

Advanced Endpoint Protection: Ransomware Protection test

The test was commissioned by Kaspersky and conducted by AV-TEST GmbH.
All rights to the test results and the report belong to Kaspersky.
Date of report: September 30, 2021

Executive Summary

In June-August 2021, AV-TEST carried out a test of ransomware protection offered by 11 different Endpoint Protection Platforms (EPP). In total, 113 different attacks were executed.

The three assessment scenarios were independently developed and executed by the test lab:

- Real-World ransomware attacks user files on local system
- Real-World ransomware attacks user files on remote shared folder
- Proof of Concept ransomware attacks user files on local system

During the test, the products were expected to detect ransomware activity and its files, block it, roll-back any changes to user files (the other words, to protect all user files) and eliminate the threat from the targeted system. Only these results were considered a true success and the relevant solution was given a credit in each test case.

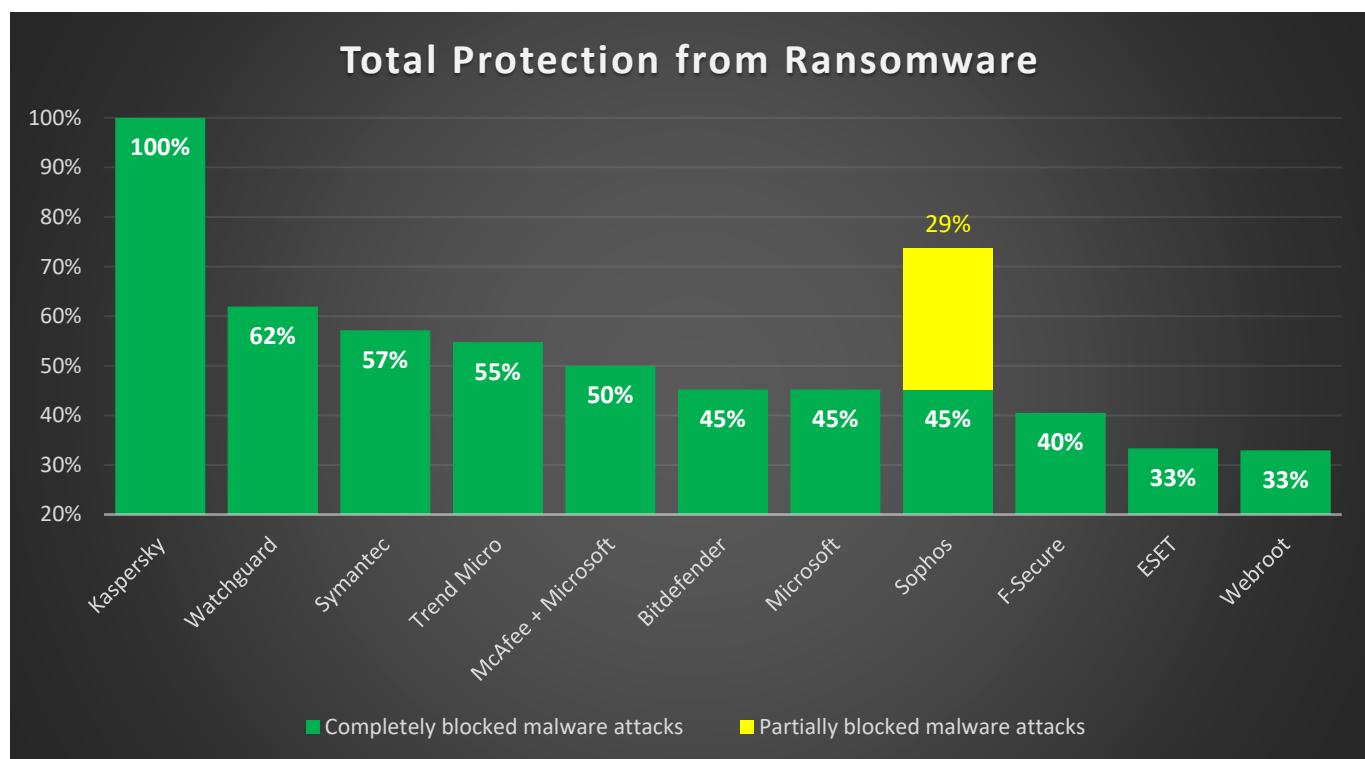


Figure 1. Total ransomware protection by different products basing on all three scenarios.

“Completely blocked” means that ransomware was detected, and all user files were protected.

“Partially blocked” means that ransomware was detected, but some user files were lost (not protected).

Arranged by “completely blocked” values.

Kaspersky Endpoint Security Cloud achieved the best results, protecting against 100% of all the ransomware attacks in the test (113 in total), without loss of a single user file.

The individual results of the three scenarios revealed a difference in the detection/protection capabilities of the products being tested.

On the one hand, all products scored very well when detecting malicious real-world samples on local systems, while 10 out of 11 products achieved a perfect result and only Webroot missed one test case, but also scored well with 98.8%.

On the other hand, the test with proof-of-concept samples showed significant differences in protection when the techniques are known to the vendors but not the samples itself. Four products protected against at least 50% or more of those test cases, Kaspersky again protected against 100% of the attacks followed by the solutions from WatchGuard, Trend Micro and McAfee + Microsoft Defender.

In addition, the scenario of ransomware attack on remote shared folders of protected systems reveals a significant difference in the protection capabilities of the tested solutions. Here, the same real-world ransomware samples which have the functionality to discover and encrypt remote shares folders are used. Only three products were able to protect user data from this kind of attack. Kaspersky again scored very well with 100% of the attacks. Symantec protected against 50% and Sophos against 7 % completely (whilst partially protecting against 86% of attacks, which means some user files were encrypted).

For more detailed information, please refer to the '[Test Results](#)' section of the report.

Content

Executive Summary	1
Content	3
1. Introduction	4
2. Test Methodology	4
2.1. Tested security solutions	4
2.2. Test scenarios and sample collections	4
2.2.1. Test scenario #1: Real-World ransomware attacks user files on local system	5
2.2.2. Test scenario #2: Real-World ransomware attacks user files on remote shared folder	5
2.2.3. Test scenario #3: Proof of Concept ransomware attacks user files on local system	5
2.3. Set of user files	6
2.4. Test execution	6
2.5. Scoring	7
3. Test results	7
3.1. Test scenario #1: Real-World ransomware attacks user files on local system	7
3.2. Test scenario #2: Real-World ransomware attacks user files on remote shared folder	8
3.3. Test scenario #3: Proof of Concept ransomware attacks on user files on local systems	9
Summary	10
Appendix 1. Description of real-world ransomware families	11
Appendix 2. Description of Proof of Concept ransomware samples	20
Appendix 3. Description of user file sets	21

1. Introduction

Targeted APT attacks have been a serious threat to companies and governments for many years. More and more targeted and complex technical attacks are being constructed to penetrate enterprise networks, to extract data or, in the case of ransomware, to encrypt it and demand outrageous payments to decrypt it. The recent trend of attacks weaponized with ransomware is to demand additional ransom for not publishing the extracted corporate data.

These attacks aren't just aimed at enterprise companies and government agencies – they're also directed at public institutions such as hospitals, and utilities like electricity and water suppliers.

It's critically important that all organizations protect their systems effectively and train their employees regularly, as it's no longer a matter of 'if' an attack occurs, but 'when'...

The aim of the test is the complex verification of the participating security solutions' ability to protect user data against ransomware attacks.

