MRG Effitas

Efficacy Assessment & Assurance

Comparative Efficiency Assessment of Enterprise Security Suites against In-the-wild Ransomware

April 2017

Table of Contents

1 Executive Summary

Kaspersky Labs trusted MRG Effitas to conduct a security evaluation of several selected AV vendors and to compare the results. To test the AV products, fresh samples were selected from 13 crypto-ransomware and screenlocker families. To cover the market, several AV vendors have been selected, contacted and finally the products in Chapter 3 have been selected in the actual testing process.

Crypto-ransomware is one of the most dangerous malware type, because if it infects a system, the crypto-ransomware can stop business processes for days or even weeks, in case no proper backup strategy was used. Crypto-ransomware attacking shared drives can affect multiple departments, not just a single computer in an enterprise environment. Effective protection against crypto-ransomware is more important than ever.

Ransomware is one of the most lucrative methods of computer related fraud. From an economical perspective, the payload (the actual piece of malware) is extremely cheap to mass-deliver and the return-on-investment ratio is exceptionally high for the most part. It is quite easy to infect a relatively large number of hosts, and once the hosts are infected, the malware distributors don’t have to spend extra cost to collect the ransom, as victims contact the malware distributors by themselves.

Following the initial policy of transparency and objectivity, after receiving the results, Kaspersky Lab confirmed its intention to publish the results of all the products from the original cohort, even though it was not the only one to score 100% in the test. This approach to fairly deliver the complete results and not only those that are beneficial to the commissioning party is appreciated by MRG Effitas, and shows that sponsored tests can be as objective as non-sponsored tests and that their results should be seen as valid. Despite all of our efforts, we could not test all the products we thought would be valuable to test. MRG Effitas had purchased a CylancePROTECT license from a Cylance reseller several months prior to contacting them about the upcoming test. On the 7th of January 2017 at 12:58 AM our CylancePROTECT license, purchased from a Cylance reseller on the 7th of September 2016 was revoked and the fee refunded. All subsequent licenses purchased have been very quickly revoked and the credit cards refunded.

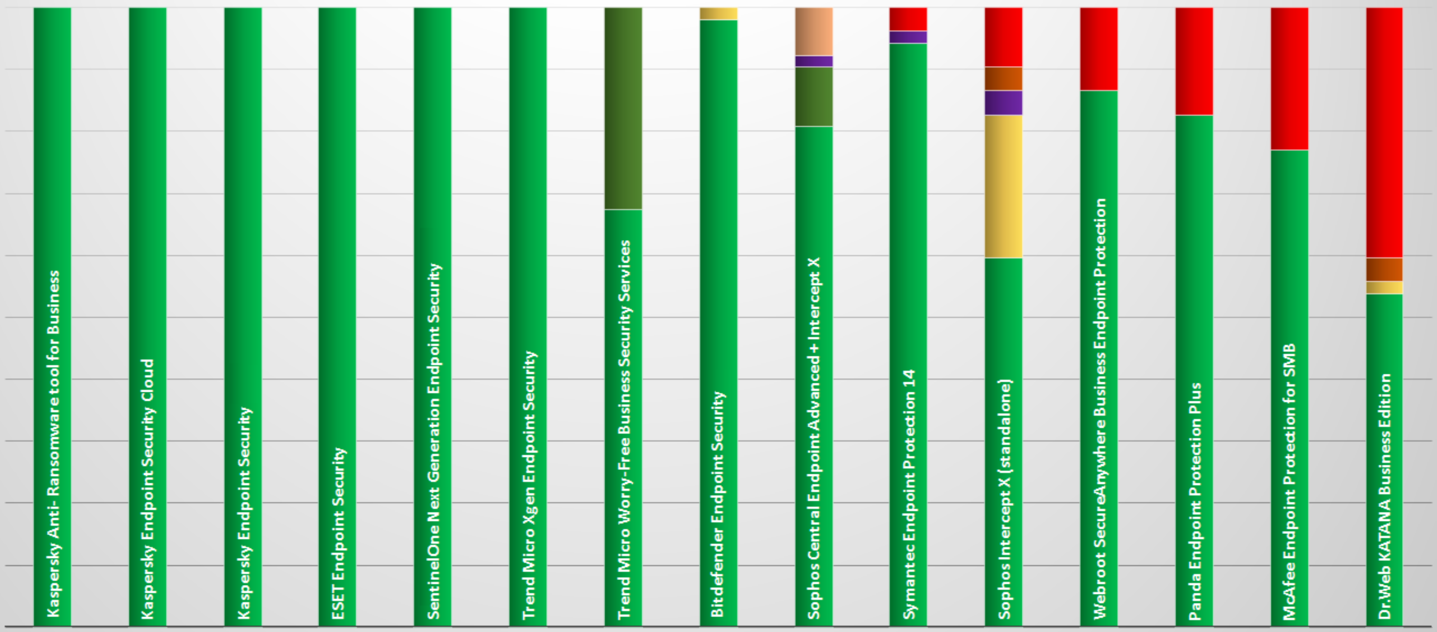
For more information about testing CylancePROTECT, please refer to “Participation in this test – Cylance ” Appendix.

The testing was carried out between January 9, 2017 and February 3, 2017.

The following products earned the MRG Effitas certified ransomware protection badge:

- Kaspersky Anti- Ransomware tool for Business (free tool)
- Kaspersky Endpoint Security
- Kaspersky Endpoint Security Cloud
- ESET Endpoint Security
- SentinelOne Next Generation Endpoint Security
- Trend Micro Worry-Free Business Security Services
- Trend Micro Xgen Endpoint Security

Samples blocked or missed



	Kaspersky Anti- Ransomware tool for Business	Kaspersky Endpoint Security Cloud	Kaspersky Endpoint Security	ESET Endpoint Security	SentinelOne Next Generation Endpoint Security	Trend Micro Xgen Endpoint Security	Trend Micro Worry-Free Business Security Services	Bitdefender Endpoint Security	Sophos Central Endpoint Advanced + Intercept X	Symantec Endpoint Protection 14	Sophos Intercept X (standalone)	Webroot SecureAnywhere Business Endpoint Protection	Panda Endpoint Protection Plus	McAfee Endpoint Protection for SMB	Dr.Web KATANA Business Edition
🟥 Fail	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	2 (3.8%)	5 (9.6%)	7 (13.5%)	9 (17.3%)	12 (23.1%)	21 (40.4%)
🟫 Fail, Screenlocked	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	2 (3.8%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	2 (3.8%)
🟧 Fail, User input	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	4 (7.7%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
🟪 Blocked but a lot of files encrypted	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	1 (1.9%)	1 (1.9%)	2 (3.8%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
🟨 Blocked but some files are encrypted	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	1 (1.9%)	0 (0.0%)	0 (0.0%)	12 (23.1%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	1 (1.9%)
🟩 Blocked but unnecessary user input	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	17 (32.7%)	0 (0.0%)	5 (9.6%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
🟩 Blocked	52 (100.0%)	52 (100.0%)	52 (100.0%)	52 (100.0%)	52 (100.0%)	52 (100.0%)	35 (67.3%)	51 (98.1%)	42 (80.8%)	49 (94.2%)	31 (80.8%)	45 (86.5%)	43 (82.7%)	40 (76.9%)	28 (53.8%)

2 Introduction

Kaspersky Labs trusted MRG Effitas to conduct a security evaluation of a number of selected AV vendors and to compare the results. Marketing rights to use the report belong to Kaspersky Lab only.

Testing focused on the scenario when all previous lines of defence have fallen, and the piece of malware is started on the victim machine. As a last line of defence, a decent AV product, monitoring the Windows API, might be able to detect quick 'file open – file read – encrypt – file write' patterns in quick succession and terminate the process. Also the samples can be detected by more traditional ways like signatures, heuristics, reputation lookups, exploit protection or URL analysis. Therefore, we considered a test Passed only if none of the user's files have been encrypted or all encrypted files have been rolled back.

2.1 Structure of this report

The remainder of this report is organised as follows.

Chapter 2 provides a brief overview of the topic, Chapter 0 and 9 describes the ransomware families in scope. The detailed results can be read in Chapter 5. Chapter 6 provides a detailed description of the testing methodology, Chapter 7 provides the conclusion, and finally, Chapter 8 provides timelines of vendor communication.

2.2 Overview

Crypto ransomware denotes a type of malware, which performs malicious activity on the users workstation applying malicious operations on the workstation preventing user access to some extent, proposing an offer that in case the victim pays a certain amount of ransom, access will be restored.

Most ransomware type malware perform at least one of the following type of actions.

- Encryption of user files (crypto ransomware)
- Locking the screen (screen locker ransomware)

Besides opening channels for other attacks (such as extraction of financial data, passwords etc.), crypto ransomware is a serious risk, since as long as local data is encrypted, it cannot be accessed and this might have detrimental effects on victims. For instance in February 2016, the Hollywood Presbyterian Medical Center fell victim to breach and a subsequent ransomware attack. Besides payroll information, patient data and medical records were encrypted and with no patient records, the daily operation of the hospital has been virtually paralysed. Thus, the CEO decided to pay the desired amount of 40 Bitcoins ($17.000 at the time), even before the authorities were notified about the incident[1].

Endpoint protection systems have had a long journey from traditional signature-based protection to that which is implemented in a modern protection system. Advanced heuristics, behaviour control, sandboxing, intrusion prevention systems, URL filtering, cloud based reputation systems, JavaScript analysers, memory corruption protection, etc. are now used to combat modern malware threats. To test an endpoint protection system, one has to test all modules of the protection employed by that system, and the test has to be done in a way which emulates standard user behaviour accurately.

Ransomware can be dropped to a user workstation via multiple different sources. It is dropped either via exploit kits, Office documents with macro code, Office documents with embedded OLE objects, LNK files, script code attached to email and used as downloader, after successful RDP brute-force via RDP,

[1] http://searchsecurity.techtarget.com/feature/Even-with-rise-in-crypto-ransomware-majority-do-not-pay

flashdrive, attacking an enterprise and dropping ransomware on the domain controller, and many more. Testing with "we downloaded the ransomware EXE from the malicious URL and executed it" is not enough anymore, as many ransomware families are not available this way anymore. Whenever possible, we emulated the full chain in the attack, but sometimes it was not available or broken.

2.3 Ransomware as a business model

Ransomware is one of the most lucrative methods of computer related fraud. From an economical perspective, the payload (the actual piece of malware) is extremely cheap to mass-deliver and the return-on-investment ratio is exceptionally high for the most part. It is quite easy to infect a relatively large number of hosts, and once the hosts are infected, the malware distributors don't have to spend extra cost to collect the ransom, as victims contact the malware distributors by themselves.

In addition, we observed that strangely, many ransomware distributors maintain 'help desk' to aid victims installing and setting up TOR browser, buying Bitcoins etc. Counterintuitive this might look like for the first time, it makes sense, as any non-paid ransom is lost for the malware distributors and many victims are not tech savvy. Furthermore, if users get the news that they won't get their data back after paying the desired ransom, the income for the malware distributors will significantly drop (a rather interesting case of 'customer satisfaction'). In a weird way, extra care is given to customer satisfaction: we also informed that in some cases (especially with the e-mail based contact model), even a negotiation of the ransom amount can also take place.

Interestingly, the Spora ransomware even provides 'packages' for victims: for $29, the malware is removed, to prevent future files from being encrypted but no actual files are recovered. For $39, some files are decrypted, full decryption costs $59, and an alleged 'immunity' feature for future infections costs $79. This immunity does not work for everyone, also does not protect against other ransomware families. These prices could fluctuate and vary depending on number of encrypted files and filetypes

Therefore, we expect an increase in the number of infected hosts soon.

3 Selection of participants

During the preparation phase of this test, we made a market research to pinpoint candidates, using methods that any non-savvy user would normally use to map their opportunities for protection against ransomware. Understandably, many of the web pages associated with the ransomware topic focused on helping victims after an infection. Many web sites even offer 'removal tools' for certain families of ransomware. Even though several decryption tools have been developed for pieces of ransomware using poor crypto (e.g. old variants of TeslaCrypt), many of such web sites advertise a universal cure (at a bargain price of a couple of US dollars) for pieces of malware, which cannot be decrypted. This is clearly a rather unethical exploit of desperate users, who think that they have an 'easy way out' for a couple of dollars, instead of paying the desired ransom.

Initially the following list of products were chosen to verify their abilities to protect against ransomware.

It includes both paid products and free tools which claim to help users against ransomware.

