly caused by ransomware, we encourage all companies to follow these eleven steps.

11 STEPS FOR PREVENTING DATA LOSS

1. Back up important data regularly
2. Patch & update your software automatically
3. Pay attention to your employees' security training
4. Show hidden file-extensions
5. Filter executable attachments in email
6. Disable files running from AppData/LocalAppData folders
7. Consider shared folders
8. Disable RDP
9. Use a reputable security suite
10. Use System Restore to get back to a known-clean state
11. Use a standard account instead of one with administrator privileges

1. Back up important data regularly

The single, best measure to defeat ransomware before it even starts its malicious activity, is to have a regularly updated backup. Remember that malware will also encrypt files on drives that are mapped and have been assigned a drive letter, and sometimes even on drives that are unmapped.

This includes any external drives such as a USB thumb drive, as well as any network or cloud file stores. Hence, a regular backup regimen is essential, ideally using an off-site, offline device for storing the backup files.

2. Patch and update your software automatically

Malware authors frequently rely on people running outdated software with known vulnerabilities, which they can exploit to silently access company devices and their systems. Businesses can significantly decrease the potential for ransomware pain if they make a practice of updating company software and devices as often as possible.

Some software vendors release security updates on a regular basis, but there are often “out-of-cycle” or unscheduled updates in cases of emergency. Enable automatic updates if you can, or go directly to vendors’ websites.

3. Pay attention to your employees' security training

One of the most common infection vectors is social engineering – methods that are based on fooling users and trying to convince them to run executable files. By claiming to be a tracking notification email from a delivery company (such as FedEx or UPS), an email from their bank, or an internal company message such as New_Wages.pdf.exe, the attackers try to dupe employees to achieve their malicious goals. To prevent this from happening, employees should be trained not to open any unknown or suspicious email attachments, links or files.

4. Show hidden file-extensions

Ransomware frequently arrives in an email attachment with the extension ".PDF.EXE". This counts on Window's default behavior of hiding known file extensions. Re-enabling the display of the full file extension makes spotting suspicious files easier.

5. Filter executable attachments in email

If your gateway mail scanner has the ability to filter files by extension, you may wish to block emails sent with ".EXE" file attachments, or those with attachments that have two file extensions ending with an executable ("*.*.EXE" files, in filter-speak). We also recommend filtering files with the following extensions: *.BAT, *.CMD, *.SCR and *.JS.

6. Disable files running from AppData/LocalAppData folders

A notable behavior of a large proportion of ransomware variants is that they run their executable from the AppData or Local AppData folder. You can create rules within Windows or with intrusion prevention software to disallow this behavior. If for some reason legitimate software is set to run from the AppData rather than the usual Program Files area, you will need to exclude it from this rule.

7. Consider shared folders

Bear in mind that any company device infected by ransomware might also cause encryption of all files in shared folders to which it has write permission. For this reason, employees should consider which valuable and sensitive files they store on shared disks, as their data in these locations might get encrypted by malware, even though their computer wasn't directly infected.

8. Disable RDP

Ransomware often accesses target machines using Remote Desktop Protocol (RDP), a Windows utility that allows others to access desktops remotely. Cybercriminals have also been known to log in via an RDP session and disable the security software. It is best practice to disable RDP unless you need it in your environment. For instructions on how to do so, visit the appropriate Microsoft Knowledge Base articles.

9. Use a reputable security suite

Malware authors frequently send out new variants of their malicious code, trying to avoid detection, so it is important to have multiple layers of protection. Even after it burrows into a system, most malware relies on remote instructions to perform serious mischief.
If you encounter a ransomware variant that is so new that it gets past antimalware software, it may still be caught when it attempts to connect with its Command and Control (C&C) server to receive instructions for encrypting files. ESET's latest software suite provides an enhanced **Botnet Protection** module that blocks malicious traffic trying to communicate with a C&C server.

10. Use System Restore to get back to a known-clean state

If System Restore is enabled on the infected Windows machine, it might be possible to take the system back to a known-clean state and restore some of the encrypted files from "shadow" files. But you have to outsmart the malware and move quickly.

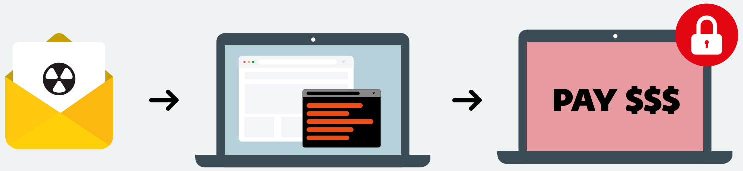
This is because some of the newer ransomware has the ability to delete the "shadow" files from System Restore. Such malware will start deleting "shadow" files whenever the executable file is run, and you might not even know that this is happening, since executable files can run without the operator knowing, as a normal part of Windows system operation.

11. Use a standard account instead of one with administrator privileges

Using an account with system administrator privileges is always a security risk, because then malware is allowed to run with elevated rights and may infect the system easily. Be sure that users always use a limited user account for regular daily tasks and the system administrator account only when it is absolutely necessary. Do not disable User Access Control.

RANSOMWARE: HOW IT WORKS

Ransomware is a type of malicious software that can lock your device and take hostage files that might have some personal or professional value to you.



Malware is often spread via email or by drive-by downloads from compromised websites. After it's done its malicious job, the ransomware generates a pop-up message telling you to pay.

What if my company desktop is already infected?

Disconnect the device

If you or any of your employees run a suspicious file and you are unable to open some of the stored files, immediately disconnect the device from internet, company network and if possible also from the electricity supply. This can prevent communication between the malware and its C&C server before it finishes encryption of the data on that device and all its mapped disks.