The main paradigm applied to the results: a security solution can be considered 100% efficient against a ransomware threat only if no single user file has been encrypted AND the ransomware threat is eliminated from the protected system. Only test cases with these results are considered a success by a particular solution in this research. It's completely irrelevant whether or not a solution made detections or how many user files were protected if even a single file was lost due to the ransomware.

The test preparation started in December 2020, and the test was conducted in June-August 2021.

This report was finalized on September 30, 2021.

2. Test Methodology

- The test has been carried out as described in this document.
- The report contains all results initially requested for testing. No valid test cases were excluded from the report.
- The results were independently verified.

2.1. Tested security solutions

The tested products are listed below. All the products were tested with their default configuration.

Product Name	Version
Bitdefender GravityZone Business Security	7.2.1.69
ESET Protect Entry	8.0.202.0
F-Secure Elements Endpoint Protection	21.6
Kaspersky Endpoint Security Cloud	11.6.0.394
McAfee Mvision + Microsoft Defender	5.7.33.245 + 4.18.2106.6
Microsoft Defender Antivirus ATP	4.18.2106.6
Sophos Intercept X Advanced	2.18.2
Symantec Endpoint Protection	14.3 RU2
Trend Micro Endpoint Security with APEX One	14.0.9672
WatchGuard Endpoint Security	8.0.18
Webroot Business Endpoint Protection	9.0.30.75

2.2. Test scenarios and sample collections

The assessment includes three scenarios.

2.2.1. Test scenario #1: Real-World ransomware attacks user files on local system

This basic scenario evaluates the efficiency of security solutions to:

- Protect local user files from being encrypted by real-world ransomware samples of different families, executed on the targeted host.
- Fully eliminate the ransomware (its file, related process (-es), AutoRun entries in the registry or other parts of the system).

Real-world ransomware collection of samples consists of 20 families, with a maximum of 5 samples each, so 85 samples in total.

The samples were selected independently, right before the test execution from real-time sources.

Ransomware samples from the following 20 real-world ransomware families were selected for this scenario:

conti, darkside, fonix, limbozar, lockbit, makop, maze, medusa (ako), mountlocker, nefilim, netwalker (aka mailto), phobos, PYSA (aka mespinoza), Ragnar Locker, ransomexx (aka defray777), revil (aka Sodinokibi or Sodin), ryuk, snatch, stop, wastedlocker

A detailed description of the ransomware families can be found in [Appendix 1](#).

2.2.2. Test scenario #2: Real-World ransomware attacks user files on remote shared folder

This enhanced scenario evaluates the efficiency of security solutions to protect local user files located on shared folders from being encrypted by real-world ransomware samples from different families, executed on a remote host.

This collection consists of 14 real-world families, represented by one sample each.

The number of real-world families is lower than in Scenario #1 because not all ransomware families have the functionality to attack (encrypt) user files on remote shared folders. The particular selected samples were additionally verified on the reference system for their ability to attack remote shared folders.

The following 14 real-world ransomware families were selected for this scenario:

avaddon, conti, fonix, limbozar, lockbit, makop, maze, medusa (ako), nefilim, phobos, Ragnar Locker, Ransomexx (aka defray777), revil (aka Sodinokibi or Sodin) and ryuk

A detailed description of the ransomware families can be found in [Appendix 1](#).

2.2.3. Test scenario #3: Proof of Concept ransomware attacks user files on local system

This enhanced scenario evaluates the efficiency of security solutions to:

- Protect local user files from being encrypted by proof of concept ransomware samples, executed on the local host.
- Fully eliminate the ransomware (its file, related process (-es), AutoRun entries in the registry or other parts of the system).

Each of these samples implements a different existing encryption technique potentially known to adversaries when they compile a targeted campaign. Although they are still not prevalent in the current

real-world ransomware landscape, their efficiency is easily verifiable. So it's extremely valuable for customers to know which security solutions can prevent this kind of ransomware.

Before the test, all test samples were created in the same way that attackers do in real life when they develop and compile the code right before they attack, to avoid detection by different security solutions by means of just a 'hash sum'.

The test set consists of 14 samples, each is represented by one sample. A detailed description of the ransomware families can be found in [Appendix 2](#).

2.3. Set of user files

To check the functionality of ransomware threats to find and encrypt user files and to reveal the ability of security solutions to prevent these attacks, a collection of user files was created and used for all the test scenarios. The collection is represented by different file types, multi-layered folder structure and file system locations on the targeted hosts.

Before the test, hash sums were calculated for each of the user files, and recorded.

After the introduction of each ransomware sample in each test scenario, the hashes of all user files were calculated again and compared with the hashes of the original user files. Only in cases where all hashes matched each other in the particular test-run was the security solution considered to be 100% efficient in protecting, and given a credit.

For the Real-World Shared test scenario, the test set consists of 20 files of 11 file formats, 11 folders and subfolders. And for the Real-World and POC scenarios, 153 files in 19 file formats and 4 folders.

A detailed description of the user files set can be found in [Appendix 3](#).

2.4. Test execution

The test was performed on virtual machines based on Hyper-V and the base VM was prepared with different user files (see [Appendix 3](#)) to encrypt by ransomware. All solutions tested were installed with their default settings. The scenarios were tested one after another. In between tests, the VMs were reset to start with a clean system every time.

During the test, it was ensured that the tested example ran successfully, encrypted the files if not blocked and, for documentation, screenshots were taken of the detections and the corresponding user folders were saved to check whether encryption took place and/or if they were protected from damage.

2.5. Scoring

For Test Scenario #1 (real-world samples) and Test Scenario #3 (proof of concept samples):

- Each security solution was given a credit in each separate test case only if all user files were protected (remained original at the end of the test run), and all ransomware traces (file, process, changes in registry and other system location entries) were eliminated. Such test cases were counted as “*Completely blocked malware attacks*”.
- In cases when some, but not all user files remained original at the end, this was noted as “*Partially blocked malware attacks*”, and no credit was given.
- In all other cases, no credit was given.

For Test Scenario #2 (real-world samples on shared folders) the approach is the same but without the requirement to eliminate traces of ransomware (file, process, changes in registry and other system location entries), because ransomware files are executed on a remote host, without a security solution being deployed on it.

3. Test results

3.1. Test scenario #1: Real-World ransomware attacks user files on local system

Figure 2 below shows the levels of protection of user files on local file systems where the real-world ransomware executed. Only test cases where 100% of user files were protected by the security solution, and the ransomware threat was eliminated from the system (process terminated, the file and its artifacts deleted), were considered a success and represented here.

Nearly all the solutions passed this test easily with 100% of protection. Only Webroot’s solution missed one ransomware threat and finished with 98.8%. All the results were considered as “*Completely blocked malware attacks*” – there were no cases of “*Partially blocked malware attacks*”.