After the analysis, some of the products were considered as non-appropriate for testing for different reasons: either strong limitation of product functionality, or refuse by vendor to participate, or blocking license by vendor.

Moreover, during analysing publicly available information we found that some marketing material could mislead users, please see details below.

Depending on vendor feedback, default setup has been used or we followed vendor recommendations instead. For detailed setup, refer to Chapter 10.

Please refer to “tested” in the tab to reveal what products were finally tested

Product name	Version	Paid	Free tool	Tested ?
Bitdefender Endpoint Security 2017	6.2.17.876	✔		tested
Cylance CylanceProtect[3]	-	✔		not tested (3)
Dr.Web KATANA Business Edition	1.0	✔		tested
ESET Endpoint Security	6.4.2014.0	✔		tested
Kaspersky Anti- Ransomware tool for Business	1.1.24.0		✔	tested
Kaspersky Endpoint Security 10	SP110.2.5.3201 (mr3)	✔		tested
Kaspersky Endpoint Security Cloud	build 2.0.0.546	✔		tested
McAfee Endpoint Protection for SMB	42865	✔		tested
Panda Endpoint Protection Plus[4]	7.65.1	✔		tested
SentinelOne Next Generation Endpoint Security	1.8.4.3502	✔		tested
Sophos Central Endpoint Advanced + Intercept X	37752	✔		tested
Sophos Intercept X (standalone)	37387	✔		tested
Symantec Endpoint Protection 14	build 1904	✔		tested
Trend Micro Worry-Free Business Security Services	9.900.1008	✔		tested
Trend Micro Xgen Endpoint Security	1222	✔		tested
Webroot SecureAnywhere Business Endpoint Protection	9.0.13.75	✔		tested
Panda Adaptive Defense 360 [2]	-	✔		not tested (2)
BitDefender Anti-ransomware tool	-		✔	not tested (1)
Talos TeslaCrypt Decryption Tool	-		✔	not tested (1)
Trend Micro Ransomware Screen Unlocker Tool	-		✔	not tested (1)

(1) limited functionality

(2) refused to provide product installer and license key.[2]

(3) issue with license, due to its revoking by vendor. For details see Participation in this test – Cylance CylancePROTECT

3.1 Inaccurate or misleading marketing

In addition, we discovered that even respected, well-known vendors advertise their products with ‘full ransomware protection’ capabilities, even though such features are missing from the actual product. Most of the confusion comes from the wide term usage of ransomware.

[2] Originally, the Panda Adaptive Defense 360 has been selected for testing. The vendor told us they cannot cooperate with us for this test, only if the test will be carried out months later. As it was not possible to acquire licenses without the vendor cooperation, we opted for testing Panda Endpoint Protection Plus. Any requests for getting anonymous Trial versions for Adaptive Defense 360 failed.

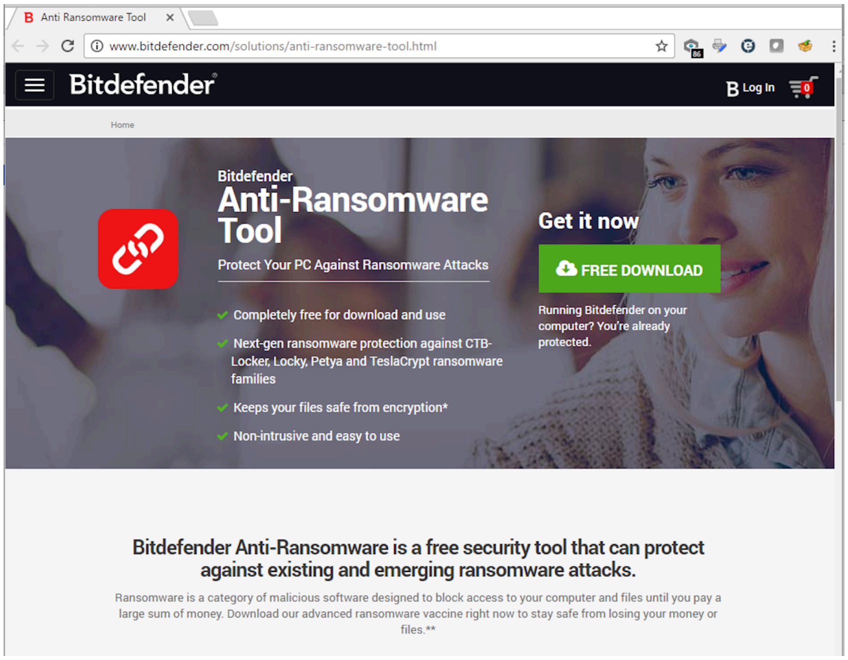
We do not suggest in any way that these marketing materials are misleading intentionally, these can be unintentional mistakes.

We recommend all vendors to use the following terminology:

- “Product X can protect against ransomware” means it can protect against all type of ransomware, including screenlockers, crypto-ransomware, doxware[3], etc. And not just old families, or only very specific families are detected, but recent ones as well.

3.1.1 Bitdefender

In another instance, the BitDefender web site advertises a product as a protection against ransomware.



Bitdefender

Anti-Ransomware Tool

Protect Your PC Against Ransomware Attacks

- ✓ Completely free for download and use
- ✓ Next-gen ransomware protection against CTB-Locker, Locky, Petya and TeslaCrypt ransomware families
- ✓ Keeps your files safe from encryption*
- ✓ Non-intrusive and easy to use

Get it now

FREE DOWNLOAD

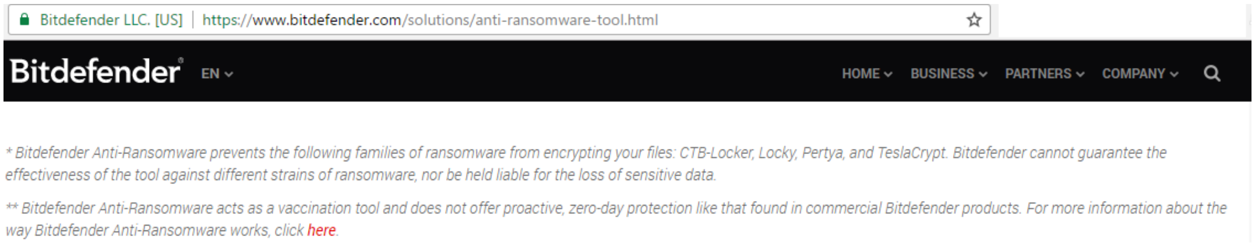
Running Bitdefender on your computer? You're already protected.

Bitdefender Anti-Ransomware is a free security tool that can protect against existing and emerging ransomware attacks.

Ransomware is a category of malicious software designed to block access to your computer and files until you pay a large sum of money. Download our advanced ransomware vaccine right now to stay safe from losing your money or files.**

Figure 1 Bitdefender marketing materials

However, the product page explicitly lists some ransomware families, which are covered and despite the marketing offering, the product admitted to lack protection features. The families listed here might be already outdated (not prevalent in-the-wild), so the effective protection is not good.


Bitdefender LLC. [US] | https://www.bitdefender.com/solutions/anti-ransomware-tool.html
Bitdefender
EN
HOME
BUSINESS
PARTNERS
COMPANY

* Bitdefender Anti-Ransomware prevents the following families of ransomware from encrypting your files: CTB-Locker, Locky, Pertya, and TeslaCrypt. Bitdefender cannot guarantee the effectiveness of the tool against different strains of ransomware, nor be held liable for the loss of sensitive data.

** Bitdefender Anti-Ransomware acts as a vaccination tool and does not offer proactive, zero-day protection like that found in commercial Bitdefender products. For more information about the way Bitdefender Anti-Ransomware works, click here.

> “▪ _* Bitdefender Anti-Ransomware prevents the following families of ransomware from encrypting your files: CTB-Locker, Locky, Pertya, and TeslaCrypt. Bitdefender cannot guarantee the effectiveness of the tool against different strains of ransomware, nor be held liable for the loss of sensitive data._

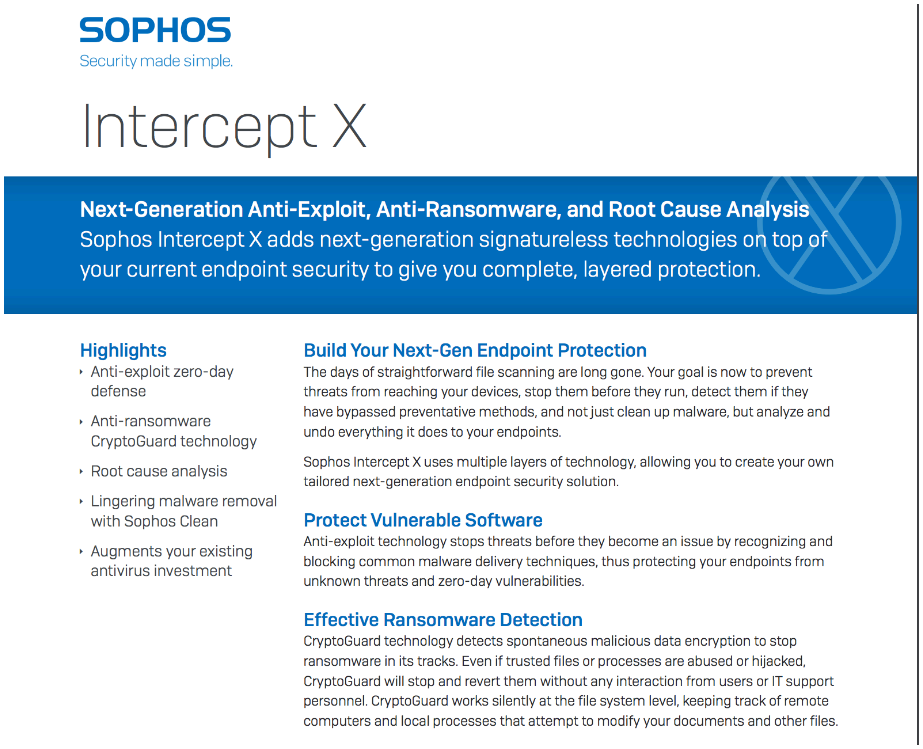
[3] a ransomware with sensitive data leakage functionality to prevent “simple” remediation from backups

- *** Bitdefender Anti-Ransomware acts as a vaccination tool and does not offer proactive, zero-day protection like that found in commercial Bitdefender products. For more information about the way Bitdefender Anti-Ransomware works, click* here*.*

3.1.2 Sophos Intercept X

The data fact sheet of Sophos Intercept X advertises to provide protection against all type of ransomware. During testing, we found that screen locker type ransomware locked the users desktop with no problem, suggesting that the protection does not cover screen lockers. It is important to note though that recovering from screenlocker type ransomware is a lot easier and cheaper than recovering from crypto-ransomware. Without proper backup, recovering from crypto-ransomware attack can be impossible. Also, crypto-ransomware can encrypt network shares, thus affecting a whole organization, while screenlockers only affect a single computer.

The marketing materials also mention “Effective ransomware detection” (see below), which is the case of poor wording, because every detected ransomware activity is also blocked by Sophos Intercept X, and in the case of ransomware, blocking is more important than detection.



SOPHOS
Security made simple.

Intercept X

Next-Generation Anti-Exploit, Anti-Ransomware, and Root Cause Analysis
Sophos Intercept X adds next-generation signatureless technologies on top of your current endpoint security to give you complete, layered protection.

Highlights

- Anti-exploit zero-day defense
- Anti-ransomware CryptoGuard technology
- Root cause analysis
- Lingering malware removal with Sophos Clean
- Augments your existing antivirus investment

Build Your Next-Gen Endpoint Protection

The days of straightforward file scanning are long gone. Your goal is now to prevent threats from reaching your devices, stop them before they run, detect them if they have bypassed preventative methods, and not just clean up malware, but analyze and undo everything it does to your endpoints.

Sophos Intercept X uses multiple layers of technology, allowing you to create your own tailored next-generation endpoint security solution.

Protect Vulnerable Software

Anti-exploit technology stops threats before they become an issue by recognizing and blocking common malware delivery techniques, thus protecting your endpoints from unknown threats and zero-day vulnerabilities.

Effective Ransomware Detection

CryptoGuard technology detects spontaneous malicious data encryption to stop ransomware in its tracks. Even if trusted files or processes are abused or hijacked, CryptoGuard will stop and revert them without any interaction from users or IT support personnel. CryptoGuard works silently at the file system level, keeping track of remote computers and local processes that attempt to modify your documents and other files.

