In-the-wild Ransomware Protection Comparative Analysis 2016 Q3

Table of Contents

1 Introduction

"Ransomware is a Cryptovirology attack carried out using covertly installed malware that encrypts the victim's files and then requests a ransom payment in return for the decryption key that is needed to recover the encrypted files. Thus, ransomware is an access-denial type of attack that prevents legitimate users from accessing files since it is intractable to decrypt the files without the decryption key". [1] Before ransomware was trendy among cyber-criminals, a malware infection was not a high priority for most users. Financial malware could be defeated via fraud detection, spammed Facebook walls were cleaned, and life could continue uninterrupted. Sometimes, the presence of the malware was not even noticed for months. But this has changed since ransomware became prevalent. The use of crypto-currencies like Bitcoin made it easy to cash out quickly. And because the malware has to only run for some minutes on the victim's computer, most reactive protections failed quickly, and left the users unprotected against these ~~cyber~~criminals. Multiple generic ransomware protection emerged to solve this issue.

WatchDogDevelopment.com, LLC commissioned MRG Effitas to conduct a comparative analysis of its Watchdog Anti-Malware product, and other prevalent generic ransomware tools.

1.1 Watchdog Anti-Malware

Watchdog Anti-Malware is a second-opinion malware scanner designed to rescue a computer from malware that has infected the computer despite all the security measures taken. It uses cloud-based scanning to reduce detection time for new virus outbreaks and to improve scanning performance. The tested version was 2.21.186.139. Besides the default settings used, Pandora Cloud-Sandbox Technology was turned on. Pandora works as a combination of cloud reputation database (blocking previously unknown files), and a cloud sandbox, where suspicious samples are sent to the cloud, and analyzed there. If a sample is detected as malicious, all Watchdog users (even where Pandora is turned off) are protected in the future against that specific threat.

[1] https://en.wikipedia.org/wiki/Ransomware

1.2 Competitor products tested

- BitDefender Anti-ransomware 1.0.12.1
- Cryptoprevent 7.4.21.0
- MalwareBytes Anti-Ransomware Beta 0.9.16.484, 1.0.0
- Hitmanpro Alert build 3.1.10 373

1.3 Watchdog reputation based on detection vs generic detection

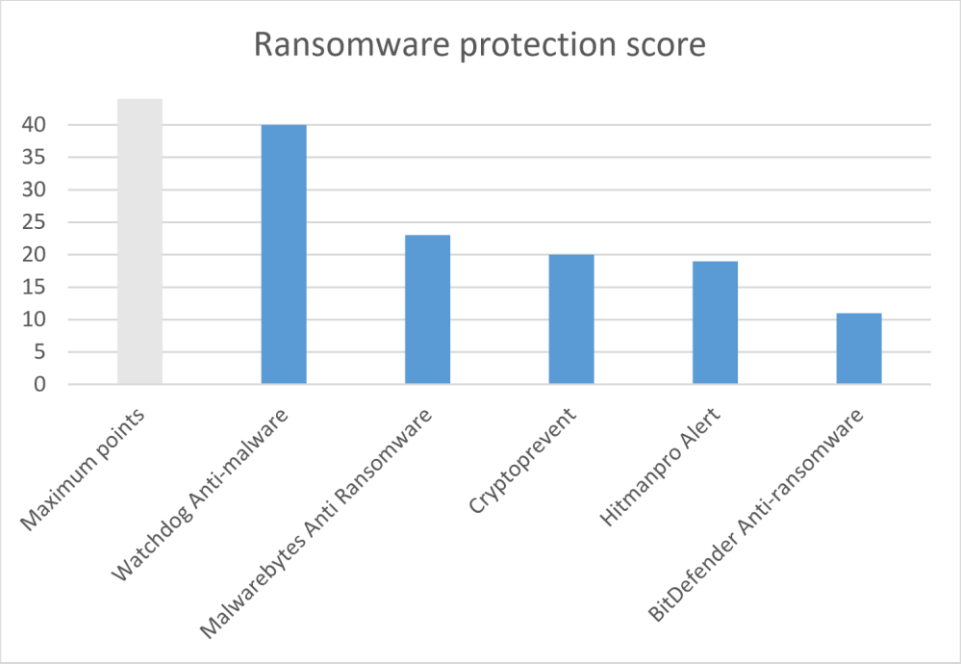
Watchdog works differently to the other generic ransomware detection tools. Some of those tools detect generic ransomware behaviour, for example, injecting into explorer.exe, or overwriting structured data with high entropy (encrypted) unstructured data. Other tools create white-lists on folders usually used by ransomware.

Meanwhile, Watchdog uses its cloud reputation system to check for unknown binaries. One might ask the question, "how can we test known malware against these different detection techniques?" Because of this, we tested Watchdog in two configurations, one where we used the original dropper, and one where we changed the hash of the dropper – thus it was totally new and unknown to Watchdog. Due to the way Pandora technology works in Watchdog, the results were the same, and all malware samples were blocked from execution. The good thing with this approach is that even Patient Zero does not get infected.

1.4 Executive summary

We tested the ransomware protection tools against eleven different ransomware, which have been prevalent in-the-wild over the past 3-4 years. First, we installed the protection tool into the system, then started the ransomware (or ransomware dropper), and when the ransomware process exited (or was killed), we scanned the system for the presence of encrypted files.

Final results



Based on this report, Watchdog Anti-Malware proved to be the best ransomware protection among the tested products during the test. These scores are not normalized with the prevalence of the ransomware samples. Usually, the most prevalent samples are included in these generic protections, but as always, life (and IT Security) is never simple.

