NO STONE UNTURNED: FIGHTING RANSOMWARE ON WORKSTATIONS AND SERVERS ALIKE

www.kaspersky.co.uk

Ransomware is one of the fastest growing classes of malicious software. Attackers don't even have to bother stealing and selling the data that you or your business relies on – they just encrypt it and demand a ransom. Over the years, ransomware has evolved from simple screen blockers demanding payment to a huge wave of far more dangerous software. You cannot afford to leave any stone unturned in the fight against crypto-locker attacks.

WHY IS RANSOMWARE SUCH A PROBLEM?

How does ransomware work, and why is it so lethal? This malware class is now based on **cryptors** – Trojans which infiltrate as you open a malicious e-mail attachment or innocently follow the link to a specially crafted website. The module then quietly encrypts any data it finds that could be of value to you. This might include personal photos, archives, documents, databases, diagrams, etc. The crypto-lockers then demand payment – often a significant sum – to decrypt these files again.

Clearly, anonymity at all times is important to the attackers. So payment may be demanded in Bitcoin, and the attackers' 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 using Tor or customary encryption algorithms, makes file decryption impossible (Trojan-Ransom.Win32. Onion, for example, uses all these techniques).

Nowadays, some crypto-lockers demand payment not only for decrypting the users' data but also for some additional "services". For example, the attacker may 'up the stakes' through blackmail: "Pay up, or we may be forced to mail your browsing history to all your contacts".

HOW WIDESPREAD IS RANSOMWARE?

	Ransomware detected (using Kaspersky Security Network)
2014	121238
2015	448430
Grand Total	**554267**

During 2015, the total number of ransomware attacks detected by us using the Kaspersky Security Network was almost four times higher than in 2014: nearly **four hundred and fifty thousand detections** in total. There are a whole raft of different types and families, such as CryptoWall, TeslaCrypt, TorrentLocker and Locky. CTB-Locker, ACCDFISA and GpCode were among the most notorious. Data from Kaspersky Security Network (below) gives an idea of the scale of different ransomware attacks throughout the European Union in 2015:

2015

Kaspersky Lab verdict	Unique users (KSN)	Unique users (KSN), combined	Other known aliases for this malware
Trojan-Downloader.JS.Cryptoload + Trojan-Ransom.Win32.Bitman	80017 1163	81180	TeslaCrypt
Trojan-Ransom.NSIS.Onion + Trojan-Ransom.Win32.Onion	16491 8571	25062	CTB-Locker
Trojan-Ransom.Win32.Cryptodef	7346	7346	CryptoDefense (early versions), CryptoWall (later versions)
Trojan-Ransom.Win32.Snocry	4998	4998	
Trojan-Ransom.Win32.Cryakl	4955	4955	
Trojan-Ransom.Win32.Crypren	1681	1681	
Trojan-Ransom.Win32.Shade	1390	1390	
Trojan-Ransom.Win32.Crypmod	1173	1173	
Trojan-Ransom.Win32.Rack	717	717	TorrentLocker
Trojan-Ransom.Win32.CryFile	395	395	

Locky, which may have been used in the recent ransomware attack on Hollywood Presbyterian Memorial Hospital, surfaced in mid-February this year, and has already emerged as one of the top ransomware tools in circulation.

TeslaCrypt, samples were first detected in February 2015, and the ransomware variant constantly mutates in its efforts to evade detection. TeslaCrypt has been widely portrayed in the media as the 'curse' of computer gamers because it targets many game-related file types (game saves, user profiles, etc.). The Trojan targets the US, Germany, Spain and other countries.

SECURITY SOLUTIONS

Despite all the advanced mechanisms implemented in malware nowadays, you can readily mitigate the threat of ransomware to you and your business. Kaspersky Lab's anti-ransomware strategy uses 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** (for example with Acronis or other specialised products), even conducted regularly, is not enough, because it leaves recently changed files unprotected, and risks overwriting by encrypted ones.