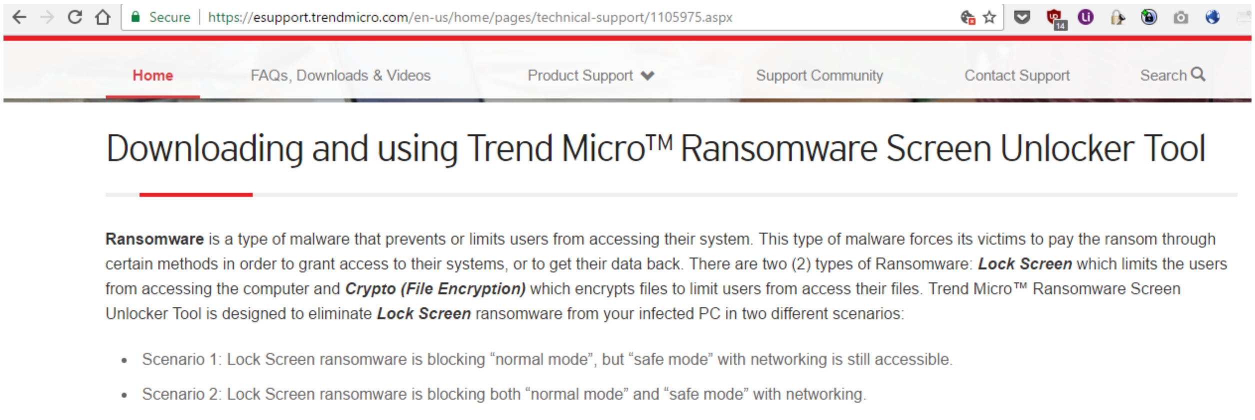
Figure 2 - Sophos Intercept X marketing materials

3.2 Utilities with limited functionality

We found that some vendors claim protection against ransomware, but after reading the marketing materials, it turns out these protections have limitations when it comes to type of ransomware or ransomware families.

3.2.1 Trend Micro Ransomware Screen Unlocker Tool

Trend Micro Ransomware Screen Unlocker Tool has limited functionality, as it only protects against screenlockers, and not against crypto-ransomware.


Secure | https://esupport.trendmicro.com/en-us/home/pages/technical-support/1105975.aspx
Home
FAQs, Downloads & Videos
Product Support
Support Community
Contact Support
Search

Downloading and using Trend Micro™ Ransomware Screen Unlocker Tool

Ransomware is a type of malware that prevents or limits users from accessing their system. This type of malware forces its victims to pay the ransom through certain methods in order to grant access to their systems, or to get their data back. There are two (2) types of Ransomware: ***Lock Screen*** which limits the users from accessing the computer and ***Crypto (File Encryption)*** which encrypts files to limit users from access their files. Trend Micro™ Ransomware Screen Unlocker Tool is designed to eliminate ***Lock Screen*** ransomware from your infected PC in two different scenarios:

- Scenario 1: Lock Screen ransomware is blocking "normal mode", but "safe mode" with networking is still accessible.
- Scenario 2: Lock Screen ransomware is blocking both "normal mode" and "safe mode" with networking.

3.2.2 Talos TeslaCrypt Decryption Tool

This tool was not taken into the test, since it does not mislead users but it is of limited functionality. This product could not be mentioned as one to protect against any Ransomware in general since it only protects against Teslacrypt family.

3.3 Vendors refusing to test their product

We planned to get the following products tested, but we were informed by vendors that they don't want their products to be tested in this specific test.

3.3.1 Cylance CylanceProtect

Due to revoked licenses, we were not able to test CylanceProtect. For more detailed information, refer to chapter 8.2.

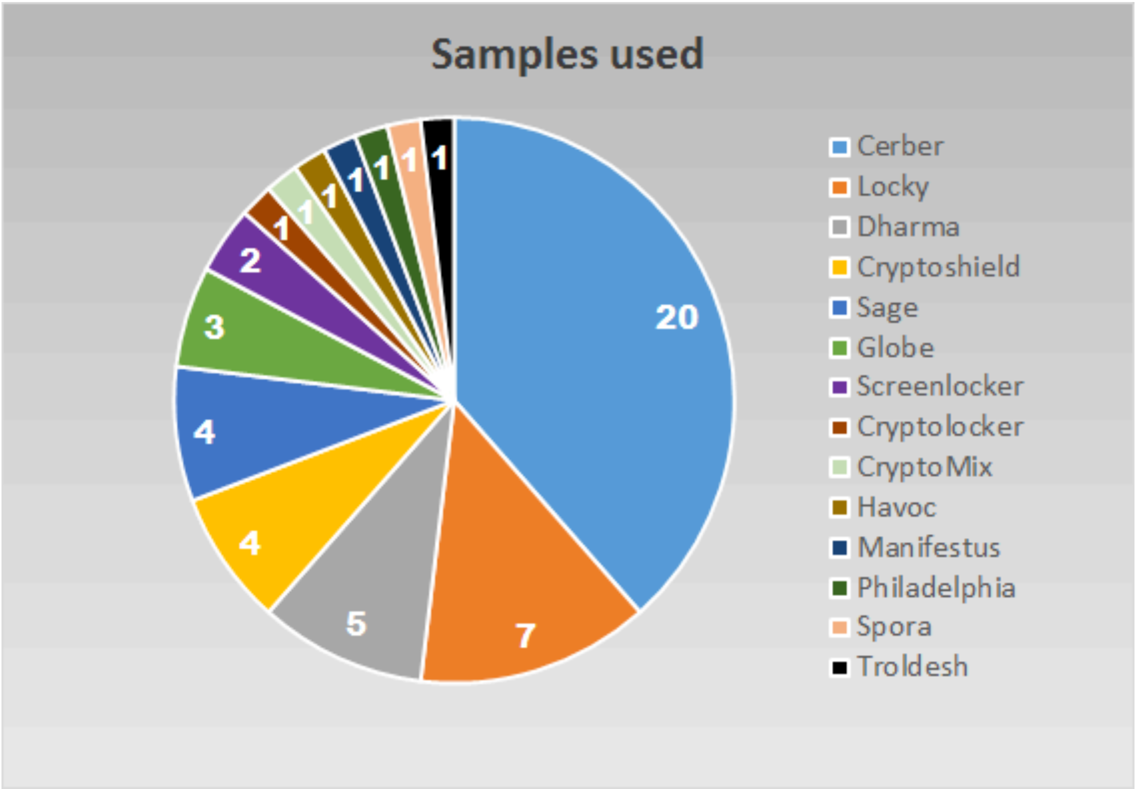
3.3.2 Panda Adaptive Defense 360

For more detailed information, refer to chapter 8.1.

4 Ransomware families in scope

For testing purposes, we used numerous samples, representing all ransomware families on the market (as of late 2016 - early 2017). The samples were collected in the wild, and more than 50% of the tested samples tested were not older than 24 hours.

The following chart represents the distribution of the ransomware samples used in the test:



For detailed information on the ransomware families used in the test, please refer to *"Appendix – ransomware families* used*"*.

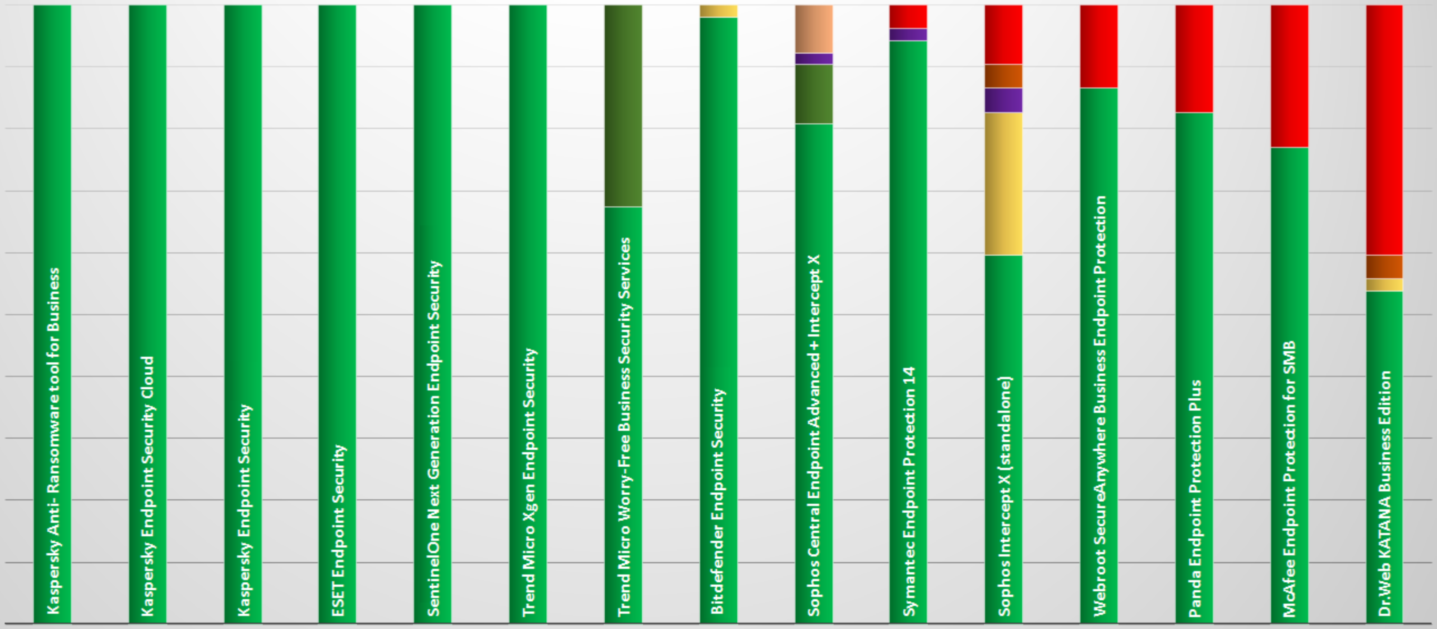
5 Detailed Results

The testing was carried out between January 9, 2017 and 3 February, 2017.

Due to the specific nature of ransomware, we have introduced multiple different categories how the product protects the user files:

1. "Block": The ransomware was blocked before it could encrypt any of the files, or if files were encrypted, all the files were rolled back automatically to the original state.
2. "Block, but unnecessary user input": Some products first warned the user about a low reputation of the file. Whenever we clicked on Allow or Execute of the file, the ransomware attack was blocked or all files were rolled back later. Some people might find these unnecessary user questions annoying, but even if they turn it off, they are protected against the attacks.
3. "Blocked, but some files are encrypted": Some products employ behaviour blocking, where they check for multiple file modifications in files with structure (images, Office documents, etc). Although the attack is stopped in the early phase of encryption, some files can be encrypted and not rolled back. This can be a small issue or a huge issue for users, depending on what specific files were encrypted.
4. "Blocked, but a lot of files encrypted": This is again some products employing behavioural blocking. Two variants of results are included there. In one case the behaviour blocker blocked the encryption just too late. In another case that were Pyton files in Python folder Some ransomware started to encrypt for example Python files in Python installation directory, which were not protected by the behaviour blocker. And when the ransomware started to encrypt files with structure (e.g. Office documents, photos), the behaviour blocker blocked the encryption.
5. "Fail, user input": As mentioned earlier, some products employ reputation based lookups, and asks the user whether this file should be allowed to run or not. In these cases, we always clicked on Yes, or Allow or Run to emulate human behaviour worst case scenarios (which is unfortunately common practice). Whenever this was the only defense from the product, we marked this as Fail, user input, because it only depends on the user what happens, and users tend to allow to execute these files regularly.
6. "Fail, Screenlocked". Screenlockers are a type of ransomware. Although not as dangerous as crypto-ransomware, a screenlocked computer can still be an issue, because people can't use their computer for hours or days.
7. "Fail": Whenever the attack was not blocked and the crypto-ransomware successfully encrypted all the files targeted on the computer.