2 Tests employed and results

This ransomware protection test was performed as follows: We created generic documents and pictures on the user's desktop folder, installed the generic ransomware protection system on a clean machine, acquired a dropper for the ransomware and started the ransomware. Then, if the ransomware was detected or blocked by the protection, after the full remediation took place we checked the filesystem for encrypted files. The scoring is based on the level of protection and remediation.

When conducting these tests, we tried to simulate normal user behaviour. We are aware that a "Real World" test cannot be conducted by a team of professionals inside a lab because we understand how a ransomware works, how it attacks and how such attacks could be prevented. Simulating normal user behaviour means that we paid special attention to all alerts given by security applications.

All tests were carried out in a virtualized environment, where malware cannot detect the presence of virtualization, on a fully patched Windows 10 64-bit. All Smartscreen protections (URL, download, execute) from Windows have been turned off, and Defender was turned off as well.

The test was carried out between June 20 and July 14, 2016.

2.1 High-level overview of the tests

Sample selection is of fundamental importance to this and all similar tests. The type of samples used is selected by MRG Effitas on the basis of a mixture of criteria, centred on key relevancies:

1. Prevalence – they are widespread (among ransomware) and so represent the most common threats.
2. Innovation – they employ innovative techniques to counter security measures.
3. It is malware having ransomware capabilities, by encrypting user files and demanding ransomware in exchange.

During our tests we did not use the latest zero day ransomware, because it is very hard to acquire working recent samples from 10 different families, as usually only 4-5 different families are active at a specific point in time. What made this test challenging is that most malware won't be working if the C&C server is down. And for some ransomware, the C&C is only up for 1-2 days. For others, it can be up for months. On a side note, if the ransomware was not designed to run without the C&C but it encrypted the files, chances are that even after paying the ransom, the files won't be decrypted.

All samples started the encryption instantly; there was no need to wait. We monitored file system changes, thus we had good list of candidates to check for and knew where we can check for encrypted files.

After we confirmed that the ransomware was working as expected on a non-protected system, we installed the generic ransomware protection tool, updated it to the latest version (both program and signatures), and started with default configuration. Cloud connectivity was allowed. Whenever the software detected the presence of the ransomware, we executed the default action (quarantine or delete). If the protection software demanded a computer reboot for remediation, we rebooted the computer.

The small number of test cases (10 in-the-wild ransomware + one ransomware simulator) is due to the fact that ransomware tests cannot be done automatically, and all remediation has to be followed by a forensics analysis, which is time consuming. Also, instead of using 100 different samples from the same ransomware family, we tested with diverse sets of ransomware. We would love to test more families, but it is not easy to find working samples. For example, one ransomware (CryptXXX) started to encrypt files on an unprotected system, then crashed.

2.2 Scoring

As there are different levels of remediation, we came up with the following scoring system. Each software was able to collect points on every test, and the security software received:

- 0 points whenever the ransomware was not detected or remediated, and all files in scope for the ransomware have been encrypted.
- 1point if the ransomware was detected and blocked, but a large portion of the files remained encrypted after remediation.
- 3 points when the ransomware was detected and blocked, but only a small portion of the files remained encrypted.
- 4 points when the rootkit was detected, fully remediated, and no files have been encrypted at the end.

2.3 Ransomware tested and results

We tested the following ransomware samples against the generic ransomware prevention tools:

2.3.1 CTB Locker

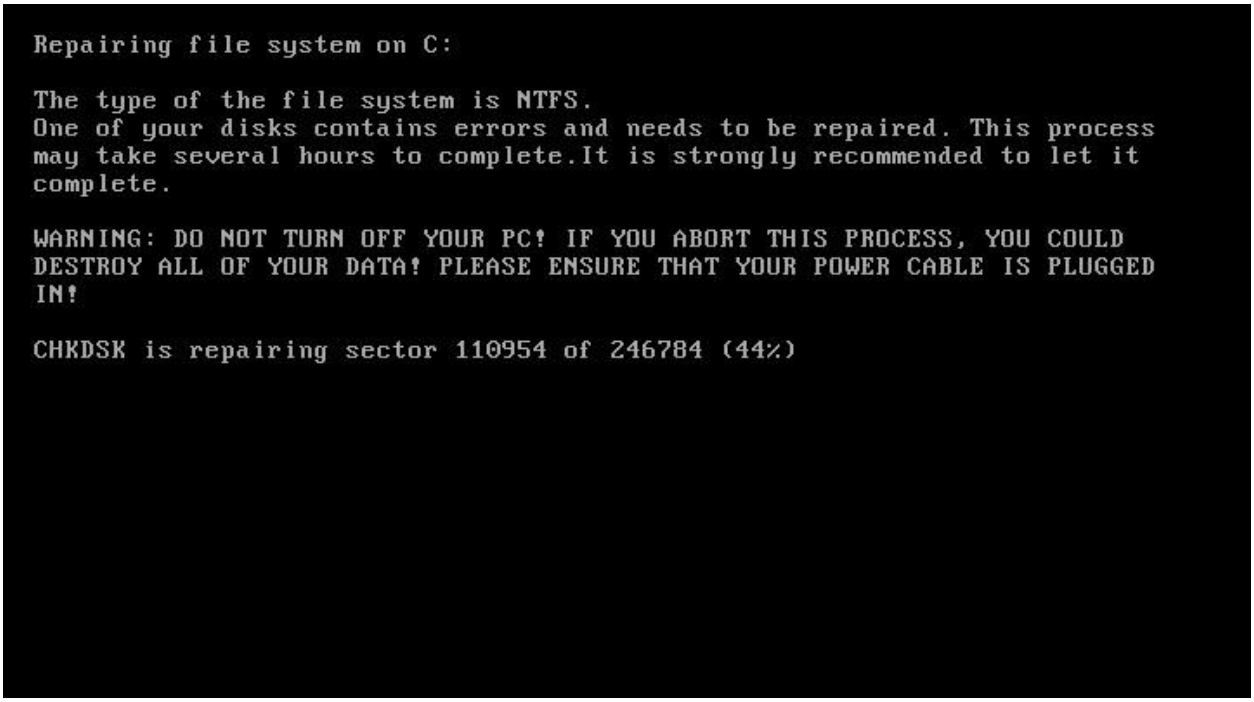
CTB-Locker was distributed via exploit kits and spam. It usually injects itself into the explorer.exe process, and start the encryption from that process. The sample is from December, 2014. SHA-256: 8567d46ff961222a2f084286b5750e462df681f4d4ea5bb787514 8cb4ab25be4