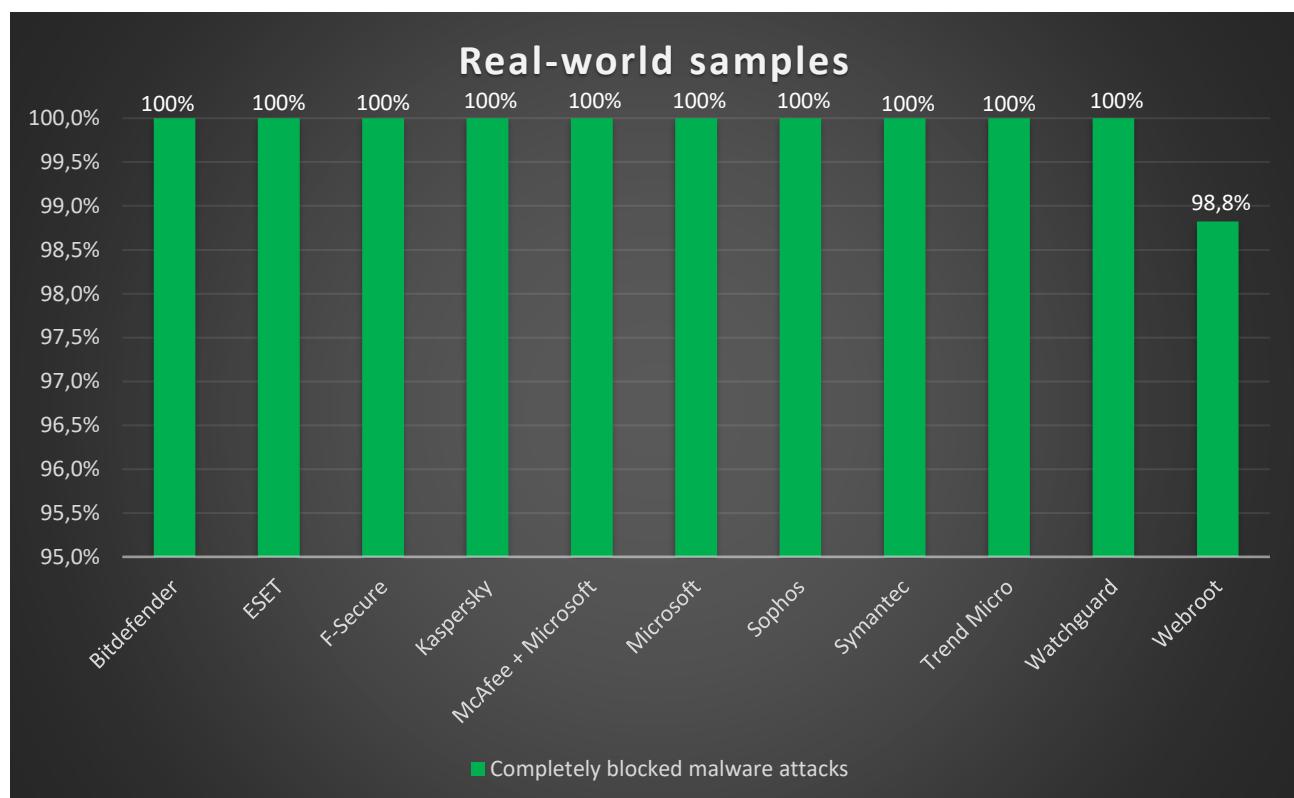


Figure 2. Protection level of local user files against real-world ransomware samples of different families.
Arranged by vendor name in alphabet order.

3.2. Test scenario #2: Real-World ransomware attacks user files on remote shared folder

Figure 3 below shows levels of protecting user files, located on local shared folders, against real-world ransomware executed on a remote attacking host. Only test cases where 100% of user files were protected by the security solution were considered a success, and represented as “*Completely blocked malware attacks*”. This means that in the rest of the test cases, security solutions turned out to be tolerant to sacrificing user files, up to 100%. Considering that any single encrypted file could be critically important for a user and the business, anything less than 100% protection against ransomware is unacceptable.

This test turned out to be a challenge for many of the security solutions.

Only Kaspersky proved to be 100% efficient in protecting all user files from all remote ransomware threats. Symantec protected user files from 50% of ransomware attacks, and Sophos from 7%. All the other solutions failed to protect user files.

Although system hardening by non-behaviour based technologies like Application Control is known to be marketed as a ‘silver bullet’ to protect user files on shared folders against remote threats, the reality looks different. Although Application Control is a resource-focused protection technique to harden application access to critical system resources, as soon as encryption on shared folders is executed by a system process, the technology doesn’t help.

Analyzing the results, we found 12 test cases out of 14 where the security solution from Sophos protected only part of user files, not the whole set (see Figure 4). Although the more user files are protected the better, it might not be enough to have anything less than 100% of user files protected. Imagine important project documentation, or a recent finance report, or a database with a recent significant update and no fresh backup copy being lost due to a ransomware attack – the amount of time and resources required to restore the data and resume operations would be substantial. Even a single lost file can be critical to a particular company or individual.

No other solutions protected just part of user files.

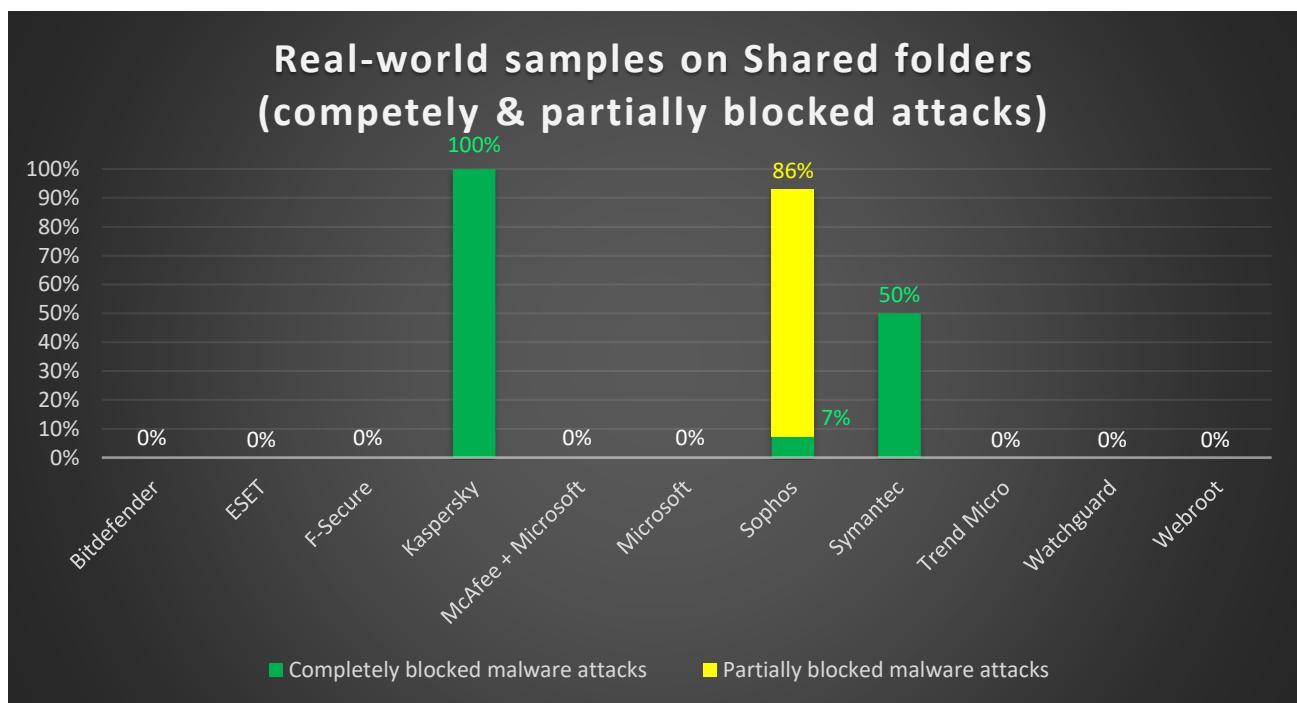


Figure 3. Protection level of local user files against real-world ransomware executed from remote attacking host.
Arranged by vendor name in alphabet order.

