HOW TO PROTECT YOURSELF AGAINST RANSOMWARE

Ransomwares are going global! How to hold them back? Better be safe than sorry - PREVENT!

Ransomwares became a serious threat. And because today's business is data-driven companies are particularly threatened by this kind of cyber-attacks. Once it's happened even well-established companies rank big losses.

Unless they are prepared and have some backup plan (both literally and figuratively).

Malware, classified today as ransomware (combination of words ransom and software) became a widely discussed topic already a few years ago. In 2013, the most famous virus belonging to this category – CryptoLocker – allowed its creators to "earn" as much as 27 million dollars during its first attack. According to the estimations of McAfee Labs, during one campaign of sending CyptoLocker criminals are able to get even 325 million dollars. Even FBI did not avoid the attack and ransom demand.

So what is ransomware? Its name already contains a very good explanation. It is a type of malware which aims at extorting money from its victim. Virus attack consists in blocking the access to files, documents or even entire computer or company server. All data the access to which is blocked by this type of malware is usually encrypted and on the screen, the owner of precious files can see the instructions what they should do in order to have them recovered. Cybercriminals usually demand money to be transferred into their bank account and in exchange they promise to provide the victim with the key as well as instructions how to decrypt the data. More and more frequently, Bitcoin digital currency platform is used to get the ransom. It makes it possible for cybercriminals to avoid official circulation of money. It is safer for them and often makes it impossible for the police to discover who has actually been responsible for the attack.

RANSOMWARE TYPES

Different types of ransomware are currently known. The first one is the so called screen-locker. Malware makes it impossible for the user to access the device by blocking its screen. It is quite irritating but it is possible to get rid of this malware on our own if the victim has sufficient technical knowledge or antivirus package.

As this type of ransomware turned out not to be effective enough for the purposes of money extortion, cybercriminals began to use crypto-ransomware malware type. It encrypts chosen file types, e.g. photos and Word documents on victim's local disc. More and more frequently it also encrypts files in different locations which it can access – including files on servers and in cloud. Then the key for data decryption is offered, which is

It takes two to tango

PHISHING + LACK OF KNOWLEDGE =

The statistics show that the the most frecuently to blame are phishing mails and unaware users who lack any security awareness.

- 46% SPAM and phishing e-mails
- 36% **Unaware users** (lack of knowledge)
- 7% Malicious websites
- 5% Web ads
- 3% Mobile applications
- 2% Other

transmitted by cybercriminals to the victim after making appropriate payment. Usually the ransom oscillates between 150 and 900 dollars.

Unfortunately, crypto-ransomware uses the same encryption type as software used for the protection of bank transactions or military communications. Files are encrypted with the use of AES 256 algorithms, so in reality they are impossible to be restored (unless you are prepared for the attack, but this is what comes next). It is estimated that crypto-ransomware is responsible for extortions of over a billion dollars per year. The third ransomware type is so called disk-encryptor. Unlike crypto-ransomware, disk-encryptor software encrypts the entire disc of a victim and in this way blocks the access to the entire computer, making it impossible to launch operational system.

Here the Spora virus should be mentioned. It appeared at the end of the year 2016. It functions in an atypical way. Ransomware almost always uses CnC (Command-and-Control) servers. Such server is responsible for generating private and public key. Ransomware installed on the computer downloads public key and uses it to encrypt data. Private key, used for decrypting information, is all the time stored by the CnC server and the victim gains the access to it after paying the ransom.

Spora attacks its victims without contacting from CnC servers and the files are encrypted offline. It uses public RSA key, embedded in the software, but it does not use it to encrypt files stored on the victim's computer, but to encrypt the unique AEX key, which is generated locally on the victim's computer. In order to pay the ransom, the victim has to send the encrypted AES key to the website specified by cybercriminals. Then they use private RSA key to decrypt AES key and send it back to the victim, who can now decrypt their files.

DANGER LURKS EVERYWHERE

In the majority of cases our computer gets infected with ransomware after opening the attachment to e-mail or clicking the link redirecting to a specially prepared website. Cheaters know different psychological methods how to make us open the attachment or click the link. It can be e.g. the information about courier delivery or tax arrears, or a funny video with a cat or a link to naked photos of a celebrity. In this way, we are encouraged to open the attachment containing dangerous software or click the link directing us to virus installer. According to the Trend Micro company, 60% of ransomware is hidden in regular multimedia files. What is worse, antivirus software is not always able to discover such attack.

Ransomware is also transmitted by malicious pop-up advertisements in web browsers, through websites, usually those containing pornographic content or illegal software, or external data carriers can be used, such as USB keys. In the last example, the attack is very often aimed at a particular victim – person or company. Creators of ransomware also attach their malicious software to pirate content which computer users are eager to download from torrents or websites with warez or films, music and TV shows.

However, one may not feel secure even if they do not visit any suspected websites at all and it is confirmed by the fact that ransomware was also

„Two biggest ransomware outbreaks in history…"

WannaCry

A ransomware cryptoworm responsible for a May 2017 worldwide cyberattack, which targeted computers running the Microsoft Windows OS.

According to Kaspersky Lab, the four most affected countries were Russia, Ukraine, India and Taiwan, but the worm have hit around 200,000 computers across 150 countries. The attack affected many companies - Telefónica, Fedex, Deutsche Bahn and even National Health Service hospitals in England and Scotland.