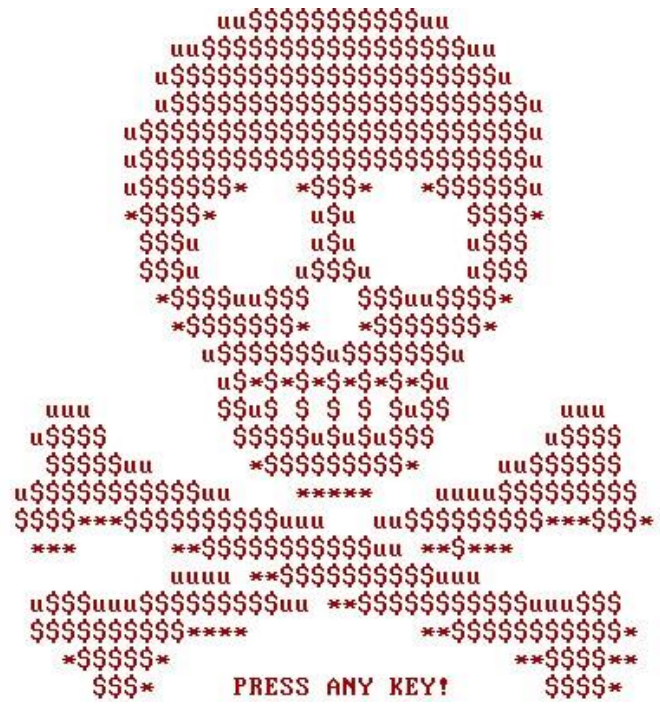
Test results

	Watchdog Anti-Malware	Bitdefender Antiransomware	Cryptoprevent	Hitmanpro Alert	MalwareBytes Anti Ransomware
Score	**4**	**4**	**4**	**4**	**3**

2.3.2 Petya

The Petya ransomware is very different from the common ransomware. It installs itself to start before Windows, causes a BSOD in Windows, and after Windows restarts, it mimics a file repair, but in reality, it encrypts the MFT (Master File Table). The sample is from March 2016. SHA-256: 26b4699a7b9eeb16e76305d843d4ab05e94d43f3201436927e13b3ebafa90739






```
You became victim of the PETYA RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade
encryption algorithm. There is no way to restore your data without a special
key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy
steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need
   help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

   http://petya37h5tbhyvki.onion/5aV6XV
   http://petya5koahtsf7sv.onion/5aV6XV

3. Enter your personal decryption code there:

   3ePUAW-ovNzkg-LLMJE2-7SCxQQ-DbWSvu-EFJmWU-QWvUpj-CXRshz-TJGxwj-2YJ5zX-
   owosVn-LGTGvS-Qih1VU-TTG8ce-xqBtdR

If you already purchased your key, please enter it below.

Key: _
```