Samples blocked or missed



	Kaspersky Anti- Ransomware tool for Business	Kaspersky Endpoint Security Cloud	Kaspersky Endpoint Security	ESET Endpoint Security	SentinelOne Next Generation Endpoint Security	Trend Micro Xgen Endpoint Security	Trend Micro Worry-Free Business Security Services	Bitdefender Endpoint Security	Sophos Central Endpoint Advanced + Intercept X	Symantec Endpoint Protection 14	Sophos Intercept X (standalone)	Webroot SecureAnywhere Business Endpoint Protection	Panda Endpoint Protection Plus	McAfee Endpoint Protection for SMB	Dr.Web KATANA Business Edition
🟥 Fail	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	2 (3.8%)	5 (9.6%)	7 (13.5%)	9 (17.3%)	12 (23.1%)	21 (40.4%)
🟧 Fail, Screenlocked	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	2 (3.8%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	2 (3.8%)
🟧 Fail, User input	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	4 (7.7%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
🟪 Blocked but a lot of files encrypted	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	1 (1.9%)	1 (1.9%)	2 (3.8%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
🟨 Blocked but some files are encrypted	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	1 (1.9%)	0 (0.0%)	0 (0.0%)	12 (23.1%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	1 (1.9%)
🟩 Blocked but unnecessary user input	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	17 (32.7%)	0 (0.0%)	5 (9.6%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
🟩 Blocked	52 (100.0%)	52 (100.0%)	52 (100.0%)	52 (100.0%)	52 (100.0%)	52 (100.0%)	35 (67.3%)	51 (98.1%)	42 (80.8%)	49 (94.2%)	31 (80.8%)	45 (86.5%)	43 (82.7%)	40 (76.9%)	28 (53.8%)

A note on Sophos Intercept X:

In the test cases where a limited number of files were encrypted, these files are usually file types which, considering a typical usage pattern are usually less likely to contain sensitive or important data. For instance txt or exe files can be encrypted, but as soon as the ransomware tries to encrypt photos or documents, the ransomware was blocked. Although in some cases, these files can be also an issue to lose (e.g. passwords in txt files, legacy EXE file, etc.).

In the case of "Blocked but a lot of files were encrypted" we checked, and the Sage ransomware family samples were responsible for this. The reason why it encrypted so many files is because it targets .py extension, and encrypted in the Python installation folder. In this case the damage level depends on interests of user, and in once case could be zero, in other could be large (e.g. in case of developers).

A note on Symantec Endpoint Protection:

In the single case where a lot of files were encrypted, Sonar did not allow 4 images on the desktop to be encrypted, but meanwhile a lot of files were encrypted in other directories.

6 Methodology

6.1 Infection methods

Testing involved the simulation of several delivery and infection methods. The samples have been collected in the wild, their delivery methods during testing were as follows.

- Copy from a local share
- Delivered using an exploit of an installed 3rd party application
- Download from a local web server
- Download from its original location (from the Internet)

The test images were standard 64-bit Windows 7 Professional installations. Each AV product has been installed, activated and updated with the latest signature packages and databases. In each test run, the samples were delivered to the machine and started. The testing environment simulated a typical Windows workstation with MS Office documents, images, movies and similar files scattered through typical locations (e.g. the Desktop, My Documents folder)

6.2 Result interpretation

The scores of this test are results of a sample based approach. Note that this approach has some inherent errors, which, despite all care, cannot be eliminated.

- The sample set represents only a subset of the ransomware type malware in the wild.
- The scores represent a snapshot, taken on a specific date. This means that some AV products are updated hourly, others are updated daily (or even updates against a specific threat can be late for weeks in rare circumstances), therefore a certain pass/fail ratio may or may not be true for the next update. But as mentioned, the products were always updated to the latest signature packages and databases.
- Most AV engines have lots of configuration options and auxiliary features, which can be individually configured or purchased. The authors of this report attempted to configure the products in an optimal fashion, and we were often aided by vendors to achieve optimal performance. The change in default policies can be found in Appendix - Non-default AV setup.

- The protection of the products is not always consistent. Some products have good protection in one month, and average protection the next month. Sometimes malware authors create samples which are not detected for days. Sometimes products can protect against new type of ransomware the first time it scans the malware. One result in one point in time can not be extrapolated to the future.
- Due to the nature of the test, that we needed fresh, valid and working ransomware samples and manually testing it against all the products, it is not possible to test with thousands of samples. More samples in the test could potentially change the results. Automating the test would change the results significantly in a way which does not represent the real world.

6.3 False positive tests

False positive test was excluded from the test, because a lot of behaviour based protection products are involved in the test. Static false-positive test is meaningless in this case, as behaviour protections have 0% false positive rate when it comes to static false positive test. Thus any results like this would be misleading. Executing and fully testing functionality of hundreds of valid applications was not feasible. Testing with less software (e.g. top 50 application) is again meaningless, as probably all product would score 0% false positive rate.

7 Conclusion

The products which protected all files in all test cases earned the MRG Effitas certified ransomware protection badge:

- Kaspersky Anti- Ransomware tool for Business
- Kaspersky Endpoint Security
- Kaspersky Endpoint Security Cloud
- ESET Endpoint Security
- SentinelOne Next Generation Endpoint Security
- Trend Micro Worry-Free Business Security Services
- Trend Micro Xgen Endpoint Security

8 Appendix – Participation in this test

8.1 Participation in this test – Panda Adaptive Defense 360

Originally, the Panda Adaptive Defense 360 has been selected for testing. The vendor told us they cannot cooperate with us for this test at the moment, only if the test will be carried out months later. As it was not possible to acquire licenses without the vendor cooperation, we opted for testing Panda Endpoint Protection Plus. Any requests for getting anonymous Trial versions for Adaptive Defense 360 failed.

8.2 Participation in this test – Cylance CylancePROTECT

In the interest of transparency and objectivity, Kaspersky Lab and MRG Effitas decided that all vendors whose products had been selected to participate should be contacted prior to the commencement of testing.

Each of the vendors in the original cohort was duly contacted and furnished with the proposed ransomware test methodology and informed that where appropriate they would be allowed to set custom policy settings. Vendors were also told that they would be supplied with all the samples their product failed against so they could independently verify the test results and that they would be given a week-long feedback period.

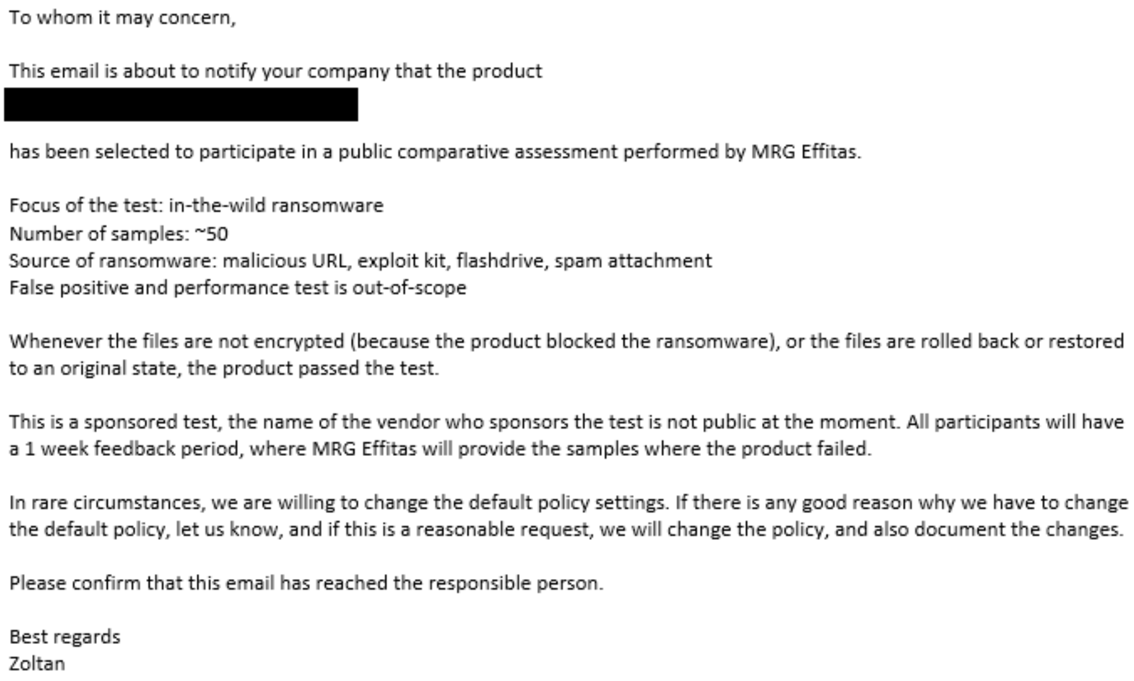
Despite the best efforts of Kaspersky Lab and MRG Effitas to make the testing as fair, appropriate and transparent for each vendor, when contacted, Cylance requested that their product CylancePROTECT was not included in the evaluation.

MRG Effitas had purchased a CylancePROTECT license from a Cylance reseller several months prior to contacting them about the upcoming test. On the 7th of January 2017 at 12:58 AM (14 Hours and 8 minutes after our email to them) our CylancePROTECT license, purchased from a Cylance reseller on the 7th of September 2016 was revoked and the fee refunded. All subsequent licenses purchased have been very quickly revoked and the credit cards refunded.

All the other vendors (except Panda) contacted had no objection to participating in this test and so their product were included.

Following the initial policy of transparency and objectivity agreed with MRG Effitas, after receiving the results, Kaspersky Lab confirmed its intention to publish the results of all the products from the original cohort, even though it was not the only one to score 100% in the test. This approach to fairly deliver the complete results and not only those that are beneficial to the commissioning party shows that sponsored tests can be as objective as non-sponsored tests and that their results should be seen as valid.

The following email was sent to every vendor Kaspersky Lab had specified to be tested.



To whom it may concern,

This email is about to notify your company that the product

[redacted]

has been selected to participate in a public comparative assessment performed by MRG Effitas.

Focus of the test: in-the-wild ransomware
Number of samples: ~50
Source of ransomware: malicious URL, exploit kit, flashdrive, spam attachment
False positive and performance test is out-of-scope

Whenever the files are not encrypted (because the product blocked the ransomware), or the files are rolled back or restored to an original state, the product passed the test.

This is a sponsored test, the name of the vendor who sponsors the test is not public at the moment. All participants will have a 1 week feedback period, where MRG Effitas will provide the samples where the product failed.

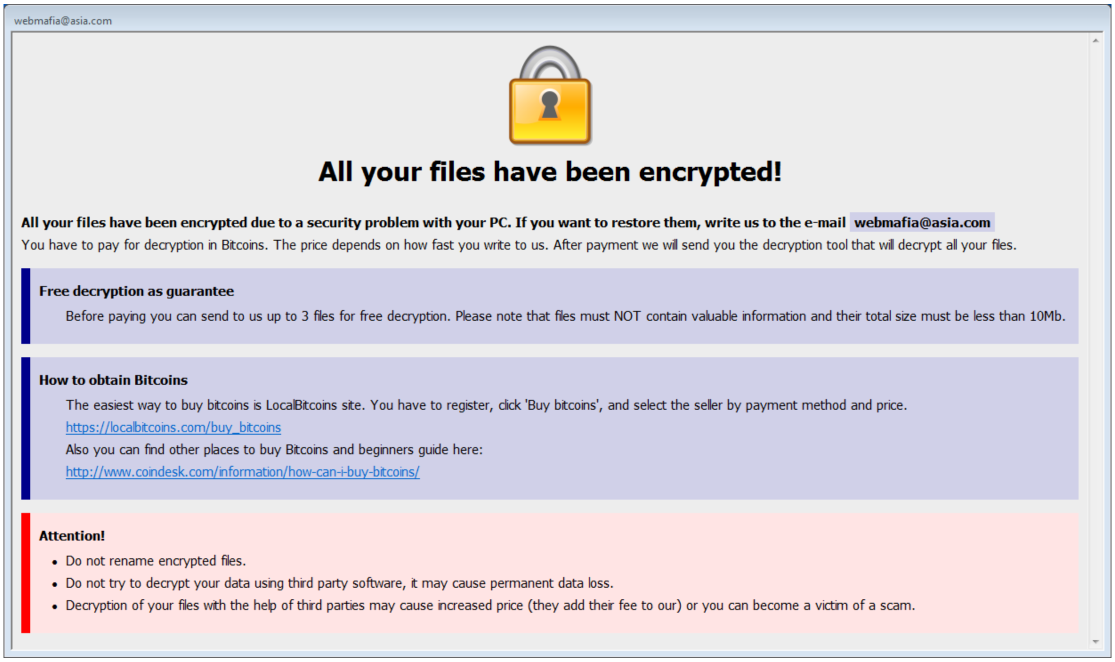
In rare circumstances, we are willing to change the default policy settings. If there is any good reason why we have to change the default policy, let us know, and if this is a reasonable request, we will change the policy, and also document the changes.

Please confirm that this email has reached the responsible person.

