Comparative Efficiency Assessment of
Enterprise Security Suites against In-the-wild
Ransomware
April 2017
Table of Contents

1 Executive Summary ............................................................................................................. 4
2 Introduction .......................................................................................................................... 6
  2.1 Structure of this report ..................................................................................................... 6
  2.2 Overview ......................................................................................................................... 6
  2.3 Ransomware as a business model ................................................................................. 7
3 Selection of participants ...................................................................................................... 7
  3.1 Inaccurate or misleading marketing .............................................................................. 8
  3.1.1 Bitdefender .................................................................................................................. 9
  3.1.2 Sophos Intercept X ....................................................................................................... 10
  3.2 Utilities with limited functionality .................................................................................. 10
  3.2.1 Trend Micro Ransomware Screen Unlocker Tool ....................................................... 11
  3.2.2 Talos TeslaCrypt Decryption Tool .............................................................................. 11
  3.3 Vendors refusing to test their product ......................................................................... 11
    3.3.1 Cylance CylanceProtect .......................................................................................... 11
    3.3.2 Panda Adaptive Defense 360 ..................................................................................... 11
4 Ransomware families in scope ........................................................................................... 12
5 Detailed Results ................................................................................................................... 13
6 Methodology ....................................................................................................................... 15
  6.1 Infection methods ......................................................................................................... 15
  6.2 Result interpretation ...................................................................................................... 15
  6.3 False positive tests ....................................................................................................... 16
7 Conclusion ........................................................................................................................... 17
8 Appendix – Participation in this test .................................................................................. 18
  8.1 Participation in this test – Panda Adaptive Defense 360 .............................................. 18
  8.2 Participation in this test – Cylance CylancePROTECT .............................................. 18
9 Appendix – ransomware families used ............................................................................. 20
  9.1 Dharma .......................................................................................................................... 20
  9.2 Troldesh .......................................................................................................................... 20
  9.3 Cerber ............................................................................................................................. 22
  9.4 Locky .............................................................................................................................. 23
  9.5 Havoc MK II .................................................................................................................... 24
  9.6 Globe3 ............................................................................................................................. 24
  9.7 CryptoMix ....................................................................................................................... 25
  9.8 Sage 2.0 .......................................................................................................................... 25
  9.9 Spora ................................................................................................................................ 26
  9.10 Manifestus .................................................................................................................... 27
9.11 Philadelphia..............................................................................................................................28
9.12 Crypt0L0cker ............................................................................................................................28
9.13 CryptoShield ............................................................................................................................29
10 Appendix - Non-default AV setup .................................................................................................29
10.1 SentinelOne ................................................................................................................................29
10.2 Kaspersky ....................................................................................................................................30
   10.2.1 Kaspersky Endpoint Security Cloud deployment guide .........................................................30
   10.2.2 How to turn on maximum protection in KES Cloud .............................................................30
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 types, 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
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 incident1.

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,

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

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

(1) limited functionality
(2) refused to provide product installer and license key.
(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, 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 marketing materials](image)

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.

---

*I 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](https://www.bitdefender.com/solutions/anti-ransomware-tool.html).

---

*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 Intercept X marketing materials](image)

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.

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.
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

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
Zolton
9 Appendix – ransomware families used

9.1 Dharma

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

Troldesh ransom page

Dharma ransom page

Figure 3 Dharma ransom page

Figure 4 Troldesh ransom page
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, 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 'DECRIPT 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

![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

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

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

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

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.
The Spora ransomware has Russian origins and emerged in the first days of 2017. It targets all MS Office, OpenOffice related files (.docx, .xlsx 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

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.

Figure 12 Manifestus ransom note
9.11 Philadelphia

![Philadelphia ransom note](image)

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

![Crypt0L0cker ransom page](image)

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

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.
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.