Analyzing the test scenario results, we discovered another very specific issue. Most of the solutions with Zero Protection (Bitdefender, Eset, F-Secure, McAfee, Microsoft, Trend Micro, WatchGuard) detected and deleted

text files with ransom messages, which were created by ransomware. From our point of view, this can cause dangerous consequences for the user, and we believe the vendors need to address the issue. These ransom text files could contain technical information valuable for the decryption process (for example, the encrypted key for decryption, etc). Having been attacked, the user may get in touch with the security vendor(s) asking for help with decryption. The security vendors may then use this information to classify the cryptor family, and make a judgment about the encryption algorithms used, searching for existing vulnerabilities in the encryption algorithm, to finally develop a decryptor utility. But if the ransom message text files have been eliminated, there is no option for the user to restore their data if no fresh backup copy is made. Furthermore, if the ransom message test files have been removed, dealing with law enforcement agencies to try and find the cybercriminals is significantly complicated.

Also, we believe that in a case of being attacked and not having ransom message text files deleted, users are advised to avoid making payments for ransom, if there are any other options still available. Only community avoidance of encouraging the ransomware industry by making payments will make it less profitable to sustain the number of attacks in general.

3.3. Test scenario #3: Proof of Concept ransomware attacks on user files on local systems

This test scenario reveals the readiness of security solutions to protect against ransomware attacks where malware developers start looking for alternative encryption methods or techniques. Even when some techniques are not popular or common, or even generally in use, this doesn't mean they are not already used in very narrow targeted attacks, or will not become popular in the future. Security solutions are expected to be ready to protect users in all conditions, no matter what the current threat landscape looks like.

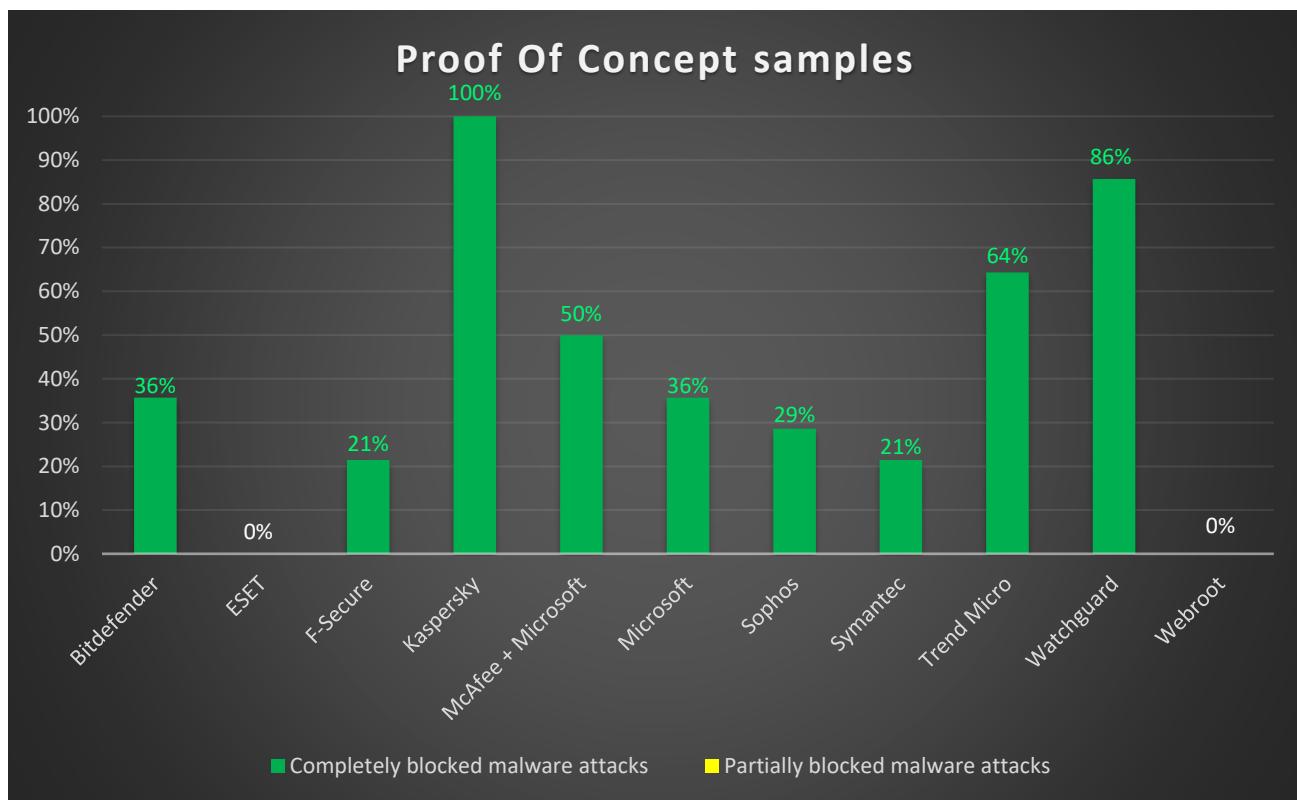


Figure 4. Protection level of local user files against Proof of Concept ransomware executed locally.
Arranged by vendor name in alphabet order.

Figure 4 represents the results of the security solutions in this test. Kaspersky has proven to be 100% effective in protecting from different encryption techniques. WatchGuard's solution managed to protect from 86% of attacks, and Trend Micro from 64% followed by combined solution from McAfee and Microsoft with 50%. And there is yet work for the other solutions to do. Bitdefender and Microsoft were able to detect just 36%. Sophos

detected 29% followed by F-Secure and Symantec with 21% each. Eset and Webroot were not able to detect the proof of concept files.

Summary

In this research, all tested products had to prove themselves in 3 scenarios.

In the first scenario “Real-world ransomware attacks user files on local system”, all products achieved a perfect or good score in protecting the local system against known real-world samples.

But if the same ransomware attacked user files on a remote shared folder (the second scenario), it proved more difficult for some of the security products to detect and prevent such cases. Only Kaspersky protected the system completely, while Symantec and Sophos provided some protection.

Attacks by Proof of Concept ransomware (the third scenario) showed how difficult it was to make generic decisions based on the behavior of an attack. Kaspersky scored perfectly again, followed by WatchGuard and Trend Micro.

