Fighting ransomware and other cryptors on workstations and servers

No Stone Unturned

kaspersky

Learn more at 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 denying the business access to its own 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, attackers have 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-malware 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 email 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 actual 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 any 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 if you don't want to see the confidential customer data you handle exposed to public view".

How widespread are cryptors?

Over the last couple of years, the total number of cryptor attacks detected by Kaspersky using the **Kaspersky Security Network** shown a slight decrease. This may be due to the fact that the market for cryptor-based blackmail may be reaching maturity, and a lack of enthusiasm for these methods among cybercriminals who have switched their attention to other areas such as web- and Trojan-based miners. Ransomware operations are also becoming more highly targeted instead of the mass spreading of crypto-malware, cyber-blackmailers now focus on specific prominent targets that are thoroughly researched before being attacked. Even though the attackers are not always capable of fulfilling their threats, public-facing businesses which depend on the processing of particularly sensitive data are more likely to yield to this kind of extortion.

Cryptor detections – Top 10

2020

	Name	Detection verdict*	No. of unique KSN users attacked
1	WannaCry	Trojan-Ransom.Win32.Wanna	80207
2	(generic verdict)	Trojan-Ransom.Win32.Gen	59233
3	(generic verdict)	Trojan-Ransom.Win32.Phny	43961
4	(generic verdict)	Trojan-Ransom.Win32.Agent	38039
5	(generic verdict)	Trojan-Ransom.Win32.Encoder	37358
6	Stop/Djvu	Trojan-Ransom.Win32.Stop	34609
7	(generic verdict)	Trojan-Ransom.Win32.Generic	29880
8	(generic verdict)	Trojan-Ransom.Win32.Crypren	21473
9	PolyRansom/VirLock	Virus.Win32.PolyRansom / Trojan-Ransom.Win32.PolyRansom	13022
10	Crysis/Dharma	Trojan-Ransom.Win32.Crusis	10993

2021 (January-May)

	Name	Detection verdict*	No. of unique KSN users attacked
1	WannaCry	Trojan-Ransom.Win32.Wanna	22151
2	(generic verdict)	Trojan-Ransom.Win32.Gen	14685
3	(generic verdict)	Trojan-Ransom.Win32.Phny	10238
4	(generic verdict)	Trojan-Ransom.Win32.Encoder	9505
5	(generic verdict)	Trojan-Ransom.Win32.Agent	8904
6	Stop/Djvu	Trojan-Ransom.Win32.Stop	4705
7	PolyRansom/VirLock	Virus.Win32.PolyRansom / Trojan-Ransom.Win32.PolyRansom	4333
8	(generic verdict)	Trojan-Ransom.Win32.Crypren	3452
9	(generic verdict)	Trojan-Ransom.Win32.Cryptor	2485
10	(generic verdict)	Trojan-Ransom.Win32.Crypmod	2003

Individual cryptor families can demonstrate considerable diversity in terms of two samples originating from the same initial strain may yield individual detections. More often than not, today's cryptors are detected by behavioral and machine learning-based mechanisms – hence the number of 'generic' verdicts in the Top 10 above.

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 will always be vulnerable systems it can infect.

The **Crysis / Dharma** family, known to researchers since 2016, was designed from the very start as a full-fledged Ransomware-as-a-Service offering. Despite its long history and the emergence of free decryption tools (such as Kaspersky's **RakhniDecryptor**) for some versions, it remains pretty popular, spawning new strains from time to time. Among its trademarks is the heavy use of hijacked RDP servers to spread infection: its earlier practice of using spam and web-based exploits for propagation seems to have been largely abandoned.

The **Stop / Djvu** family (also known as KeyPass ransomware) is known for its use of fake installers to propagate itself. There are as yet no signs of it using other vectors, but things can, of course, change, if its creators so choose. Despite its rather simplistic design and a clear decrease in the frequency if its appearances, Stop/Djvu remains in the Top 10. It's now fully automated, having moved on from its earlier incorporation of features designed for manual operation.

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

Security solutions

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

To take full advantage of these, 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 that have been effectively encrypted by today's 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.

Email and Internet Gateway Security

Emails and malicious downloads are among the primary delivery vectors for ransomware infections. As many attackers still rely more on foundational security flaws and social engineering rather than on programming and operational finesse, it makes sense to implement protection acting earlier on the killchain, seizing the chance to stop the threat before it makes to endpoint level. **Kaspersky Security for Mail Server** and **Kaspersky Security for Internet Gateway** are well up to the task, equipped with the latest detection techniques leveraging Machine Larning algorithms.

Endpoint security

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

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's 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 with low trust levels from accessing certain resources within a system. By restricting access to sensitive file types (such as MS Office files, graphics, etc.), an administrator can considerably reduce the chance of a cryptor succeeding.