Host-based security

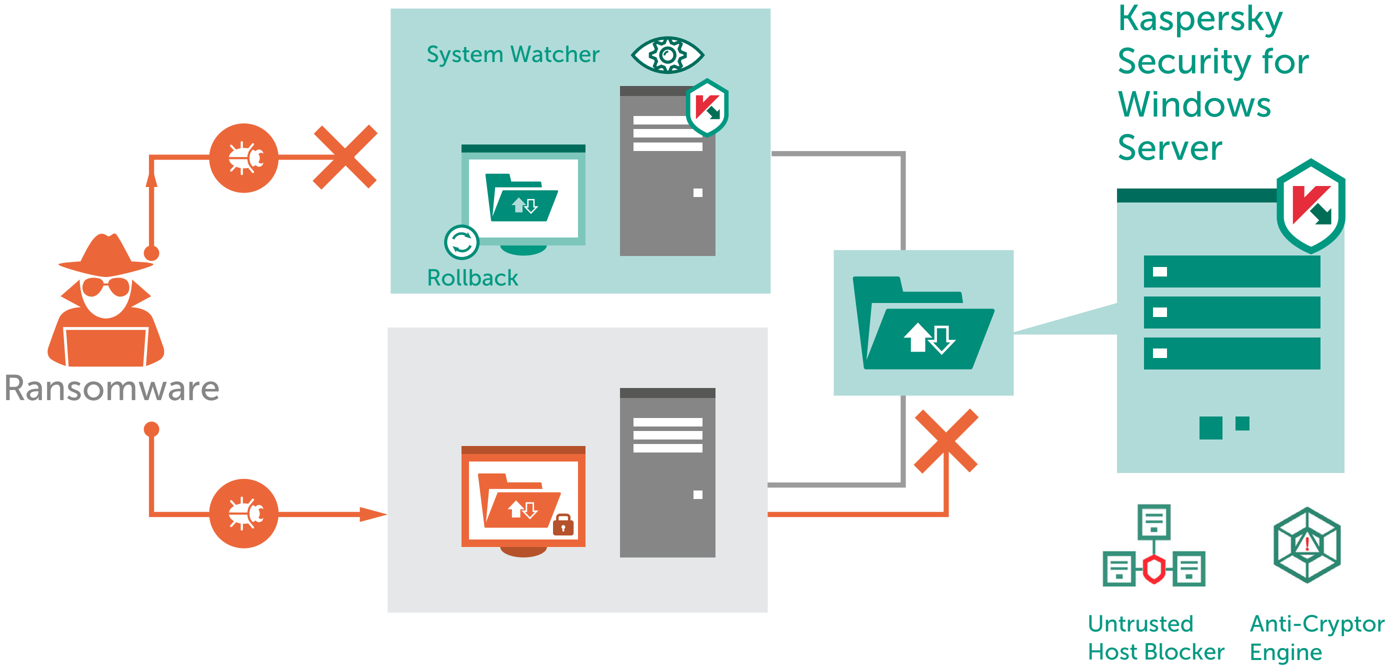
This is one reason why Kaspersky Lab products feature Kaspersky System Watcher technology. The host-based Kaspersky System Watcher analyses relevant system event data, including information on the modification of files. On registering a suspicious application attempting to open a user's personal files, it immediately makes a local protected backup copy. If the application is found to be crypto-malware (or otherwise malicious), Kaspersky System Watcher automatically rolls back the unsolicited changes. All you see are notifications that this is happening – there is no disruption, and no action need be taken.

Kaspersky System Watcher keeps users' data safe, and stops the indirect funding of cybercriminals through ransom payments, which feed the industry and prompt the creation of even more malicious software. Another host-based Kaspersky Lab approach to mitigating the risk from crypto-lockers is through creating Application Startup Control rules which prevent unauthorised applications from launching.

Server based anti-ransomware solution

Some hosts inside the security perimeter may use shared SMB/CIFS folders on corporate servers. And not every host has System Watcher enabled. Some could be even unprotected, or secured by other software which lacks anti-ransomware functionality. If so, any cryptor penetrating via email or a vulnerable browser will also affect shared folders on corporate servers. Under this scenario, only **server-side security software** can defend the data.

Kaspersky Lab anti-ransomware functionality is provided not just for endpoints, but is also for Windows servers. Our Kaspersky Security for Windows Server solution incorporates a new layer of defense, specifically developed to protect against cryptor threats. Watching over selected data folders – including file shares, it **compares the contents of every file before** and after any access attempt. Of course, the crypto-lockers' work changes the file contents dramatically – it is encrypted! So this mechanism will almost invariably detect the presence of ransomware and block its further execution.