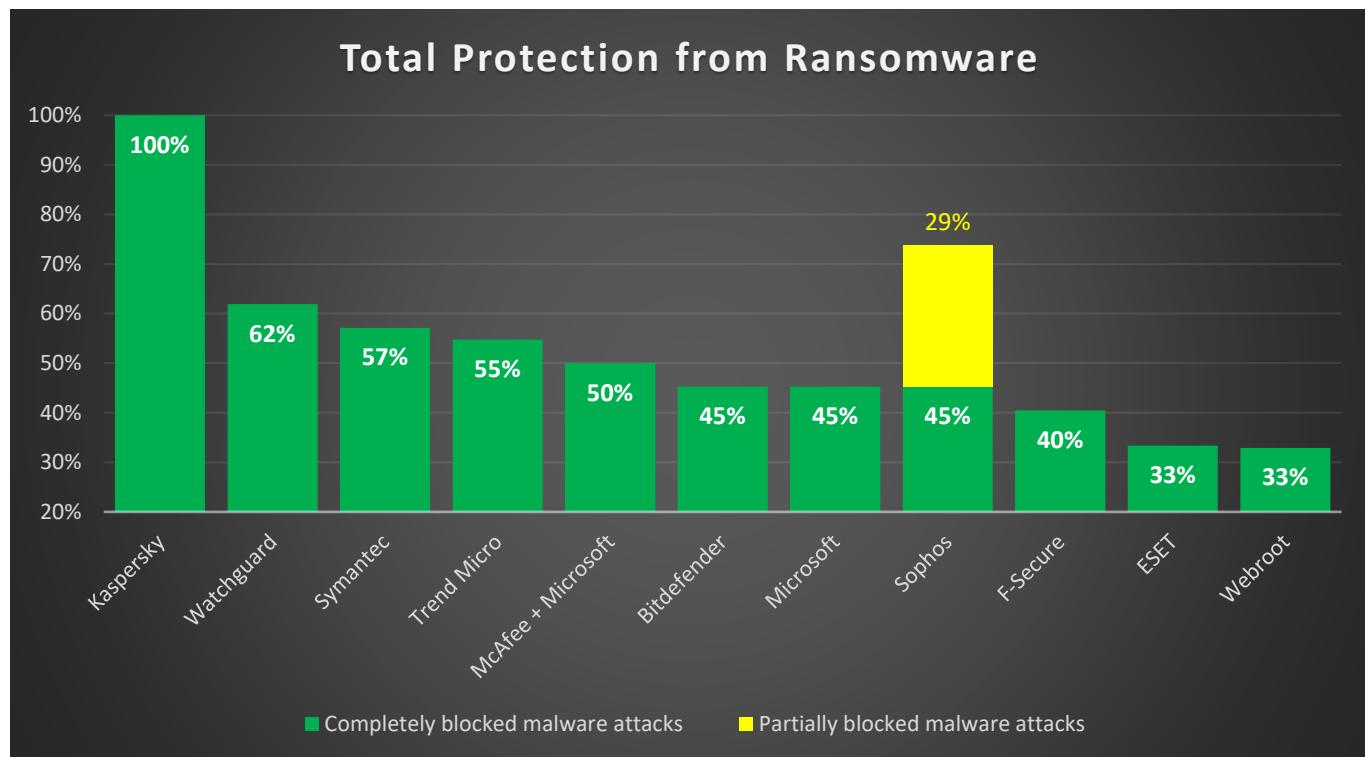


Figure 5. Total ransomware protection by different products basing on all three scenarios.

“Completely blocked” means that ransomware was detected, and all user files were protected.

“Partially blocked” means that ransomware was detected, but some user files were lost (not protected).

Arranged by “completely blocked” values.

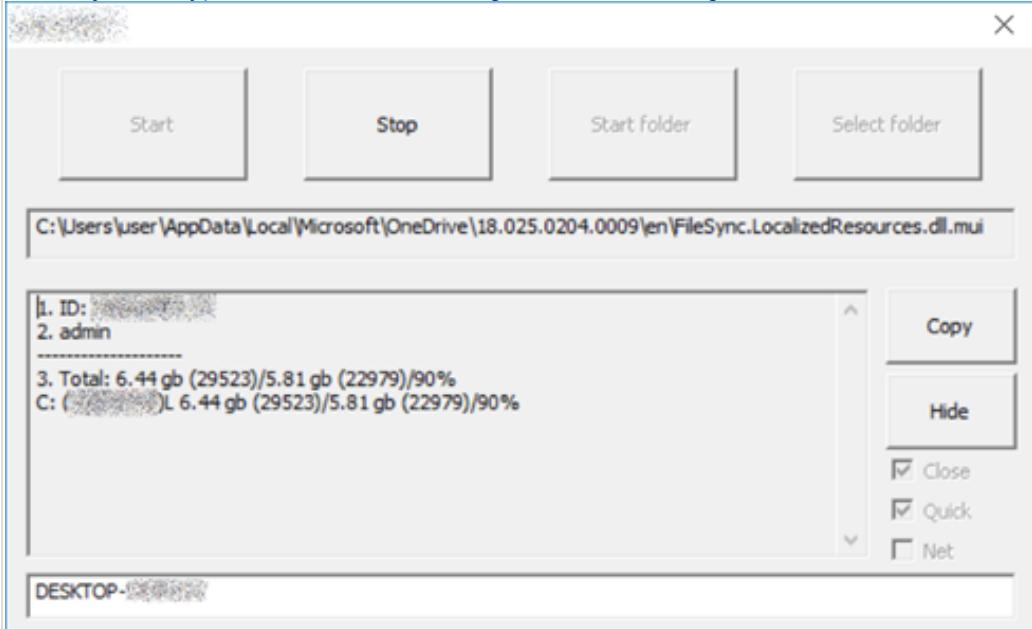
Overall, in the three different parts of the test, Kaspersky’s solution performed the best at detecting and blocking all attacks and protecting 100% of all user files. The other solutions protected between 62% of test cases (WatchGuard) and only 33% (ESET and Webroot). Right after WatchGuard, Symantec scored 57%, Trend Micro 55% and the combination of McAfee and Microsoft Defender scored 50%. Bitdefender, Microsoft and Sophos achieved 45% and F-Secure 40%. The Sophos product is an exception: it blocked 45% of attacks completely but it partially blocked 29% of test cases with loss of a part of the user files.

Appendix 1. Description of real-world ransomware families

RW	RW #	Name	Description
-	+ 1	Avaddon	<p>'Avaddon' ransomware is a targeted ransomware family involved in 'big game hunting' - attacks against high-profile targets.</p> <p>Threat actors behind this malware typically employ data theft and double extortion. This means that in case a victim is not willing to pay for decryption (e.g. they have reliable backups), threat actors will attempt to intimidate them by threatening to leak the stolen confidential data online.</p> <p>Avaddon encrypts the victim's files using AES and RSA algorithms.</p>  <p style="text-align: center;">Your network has been infected by Avaddon</p> <p>All your documents, photos, databases and other important files have been encrypted and you are not able to decrypt it by yourself. But don't worry, we can help you to restore all your files!</p> <p>The only way to restore your files is to buy our special software - Avaddon General Decryptor. Only we can give you this software and only we can restore your files!</p> <p>You can get more information on our page, which is located in a Tor hidden network.</p> <p>How to get to our page</p> <ul style="list-style-type: none"> • Download Tor browser - https://www.torproject.org/ • Install Tor browser • Open link in Tor browser - avaddon[REDACTED].onion • Follow the instructions on this page <p>Your ID:</p> <p>[REDACTED]</p>
+ +	2	Conti	<p>'Conti' ransomware is another targeted ransomware family involved in attacks against corporations, government organizations and healthcare.</p> <p>Threat actors behind this malware typically employ data theft and double extortion in their attacks.</p> <p>Conti is believed to be a successor of Ryuk, however, based on reverse engineering, the code of these malware families is not derived from the same sources.</p> <p>Different variants of Conti have been observed to be using AES + RSA algorithms, as well as ChaCha + RSA.</p>

