What is ransomware?

Ransomware is a malware type of malware that cuts access to the system of a victim or to the personal files by keeping them “hostage” and demanding ransom payment to free them. As [1] states, the first time this type of attack was introduced was in the late 80s, and ransom was payed through post. Today the technology advanced so the authors demand payment in cryptocurrency or credit card.

According to [2] a categorization of ransomware by the means used is described, as seen in the source the ransomware can range from mild to dangerous:

First category is Scareware, which includes rogue software and scams. The victim may receive messages that malware has been detected and they need to pay in order to eliminate these messages. This is just an attempt in scaring the victim, but the files are safe. The messages will continue but it’s no need to worry more.

Another category are the screen lockers, which are at terror level. When infested with this type of malware, the victim is locked out of his computer entirely. The hackers use FBI or another Department of Justice logo to announce that illegal activity was found on the device and that a fine must be paid.

Lastly, they talk about the encrypting ransomware, which is the most damaging ransomware type from all. In this case the hackers capture your files and encrypt them and demand payment from the victim in order to give the files back. This type is so dangerous because nothing can restore the files, only if you pay, but even then, you cannot be sure you get the files back – for the most part even after payment the files are gone.

Talking about categories, in [1] and [3] more possibilities to divide the ransomware are suggested.

They divide this malware by propagations and by payment method. The first method is divided in three types, that are: Exploitation Kits, so pre-packed bundle of tools, Affiliate Programs, where outsourced code is developed and propagated and lastly Malvertising Campaigns, where spam emails target different users. Moving on to the second category of classification, by payment, [1] and [3] agree that there are two ways to pay, first through Direct Payment and second trough Indirect Payment, as pre-paid vouchers for example.

As mentioned above ransomware was introduced in the 1980s and it is known as PC Cyborg or AIDS. This would encrypt the C: partition after a certain amount of device restart and demanded to the victim to send the money ($189) per post. The encryption was simple, so it was easy to reverse it and it represented no danger.

When the world started to be affected by ransomware, and then later re-introduced to this expression, the victims where regular people with individual systems. Later only the criminals realized the potential of the ransomware and started going after businesses. They inflected a lot of damage in the business branch resulting in data loss and dropping productivity.

In the current times from the end of 2016 more than 10% of all the global malware detections were categorized as ransomware.

What to do if infected?

There are many different ways how you can get infected, the most common is through evil spam mails, which can include booby-trapped malware hiding attachments.

If you get infected, remember never pay the ransom, this advice is supported by the FBI, and other agencies which fight ransom demands. By paying all we do is encourage the attackers to keep holding our systems and files “hostage”. The problem is that even if we pay, there are thousands of ways to encrypt files and not all have decryptions, so the danger lies there that we could encrypt our files further by using the wrong decryption software.

Another way to protect yourself is to install security products which scan your computer and remove the threat. Maybe the files won’t be restored, but at least the problem is gone.

Because the ransomware re-appeared, a couple of information security organizations as well as law enforcement agencies have been raising awareness about this threat. Under these agencies important to note are the No More Ransom Project, which is created by the National High-Tech Crime Unit of the Netherlands’ police and Europol’s European Cybercrime Centre in coordination with two security companies Kaspersky Lab and McAfee. Another important mention is the FBI Ransomware Prevention & Response project, where the Federal Bureau of Investigation has created special sections to educate people about ransomware threats. Lastly, same as the US initiative, in the UK the National Cybercrime Security Center has been created, this includes dedicated webpages where the citizens get information, support and help other people by raising awareness about this topic.

How to protect yourself against it?

First thing is to invest in security software which can shield even the vulnerable software from malware.

Keep your files secure, with regular back-ups, either on cloud, where encryption is an important factor or on encrypted external hard drives.

Lastly, you need to make sure your software and apps are updated. Update means that bugs and vulnerable backdoors have been fixed and these are safer now.

Most important is to educate yourself and stay informed. Learn how to detect the malicious programs and apps and help others learn too.