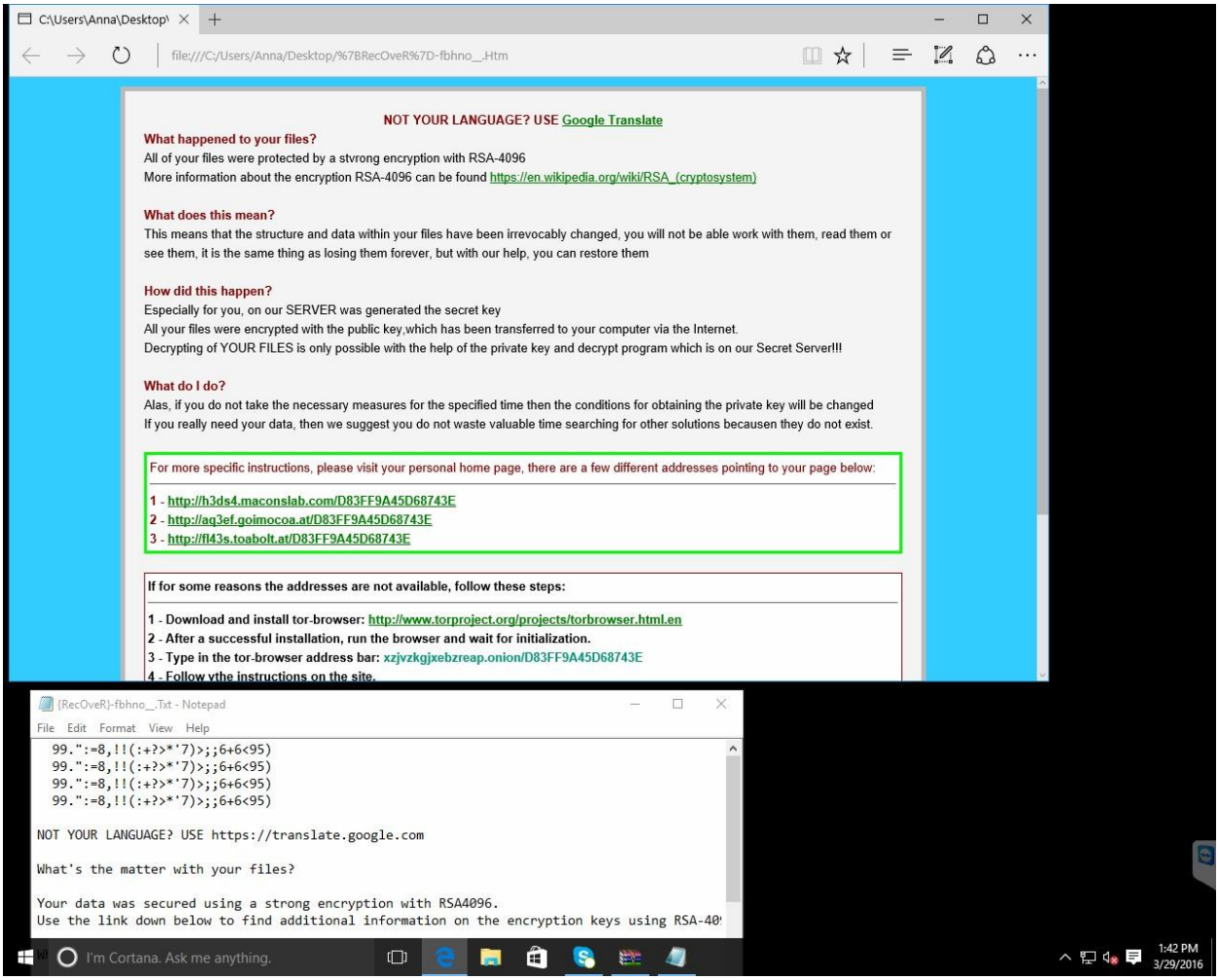
Test results

	Watchdog Anti-Malware	Bitdefender Antiransomware	Cryptoprevent	Hitmanpro Alert	MalwareBytes Anti Ransomware
Score	**4**	**0**	**0**	**0**	**0**

Because Petya works totally different than other ransomware, most generic ransomware protection was totally ineffective against this threat.

2.3.3 TeslaCrypt

This malware was usually distributed via the Angler exploit-kit. It has multiple anti-debug features, and injects itself into other processes before encrypting. It also deletes shadow copy files. The sample is from April, 2016. SHA-256: d8ee200589d8e7d72878ea79bcfc9d18ee52569c046df74fa0dfe7e33d9ec422

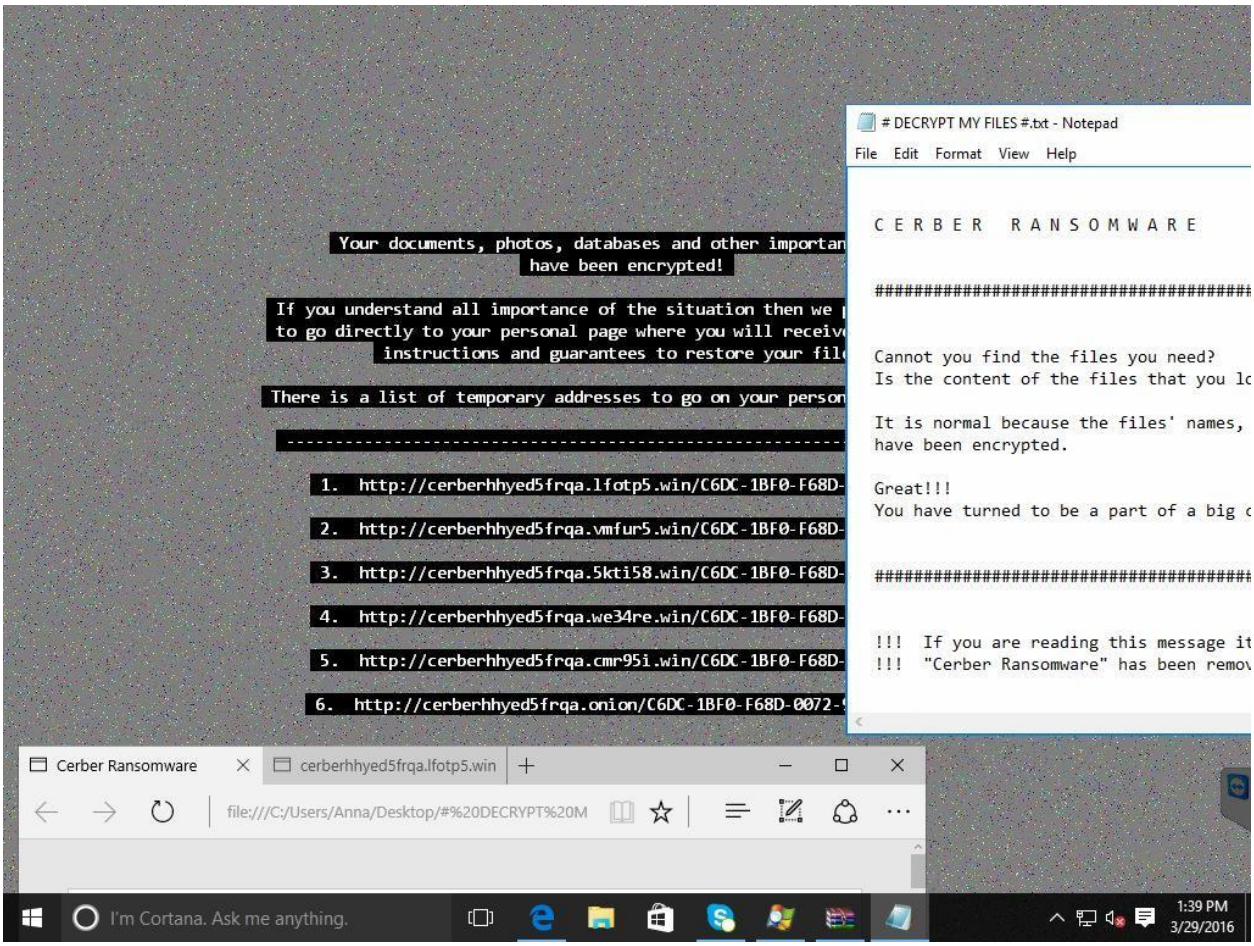


Test results

	Watchdog Anti-malware	Bitdefender Antiransomware	Cryptoprevent	Hitmanpro Alert	MalwareBytes Anti Ransomware
Score	**4**	**3**	**4**	**3**	**3**

