Ransomware: What You Need to Know

A Joint Report by Check Point and Europol

Cyber Intelligence Team

The Hague,
15/12/2016

Contents

1 Introduction

Ransomware are malware designed to extort money from users whose computers they infect. Recent innovative methods for infecting, monetising and targeting lucrative targets show that this attack vector is growing in sophistication since its primitive yet effective origins.

In recent years, there has been a surge of ransomware. It's been reported all over security blogs, tech websites and even on the news. It doesn't seem to stop; in fact, it seems to be getting worse in both spread and sophistication.

CryptoLocker, the first famous ransomware, was observed in the wild in 2013. From then until the end of 2015 there were only a few active ransomware variants. Some of these variants were weak enough that it was possible to decrypt the encrypted files without any need to give in to the ransom demand[1]. The infection methods were limited.

While quite a lot of variants have been created since then, many of them either don't persist in infecting users' computers or they run a low profile campaign. A good example is TeslaCrypt, an infamous ransomware whose authors released a master key for anyone to use.

In other cases, new ransomware variants - even ones that are widely distributed and constantly make headlines – have quickly been found to have bugs when it comes to implementing the encryption itself, such as the recently published decryption tool for the Jigsaw ransomware. These flaws are either fixed in a newer version, or the ransomware is abandoned.

There seems to be a fairly large difference between the top-tier of ransomware, which usually maintain several active campaigns, and the trendy new ransomware variants which come and go. In this report, we provide an overview of the scary world of ransomware. We highlight the differences between the most prevalent ransomware families, and present several others, smaller yet unique in their characteristics. Finally, we share some basic methods for protection and mitigation.

[1] It should be noted that paying the ransom does not always result in the release of the encrypted files.

2 The Founding Fathers

While not the first ransomware ever observed in the wild, these are the ones that have blazed the trail:

CryptoLocker

CryptoLocker was the first leader of the ransomware trend and rapidly became a top threat for law enforcement. In May 2014, a multi-national law enforcement operation involving partners from the security industry and academia led to the arrest of the malware creators and the end of CryptoLocker infections. Most current ransomware follows the CryptoLocker pattern, including encryption and the ransom note style.

To confuse matters further, when reporting or recording ransomware incidents, both the media and law enforcement commonly use the term "CryptoLocker" as a synonym for any new or unidentified ransomware using encryption, making clear assessments of the threat difficult.

CryptoWall

CryptoWall started as a CryptoLocker *doppelgänger* but, after its takedown, CryptoWall became one of the most prominent ransomware variants to date. It remains one of the leading ransomware threats for law enforcement in the EU, with half of Member States reporting cases of CryptoWall. Typically installed by an exploit kit or malicious email attachment, CryptoWall is known for its use of AES encryption and for conducting its Command and Control (C&C) communications over the Tor anonymous network.

TeslaCrypt

Until May 2016, TeslaCrypt was one of the most notable ransomware variants. The ransomware, which was spread mainly via common exploit kits such as Angler, is now defunct: its authors stopped the malware campaign and released a public recovery key.

CTB-Locker

Emerging in mid-2014, Curve-Tor-Bitcoin (CTB) Locker (also known as Critroni) was one of the first ransomware variants to use Tor to hide its C&C infrastructure. While active during 2015, CTB-Locker activity dropped off in 2016. However, a more recent variant has been targeting web servers and is uniquely using the Bitcoin blockchain to deliver decryption keys to victims. Marginally less prominent among EU law enforcement investigations compared to CryptoWall, CTB-Locker was one of the top malware threats for the financial services industry.

3 The Current Top Tier

These currently active malware families demonstrate the most professional implementation and maintain a high infection rate:

Locky

During its first month in the wild, Locky's reported infection rates were between one to five computers every second and approximately 250 000 PCs were infected within its first three days of activity. Locky made headlines after causing a USA hospital to enter a state of emergency but only began to appear in EU law enforcement at the beginning of 2016. According to the findings of IntSights, a security provider specialising in advanced cyber intelligence, threat actors often design malware based on Locky's characteristics and market them as related to Locky. However, Locky is run by a single attacker who operates worldwide via exploit kits and spam campaigns, and does not have specific targets.