Best regards
Zoltan

9 Appendix – ransomware families used

9.1 Dharma



webmafia@asia.com

All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail webmafia@asia.com
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee
Before paying you can send to us up to 3 files for free decryption. Please note that files must NOT contain valuable information and their total size must be less than 10Mb.

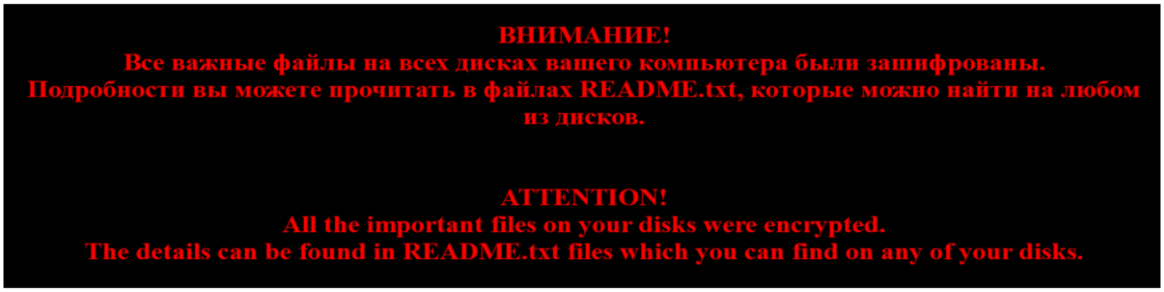
How to obtain Bitcoins
The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
http://www.coindesk.com/information/how-can-i-buy-bitcoins/

Attention!
- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

Figure 3 Dharma ransom page

Dharma is a new variant of Crysis - a high-risk ransomware-type virus. Following successful infiltration, Dharma encrypts stored files using AES. In addition, this file-encoder usually appends the ".[webmafia@asia.com]. wallet" ".[webmafia@asia.com]. dharma" or ".[webmafia@asia.com].zzzzz" extension and encrypts the filename too. If the ransomware is not eradicated from the system, it loads itself with every reboot and it will result in new encrypted files. The encryption cost varies for each individual. Dharma is usually dropped after an RDP brute-force attack is successful.

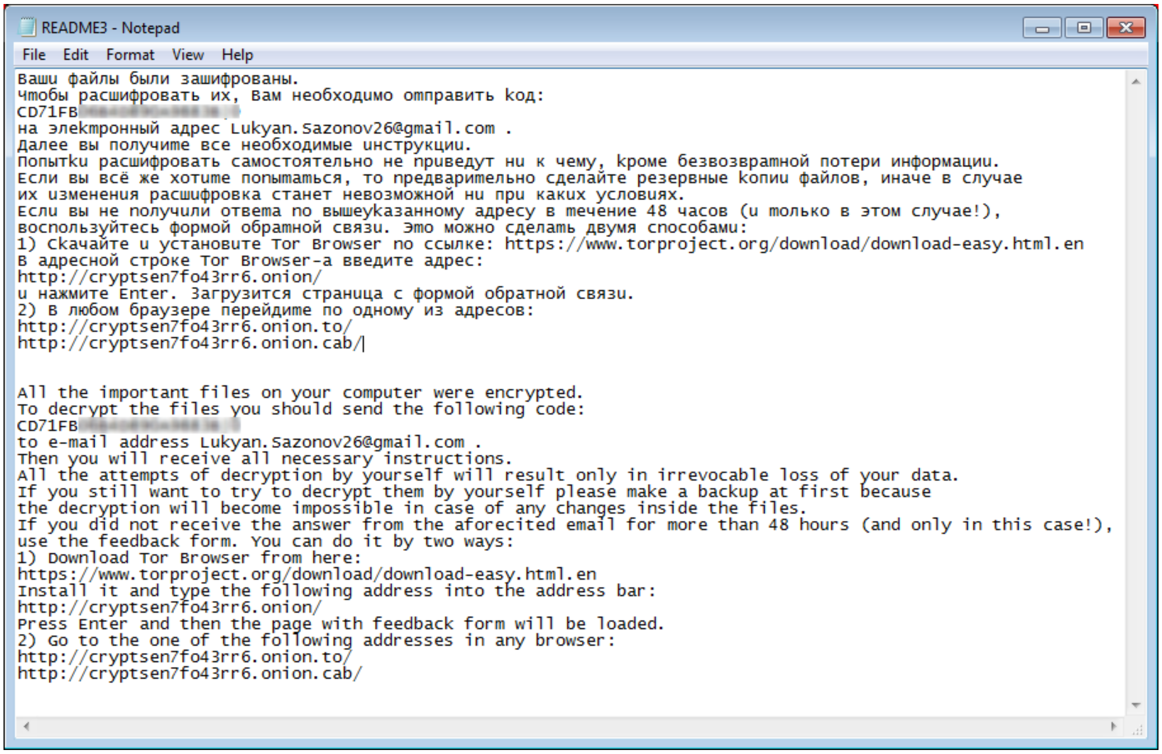
9.2 Troldesh



ВНИМАНИЕ!
Все важные файлы на всех дисках вашего компьютера были зашифрованы.
Подробности вы можете прочитать в файлах README.txt, которые можно найти на любом из дисков.

ATTENTION!
All the important files on your disks were encrypted.
The details can be found in README.txt files which you can find on any of your disks.

Figure 4 Troldesh ransom page

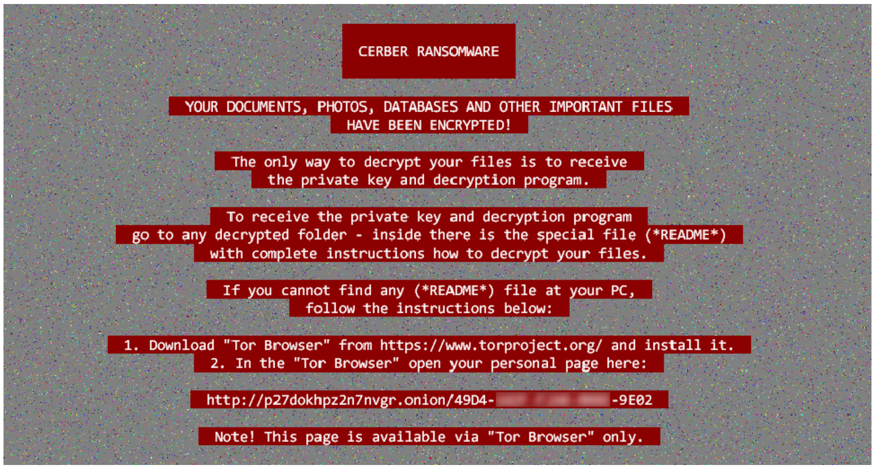


```
Ваши файлы были зашифрованы.
Чтобы расшифровать их, Вам необходимо отправить код:
CD71FB[redacted]
на электронный адрес Lukyan.Sazonov26@gmail.com .
Далее вы получите все необходимые инструкции.
Попытки расшифровать самостоятельно не приведут ни к чему, кроме безвозвратной потери информации.
Если вы всё же хотите попытаться, то предварительно сделайте резервные копии файлов, иначе в случае
их изменения расшифровка станет невозможной ни при каких условиях.
Если вы не получили ответа по вышеуказанному адресу в течение 48 часов (и только в этом случае!),
воспользуйтесь формой обратной связи. Это можно сделать двумя способами:
1) Скачайте и установите Tor Browser по ссылке: https://www.torproject.org/download/download-easy.html.en
В адресной строке Tor Browser-а введите адрес:
http://cryptsen7fo43rr6.onion/
и нажмите Enter. Загрузится страница с формой обратной связи.
2) В любом браузере перейдите по одному из адресов:
http://cryptsen7fo43rr6.onion.to/
http://cryptsen7fo43rr6.onion.cab/


All the important files on your computer were encrypted.
To decrypt the files you should send the following code:
CD71FB[redacted]
to e-mail address Lukyan.Sazonov26@gmail.com .
Then you will receive all necessary instructions.
All the attempts of decryption by yourself will result only in irrevocable loss of your data.
If you still want to try to decrypt them by yourself please make a backup at first because
the decryption will become impossible in case of any changes inside the files.
If you did not receive the answer from the aforecited email for more than 48 hours (and only in this case!),
use the feedback form. You can do it by two ways:
1) Download Tor Browser from here:
https://www.torproject.org/download/download-easy.html.en
Install it and type the following address into the address bar:
http://cryptsen7fo43rr6.onion/
Press Enter and then the page with feedback form will be loaded.
2) Go to the one of the following addresses in any browser:
http://cryptsen7fo43rr6.onion.to/
http://cryptsen7fo43rr6.onion.cab/
```

Figure 5 Troldesh ransom note

The Troldesh ransomware is also known as Encoder.858. It carries out a similar attack like most ransomware. But it will replace the files' names with random characters – making it harder to identify the files - and uses AES encryption. Although most ransomware attacks use an online page, often through TOR and automated payment methods, the Troldesh ransomware provides an email address through which attackers communicate with the victim directly and establish the ransom and payment in rubles.

9.3 Cerber



CERBER RANSOMWARE

YOUR DOCUMENTS, PHOTOS, DATABASES AND OTHER IMPORTANT FILES
HAVE BEEN ENCRYPTED!

The only way to decrypt your files is to receive
the private key and decryption program.

To receive the private key and decryption program
go to any decrypted folder - inside there is the special file (*README*)
with complete instructions how to decrypt your files.

If you cannot find any (*README*) file at your PC,
follow the instructions below:

1. Download "Tor Browser" from https://www.torproject.org/ and install it.
2. In the "Tor Browser" open your personal page here:

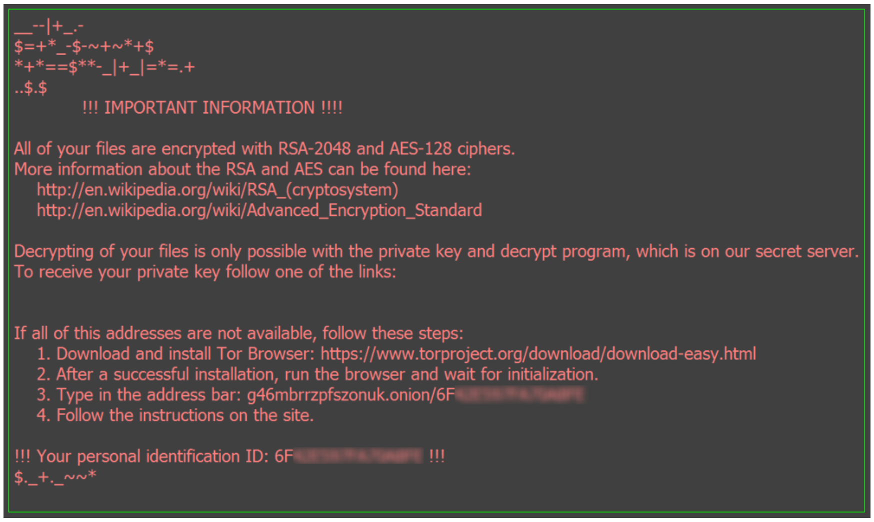
http://p27dokhpz2n7nvgr.onion/49D4-[redacted]-9E02

Note! This page is available via "Tor Browser" only.

Figure 6 Cerber ransom note

Cerber ransomware, much like many other encryption type ransomware, is known to encrypt files with AES-256 encryption on the infected computer. It creates random filenames and appends pseudo-random extension and hold those files for a substantial ransom fee. As it encrypts the victim's files, it creates TXT, HTML, and VBS files named 'DECRYPT MY FILES' with instructions on how to pay and it has audible voice saying, "Attention! Attention! Attention!, Your documents, photos, databases, and other files have been encrypted!" The victim has to pay the 1-1.25 Bitcoin ($1000-$1250) ransom via TOR browser within one week or the amount is doubled.