2.3.4 Cerber

Cerber is a very recent ransomware. It can work offline by design; thus it can more easily attack enterprise systems. It can also bypass UAC for better destruction. The sample is from June, 2016. SHA-256: 7b6c225989d2a1f1bd845fa620c1fc2e5196ab2673cca16a05b9929c152e7d65



Test results

	Watchdog Anti-Malware	Bitdefender Antiransomware	Cryptoprevent	Hitmanpro Alert	MalwareBytes Anti Ransomware
Score	**4**	**0**	**4**	**3**	**3**

2.3.5 Mircop (Autoit)

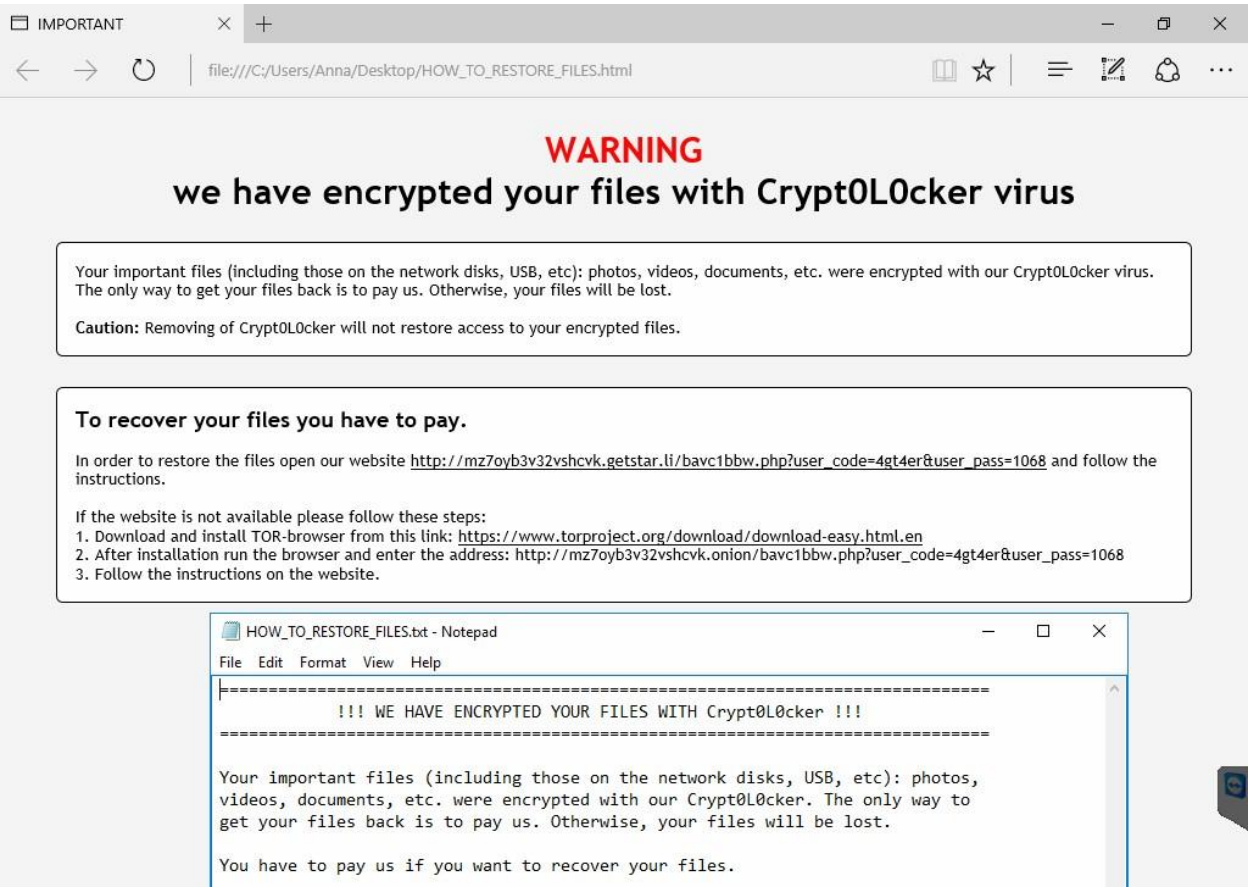
When we tested this sample, three strange things happened. First, it was not documented anywhere on the Internet, so it was a totally new malware family at the time of test. Also, the amount of BTC is incredibly high. The usual amount is around ~2-3 BTC, not 48.48. Last but not least, there are no instructions how one can decrypt the files, or where to contact the ransomware operators. Which means, after paying, there is no way to get back the files via "official channels" – luckily, a decrypter tool is already available. The malware is usually distributed via spam, and uses DES to encrypt files. It can also steal credentials from popular software, and SHA-256: af84eda1d8264f2babf6d3771868eb2f7655d52b6d4e66675efd7e3a1101d9b0

Test results

	Watchdog Anti-Malware	Bitdefender Antiransomware	Cryptoprevent	Hitmanpro Alert	MalwareBytes Anti Ransomware
Score	**4**	**0**	**0**	**0**	**0**

2.3.6 Crypt0L0cker

This ransomware is a descendant of the TorrentLocker ransomware. It is usually distributed via spam, uses geolocation check before infection, can bypass UAC, deletes shadow copy files, and encrypts files with AES-256 in CBC mode. The sample is from June, 2016. SHA-256: 67fd7ec290f03bbd4a0a68eae1f28ea41036008883ee57e52092257e6ced71c7

