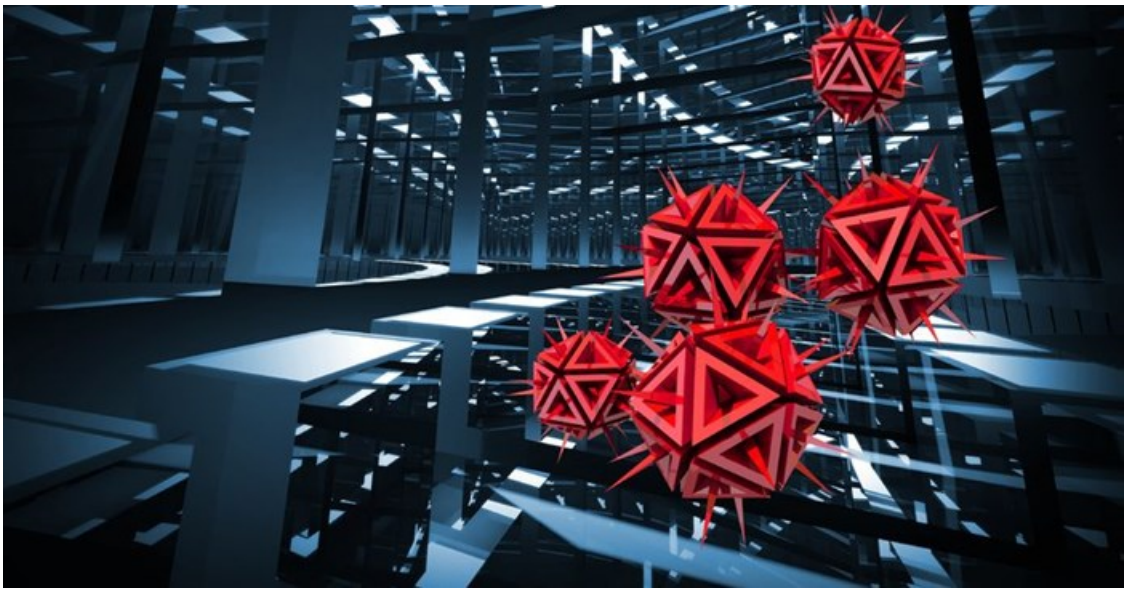
# Crypto-ransomware approaches epidemic status

The number of users attacked with encryption ransomware is soaring, with 718,536 users hit between April 2015 and March 2016: an increase of 5.5 times compared to the same period in 2014-2015. The irreversible consequences of this kind of malware infection, along with the high value data that is being encrypted by ransomware tempts victims to pay for decryption, which in turn draws more cybercriminals into the business.



©Eugene Sergeev via 123RF

It's no secret that crypto-ransomware, which encrypts data on users' systems has become a huge problem for cybersecurity over the last few years. It has become so widespread that it could easily be called an epidemic. In order to accurately understand its scale, Kaspersky Lab has researched how the ransomware threat has evolved over a period of 24 months. The company's analysis includes attack statistics for classic screen-blocker ransomware as well as crypto-ransomware.

The report covers the full two-year period, which for comparison reasons has been divided into two parts of 12 months each: from April 2014 to March 2015 and from April 2015 to March 2016. These particular timescales were chosen, because they witnessed several significant changes in the ransomware threat landscape. Here are the key points revealed by the research.

## Report results

The total number of users encountering any type of ransomware between April 2015 and March 2016 increased by 17.7% compared to the period April 2014 to March 2015 (from 1,967,784 to 2,315,931 users around the world). The number of users attacked with crypto-ransomware rose 5.5 times (from 131,111 in 2014-2015 to 718,536 in 2015-2016). The share of users encountering ransomware at least once as a proportion of the total number of users encountering malware rose from 3.63% in 2014-2015 to 4.34% in 2015-2016.

The share of users encountering crypto-ransomware as a proportion of those encountering ransomware rose dramatically – up 25 percentage points, from 6.6% in 2014-2015 to 31.6% in 2015-2016. At the same time the number of users attacked with blockers (ransomware that locks screens) decreased by 13.03%, from 1,836,673 in 2014-2015 to 1,597,395 in 2015-2016.

In 2015 Kaspersky Lab's solutions protected 443,920 users and corporate customers worldwide from crypto-ransomware. Knowing both the share of protected users who would agree to pay, and the average ransom amount, it is easy to calculate that in 2015 Kaspersky Lab saved $53 million for its clients.

"The biggest problem with crypto-ransomware today is that sometimes the only way to get the encrypted data back is to pay the criminals, and victims tend to pay. That brings a lot of money into the underground ecosystem that has grown up around this malware, and as a result we are seeing new cryptors appear almost daily. Companies and regular users can protect themselves by implementing regular backups, using a proven security solution and keeping themselves informed about current cybersecurity risks. The ransomware business model seems to be profitable and safe for criminals, and the security industry and users can change that just by implementing these basic measures," said Fedor Sinitsyn, senior malware analyst at Kaspersky Lab.

As crypto-ransomware is one of the most dangerous types of malware ever created, and the consequences of it can be very severe, Kaspersky Lab offers advice on how to protect yourself or your organisation against this threat.

## Tips for consumers:

• Back-up is a must. The sooner back-up becomes yet another rule in your day-to-day PC activity, the sooner you will become invulnerable to any kind of ransomware.

• Use a reliable security solution. And when using it do not turn off the advanced security features which it most certainly has. Usually these are features that enable the detection of new ransomware based on its behaviour.

• Keep the software on your PC up-to-date. Most widely-used applications (Flash, Java, Chrome, Firefox, Internet Explorer, Microsoft Office) and operating systems (like Windows) have an automatic updates feature. Keep it turned on, and don't ignore requests from these applications for the installation of updates.

• Keep an eye on files you download from the internet and receive via email. Especially from untrusted sources. In other words, if what is supposed to be an mp3 file has an .exe extension, it is definitely not a musical track but malware. The best way to be sure that everything is fine with the downloaded content is to make sure it has the right extension and has successfully passed the checks run by the protection solution on your PC.

• If, for some reason your files are encrypted with ransomware and you are asked to pay a ransom, don't pay. Every bitcoin transferred to the hands of criminals builds their confidence in the profitability of this kind of cybercrime, which in turn leads to the creation of new ransomware. At the same time, a lot of security companies fight ransomware on daily basis. Sometimes it is possible to create a decryption tool for certain kinds of ransomware, and sometimes as a result of cooperation with law enforcement agencies, it becomes possible to get the encryption keys for certain families of ransomware, which can eventually lead to decryption of your files.

Last but not least: the creation, spreading and demanding of a ransom for decryption are all actions that are defined as criminal in most countries around the globe. Report an attack to the police in order to start an investigation.

## Tips for businesses

• Back-up is a must. Upon the infection of your corporate PCs, the ransomware is likely to start encrypting files that are required for the daily work of your company. If it is technically impossible to back-up all the files you have in the corporate network, choose the most critical (accounting documents, clients' data, legal documents etc.), isolate them and back-up regularly.

• Use a reliable, corporate-grade security solution and don't switch off its advanced features, as these enable it to catch unknown threats.

• Undertake regular patch management.

• Educate your personnel: very often the ransomware infection happens due to a lack of knowledge about common cyberthreats and the methods criminals use to infect their victims.

• Avoid paying a ransom and report the attack to police.