Fighting ransomware and other cryptors on workstations and servers

No Stone Unturned

kaspersky

Learn more on kaspersky.com

Fighting ransomware and other cryptors on workstations and servers

Crypto-malware is one of the most dangerous types of malware, capable of causing considerable damage to businesses of every size through denial of access to working data.

Crypto-ransomware in particular has become a very popular form of attack over the last few years. Attackers don't even have to bother stealing and selling the data that your business relies on – they just encrypt it and demand a ransom from you.

Crypto-malware has evolved, paving the way for highly sophisticated, targeted blackmailing operations. Recognizing the destructive potential of cryptors, cybercriminals started to experiment, creating full-disk cryptors (like ExPetr), worm-like self-propagating strains (such as WannaCry) and many more new cryptor families.

The message is clear: You can't afford to leave any stone unturned in the fight against crypto-locker attacks.

Why are cryptors such a problem?

How do cryptors work, and why they are so lethal? Cryptors are a type of malware based on Trojans, which infiltrate when you open a malicious e-mail attachment or innocently follow a link to a specially created or compromised website. The module then quietly encrypts any data it finds that could be of value to you. This may include personal photos, archives, documents, databases, diagrams, etc. The cryptors then demand payment to decrypt these files and, depending on their nature, they may be capable of decryption after payment is made – or, in the case of cryptor wipers, they may just be mimicking a blackmailing scenario without having the means to decrypt at all.

In an actual criminal operation, anonymity is important to the attackers, so they may demand the ransom in Bitcoin or other cryptocurrencies, and their command and control servers may be hidden in the anonymous Tor network. If traffic is intercepted between the Trojan and its server, the use of unorthodox cryptographic schemes, such as Tor or custom encryption algorithms, makes its decryption impossible (Trojan-Ransom.Win32.Onion ransomware, for example, uses all these techniques).

Some ransomware cryptors demand payment not only for decrypting data but for additional 'services' too. For example, an attacker may raise the stakes with blackmail: "Pay up, or we will email your browsing history to all your contacts".

How widespread are cryptors?

During 2019, the total number of cryptor attacks detected by Kaspersky using the Kaspersky Security Network has stayed more or less the same compared to previous years. There are a number of reasons for this, including the fact that the market for cryptor-based blackmailing may be reaching maturity, and less enthusiasm for these methods among cybercriminals who have switched their attention to other areas such as web- and Trojan-based miners. Another factor is the targetization of ransomware operations; instead of mass spreading of crypto-malware, cyber-blackmailers focus on specific prominent targets that are thoroughly researched before being attacked. More affluent businesses which depend on particularly sensitive data are generally more likely to pay a ransom.

Ransomware detected (2014-2019)

Year	Unique KSN users reporting cryptor detections
2014	118029
2015	402210
2016	1388513
2017	785014
2018	757420
01-09.2019	603190
Grand Total	**3596796**

Cryptor detections – Top 10

Jan, 2019 – Sep, 2019 (inclusive)

	Name	Detection verdict*	No. of unique KSN users attacked
1	WannaCry	Trojan-Ransom.Win32.Wanna	135235
2	(generic verdict)	Trojan-Ransom.Win32.Phny	105805
3	GandCrab	Trojan-Ransom.Win32.GandCrypt	71130
4	(generic verdict)	Trojan-Ransom.Win32.Gen	39634
5	(generic verdict)	Trojan-Ransom.Win32.Encoder	30982
6	(generic verdict)	Trojan-Ransom.Win32.Crypmod	29371
7	Shade	Trojan-Ransom.Win32.Shade	16016
8	(generic verdict)	Trojan-Ransom.Win32.Crypren	15321
9	PolyRansom/VirLock	Virus.Win32.PolyRansom Trojan-Ransom.Win32.PolyRansom	14992
10	Stop	Trojan-Ransom.Win32.Stop	13533

As for the particular cryptor families, they demonstrate considerable diversity in their form, so even two samples originating from the same initial strain may yield different detections. More often than not, modern cryptors are detected by behavioral and machine learning-based mechanisms – hence the number of 'generic' verdicts in the Top 10.

Nevertheless, a couple of records deserve particular attention. The #1 place holder, the infamous 'WannaCry' cryptor worm, is likely to haunt global cyberspace forever – there always will be vulnerable systems it can infect.

GandCrab was another very successful cybercriminal operation until June 2019 when its owners decided they'd had enough – or was it thanks to the growing number of effective decryptors becoming available? – and announced they were shutting it down. Despite this, GandCrab's spread was so active (with some help from Ransomware-as-a-Service users) that it remains in the TOP3 for 2019.

Security Solutions

Despite all the advanced mechanisms implemented in malware nowadays, you can readily ease the crypto-malware threat to your business. Kaspersky's anti-cryptor approach employs a number of crypto-malware countermeasures.

Your **security solution should be turned on** at all times and with as many security layers enabled as possible. The solution **should also be up to date.**

It is currently impossible to decipher files properly encrypted by modern crypto-malware, so the only way to save your data from a successful attack is through some form of file backup. But a **general backup**, even conducted regularly, is not enough, because it leaves recently changed files unprotected, and risks overwriting by encrypted ones.