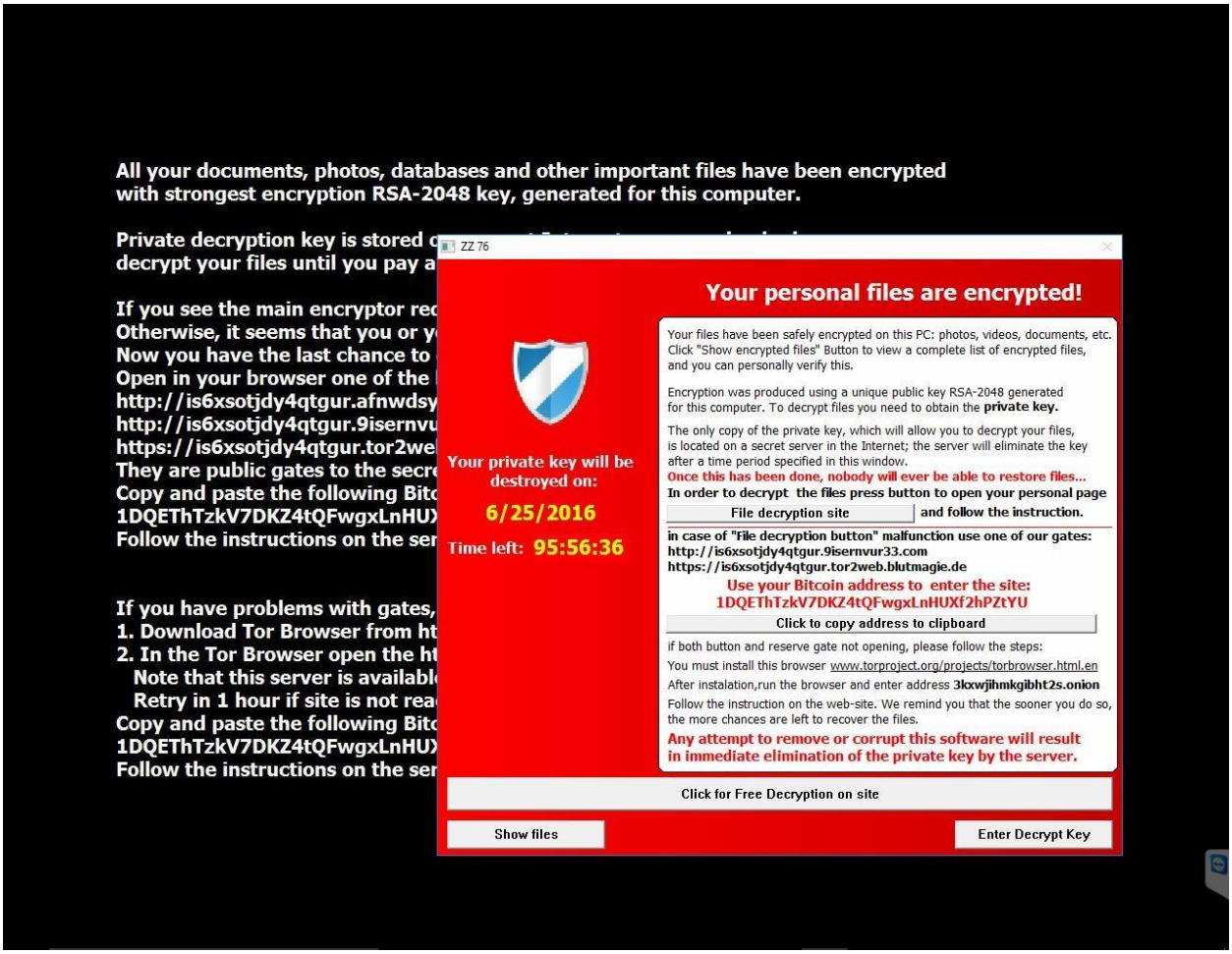


Test results

	Watchdog Anti-Malware	Bitdefender Antiransomware	Cryptoprevent	Hitmanpro Alert	MalwareBytes Anti Ransomware
Score	**4**	**0**	**0**	**3**	**3**

2.3.7 Alphacrypt

As other ransomware, this deletes the shadow copy before encryption. It was usually distributed via exploit kits (Angler). It can also delete shadow copy files, and uses AES to encrypt files. The sample is from March, 2015. SHA-256: 99fc04d82877aea0247286d41186b985ab773b19c8cef8786ffc1fa50e35af29