9.4 Locky

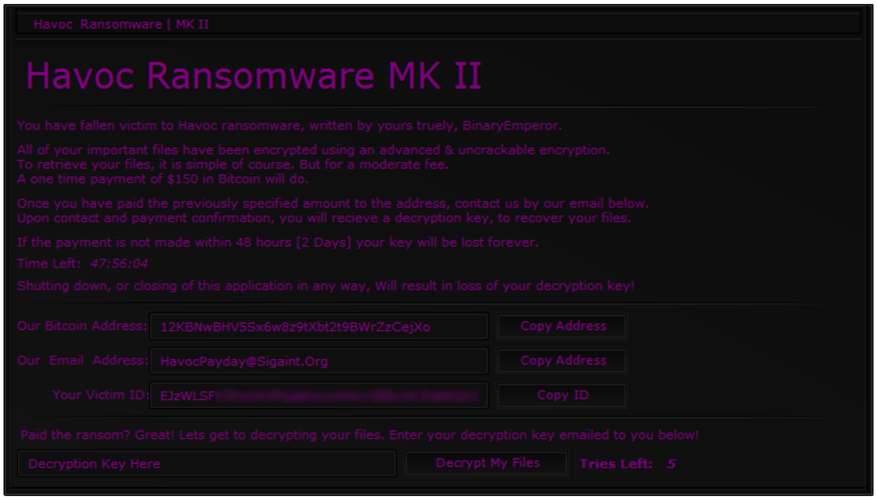


```
__--|+_.-
$=+*_-$-~+~*+$
*+*==$**-_|+_|=*=.+
..$.$
          !!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
    http://en.wikipedia.org/wiki/RSA_(cryptosystem)
    http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:


If all of this addresses are not available, follow these steps:
    1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
    2. After a successful installation, run the browser and wait for initialization.
    3. Type in the address bar: g46mbrrzpfszonuk.onion/6F[redacted]
    4. Follow the instructions on the site.

!!! Your personal identification ID: 6F[redacted] !!!
$._+._~~*
```

Figure 7 Locky ransom note

Locky ransomware is one of the most dangerous ransomware families based on the number of infections. Once it is installed on the victim's computer it will perform a scan and encrypt user files using its RSA-2048 & AES-128 encryption algorithm. It converts the filenames to a unique character letter and number combination and appends ".locky" or ".osiris" extension and deletes Shadow Volume copies of encrypted files as well as System Restore points. After encryption, a message (displayed on the user's desktop) instructs them to download the Tor browser and visit a specific website for further information where Locky demands a payment between 0.5-1 Bitcoin ($500-$1000).

9.5 Havoc MK II



Havoc Ransomware | MK II

Havoc Ransomware MK II

You have fallen victim to Havoc ransomware, written by yours truely, BinaryEmperor.

All of your important files have been encrypted using an advanced & uncrackable encryption.
To retrieve your files, it is simple of course. But for a moderate fee.
A one time payment of $150 in Bitcoin will do.

Once you have paid the previously specified amount to the address, contact us by our email below.
Upon contact and payment confirmation, you will recieve a decryption key, to recover your files.

If the payment is not made within 48 hours [2 Days] your key will be lost forever.

Time Left: *47:56:04*

Shutting down, or closing of this application in any way, Will result in loss of your decryption key!

Our Bitcoin Address: 12KBNwBHV5Sx6w8z9tXbt2t9BWrZzCejXo

Our Email Address: HavocPayday@Sigaint.Org

Your Victim ID: EJzWLSF[redacted]

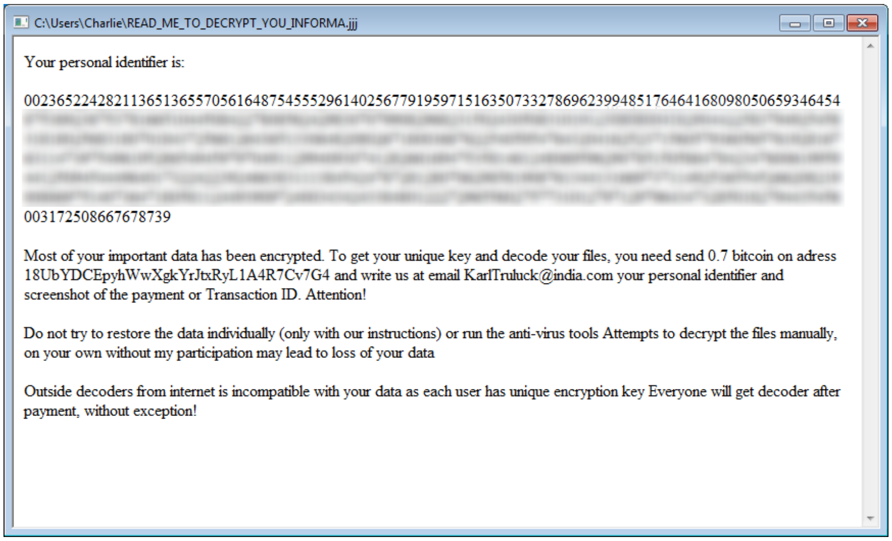
Paid the ransom? Great! Lets get to decrypting your files. Enter your decryption key emailed to you below!

Decryption Key Here

Tries Left: *5*

The Havoc MK II Ransomware's bright violet ransom note first appeared in public in January 2017. It uses RSA256 encryption and ".havokcrypt" extension to lock the victim's files, targeting a wide variety of files that can include video and audio files, text files, databases, images, and numerous other commonly used file types. However, Havoc Ransomware will not encrypt files that are larger than a certain limit, to make sure that the attack is as fast as possible. The user has 2 days to pay 0.15 Bitcoin ($150) ransom fee to restore the data or the restore key is deleted.

9.6 Globe3



C:\Users\Charlie\READ_ME_TO_DECRYPT_YOU_INFORMA.jjj

Your personal identifier is:

0023652242821136513655705616487545552961402567791959715163507332786962399485176464168098050659346454
[redacted]
003172508667678739

Most of your important data has been encrypted. To get your unique key and decode your files, you need send 0.7 bitcoin on adress 18UbYDCEpyhWwXgkYrJtxRyL1A4R7Cv7G4 and write us at email KarlTruluck@india.com your personal identifier and screenshot of the payment or Transaction ID. Attention!

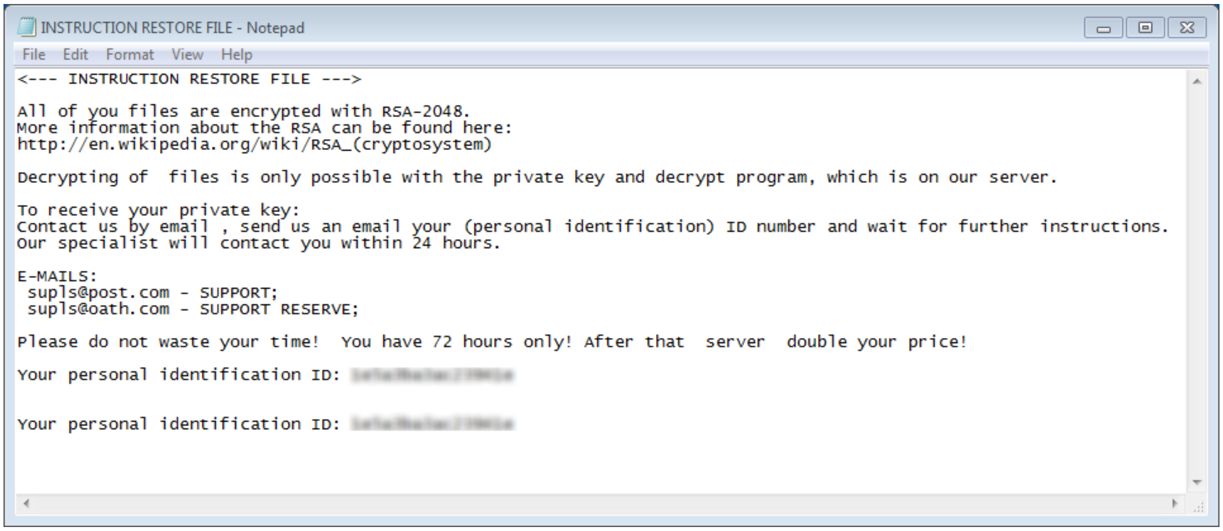
Do not try to restore the data individually (only with our instructions) or run the anti-virus tools Attempts to decrypt the files manually, on your own without my participation may lead to loss of your data

Outside decoders from internet is incompatible with your data as each user has unique encryption key Everyone will get decoder after payment, without exception!

Figure 8 Globe ransom note

The main targets of the Globe Ransomware are small business but it causes damage to any computer it infects. This crypto Trojan encrypts user data using AES-256 + RSA and adds ".wuciwug" extension to the files. The main difference from the previous two versions of the Globe3 is on the level of encryption operations. The first version of the Globe used the Blowfish algorithm to encrypt files, Globe2 used RC4 and RC4 + XOR. After encrypting a victim's files, the Globe3 shows "How to restore your files.hta" ransom note which advises the user about the 0.7 Bitcoin ($700) ransom fee and contains instructions on how to pay to recover the encrypted files.

9.7 CryptoMix

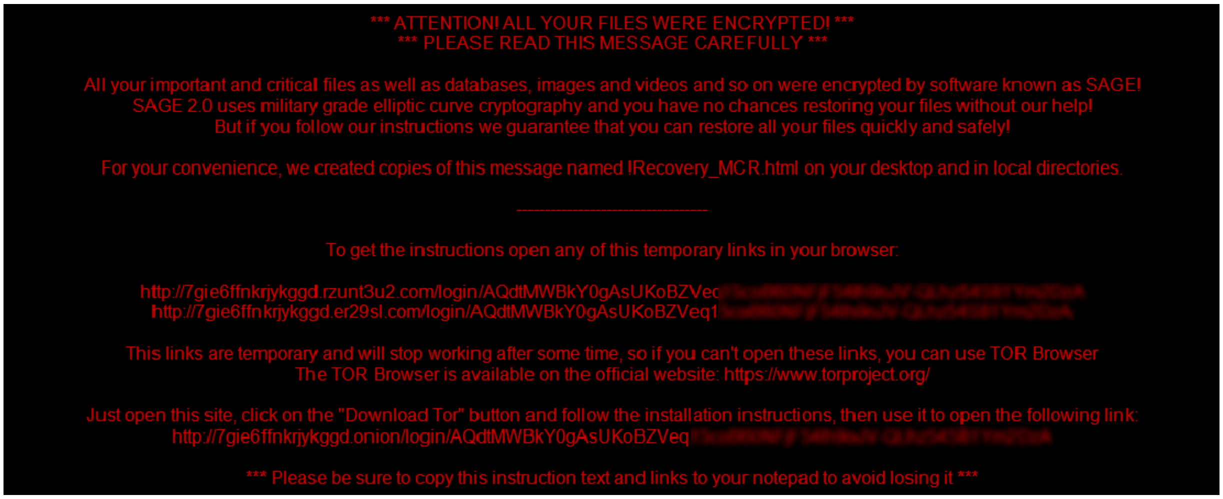

INSTRUCTION RESTORE FILE - Notepad
File Edit Format View Help

```
<--- INSTRUCTION RESTORE FILE --->

All of you files are encrypted with RSA-2048.
More information about the RSA can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)

Decrypting of  files is only possible with the private key and decrypt program, which is on our server.

To receive your private key:
Contact us by email , send us an email your (personal identification) ID number and wait for further instructions.
Our specialist will contact you within 24 hours.

E-MAILS:
 supls@post.com - SUPPORT;
 supls@oath.com - SUPPORT RESERVE;

Please do not waste your time!  You have 72 hours only! After that  server  double your price!

Your personal identification ID: [redacted]


Your personal identification ID: [redacted]
```

Figure 9 CryptoMix ransom note

CryptoMix Ransomware is made similarly to CryptoWall 3.0, CryptoWall 4.0 and CryptXXX. Just like many other encrypting trojans it uses AES + RSA-2048 ciphers to encrypt predetermined files but adds ".rdmk extension. Victims have to email the cyber criminals on the given email address and wait around 12 hours for a response which is encrypted and password protected. The ransom fee is usually around 5 Bitcoins ($500). CryptoMix claims that the collected profit is used for charity as the developers are calling themselves the Charity Team, who also offer a "Free tech support" for those who decided to pay up.