The malware modus operandi is to send a .doc file with malicious macros in it and ask the user to enable macros in Microsoft Word. Once enabled, the ransomware will encrypt the files and add the characteristic ".locky" extension to them. The latest version of Locky adds the extension ".osiris" to the encrypted files, and scrambles their names. For example, a file called test.jpg could be renamed to 4f594feb4104a2e1_wpxan7ix--dzy9--jah6--67d63cb8--15140b74ba3a.osiris. After encryption, the victim is presented with a note that provides information on how to pay the ransom. The ransom payment typically varies between 0.5 and 1 Bitcoin (BTC). The names of these ransom notes have changed for the OSIRIS Locky variant and are now named desktopOSIRIS.htm or desktopOSIRIS.bmp. In another campaign that was recently observed, Locky was spread via Facebook Messenger as part of a two-stage attack.

Unfortunately, there are currently no free tools available to decrypt files encrypted by the Locky ransomware. The only way to recover encrypted files is via a backup, or if you are incredibly lucky, through Volume Shadow Copies. Though Locky does attempt to remove Volume Shadow Copies, in rare cases ransomware infections fail to do so for whatever reason.

CryptXXX

CryptXXX is distributed by both the Angler Exploit Kit and the Bedep Trojan, which drop it as a second-stage infection. Due to several similarities in the attack vector, researchers speculate that the same operator is behind both Angler and CryptXXX.

This malware was recently revamped (version 3.0) with a new encryption algorithm and a new credential-stealing module so that attackers can drain your bank account

directly if you refuse to pay up. Exploits used by the Neutrino exploit kit to get CryptXXX 3.0 onto your machine include ever-popular Adobe Flash flaws, most recently based on CVE-2016-4117. The ransomware encrypts files with AES CBC 256-bit encryption and adds the ".cryp1" extension to all affected files. Currently many antiviruses can remove it, but there are no 100% effective decryptors for encrypted files.

TorrentLocker

TorrentLocker is referred to by its operators as 'CryptoLocker', similar to the old and famous ransomware. The first three versions of TorrentLocker contain a bug which enables recovery of the decrypted files. Before the release of version four, the flaw was fixed and from this version on, the files cannot be recovered.

Jigsaw

Jigsaw ransomware became infamous thanks to an image of the killer from the horror movie 'The Saw' displayed on the ransom note. A decryption tool which can recover files encrypted by multiple Jigsaw variants has been released to the public.

Cerber

Cerber version 5.0.1 has already been released. Cerber 3 evolved into Cerber 4 in just one month, and Cerber 4.1.x evolved into 5.0.x in less than a month. In addition to the previous versions of the malware, it adds a four digit extension to the encrypted files which is the fourth segment of the "MachineGuid" value of the HKLM\Software\Microsoft\Cryptography registry key. Instruction files are dropped to notify the victims that their files have been encrypted, and to explain how to pay the ransom. The instruction file of this version has the same filename "_README_XXXX_.hta" as in previous versions, and the format remains the same. Cerber also changes the wallpaper of the infected machine to notify victims that they have been compromised. As explained above, previous indicators of Cerber versions were the file extensions of encrypted files. This is no longer the case for versions after Cerber 4, since now there is no fixed file extension. Instead, the version number is displayed on the modified wallpaper. It also appears that the code in this latest version has been optimised compared to Cerber 4.0.2.

Crysis

First discovered in February 2016, Crysis is quickly yet quietly spreading to businesses across the globe. It can infect Windows and Mac systems and encrypts about 200 file types across internal and external storage, as well as network shares through a combination of RSA and AES encryption algorithms. In addition, to ensure infection,

Crysis deletes the system´s shadow copies, which serve as back-up copies of the computer´s files or volumes.

As a measure of persistence, Crysis also sets registry entries in order to be executed at every system start. Upon execution, it encrypts all file types (including those with no extension), leaving only necessary operating system and malware files untouched.

After encryption, a text file named "How to decrypt your files.txt" is dropped into the Desktop folder; the information initially provided is limited to two email addresses which victims can use to communicate with the cybercriminals. After sending the email, the victim receives further instructions to buy the decryption tool needed to unlock the files.

Crysis was mainly distributed via brute-forced RDP credentials and through spam emails with malicious attachments or links to compromised websites.

4 Latest Advancements

Here are the latest advancements in the ransomware world:

Extortion to recruit insiders: Delilah

Delilah tries to recruit insiders via social engineering and extortion, sometimes using ransomware techniques.