RW	RW	#	Name	Description
				<pre>All of your files are currently encrypted by CONTI ransomware. If you try to use any additional recovery software - the files might be damaged or lost. To make sure that we REALLY CAN recover data - we offer you to decrypt samples. You can contact us for further instructions through our website : TOR VERSION : (you should download and install TOR browser first https://torproject.org) http://m232fdxbfmbrcehbrj5laky.onion HTTPS VERSION : https://contiransomware.info YOU SHOULD BE AWARE! Just in case, if you try to ignore us. We've downloaded your data and are ready to publish it on our news website. ---BEGIN ID--- http://m232fdxbfmbrcehbrj5laky.onion ---END ID---</pre>
+/-	-	3	DarkSide	<p>'DarkSide' ransomware is another targeted ransomware family involved in 'big game hunting', data theft, and double extortion.</p> <p>In addition to PE versions of this malware that are built to attack Windows machines, the developers of DarkSide also created a special ELF version that is tailored to infect Linux systems, specifically, VMWare ESXi hosts, in order to encrypt virtual machine files.</p> <p>Different variants of this ransomware use Salsa20 + RSA or ChaCha + RSA algorithms to encrypt the victim's data.</p> <pre>----- [Welcome to Dark] ----- What happened? ----- Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data. But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network. Follow our instructions below and you will recover all your data. Data leak ----- First of all we have uploaded more than 100 GB data. Example of data: - Accounting data - Executive data - Sales data - Customer Support data - Marketing data - Quality data - And more other... Your personal leak page: http://darksideleak.onion/blog/article/14/6/ The data is preloaded and will be automatically published if you do not pay. After publication, your data will be available for at least 6 months on our tor cdn servers. We are ready: - To provide you the evidence of stolen data - To give you universal decrypting tool for all encrypted files. - To delete all the stolen data. What guarantees? ----- We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests. All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of problems. We guarantee to decrypt one file for free. Go to the site and contact us. How to get access on website? ----- Using a TOR browser: 1) Download and install TOR browser from this site: https://torproject.org/ 2) Open our website: http://darksideleak.onion/ When you open our website, put the following data in the input form: Key:</pre>
+	+	4	Fonix (XINOF)	The threat actors behind 'Fonix' ransomware don't use a targeted approach, attacking a wide range of victims instead. This ransomware is mainly distributed in spam campaigns. This trojan encrypts the victim's files using RSA, Salsa20 and ChaCha ciphers.

RW	RW	#	Name	Description
				<p>XINOF v4.4.1</p> <p><input checked="" type="checkbox"/> logo</p> <h1>All Of Your Files Have Been Encrypted By XINOF!</h1> <p>All your files have been encrypted due to a security problem with your PC. If you want to restore them, please send an email to CrXL@hackorans.com</p> <p>You have to pay for decryption in Bitcoin. The price depends on how fast you contact us. After payment we will send you the decryption tool. You have to 48 hours(2 Day) To contact or paying us After that, you have to Pay Double. in case of no answer in 6 hours email us at = CrXL@cock.li The crypter person username : CrXL your SYSTEM ID is : </p> <p style="text-align: right;">05d,20:55:40 </p> <p>Attention!</p> <ul style="list-style-type: none"> • DO NOT pay any money before decrypting the test files. • DO NOT trust any intermediary, they wont help you and you may be victim of scam. just email us , we help you in any steps. • DO NOT reply to other emails, ONLY this two emails can help you. • Do not rename encrypted files. • Do not try to decrypt your data using third party software, it may cause permanent data loss. <p>What is our decryption guarantee?</p> <ul style="list-style-type: none"> • Before paying you can send us up to 3 test files for free decryption. The total size of files must be less than 2Mb (non archived), and files should not contain valuable information. (databases, backups, large excel sheets, etc.) <p>You only have LIMITED time to get back your files!</p> <ul style="list-style-type: none"> • if timer runs out and you dont pay us , all of files will be DELETED and your hard disk will be seriously DAMAGED. • you will lose some of your data on day 2 in the timer. • you can buy more time for pay. Just email us . • THIS IS NOT A JOKE! you can wait for the timer to run out ,and watch deletion of your files :) <p>Regards-FonixTeam</p>
		5	Limbozar	<p>'Limbozar (Ouroboros, VoidCrypt)' is a trojan mainly distributed by the means of RDP brute-force/credential stuffing. The threat actors search the Internet for machines with an open RDP port and attempt to connect to it using lists of most used or leaked credentials, or automatically trying all alphanumerical combinations. In case their login attempt succeeds, they will launch the ransomware on the compromised machine.</p> <p>This ransomware uses AES and RSA algorithms to encrypt the victim's files.</p> <p>All Your Files Has Been Encrypted</p> <p>You Have to Pay to Get Your Files Back</p> <p>1-Go to C:\ProgramData\ folder and send us prvkey*.txt.key file , * might be a number (like this : prvkey3.txt.key)</p> <p>2-You can send some file little than 1mb for Decryption test to trust us But the test File should not contain valuable dat</p> <p>3-Payment should be with Bitcoin</p> <p>4-Changing Windows without saving prvkey.txt.key file will cause permanete Data loss</p> <p>Our Email:...@tutanota.com</p> <p>in Case of no Answer:...@aol.com</p>
		6	LockBit	<p>'LockBit' ransomware, formerly known as "ABCD" ransomware, is another player on the 'big game hunting' scene. It focuses mostly on enterprises and government organizations rather than individuals.</p> <p>For more info, refer to: https://www.kaspersky.com/resource-center/threats/lockbit-ransomware</p>

RW	RW sha red	#	Name	Description
+ +	+ +	7	Makop	<p>'Makop' ransomware family is typically distributed via RDP brute-force/credential stuffing with subsequent manual launch by the malware operator. Variants of this trojan often have a graphical interface (GUI) to make the task easier for the operator. This trojan encrypts the victim's files using AES and RSA algorithms.</p>  <pre> ::: Greetings ::: Little FAQ: .1. Q: What's Happen? A: Your files have been encrypted and now have the "makop" extension. The file structure was not damaged, we did everything possible so this could not happen. .2. Q: How to recover files? A: If you wish to decrypt your files you will need to pay in bitcoins. .3. Q: What about guarantees? A: Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will cooperate with us. Its not in our interests. To check the ability of returning files, you can send to us any 2 files with SIMPLE extensions(jpg,xls,doc, etc... not databases!) and sizes(max 1 mb), we will decrypt them and send back to you. That is our guarantee. .4. Q: How to contact with you? A: You can write us to our mailbox: makop@tuta.io or makop@elude.in .5. Q: How will the decryption process proceed after payment? A: After payment we will send to you our scanner-decoder program and detailed instructions for use. With this program you will be able to decrypt all your encrypted files. .6. Q: If I don't want to pay bad people like you? A: If you will not cooperate with our service - for us, it's does not matter. But you will lose your time and data, cause only we have the private key. In practice - time is much more valuable than money. :::BEWARE::: DON'T try to change encrypted files by yourself! if you will try to use any third party software for restoring your data or antivirus solutions - please make a backup for all encrypted files! Any changes in encrypted files may entail damage of the private key and, as result, the loss all data. </pre>
+ +	+ +	8	Maze	<p>The threat actors behind 'Maze' ransomware started targeting corporations and municipal organizations in order to maximize the amount of money extorted. The distribution tactic of Maze ransomware initially involved infections via exploit kits (namely, Fallout EK and Spelevo EK) as well as via spam with malicious attachments. For more info, refer to: https://securelist.com/maze-ransomware/99137/</p>
+ +	+ +	9	Medusa (AKO)	<p>'Medusa' is another targeted ransomware family involved in 'big game hunting', data theft, and double extortion. This malware encrypts the victim's files using AES and RSA algorithms.</p>