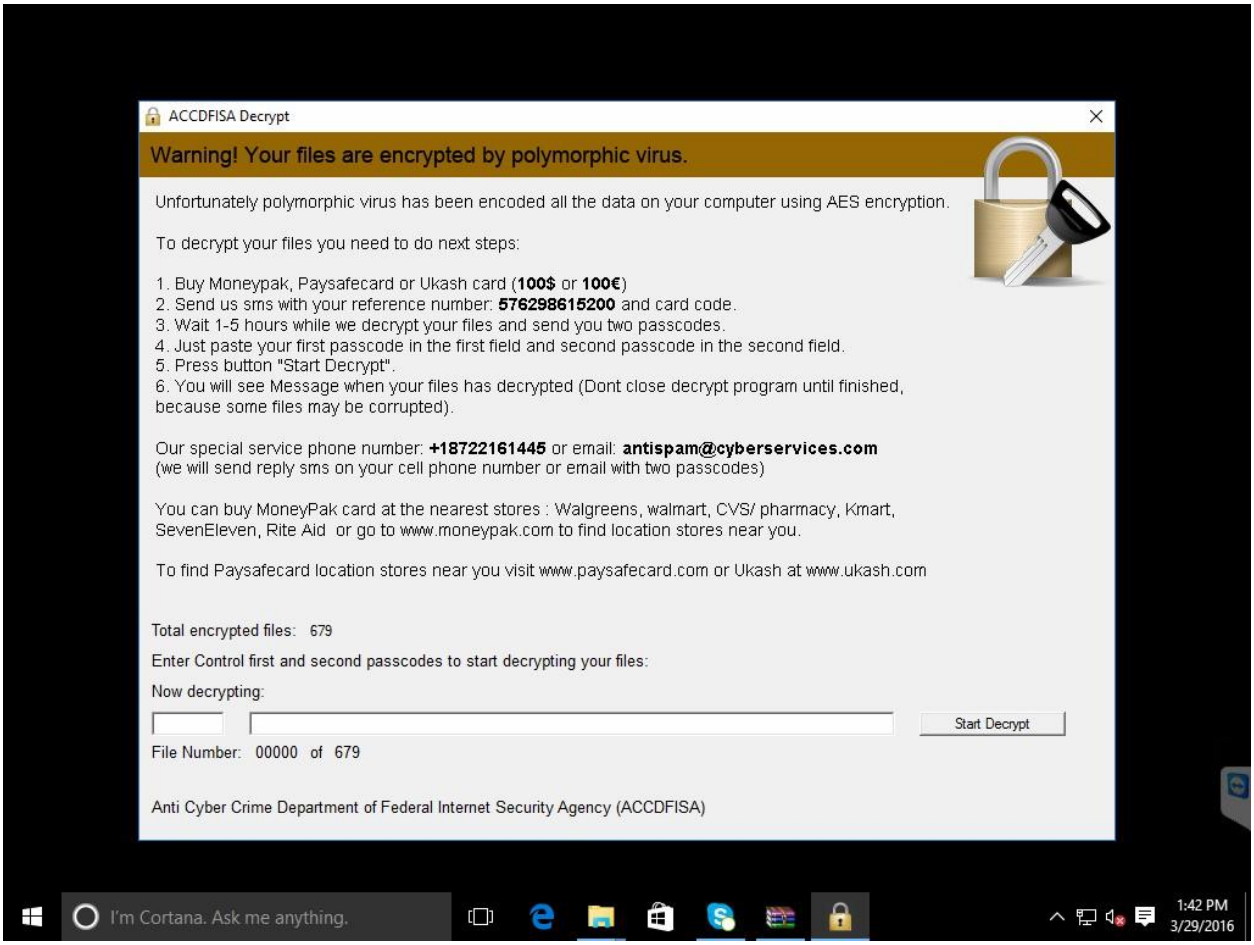


Test results

	Watchdog Anti-Malware	Bitdefender Antiransomware	Cryptoprevent	Hitmanpro Alert	MalwareBytes Anti Ransomware
Score	**4**	**0**	**4**	**3**	**4**

2.3.8 ACCDFISA (Winrar based)

This ransomware is an old and strange one. It was usually distributed via unprotected RDP sessions. The authors did not bother to write their own encryption, they just used WinRAR to do that. The sample is from February, 2012. SHA-256: 59ed7a26c56a644bf3f5ba45459965be8a6e6b79dcf4f90a5c51f2bb12190bf9



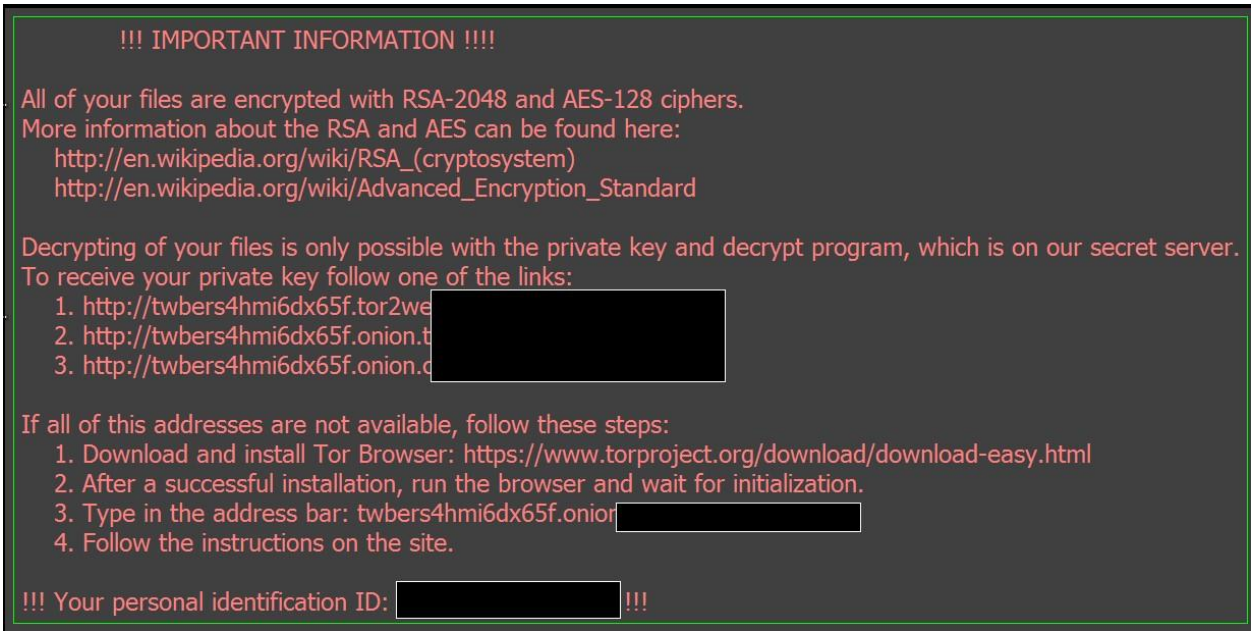
Test results

	Watchdog Anti-Malware	Bitdefender Antiransomware	Cryptoprevent	Hitmanpro Alert	MalwareBytes Anti Ransomware
Score	**4**	**0**	**0**	**0**	**0**

It is possible that generic detection did not work on this ransomware because it uses legitimate tools to encrypt files. It is quite interesting to see that primitive methods can bypass generic detection.