The malware is delivered to victims via indecent sites. It infects the user's PC and starts gathering personal information from the victim so that the individual can later be manipulated or extorted.

This includes information on the victim's family and workplace and includes webcam operations to record the target's behaviour. These bots involve a high level of manual labour from the attacking actor to build the extortion motive. Once built, the target can be manipulated into insider malicious data gathering and actions.

This extortion technique was previously reported as being executed on dating websites, where the targets were fooled into sending embarrassing self-recordings, to be later used for extortion. The attacker warned the target they will share the recording on Facebook if the extortion fee is not met.

Ransomware attackers are targeting specific users and not just "casting a net". This is now done in order to extort higher amounts or to manipulate the target into a more lucrative action.

Encryption without Command and Control: SamSam

Attackers are targeting networks which are not connected to the internet. At first the attacker creates a foothold in the organisation by scanning the target for vulnerabilities and getting onto the network. Then the attacker moves to infect the machines without need for network connectivity and hold the whole organisation to ransom at the same time. Throughout 2016, SamSam was noted to be targeting organisations in the healthcare industry, including hospitals.

The current common ransomware behaviour is to have a default encryption method without the need for a Command and Control (C2). Cutting out the need for a C2 infrastructure, and residing in the Tor network, allows for these campaigns to keep going after successful take downs of C2 infrastructure.

Complete Hard-Drive encryption: Petya

Petya ransomware not only encrypts all files found on the victim's hard-drive, but its operators hold the entire hard-drive's content hostage as well, by encrypting its Master-File-Table (MFT). Check Point researchers revealed multiple flaws in the encryption algorithm implementation, and provided a method to restore all data encrypted by Petya.

Synchronising attacks: Cerber

Attackers are searching for holes in defences. Once found, they synchronize the attacks to massively exploit the hole. This results in a high wave of undetectable malware bypassing different layers of protection. Such attacks were found to bypass Office 365 cloud email security solutions and have a very low detection rate by anti-virus software at the date of the synchronised attack.

First published in February 2016, Cerber has been one of the most widespread ransomware variants in the past year. Its features include audio delivery of the ransom message using Microsoft Speech API, and ignoring machines from several countries such as Russia, Georgia and Ukraine. Its latest version, dubbed Cerber v5.0.1, was released in November 2016. It relies on redirects via Google and the use of a Tor2Web proxy service to disguise its activity and block attempts to shutter servers hosting the malicious content. Emails are distributed with the recipient's name in the subject, giving them the appearance of legitimacy, and presents hyperlinks to the usual subjects of potential interest: pictures, order details, transaction logs, loan acceptance letters, etc. But hidden within the message, a URL employs Google redirection, leading unwitting victims to the malicious payload hosted on the Tor network. By clicking the bad link, it delivers a Word document containing the malware downloader with the Cerber variant.

Cerber is ransomware-as-a-service which is advertised and sold in closed forums on the Dark Web, and thus its targets are varied and depend on the participating affiliates. The affiliates operate their own campaigns, while choosing the targets and the distribution method, and the income from their attacks is divided between them and the ransomware creator.

Open source ransomware: LockLock

This ransomware has been observed to be based on the open-source ransomware EDA2, and initial analysis of attacks show victims whose IP addresses appear to come from China. This particular ransomware encrypts using the AES-256 algorithm and appends a ".locklock" extension to its targeted file types. The ransom note, found in the file "READ_ME.TXT", demands that the victim communicates with the cybercriminals via an email address or Skype.

Spear phishing attacks: RAA

Last June, RAA made its first rounds, notably using JScript scripting language. Much more recently, a new RAA variant targeting companies via spear phishing attacks was spotted. This evolved variant now arrives in the form of a password-protected .zip archive attachment. This is an age-old technique that would thwart anti-malware systems from unpacking the file and scanning it for its malicious content. However, the new variant proceeds with the encryption process without the need to communicate to a Command & Control server. Unlike its earlier version, the ransom note, written in Russian, does not ask for a specific amount in bitcoins.

Threat from Romania: NoobCrypt

There is a new variant that reportedly made the mistake of using the same password for all of its victims. This allowed some researchers to develop a list of decryption keys based on the password. When the screen gets locked, a ransom note flashes up saying "Made in Romania." A ransom amount, deadline, and specific bitcoin address are then provided for the particular release on a per-victim basis.