RW	RW	#	Name	Description
				<p style="text-align: center;">YOUR PERSONAL ID:</p>  <p style="text-align: center;">52A18AF39E164752FC7A38D010F7973042F445C9ED184BACF679478B261D83D45C9C14810F9B4FAD3D94D1E8AA55FD1B7E1A5EADFB77513AC1B96E52E9B51E 3283B566B4C1481B26CC9E777BC</p> <p style="text-align: center;">/!\ YOUR COMPANY NETWORK HAS BEEN PENETRATED /! All your important files have been encrypted!</p> <hr/> <p>Your files are safe! Only modified. (RSA+AES)</p> <p>ANY ATTEMPT TO RESTORE YOUR FILES WITH THIRD-PARTY SOFTWARE WILL PERMANENTLY CORRUPT IT. DO NOT MODIFY ENCRYPTED FILES. DO NOT RENAME ENCRYPTED FILES.</p> <p>No software available on internet can help you. We are the only ones able to solve your problem.</p> <p>We gathered highly confidential/personal data. These data are currently stored on a private server. This server will be immediately destroyed after your payment. If you decide to not pay, we will release your data to public or re-seller. So you can expect your data to be publicly available in the near future..</p> <p>We only seek money and our goal is not to damage your reputation or prevent your business from running.</p> <p>You will can send us 2-3 non-important files and we will decrypt it for free to prove we are able to give your files back.</p> <hr/> <p>Contact us for price and get decryption software.</p> <p><i>http://gvlay6u4[REDACTED].onion</i></p> <p style="text-align: center;">[REDACTED]</p> <p>* Note that this server is available via Tor browser only</p> <p>Follow the instructions to open the link: 1. Type the address "https://www.torproject.org" in your Internet browser. It opens the Tor site. 2. Press "Download Tor", then press "Download Tor Browser Bundle", install and run it. 3. Now you have Tor browser. In the Tor Browser open "{URL}." 4. Start a chat and follow the further instructions.</p> <hr/> <p>If you can not use the above link, use the email:</p> <p>[REDACTED]@tutanota.com [REDACTED]@outlook.com</p> <p>* To contact us, create a new mail on the site: protonmail.com</p>
		10	MountLocker	'MountLocker' is another targeted ransomware family involved in 'big game hunting', data theft, and double extortion.

RW	RW	#	Name	Description
				<p>This trojan encrypts the victim's files using RSA and ChaCha algorithms.</p> <p>Your ClientId:</p> <p>[REDACTED]</p> <hr/> <p>/!\ YOUR NETWORK HAS BEEN HACKED /!\</p> <p>All your important files have been encrypted!</p> <hr/> <p>Your files are safe! Only encrypted.</p> <p>ANY ATTEMPT TO RESTORE YOUR FILES WITH THIRD-PARTY SOFTWARE WILL PERMANENTLY CORRUPT IT. DO NOT MODIFY ENCRYPTED FILES. DO NOT RENAME ENCRYPTED FILES.</p> <p>No software available on internet can help you. We are the only ones able to solve your problem.</p> <p>You can send us 2-3 files and we will decrypt it for free to prove we are able to give your files back.</p> <p>Also we gathered highly confidential/personal data from your network. These data are currently stored on a private server. This server will be immediately destroyed after your payment. If you won't pay, we will release your data to public or reseller. So you can expect your data to be published or improperly used in the near future. In this case you will face all legal and reputational consequences of the leak. We only desire to get a ransom and we don't aim to damage your reputation or destroy your business.</p> <hr/> <p>Contact us to discuss your next step.</p> <p>http://yh6vhwkjfsinwqwfyz5dpn.onion</p> <p>* Password field could be blank</p>
+ +	+ +	11	Nefilim	<p>'Nefilim' ransomware is one of the variants of a larger family named JSWorm. The earlier variants were very similar. Based on the binary code analysis, they must have originated from the same source code.</p> <p>The later variants have been rewritten from scratch using another programming language (Go language). However, the implemented cryptographic scheme and some other characteristics lead us to believe that these new strains belong to the same malware family.</p>
+ -	- -	12	NetWalker (Mailto)	<p>'NetWalker (Mailto)' is another targeted ransomware family involved in attacks against corporations, government organizations and healthcare.</p> <p>Threat actors behind this malware typically employ data theft and double extortion in their attacks.</p> <p>The malware uses elliptic cryptography (ECDH algorithm) and a stream cipher ChaCha to encrypt the victim's files.</p>

RW	RW	#	Name	Description
				<p>Your ClientId:</p> <p>[REDACTED]</p> <hr/> <p>/!\ YOUR NETWORK HAS BEEN HACKED /!\ All your important files have been encrypted!</p> <p>Your files are safe! Only encrypted.</p> <p>ANY ATTEMPT TO RESTORE YOUR FILES WITH THIRD-PARTY SOFTWARE WILL PERMANENTLY CORRUPT IT. DO NOT MODIFY ENCRYPTED FILES. DO NOT RENAME ENCRYPTED FILES.</p> <p>No software available on internet can help you. We are the only ones able to solve your problem.</p> <p>You can send us 2-3 files and we will decrypt it for free to prove we are able to give your files back.</p> <p>Also we gathered highly confidential/personal data from your network. These data are currently stored on a private server. This server will be immediately destroyed after your payment. If you won't pay, we will release your data to public or reseller. So you can expect your data to be published or improperly used in the near future. In this case you will face all legal and reputational consequences of the leak. We only desire to get a ransom and we don't aim to damage your reputation or destroy your business.</p> <hr/> <p>Contact us to discuss your next step.</p> <p>http://yh6vhwkJfsinwqwfyz5dpn.onion /?cid=[REDACTED]</p> <p>* Password field could be blank</p>
+ +		13	Phobos	<p>'Phobos' ransomware is distributed via hacked RDP connections. Once started, it terminates some processes from its deny list, then deletes shadow copies of all volumes, disables Windows recovery options, deletes backups and turns off the firewall. After that, it starts the encryption process. The malware encrypts files with extensions from a large list. This list includes a large number of user file extensions, such as documents, images, and music. It encrypts files by using the AES cipher, on all logical drives and network shares. The AES key is unique for each drive.</p>
+ -		14	PYSA (aka Mespinosa)	<p>'PYSA' - the name of this malware, is an acronym for 'Protect Your System Amigo'. It is another targeted family involved in 'big game hunting'. Threat actors behind this malware typically employ data theft and double extortion in their attacks.</p> <p>PYSA encrypts the victim's files using AES and RSA algorithms.</p>