ExPetr/Petya/NotPetya

A major global cyberattack began on 27 June 2017. Ukrainian companies were among the first to state they were being attacked. During that day the radiation monitoring system at Ukraine's Chernobyl Nuclear Power Plant went offline and several Ukrainian ministries, banks and metro systems were also affected.

According to the Kaspersky Lab this variant of Petya worm was unable to actually revert its own changes. So there was never ever a slight chance to decrypt victims' disk... Even if a payment was made. That's why the data destruction motive seems to be the most likely.

How to beat ransomware? Good antivirus, precaution and of course BACKUP DONE ON REGULAR BASIS.

found on very popular news websites. Among websites which have already experienced a ransomware attack there are among others msn.com, nytimes.com, bbc.com, theweathernetwork.com or newsweek.com.

LIFE AFTER RANSOMWARE... BETTER PREVENT AND BE READY BEFORE MALWARE ATTACKS

It can be seen that cybercriminals are motivated by money and all computer users, without any exceptions, are vulnerable. If you get attacked by a ransomware virus, first switch your computer off. Some malicious software first shows the message concerning infection and then it encrypts our files. In such case we can prevent the encryption of at least some data. Files should then be restored by connecting the disc to a different computer, which hasn't been connected to the network in order to eliminate for the virus the possibility to connect with the CnC server. Without this it is unable to encrypt files.

However, protection relies on good antivirus software and computer hygiene. Do not click in every link and do not open all attachments to your e-mails, on social networking sites as well as in communicators. We should also avoid logging in to the account with administrator privileges. On a daily basis we should work from the user account and the administrative account should be used only when necessary – for example for software installation.

In the company it is necessary to correctly assign permissions to the resources of company network and company cloud made available to the users. Providing company managers with the access to all company resources constitutes a very common mistake. These people are the most frequently at the risk of personalized attacks of cybercriminals and it has frequently been the case during ransomware attacks that all files with documents on all company servers and in all locations were encrypted from CEO's laptop, thus paralyzing company's activity for a few days, until the ransom was paid.

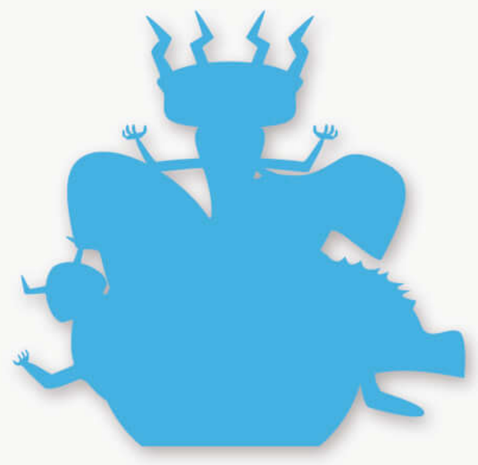
Act before it is TOO LATE

1. Ransomware usually spreads by phishing mails, through malicious attachments like .zip, .pdf, .doc, .exe or.js files (and many more).

2. Locker ransomware uses asymmetric encryption which can be extremely difficult or even impossible to crack.

3. Because ransomware attack are mostly designed to make an easy money, new malwares are becoming more and more dangerous and sophisticated.

4. Victims are usually forced to pay a ransom in bitcoins, which makes tracing and prosecuting the perpetrators difficult.



BACKUP – YOUR DEFENSE LINE

Backup constitutes the best way to protect the company against ransomware attack. In case of the infection it is often much easier to format the entire hard disc and load the data from backup copy than to bother with removing the virus or paying cybercriminals. Backup enables fast and trouble-free going back to the moment before the attack. In addition, in such solutions as Xopero QNAP Appliance, which cooperates with QNAP NAS servers, it is possible to launch the image of restored computer in virtual environment from USB key. Image downloaded from the NAS server remains then in safe virtual environment, where we can without any problem check whether the restored data has been infected. Often before encrypting the data, ransomware for several days remains hidden on the victim's computer.

Automatic cloud backup constitutes a recommended solution. It is worth to remember that at the moment of the attack, data is encrypted in all locations accessible from the operating system level – including external and network carriers, including portable hard discs or NAS servers (when it comes to QNAP NAS, the functionality of system/data restoring from the snapshot prepared in advance turns out to be particularly useful). Cloud backup is not easily accessible from the user level. In this way, ransomware does not have direct access to backed up data.

For cloud backup, automatic tools performing the work for us are a good idea. We do not have to remember about physical backup activity as it will be performed in the background without our participation always at a given time or moment when the computer or network are not overloaded. Cloud backup systems Xopero Cloud and Xopero Cloud Personal are among others equipped with mechanisms of this type.

It is worth to remember that backup technology may without any problem provide protection against ransomware attack not only to the computers and laptops of subsequent users, but also to servers – physical and virtual ones. In this way we are sure that in case of any trouble, we will overcome it without paying cybercriminals a single penny.

About us
XOPERO SOFTWARE S.A.

Xopero develops and produces a comprehensive range of professional tools for protecting and restoring critical business data. We are Europe's leading provider of data backup solutions. Our offer includes: appliance backup, local backup, cloud backup, mobile backup, disaster recovery and business continuity solutions.

We understand how important our client's data is to their business. We constantly develop and improve Xopero products to provide even better data protection, data security and business continuity. Our aim is to limit the risk of data loss and business downtime to zero.

Our customers reflect a wide range of business sectors: small to medium-sized organisations, large companies, public administration, banking and finance, education, medicine, telecommunications and IT.