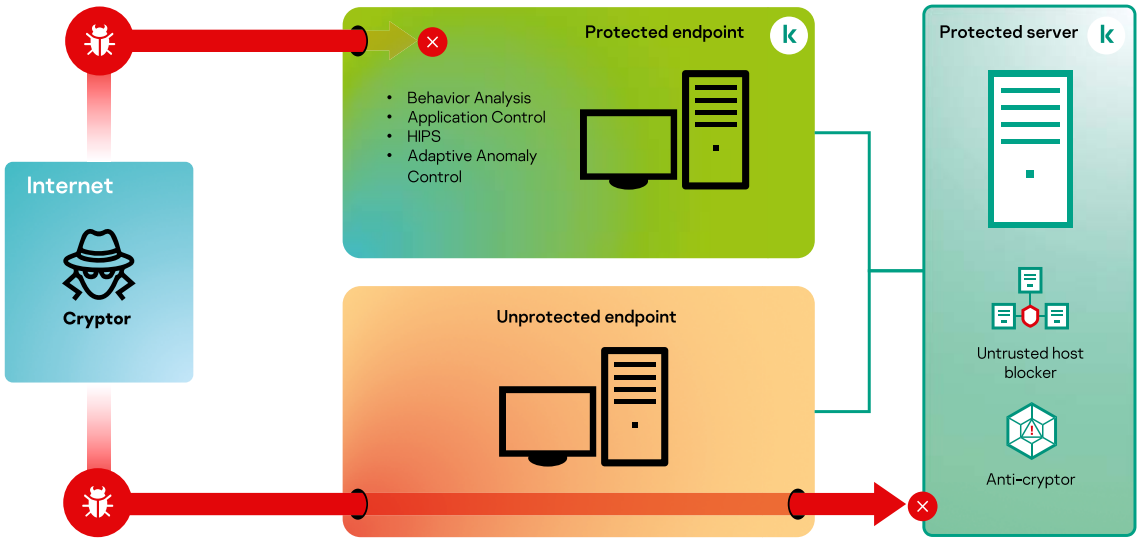
Adaptive Anomaly Control

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.

Anti-Cryptor



Kaspersky anti-ransomware functionality is provided not just for endpoints, but also for Windows servers and some connected storages, 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 strategy. Kaspersky Security for Windows Server **allows the administrator to add exceptions** for directories where such encryption is implemented.

Tackle targeted / combined cyberblackmailing

This scenario involves the use of a broader arsenal of tools brought along to stealthily explore the full extent of the attacked IT network, locate the most precious data and probably even grab something that can be later used in doxing, to fortify the claim. Do do this, dual-purpose (not inherently malicious) software is often used, which can be hard to detect without thoroughly customized detection policies. Another approach is about looking more closely at, say, *other things* surrounding the detection your endpoint security solution may have made.

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

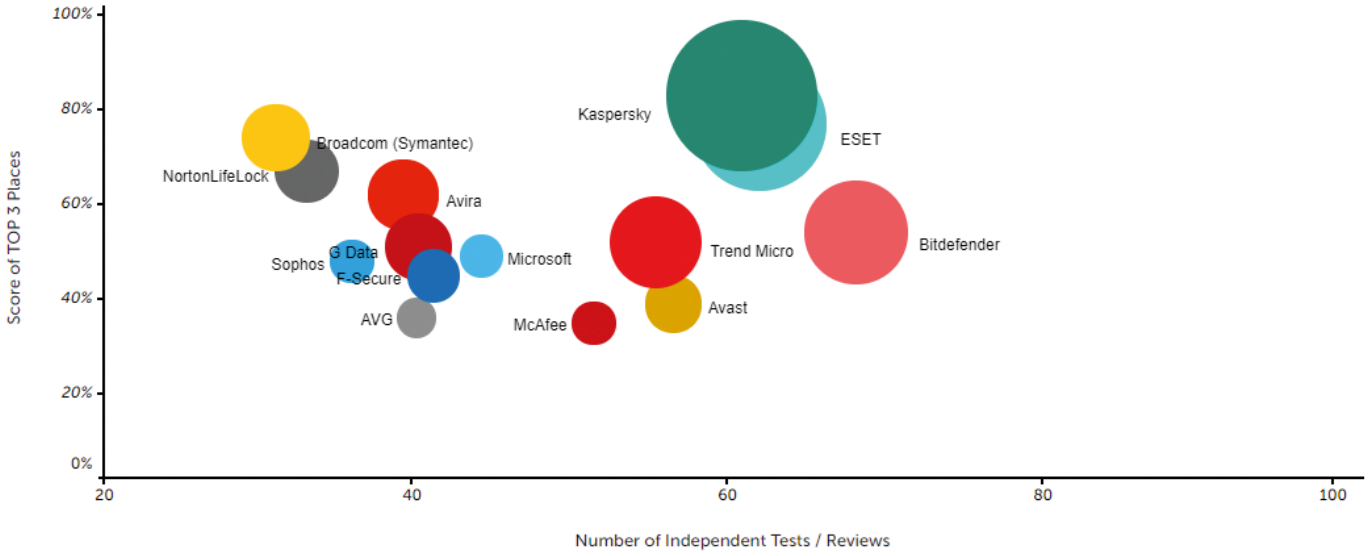
Kaspersky EDR Optimum is a next step beyond the Kaspersky endpoint security you might be familiar with. It offers convenient, easy-to-use tools allowing not only the exploration of circumstances and artifacts surrounding a particular detection – but also launching a response spanning multiple endpoints on the network. Today's ransomists are rumoured to be paying less attention to encryption and counting on doxing instead; this solution can easily become instrumental in profoundly disappointing them.

But, if you feel your company has become a prominent player on its market, controls a lot of sensitive data and is likely to attract high-level attackers, it is worth considering even more granular detection tools. Full **Kaspersky EDR** requires expert level skills - but mature enterprises tend to have dedicated ITSec departments or even a SOC, so it should not be a problem. But if you feed you don't have the required expertise (and/or time is also a factor), you can opt for **Kaspersky Managed Detection & Response** service. Both solutions allow to detect even the most stealthy activities - with the right knowledge about where and what to look for.

62
Tests/Reviews

45
First Places

81%
TOP 3



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 2021, Kaspersky products participated in 62 independent tests and reviews. Our products were awarded 45 firsts and achieved 81 top-three finishes. Kaspersky was also again named as a 2021 Gartner Peer Insights Customer's Choice for Endpoint Protection Platforms.

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

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

www.kaspersky.com