Although this isn't a bulletproof technique, it gives your company at least some chance to save some of the valuable files before they are fully encrypted. We recommend a hardware shutdown, as ransomware might be programmed to monitor software shutdown and cause more damage.

Contact ESET technical support

If the ransomware has already run its course and you don't have a functional backup, contact ESET technical support. Don't forget to attach a log from ESET Log Collector and a few samples of the encrypted files—if possible, send approximately five MS Word or MS Excel files.

If your company license has 100 or more seats, our specialists will contact you requesting more information about the infection after you submit a ticket via our online system. In cooperation with the ESET Malware Research Laboratory, our specialists will attempt to decrypt and recover the affected files.

But please bear in mind that the authors of malicious code have gone to considerable lengths to make their ransomware effective, using ever stronger and more advanced encryption. It is therefore often impossible to decrypt everything, or to do so quickly.

Nowadays, encryption is a technological standard protecting bank and financial transfers, e-shop transactions and many other online services and the latest versions are close to impenetrable. It is for this reason that no vendor can guarantee to recover your files.

ESET experts will attempt to find ransomware loopholes that will allow them to repair the damage caused to your affected disks and devices. If they are successful, they will provide you with a decryption tool tailor-made for your business.

Based on our experience, this outcome is possible for one in five ransomware cases. This process can take up to several weeks, depending on how skillful the malware authors were. It is possible that the attempt will not succeed. If you have opted for ESET Premium Support, our specialists are available to answer your requests 24 hours a day, 365 days a year.

Don't forget about company Android devices

As we already mentioned, malware authors are not focusing solely on Windows. In recent years they have shifted their attention to the *most dominant mobile operating system, Android*, which is used by many businesses smartphones and tablets.

ESET has seen various families of Android ransomware designed to target mobile devices specifically. Attackers use various techniques, such as pretending to be antivirus software or disguising their ransom demand as a local law enforcement agency and blocking the device (an example of such ransomware is *Reveton*).

In 2014, our researchers encountered the first ransomware that attempted to *encrypt data on mobile* devices running Android. Since then, attackers have come up with more than 50 variants, each more dangerous and more advanced than the last. Only a year later, the *first ransomware that blocked access* to a device by setting a random four-digit screen-lock appeared.

Remember that all of these malicious codes were able to effectively block access to resources vital for everyday business, and demanded hundreds of dollars from the victims and their companies to restore access.

HOW TO KEEP YOUR ANDROID DEVICES PROTECTED?

A. Train your employees

For employees using Android devices, it's important to be aware of ransomware threats and to take preventive measures. Training is therefore an essential countermeasure.

- Among the most important steps to take is to avoid unofficial or third-party app stores.
- Before employees download anything from the official store, they should read the reviews by other users. Malicious behavior is quickly identified by users and comments about it are published directly on the app page.
- Employees should always check if the permissions that the app is requesting are necessary for its proper function.
- If possible, create a whitelist of apps allowed on company Android devices.

B. Use security software

Have a mobile security app installed and kept up to date in all the company Android devices. If you are an ESET customer, you can install ESET Endpoint Security for Android as a part of the following ESET Business Solutions security packages:

- ESET Endpoint Protection Standard
- ESET Endpoint Protection Advanced
- ESET Secure Business
- ESET Secure Enterprise

C. Backup all the important data

Additionally, it is important to have a functional backup of all important data from each Android device. The chances are that users who take appropriate measures against ransomware will never face any request for ransom. And even if they fall victim and – in the worst-case scenario – see their data encrypted, having a backup turns such an experience into nothing more than a nuisance.

What if my company Android device has already been infected?

If your device or your employee's device gets infected by ransomware, you have several options for its removal, depending on the specific malware variant.

1. Boot in safe mode

For the most simple lock-screen ransomware families, booting the device into Safe Mode – so third-party applications (including the malware) will not load – will do the trick and the user can easily uninstall the malicious application. The steps for booting into Safe Mode can vary on different device models (to find out which apply to your device(s) consult your manual, or Google the results).

2. Revoke administrator privileges for malware

In the event that the application has been granted Device Administrator privileges – as it is often the case with new variants of ever-more aggressive ransomware – these must first be revoked from the settings menu before the app can be uninstalled.

3. Reset password via Mobile Device Manager

If ransomware with Device Administrator rights has locked the device using Android's built-in PIN or password screen lock functionality, the situation gets more complicated. It should be possible to reset the lock using Google's Android Device Manager or an alternative MDM solution. Rooted Android phones have even more options.

4. Contact technical support

If files on the device have been encrypted by crypto-ransomware such as Android/Simplocker, we advise users to contact their security provider's technical support. Depending on the specific ransomware variant, decrypting the files may or may not be possible.

5. Factory reset

A factory reset, which will delete all data on the device, can be used as the last resort in case none of the previous solutions are available.

Last but not least: Should I pay a ransom?

ESET advises its business customers as well as all other users **not to pay ransoms**.

First of all, the attackers are not acting legally, so they have no obligation to fulfill their end of the bargain by decrypting the affected data or unlocking your device in return for payment.

Paying a ransom also helps them to finance their ongoing malicious activities.

Even if the malware authors provide you with a decryption key, there is no guarantee that it will actually work. ESET has seen many cases in which the tool sent by the attackers wasn't able to decrypt the files, or worked only partially. In some cases of Android ransomware, the randomly generated PIN code blocking the device wasn't sent to the cybercriminal and there was therefore no way to unlock it.

Also, if you pay the cybercriminals, how do you know they won't come back for more? If they were successful in attacking your company, they may regard that as weakness and try to exploit you again.