Endpoint security

Regular endpoints are the no.1 attack target for all kinds of cyberattacks, and the point where cryptors usually penetrate the system and start operating. Kaspersky understands this, and offers multiple security layers to mitigate the effects of cryptors.

* The statistics are based on Kaspersky products' detections. The information is provided by Kaspersky product users who have given their consent to share threat detection statistics.

Behavior analysis

This host-based subsystem analyzes relevant system event data, including information about the modification of files. On registering a suspicious application attempting to open a user's personal files, it immediately makes a local protected backup copy. If the application is found to be crypto-malware (or otherwise malicious), Kaspersky Behavior Analysis technology features a roll-back function that automatically reverses the unsolicited changes. All you see are notifications that this is happening – there is no disruption, and you don't need to take any action.

Kaspersky Behavior Analysis keeps users' data safe, and stops the indirect funding of cybercriminals through ransom payments, which feed the industry and fund the development of even more malicious software.

Application Control

Another host-based Kaspersky approach to mitigating the risk from crypto-malware is through creating Application Startup Control rules which prevent unauthorized applications from launching – which, naturally, includes executable crypto-Trojans.

Host-based Intrusion Prevention System (HIPS)

This subsystem allows the configuration of rules that would disallow applications having low trust levels to access certain resources within a system. By restricting access to sensitive file types (such as MS Office files, graphics, etc.), an administrator can reduce the chance of a cryptor succeeding considerably.

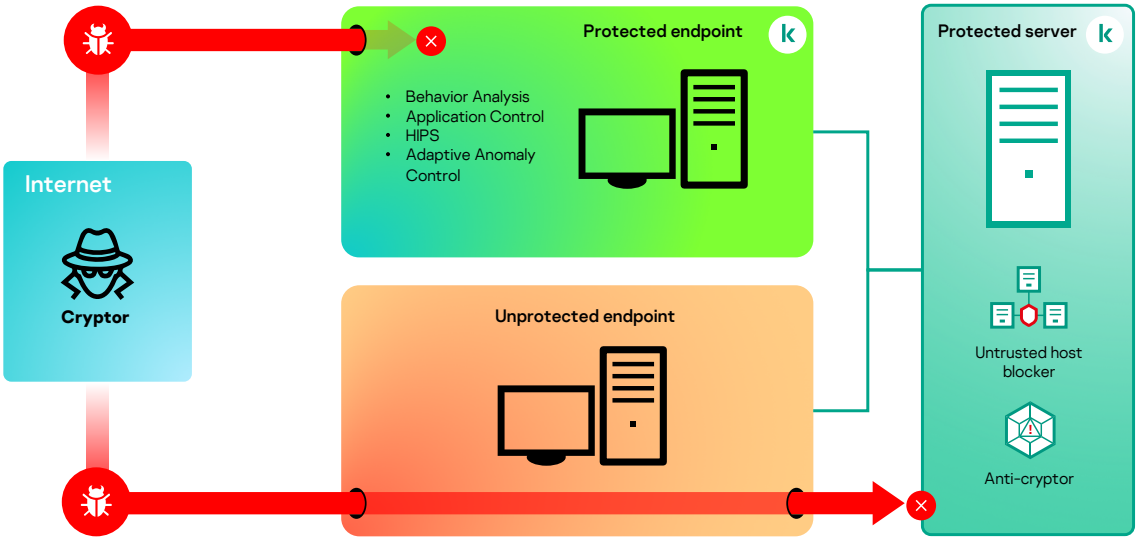
Adaptive Anomaly Control

The Adaptive Anomaly Control security layer reduces the likelihood of typical cryptor infection scenarios succeeding. Using machine learning, it recognizes and analyzes typical user behavior and patterns, so that any unusual user activity – a malicious email attachment of an unlikely type being opened, for example – is proactively blocked.

A server-based anti-cryptor solution

Some hosts inside the security perimeter may use shared SMB/CIFS folders on corporate servers or connected storage. And some scenarios restrict the use of full-scale multi-layered protection on endpoints, leaving them vulnerable to infection by cryptors. Some may be completely unprotected, or secured by other vendors' software which lacks anti-ransomware functionality. If this is the case, any cryptor penetrating via email or a vulnerable browser will also affect the shared folders on corporate servers and storage, reached via the network. In this situation, only specific **server- or storage-side security** software can protect the data.

AntiCryptor



Kaspersky anti-ransomware functionality is provided not just for endpoints, but also for Windows servers and some connected storage allowing API integration. Our Kaspersky Security for Windows Server application, used to protect both servers and storage[1], incorporates a layer of defense that was specifically developed to protect against cryptor threats. Watching over selected data folders, including shared files, it **compares the contents of every file before** and after any access attempt.Of course, the crypto-malware changes the contents of the file dramatically – it is encrypted! So this mechanism detects the effects of a cryptor and triggers a prevention mechanism.