Cerber look alike: Razy 5.0

Back in July, a ransomware variant that appears to have the same text-to-speech feature similar to Cerber was sighted. Razy encrypted files use AES before appending the extension .razy to the locked files. The new variant of Razy, dubbed as Razy 5.0 uses a Jigsaw ransomware-inspired note that demands a payment of EUR 10 via PaySafeCard. The ransom note issues a soft threat though—it is noted that, unlike Jigsaw, it does not delete the encrypted files after its set deadline.

Based on EDA2: Fantom

Following the surfacing of Fantom – a variant based on the open-source ransomware EDA2 – by the end of August 2016, a new variant was spotted with several updates. Now, Fantom follows the trend of evolved ransomware variants that can encrypt files without having to connect to its Command & Control servers for the keys. Apart from the offline encryption feature, this updated variant adds network share enumeration, and a per-victim display of ransom values based on the targeted victim's files in its routines.

Ransomware for Android: Dogspectus

This is an exploit kit being used to deliver ransomware to Android devices. It uses several vulnerabilities to silently install malware onto the victim's phone or tablet in the background. A novel attack method was discovered when a test android device in a lab environment was hit with the ransomware when an advertisement containing hostile JavaScript loaded from a web page. During the attack, the device did not display the normal "application permissions" dialogue box that typically precedes installation of an Android application.

Shade (aka Encoder.858, aka Troldesh)

Shade is a family of ransomware cryptors that emerged in early 2015. Shade uses malicious spam or exploit kits as primary attack vectors. The latter is the more hazardous method because a victim does not have to open any files - a single visit to an infected website does the trick. When the ransomware infiltrates a victim's computer system, the Trojan requests an encryption key from the criminal's Command-and-Control (C&C) server or, should the server be unavailable, uses one of the keys embedded in advance. That means that even if the PC is disconnected from the internet, the ransomware functions, provided it's already in the system. Once started, it encrypts personal files stored on computer drives and attached network drives. It uses very strong hybrid encryption with a large key (RSA-3072). When the ransomware encrypts a file, it will add the .no_more_ransom extension to each encrypted file. Once the malware has finished encrypting all files, it will create a file named "README.txt" with instructions on how to decrypt all encrypted files. The No_more_ransom (Shade) ransomware requests a payment in bitcoins to get a key to decrypt the files. It is important to know that it is currently not possible to decrypt the .no_more_ransom files without the private key and decrypt program. Making use of a "brute force" method is also not a way because of the long length of the key. No_more_ransom is a variant of the Shade ransomware infection. It affects all current versions of Windows operating systems such as Windows XP, Windows Vista, Windows 7, Windows 8 and Windows 10. When the virus infects a computer, it uses system directories to store its own files. In

order to run automatically whenever you turn on your computer, the No_more_ransom ransomware creates a registry entry in Windows.

Popcorn Time

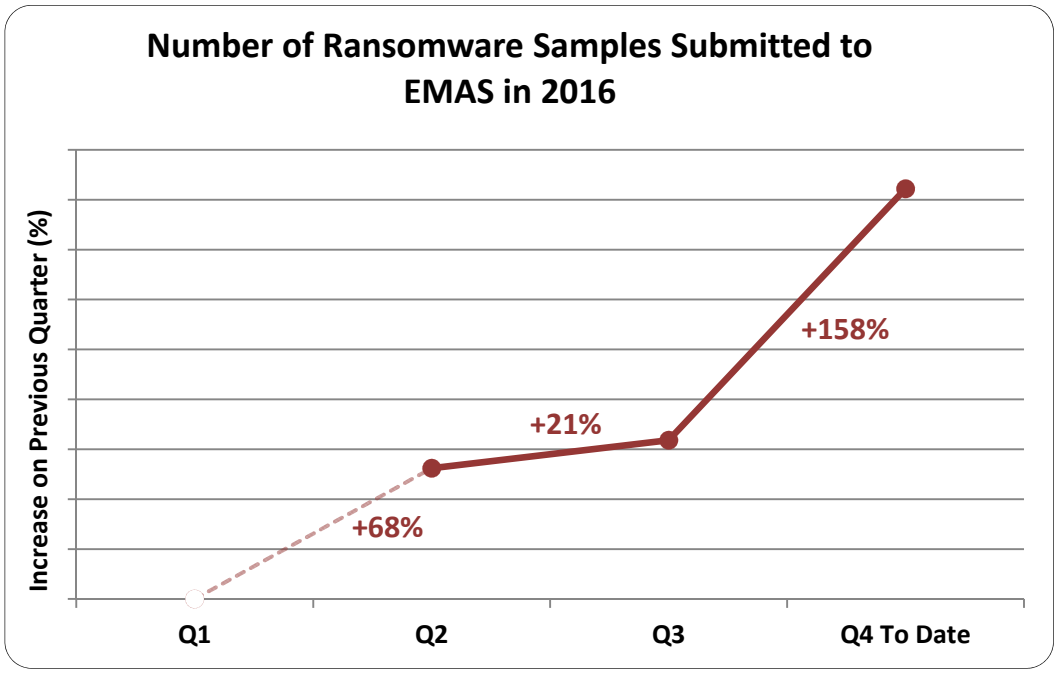
Initially discovered by MalwareHunterTeam, the new Popcorn Time ransomware has been designed to give the victim an illegal way of getting a free decryption key for their encrypted files and folders. The ransomware asks the user to pay 1 BTC to decrypt the files on their computer, or to spread the ransomware to two other users to pay the ransom instead. It also provides an onion link in the ransom note that can be used to make other users download the file via Tor. The victims are allowed to pay the ransom within seven days, otherwise their files could be deleted. The source code of the ransomware appears to be not yet finished.