9.8 Sage 2.0

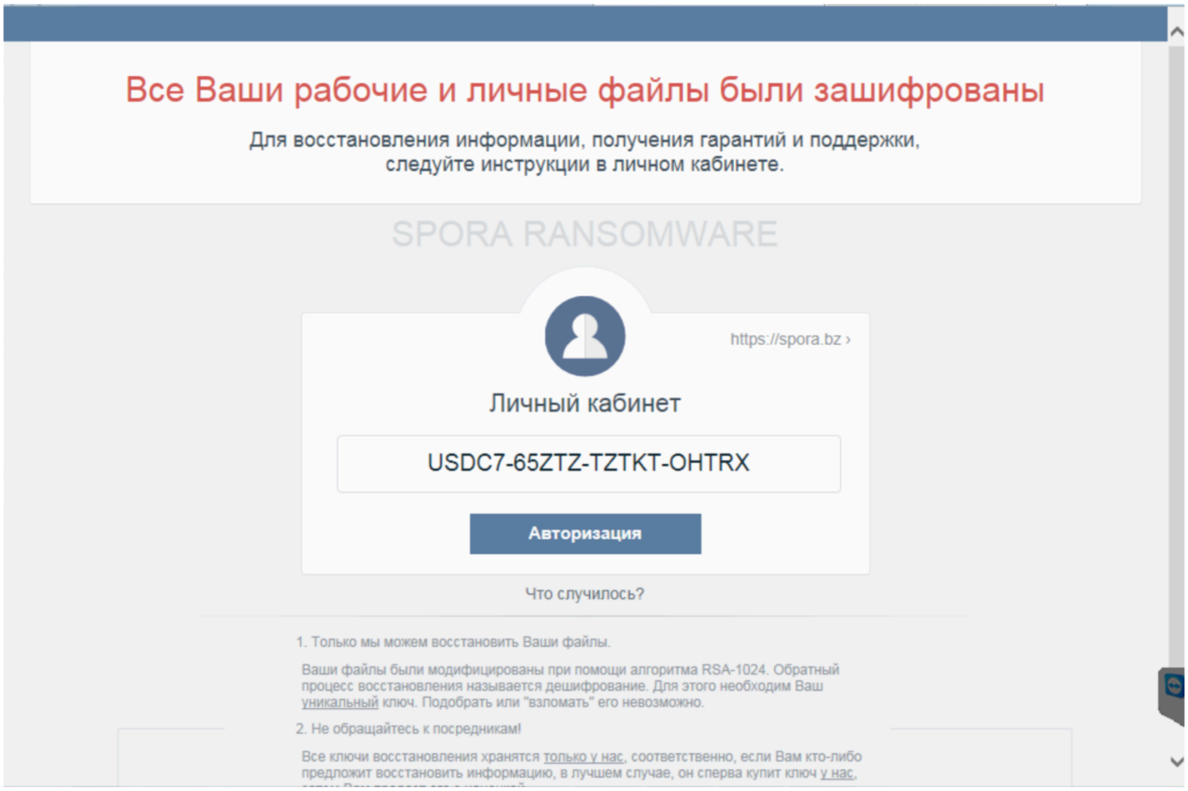


```
*** ATTENTION! ALL YOUR FILES WERE ENCRYPTED! ***
*** PLEASE READ THIS MESSAGE CAREFULLY ***

All your important and critical files as well as databases, images and videos and so on were encrypted by software known as SAGE!
SAGE 2.0 uses military grade elliptic curve cryptography and you have no chances restoring your files without our help!
But if you follow our instructions we guarantee that you can restore all your files quickly and safely!

For your convenience, we created copies of this message named !Recovery_MCR.html on your desktop and in local directories.

--------------------------------

To get the instructions open any of this temporary links in your browser:

http://7gie6ffnkrjykggd.rzunt3u2.com/login/AQdtMWBkY0gAsUKoBZVe[redacted]
http://7gie6ffnkrjykggd.er29sl.com/login/AQdtMWBkY0gAsUKoBZVeq1[redacted]

This links are temporary and will stop working after some time, so if you can't open these links, you can use TOR Browser
The TOR Browser is available on the official website: https://www.torproject.org/

Just open this site, click on the "Download Tor" button and follow the installation instructions, then use it to open the following link:
http://7gie6ffnkrjykggd.onion/login/AQdtMWBkY0gAsUKoBZVeq[redacted]

*** Please be sure to copy this instruction text and links to your notepad to avoid losing it ***
```

Figure 10 Sage ransom note

Sage Ransomware is related to the TeslaCrypt family. This crypto ransomware encrypts user data using AES-256 and RSA-1024 cipher and adds ".sage" file extension to them. After encrypting, Sage delivers its ransom note as a text file on the victim's Desktop and opens an HTML file in the default browser. It will also change the victim's Desktop image into its ransom note. It then instructs the victim to use a Tor-site to pay the 2 Bitcoin ($2000) ransom – which is doubled after 7 days – and get instructions on how to restore files.

9.9 Spora



Все Ваши рабочие и личные файлы были зашифрованы

Для восстановления информации, получения гарантий и поддержки,
следуйте инструкции в личном кабинете.

SPORA RANSOMWARE

https://spora.bz ›

Личный кабинет

USDC7-65ZTZ-TZTKT-OHTRX

Что случилось?

1. Только мы можем восстановить Ваши файлы.

Ваши файлы были модифицированы при помощи алгоритма RSA-1024. Обратный процесс восстановления называется дешифрование. Для этого необходим Ваш уникальный ключ. Подобрать или "взломать" его невозможно.

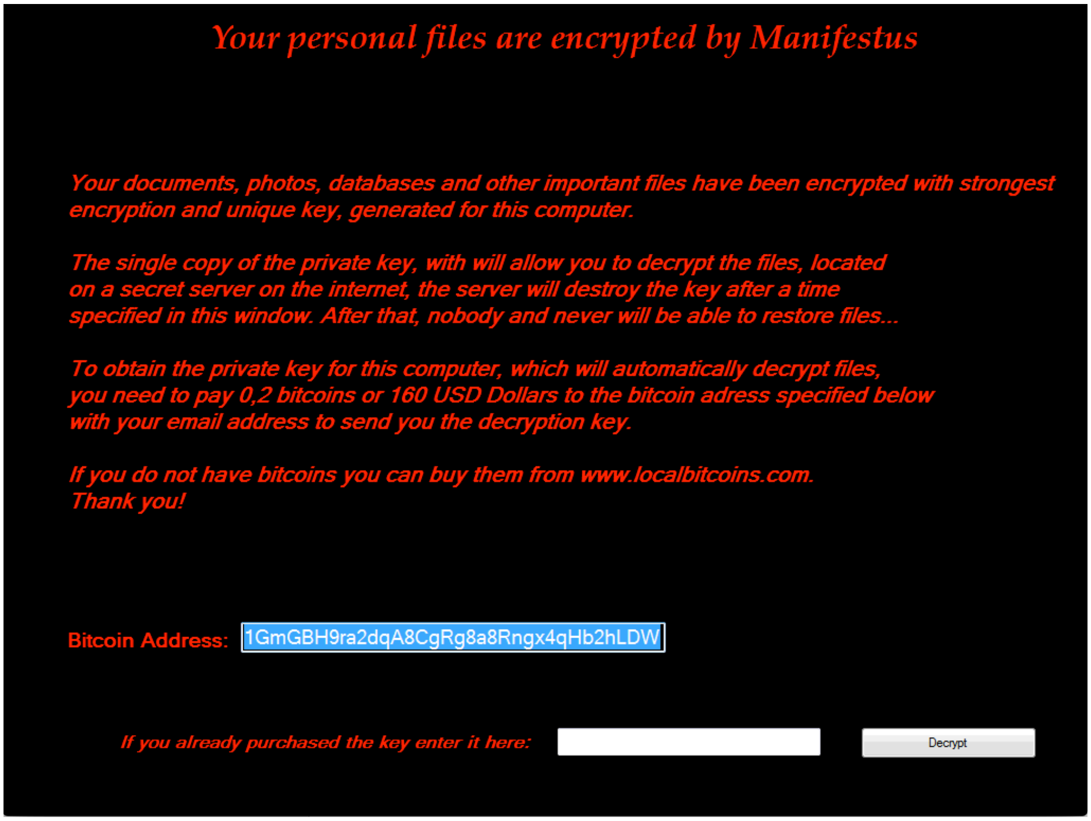
2. Не обращайтесь к посредникам!

Все ключи восстановления хранятся только у нас, соответственно, если Вам кто-либо предложит восстановить информацию, в лучшем случае, он сперва купит ключ у нас,

Figure 11 Spora ransom note

The Spora ransomware has Russian origins and emerged in the first days of 2017. It targets all MS Office, OpenOffice related files (.docx, .xslx etc.) as well as compressed zip archives. It uses the usual 'generated-AES key-encrypted-using-the-public-key-of-the-distributor' scheme for encryption. After a successful infection, the default browser is fired up, displaying a ransom note in Russian.

9.10 Manifestus



Your personal files are encrypted by Manifestus

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

The single copy of the private key, with will allow you to decrypt the files, located on a secret server on the internet, the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay 0,2 bitcoins or 160 USD Dollars to the bitcoin adress specified below with your email address to send you the decryption key.

If you do not have bitcoins you can buy them from www.localbitcoins.com.
Thank you!

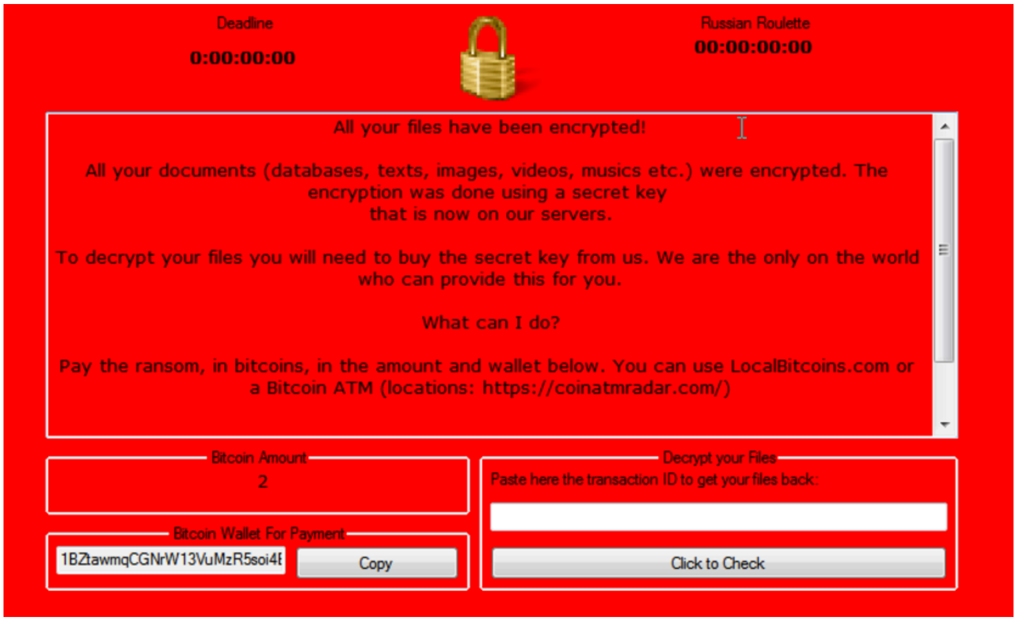
Bitcoin Address: 1GmGBH9ra2dqA8CgRg8a8Rngx4qHb2hLDW

If you already purchased the key enter it here:

Figure 12 Manifestus ransom note

Manifestus is a ransomware, first spotted in the wild in late 2016. The scrambled files are renamed to '[original].fucked' extension, the ransomware note instructs the use to pay 0.2 bitcoins ($160) for decryption.

9.11 Philadelphia



Deadline

0:00:00:00

Russian Roulette

00:00:00:00

All your files have been encrypted!

All your documents (databases, texts, images, videos, musics etc.) were encrypted. The encryption was done using a secret key
that is now on our servers.

To decrypt your files you will need to buy the secret key from us. We are the only on the world who can provide this for you.

What can I do?

Pay the ransom, in bitcoins, in the amount and wallet below. You can use LocalBitcoins.com or a Bitcoin ATM (locations: https://coinatmradar.com/)

Bitcoin Amount

2

Bitcoin Wallet For Payment

1BZtawmqCGNrW13VuMzR5soi4E

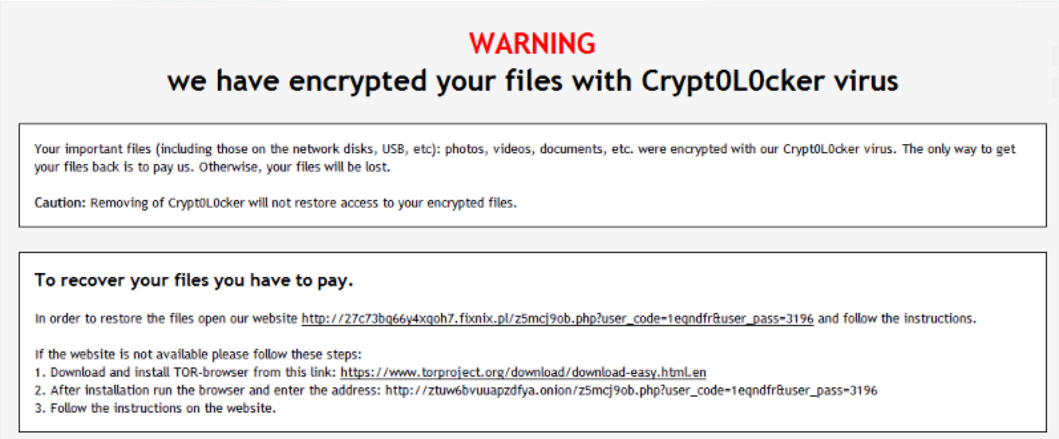
Decrypt your Files

Paste here the transaction ID to get your files back:

Figure 13 – Philadelphia ransom note

Philadelphia is one of the kit-in-a-box type of ransomware, which is marketed as the easiest-to-operate piece of kit. Encrypted files are provided with the extension .locked.