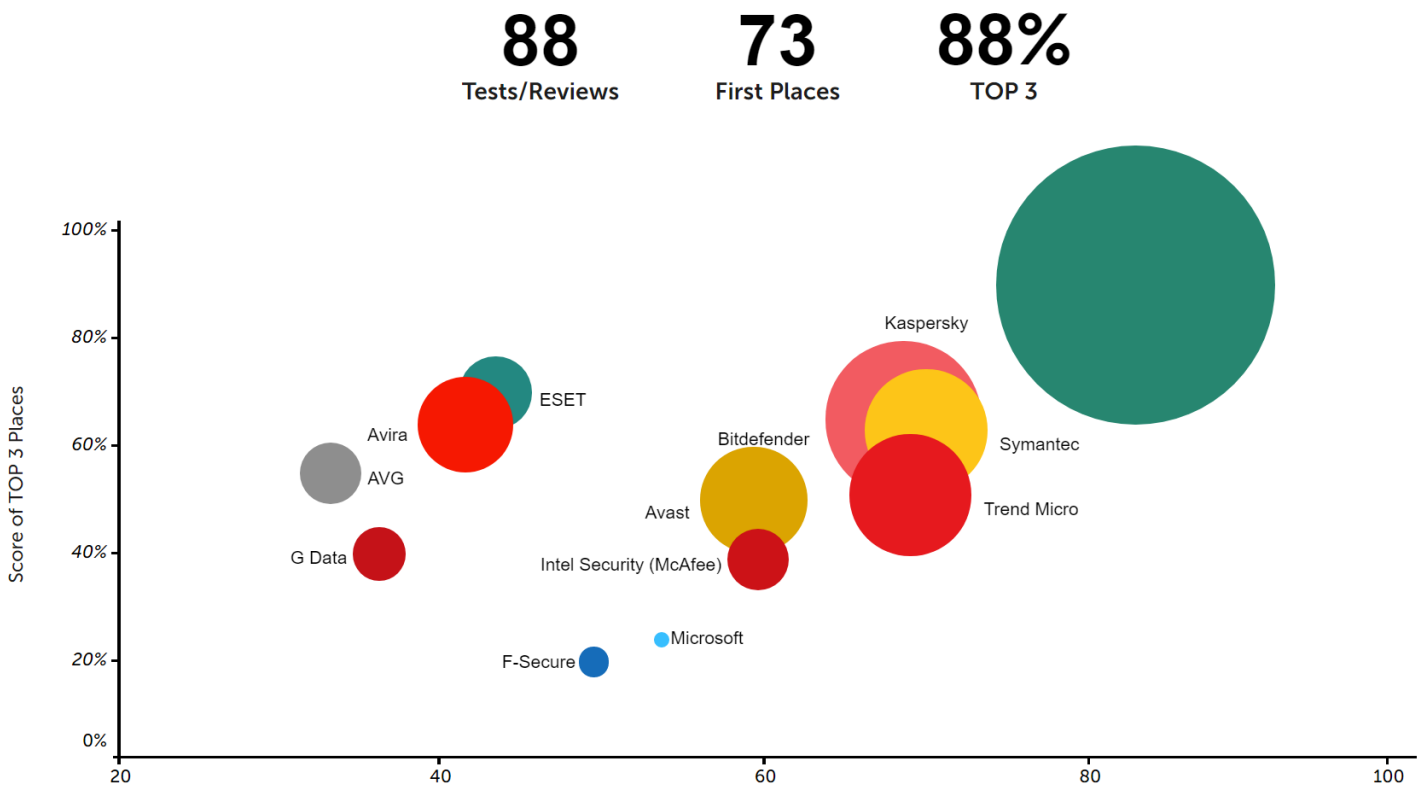
While SMB/CIFS protocols used to work with shared folders can't give us information about the process on the ransomware's host, we can obtain the host's IP address. Based on this information, the **Host Blocker** technology severs the network connection and includes the encryption-initiating machine address into the Untrusted Hosts list, thus preventing the infected host from engaging in any further activity with shared folders. After the infection is dealt with, the address can be removed from theblocking list.

Encrypting folders on some servers can be a legitimate part of an organization's security perimeter. Kaspersky Security for Windows Server **allows the administrator to add exceptions** for directories where such encryption is implemented.

Leaving no stone unturned – protection against ransomware with Kaspersky

The threat landscape is constantly developing, and Kaspersky is committed to keeping pace with every new threat, providing multi-layered security to protect our customers. We are ready to deal with crypto-malware on workstations and servers.

Kaspersky is constantly renewing and developing our arsenal of technologies powered by our proven Security Intelligence. We can also prove our performance claims through independent rest results and recognition by leading global industry analysts (TOP3).



In 2018, Kaspersky products participated in 88 independent tests and reviews. Our products were awarded 73 firsts and achieved 77 top-three finishes. Kaspersky was also again named as a 2018 Gartner Peer Insights Customer's Choice for Endpoint Protection Platforms.

See more information about the TOP3 metrics here:
www.kaspersky.com/top3

[1] Available in Kaspersky Hybrid Cloud Security for servers and Kaspersky Security for Storage for connected storage, respectively.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com

www.kaspersky.com