When the user enters the decoding code wrong four times, all of their files will be deleted. Once infected, the Popcorn Time ransomware will check to see if the ransomware has been already run on the PC, by checking some files that it leaves behind after removal. If it has, the ransomware will terminate itself. If not, the Popcorn Time ransomware will either download various images to use as backgrounds or start encrypting the files using AES-256 encryption. The encrypted files will have the ".filock" or ".kok" extension appended to them.

While encrypting the data, the ransomware will display a fake screen that pretends to be the installation of the program. As soon as the encryption is finished, it will save two ransom notes called restore_your_files.html and restore_your_files.txt, and will then automatically display the HTML ransom note asking for 1 Bitcoin. The latest version of the ransomware encrypts files located in My Documents, My Pictures, My Music, and on the desktop.

5 Statistics

EU Member States (MS) and third parties submit samples of malware to Europol for analysis in the Europol Malware Analysis System (EMAS[2]). The graph below shows the percentage increase of ransomware samples, quarter-on-quarter, submitted during 2016. In Quarter 4 there was a particular increase, with the number of submissions 158% higher than the previous quarter.



Of these contributions, the ransomware families listed below were the most submitted:

- Locky;
- Troldesh;
- Cerber;
- CryptoLocker;
- CryptoWall.

2 The Europol Malware Analysis Solution (EMAS) is a dynamic, automated malware analysis solution, which executes malware samples submitted by Member States and third parties in a tightly controlled sandbox environment.

All the information received is stored in a central database. The automated cross-checks can unveil links between attacks performed in different countries with the same malware, or with the same criminal organisation behind the same malware family, connecting to the same domains and related to different investigations within the EU and beyond.

The table below shows the most common ransomware infections for Europe and each of the EU MS countries between January and December 2016 within business, government and academia, as researched by Check Point:

	No.1	No.2	No.3
Europe	Locky	Cryptowall	TeslaCrypt
AT	Locky	Cryptowall	TeslaCrypt
BE	Locky	TeslaCrypt	Cryptowall
BG	Locky	Cryptowall	Fareit
CY	Locky	Cryptowall	TeslaCrypt
CZ	Locky	TeslaCrypt	Cryptowall
DE	TeslaCrypt	Locky	Cryptowall
DK	Locky	Cryptowall	TeslaCrypt
EE	Locky	TeslaCrypt	Cryptowall
ES	Locky	Cryptowall	TeslaCrypt
FI	Locky	TeslaCrypt	Cryptowall
FR	Locky	TeslaCrypt	Cryptowall
UK	Locky	TeslaCrypt	Cryptowall
EL	Locky	TeslaCrypt	Cryptowall
HR	Locky	Cryptowall	TeslaCrypt
HU	TeslaCrypt	Locky	Cryptowall
IE	Locky	TeslaCrypt	Cryptowall
IT	Locky	Cryptowall	TeslaCrypt
LT	Locky	TeslaCrypt	CryptoLocker
LU	Locky	TeslaCrypt	Cryptowall