RW	RW	#	Name	Description
				<p>Hi Company,</p> <p>Every byte on any types of your devices was encrypted. Don't try to use backups because it were encrypted too.</p> <p>To get all your data back contact us:</p> <p>[REDACTED]</p> <p>-----</p> <p>FAQ:</p> <ol style="list-style-type: none"> 1. Q: How can I make sure you don't fooling me? A: You can send us 2 files(max 2mb). 2. Q: What to do to get all data back? A: Don't restart the computer, don't move files and write us. 3. Q: What to tell my boss? A: Protect Your System Amigo.
+	+	15	RagnarLocker	<p>'RagnarLocker' is highly targeted, to the extent that each individual sample is specifically tailored for the organization the actors are attacking. The group behind it loves to abuse RDP, while their preferred payment method is bitcoins. For file encryption RagnarLocker uses a custom stream cipher based on the Salsa20 cipher. Instead of the standard initialization 'magic' constants sigma = "expand 32-byte k" and tau = "expand 16-byte k" normally used in Salsa20.</p> <p>For more info, refer to: https://securelist.com/targeted-ransomware-encrypting-data/99255/</p> <p>Some of this family samples include "sleep" functional ~30 seconds</p>
+	+	16	RansomExx (Defray777)	<p>'RansomExx (Defray777)' is malware is notorious for attacking large organizations and was most active in 2020.</p> <p>RansomExx is a highly targeted Trojan. Each sample of the malware contains a hardcoded name of the victim organization. Moreover, both the encrypted file extension and the email address for contacting the extortionists make use of the victim's name.</p> <p>The files are encrypted using AES and RSA algorithms.</p>
+	+	17	REvil (Sodinokibi, Sodin)	<p>'REvil (Sodinokibi, Sodin)' ransomware was first identified on April 17, 2019. It is used by the financially motivated GOLD SOUTHFIELD threat group, which distributes ransomware via exploit kits, scan-and-exploit techniques, RDP servers, and backdoored software installers.</p> <p>REvil uses a hybrid scheme to encrypt victim files. The file contents are encrypted with the Salsa20 symmetric stream algorithm, and the keys for it with an elliptic curve asymmetric algorithm.</p> <p>For more info, refer to: https://securelist.com/sodin-ransomware/91473/</p>
+	+	18	Ryuk	<p>The threat actors behind 'Ryuk' ransomware employ a multi-stage scheme to deliver this ransomware to their victims. Ryuk uses a hybrid encryption scheme employing the AES algorithm to encrypt the content of the victim's files, and the RSA algorithm to encrypt the AES keys. Ryuk uses the standard implementation of cryptographic routines provided by Microsoft CryptoAPI.</p> <p>For more info, refer to: https://securelist.com/story-of-the-year-2019-cities-under-ransomware-siege/95456/</p>
+	-	19	Snatch	<p>'Snatch' is another targeted ransomware family involved in 'big game hunting', data theft, and double extortion.</p> <p>This malware is developed in Go language and uses PGP public encryption scheme to</p>

RW	RW	#	Name	Description
				<p>encrypt the victim's files.</p> <pre>Hello! All your files are encrypted and only I can decrypt them. Contact me: [REDACTED]@mail.fr or [REDACTED]@cock.li Write me if you want to return your files - I can do it very quickly! The header of letter must contain extension of encrypted files. I'm always reply within 24 hours. If not - check spam folder, resend your letter or try send letter from another email service. Attention! Do not rename or edit encrypted files: you may have permanent data loss. To prove that I can recover your files, I am ready to decrypt any three files (less than 1Mb) for free (except databases, Excel and back HURRY UP! ! ! ! If you do not email me in the next 48 hours then your data may be lost permanently ! ! !</pre>
+ -	20	Stop		<p>'Stop' ransomware is propagated by means of fake installers that download the ransomware module. Stop enumerates local drives and network shares accessible from the infected machine and searches for all files, regardless of their extension. Early variants of the malware used the symmetric algorithm AES-256 in CFB mode with zero IV and the same 32-byte key for all files. Newer ones encrypt the files using the Salsa cipher.</p> <p>For more info, refer to: https://securelist.com/keypass-ransomware/87412/ (Note that at the time of publication, it was not yet called 'Stop').</p>
+ -	21	WastedLocker		<p>'WastedLocker' is another targeted ransomware family involved in attacks against corporations. To encrypt victims' files, the developers of the trojan employed a combination of the AES and RSA algorithms that has already become a 'classic' among different crypto-ransomware families. The search mask to choose which files will be encrypted, as well as the list of the ignored paths are set in the configuration of the malware.</p> <p>For more info, refer to: https://securelist.com/wastedlocker-technical-analysis/97944/</p>

Appendix 2. Description of Proof of Concept ransomware samples

The prepared samples implement different techniques which can be used to encrypt user data followed by a ransom demand. Most of the implemented techniques are known to have been used in targeted attacks in the recent times.

1. **encryption-test-01-simple**

Files are processed using ReadFile/WriteFile. The same handle is read and written, the encrypted file is not renamed.

2. **encryption-test-02-mail-ext**

Same as encryption-test-1-simple, but after encryption the encrypted file is renamed so that it has an added extension ".threat-actor@mail.com".

3. **encryption-test-03-mapping**

Files are processed using file mappings (CreateFileMapping/MapViewOfFile) instead of ReadFile/WriteFile.

4. **encryption-test-04-efs**

This PoC abuses the EFS (Encrypting File System), a built-in feature of Windows OS.

5. **encryption-test-05-randnames**

For each processed victim file, its encrypted content is saved into a new file with a random name.

6. **encryption-test-06-hardlink**

File encryption via hard links.

7. **encryption-test-07-symlink**

Same as encryption-test-06-hardlink, but instead of a hard link, a symbolic link is used.

8. **encryption-test-08-dosdevice**

File encryption via DOS device.

9. **encryption-test-09-dosdevice-with-mapping**

Same as encryption-test-08-dosdevice, but with file operations using mappings.

10. **encryption-test-10-deferred**

Victim files are processed in batches. The encrypted contents are written to disk when the whole batch has been processed.

11. **encryption-test-11-certutil**

This PoC abuses a legitimate Windows utility certutil.exe to hide the encryption activity.

12. **encryption-test-12-esentutl**

This PoC abuses a legitimate Windows utility esentutl.exe to hide the encryption activity.

13. **encryption-test-13-type**

This PoC abuses "type", a built-in command in the Windows Command shell to hide the encryption activity.

14. **encryption-test-14-bitlocker**

This PoC abuses BitLocker (a feature of Windows OS) with a password unknown to the victim, then reboots the machine, locking the user out of it.

Appendix 3. Description of user file sets

This set of clear user files was used as a traps set of files in the real-world shared scenario to:

- Check the ability of ransomware threats to find and encrypt them,
- and reveal the capabilities of security solutions to prevent these attacks and protect the files (prevent their modification to their non-original state).

The collection is represented by different file types, multi-layered folder structure and file system location on an targeted hosts, as described below.

- 20 files with 11 file extensions: ".7z" (2 files), ".zip" (2 files), ".rar" (2 files), ".jpeg" (2 files), ".jpg" (2 files), ".png" (2 files), ".doc" (1 file), ".docx" (1 file), ".xls" (1 file), ".pdf" (1 file), ".txt" (4 files).
- location folders:
 - C:\work\
 - C:\home\media\
 - C:\home\data\
 - C:\Users\<username>\Documents\
 - C:\Users\<username>\Documents\
 - C:\Users\<username>\Pictures\
 - C:\Users\<username>\Downloads\
 - C:\Users\<username>\Desktop\
 - C:\Users\<username>\
 - C:\Users\<username>\AppData\Roaming\
 - C:\Users\<username>\AppData\Local\

This set of clear user files was used as a traps set of files in the real-world and POC scenarios to:

- Check the ability of ransomware threats to find and encrypt them,
- and reveal the capabilities of security solutions to prevent these attacks (remediate the system from the threat) and protect the files (prevent their modification to their non-original state).

The collection is represented by different file types and file system location on targeted hosts, as described below.

- 153 files with 19 file extensions: ".odb" (5 files), "pptx" (10 files), "txt" (10 files), "xls" (11 files), "pdf" (4 files), "docx" (5 files), ".ods" (5 files), ".mp3" (17 files), ".mid" (8 files), "wav" (24 files), ".bmp" (6 files), ".gif" (15 files), ".jpg" (14 files), ".png" (12 files), ".tif" (1 file), ".wmf" (1 file), ".avi" (1 file), ".mov" (1 file), ".mp4" (3 files).
- location folders:
 - C:\Users\<username>\Documents\
 - C:\Users\<username>\Pictures\
 - C:\Users\<username>\Videos\
 - C:\Users\<username>\Music\