In addition to **detection**, there is a prevention mechanism in Kaspersky Security for Windows Server. While SMB/CIFS protocols can't give us information about the process on the ransomware's host, we can obtain the host's IP address. **Host Blocker** technology can then prevent this infected host from engaging in any further activity with shared folders.

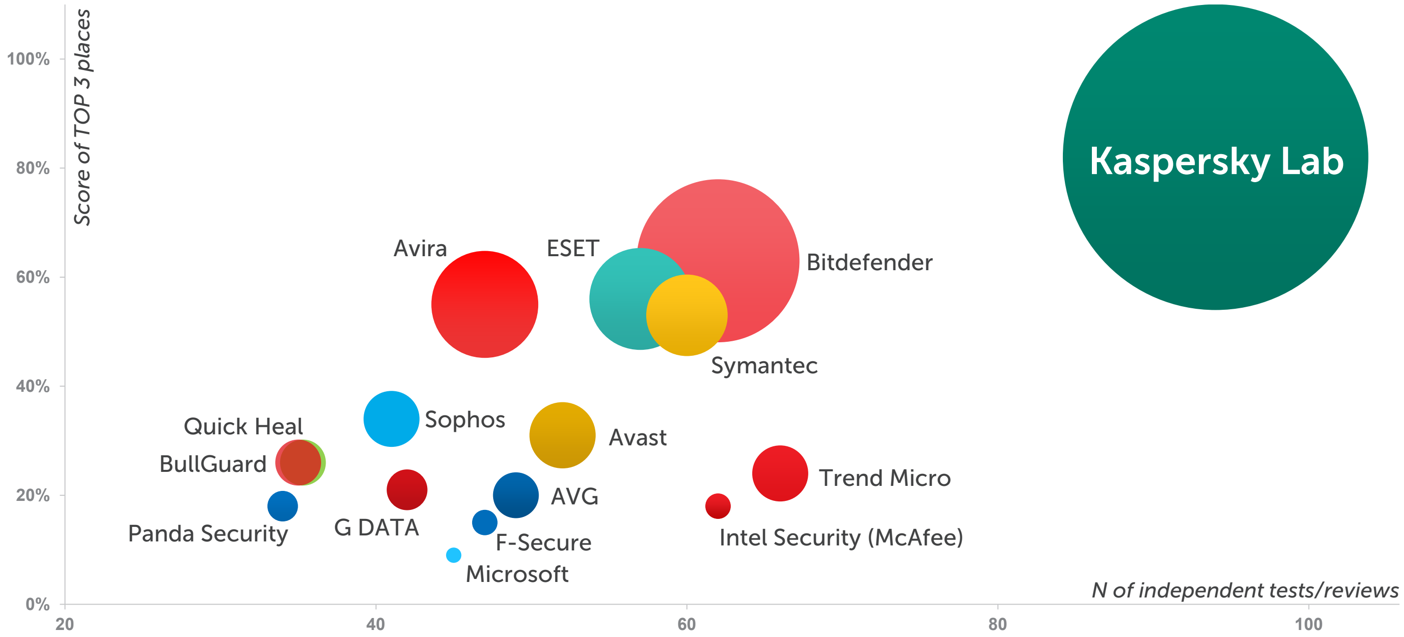
Encrypting folders on some servers can be a legitimate part of the organisation's security perimeter. Kaspersky Security for Windows Server **allows the administrator to add exceptions** for directories where such encryption is implemented.

Leaving no stone unturned – security against ransomware with Kaspersky Lab

The threat landscape is constantly developing, and Kaspersky Lab is committed to keeping pace with every new threat generation, providing multi-layered security to protect our customers. We are ready to mitigate the issue of ransomware both on workstations (Kaspersky System Watcher) and server-side (anti-ransomware technology implemented in the Kaspersky Security for Windows Server).

Kaspersky Lab constantly renews its arsenal of technologies powered by our proven Security Intelligence. And we also offer proof of our performance claims through of independent test results and the views of analytical agencies (TOP3).

In 2015 Kaspersky Lab products participated in 94 independent tests and reviews. Our products were awarded 60 firsts and achieved 77 top-three finishes.



See full information about TOP3 metrics here www.kaspersky.co.uk/top3

Twitter.com/
KasperskyUK

Facebook.com/
KasperskyLabUK

Youtube.com/
Kaspersky

Kaspersky Lab, London, UK
www.kaspersky.co.uk

All about Internet security:
www.securelist.com