LV	Cryptowall	Locky	Fareit
MT	Locky	TeslaCrypt	Autoitcrypt
NL	Locky	TeslaCrypt	Cryptowall
PL	Cryptowall	Locky	TeslaCrypt
PT	Locky	TeslaCrypt	Cryptowall
RO	Locky	TeslaCrypt	Cryptowall
SE	Cryptowall	Locky	TeslaCrypt
SI	Locky	Cryptowall	TeslaCrypt
SK	Locky	Cryptowall	TeslaCrypt

6 The 'No More Ransom' Project

The 'No More Ransom' Project is a joint initiative between law enforcement and the private sector to combat ransomware by creating an online portal aimed at victim mitigation and informing the public about the dangers of ransomware. The project was officially launched on 25 July 2016. Since then, there have been two further rounds where additional partners have been added. This is expected to continue, with the addition of more and more new partners, tools and language versions.

The initial founding project partners were the Dutch Police, Europol's European Cybercrime Centre (EC3), Kaspersky Lab, and Intel Security. Three months after the launch of the project, law enforcement agencies from a further 13 countries signed up to participate in the initiative, namely: Bosnia and Herzegovina, Bulgaria, Colombia, France, Hungary, Ireland, Italy, Latvia, Lithuania, Portugal, Spain, Switzerland and the United Kingdom. The European Commission and Eurojust also joined. The second round of 21 additional public and private partners joined the project officially on 15 December. The online portal is now available in Dutch, Russian, French, Italian and Portuguese, in addition to English. Translations to yet more languages are currently ongoing, and their implementation will follow very soon.

The portal aims to help victims recover their data without having to pay cybercriminals after ransomware attacks. The users can download decryption tools that have been

created based on implementation errors from the criminals, reverse engineering of algorithms, law enforcement actions, or data leaked by criminals online. Victims only need to upload two encrypted files and the ransom note in order to check for available decryption solutions. The project also provides prevention information and links to report cybercrime to the respective national police forces.

7 Tips & Advice – How to Prevent Ransomware from Infecting Your Electronic Devices

Ransomware is malware that locks your computer and mobile devices, or encrypts your electronic files, demanding that a ransom is paid through certain online payment methods (and by an established deadline) in order to regain control of your data.

Ransomware can be downloaded through fake application updates or by visiting compromised websites. It can also be delivered as email attachments in spam or dropped/downloaded via other malware (i.e. a Trojan).

It is a scam designed to generate huge profits for organised criminal groups. To prevent and minimise the effects of ransomware, Europol's European Cybercrime Centre advises you take the following measures:

DOS

REGULARLY BACK UP THE DATA STORED ON YOUR COMPUTER.

Full data backups will save you a lot of time and money when restoring your computer. Even if you are affected by Ransomware, you will still be able to access your personal files (pictures, contact lists, etc.) from another computer. There are a number of high quality data backup solutions available on the internet for free.

REPORT IT.

If you are a victim of Ransomware, report it immediately to your local police and the payment processor involved. The more information you give to the authorities, the more effectively they can disrupt the criminal infrastructure.

CONSULT YOUR ANTI-VIRUS PROVIDER ON HOW TO UNLOCK AND REMOVE THE INFECTION FROM THE DEVICE.

There are numerous official websites and blogs with instructions on how to safely remove this type of malware from your electronic devices. Always consult www.nomoreransom.org to check whether you have been infected with one of the Ransomware variants for which there are decryption tools available free of charge.

DON'TS

TAKE ANYTHING FOR GRANTED.

If a website warns you about obsolete software, drivers or codecs (programs that encode and decode your data) installed on your computer, do not fully trust it. It is really easy for criminals to fake company and software logos. A quick web search can tell you if your software is really out of date.

INSTALL OR RUN NON-TRUSTED OR UNKNOWN SOFTWARE.

Do not install programs or applications on your computer if you do not know where they come from. Some pieces of malware install background programs that try to steal personal data – for more information on this, see our information sheet on Identity Theft.

DO NOT PAY OUT ANY MONEY.

Paying does not guarantee that your problem will be solved and that you will be able to access your files again. In addition, you will be supporting the cybercriminals' business and the financing of their illegal activities.

An infographic with the same information is available for download from the Europol website at: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/tips-advice-to-prevent-ransomware-infecting-your-electronic-devices