9.12 Crypt0L0cker



WARNING

we have encrypted your files with Crypt0L0cker virus

Your important files (including those on the network disks, USB, etc): photos, videos, documents, etc. were encrypted with our Crypt0L0cker virus. The only way to get your files back is to pay us. Otherwise, your files will be lost.

Caution: Removing of Crypt0L0cker will not restore access to your encrypted files.

To recover your files you have to pay.

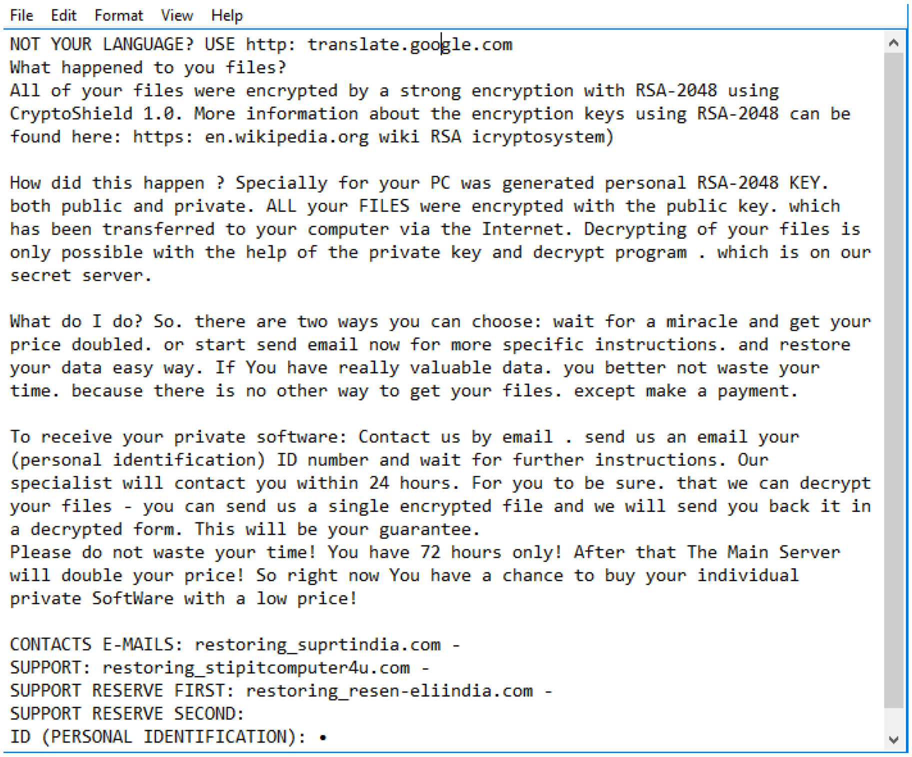
In order to restore the files open our website http://27c73bq66y4xqoh7.fixnix.pl/z5mcj9ob.php?user_code=1eqndfr&user_pass=3196 and follow the instructions.

If the website is not available please follow these steps:
1. Download and install TOR-browser from this link: https://www.torproject.org/download/download-easy.html.en
2. After installation run the browser and enter the address: http://ztuw6bvuuapzdfya.onion/z5mcj9ob.php?user_code=1eqndfr&user_pass=3196
3. Follow the instructions on the website.

Figure 14 – Crypt0l0cker ransom page

After infection, Crypt0l0cker encrypts files with a set of known extensions and prompts the user to pay the desired ransom.

9.13 CryptoShield



```
NOT YOUR LANGUAGE? USE http: translate.google.com
What happened to you files?
All of your files were encrypted by a strong encryption with RSA-2048 using
CryptoShield 1.0. More information about the encryption keys using RSA-2048 can be
found here: https: en.wikipedia.org wiki RSA icryptosystem)

How did this happen ? Specially for your PC was generated personal RSA-2048 KEY.
both public and private. ALL your FILES were encrypted with the public key. which
has been transferred to your computer via the Internet. Decrypting of your files is
only possible with the help of the private key and decrypt program . which is on our
secret server.

What do I do? So. there are two ways you can choose: wait for a miracle and get your
price doubled. or start send email now for more specific instructions. and restore
your data easy way. If You have really valuable data. you better not waste your
time. because there is no other way to get your files. except make a payment.

To receive your private software: Contact us by email . send us an email your
(personal identification) ID number and wait for further instructions. Our
specialist will contact you within 24 hours. For you to be sure. that we can decrypt
your files - you can send us a single encrypted file and we will send you back it in
a decrypted form. This will be your guarantee.
Please do not waste your time! You have 72 hours only! After that The Main Server
will double your price! So right now You have a chance to buy your individual
private SoftWare with a low price!

CONTACTS E-MAILS: restoring_suprtindia.com -
SUPPORT: restoring_stipitcomputer4u.com -
SUPPORT RESERVE FIRST: restoring_resen-eliindia.com -
SUPPORT RESERVE SECOND:
ID (PERSONAL IDENTIFICATION): •
```

Figure 15 – Cryptoshield ransom note

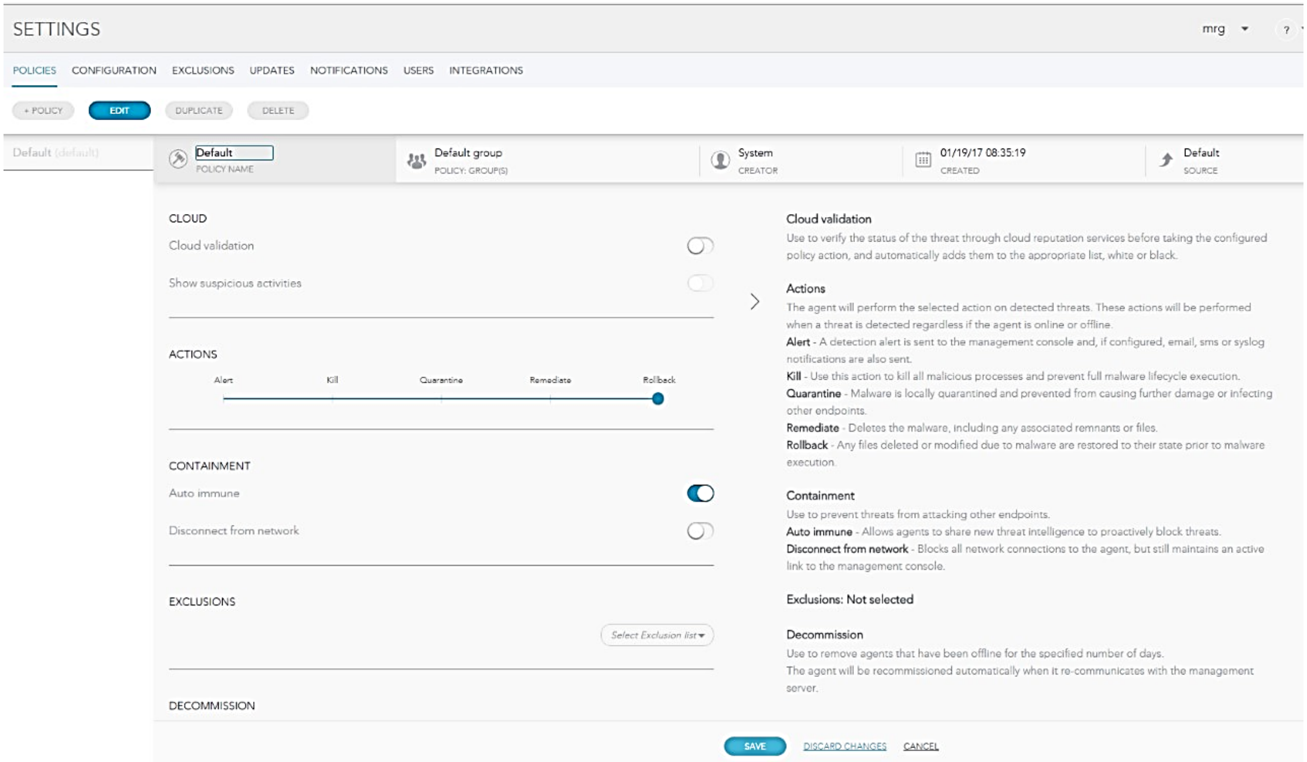
CryptoShield uses 2048-bit RSA for key encryption and AES-256 for file encryption. The encrypted file names are scrambled and they are appended the .CRYPTOSHIELD extension. Besides encryption, the piece of malware also deletes Volume Shadow Copy backups from all drives it has access to.

10 Appendix - Non-default AV setup

Most tests have been carried out using default settings. In this chapter, we describe all cases, where we deviated from the default setup.

10.1 SentinelOne

The following image shows the setup.



Default — POLICY NAME

Default group — POLICY: GROUP(S)

System — CREATOR

01/19/17 08:35:19 — CREATED

Default — SOURCE

CLOUD

Cloud validation ○

Show suspicious activities ○

ACTIONS

Alert — Kill — Quarantine — Remediate — Rollback ●

CONTAINMENT

Auto immune ●

Disconnect from network ○

EXCLUSIONS

Select Exclusion list ▾

DECOMMISSION

Cloud validation
Use to verify the status of the threat through cloud reputation services before taking the configured policy action, and automatically adds them to the appropriate list, white or black.

Actions
The agent will perform the selected action on detected threats. These actions will be performed when a threat is detected regardless if the agent is online or offline.
Alert - A detection alert is sent to the management console and, if configured, email, sms or syslog notifications are also sent.
Kill - Use this action to kill all malicious processes and prevent full malware lifecycle execution.
Quarantine - Malware is locally quarantined and prevented from causing further damage or infecting other endpoints.
Remediate - Deletes the malware, including any associated remnants or files.
Rollback - Any files deleted or modified due to malware are restored to their state prior to malware execution.

Containment
Use to prevent threats from attacking other endpoints.
Auto immune - Allows agents to share new threat intelligence to proactively block threats.
Disconnect from network - Blocks all network connections to the agent, but still maintains an active link to the management console.

Exclusions: Not selected

Decommission
Use to remove agents that have been offline for the specified number of days.
The agent will be recommissioned automatically when it re-communicates with the management server.

Figure 16 Sentinel One setup

10.2 Kaspersky

Kaspersky provided us with a detailed document regarding test setup. Relevant sections of the document can be found below.

The following settings only applies to Kaspersky Endpoint Security Cloud. It does not apply to Kaspersky Anti-Ransomware tool for Business or Kaspersky Endpoint Security.

10.2.1 Kaspersky Endpoint Security Cloud deployment guide

10.2.2 How to turn on maximum protection in KES Cloud

1) Go to Security profiles – Select Default – you should have pre-selected Windows OS and Protection section enabled.
2) For File anti-virus please click Settings button and select high security level inside. Save change. Click on the Protection settings title. Do the same for mail anti-virus, save changes. Click on the protection settings title again. Do same for the web anti-virus, save changes, click on Protection settings title.
3) Make sure Network attack blocker is enables, System watcher is enabled, firewall is enabled.
4) Go to Advanced section. Click on Settings for Threats and Exclusions. Turn on Detection of other types of objects. Save changes. Turn on Advanced Disinfection technology. Save changes.
5) Click on Advanced Title. Save changes.
6) Click on Settings button near Information for Technical Support section. Make sure dump writing is enabled.
7) Click Setting for Protection and Self-Defense. Enable External control of system service. Click Save. Click Settings button near Scan removable drives on connection. In the opened window select Full scan and click OK. Click Save button. Click Advanced title of the page section. Click Save.