2.3.9 Locky

The Locky sample was the most challenging of all to start, by far. It employs lot of different anti-sandbox features, and usually, the C&C is up for days only. Usually it is distributed via spam, and uses AES to encrypt precious user files. The sample is from June, 2016. SHA-256:
3f5ff5d9d0615cc04e644297dcbfa999f6d6930850848f038464d0a486e6b8d0



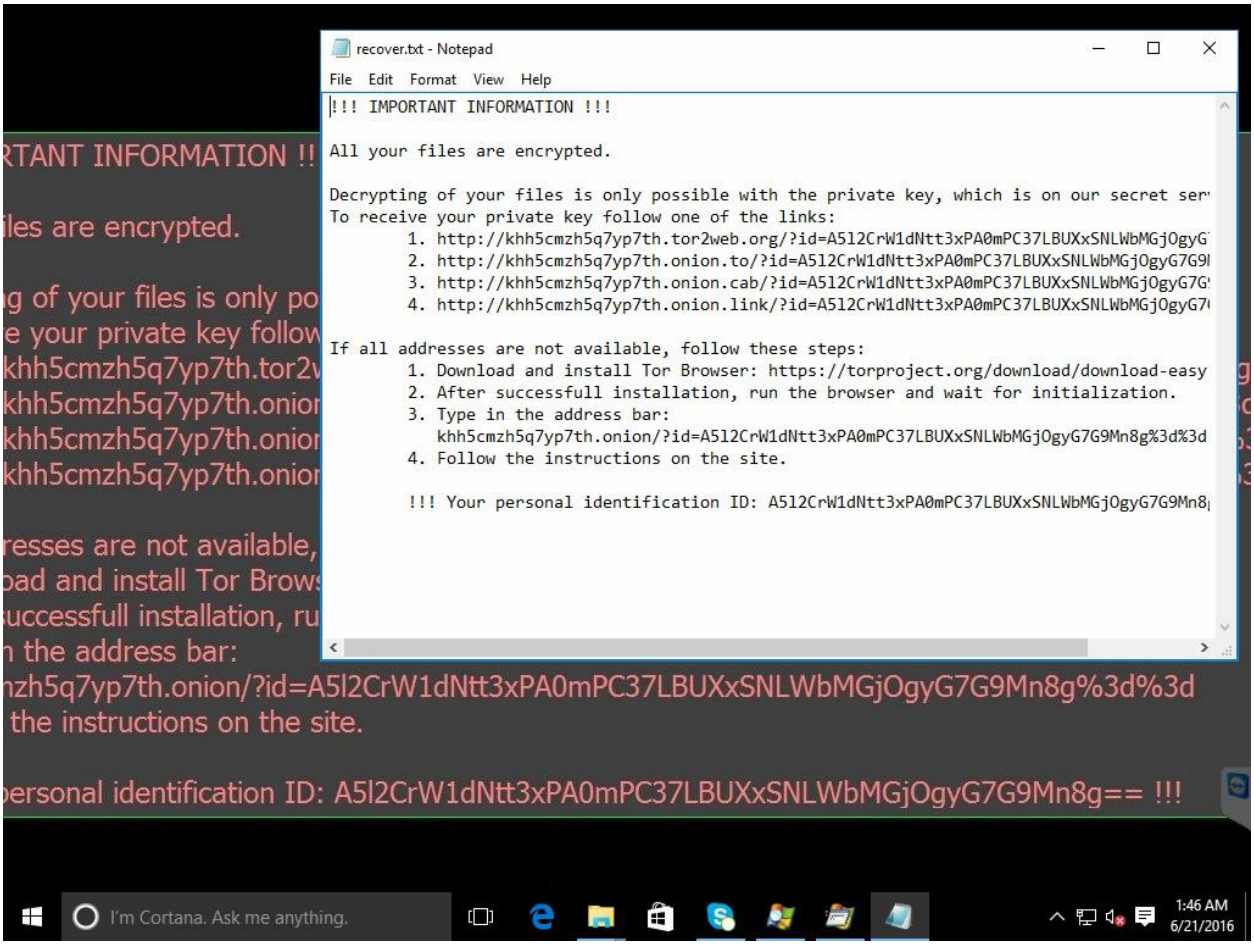
Test results

	Watchdog Anti-Malware	Bitdefender Antiransomware	Cryptoprevent	Hitmanpro Alert	MalwareBytes Anti Ransomware
Score	**4**	**4**	**4**	**3**	**3**

Although these generic protections worked fairly well against Locky, it is important to recognise that Locky is famously known to bypass most AV. Again, it is interesting that one of the most advanced ransomware is caught by generic detection.

2.3.10 Bart

Bart basically shares the code with Locky – probably, the same developers are behind this. The biggest difference is that it can operate in offline mode. Also, it uses different encryption technique, which is not yet detected by most generic ransomware protection. The sample is from June, 2016. SHA-256: 51ff4a033018d934304930506 1dcde77cb5f26f5ec48d1be42669f368b1f5705



Test results

	Watchdog Anti-Malware	Bitdefender Antiransomware	Cryptoprevent	Hitmanpro Alert	MalwareBytes Anti Ransomware
Score	**4**	**0**	**0**	**0**	**4**

2.3.11 MRG Effitas ransomware simulator

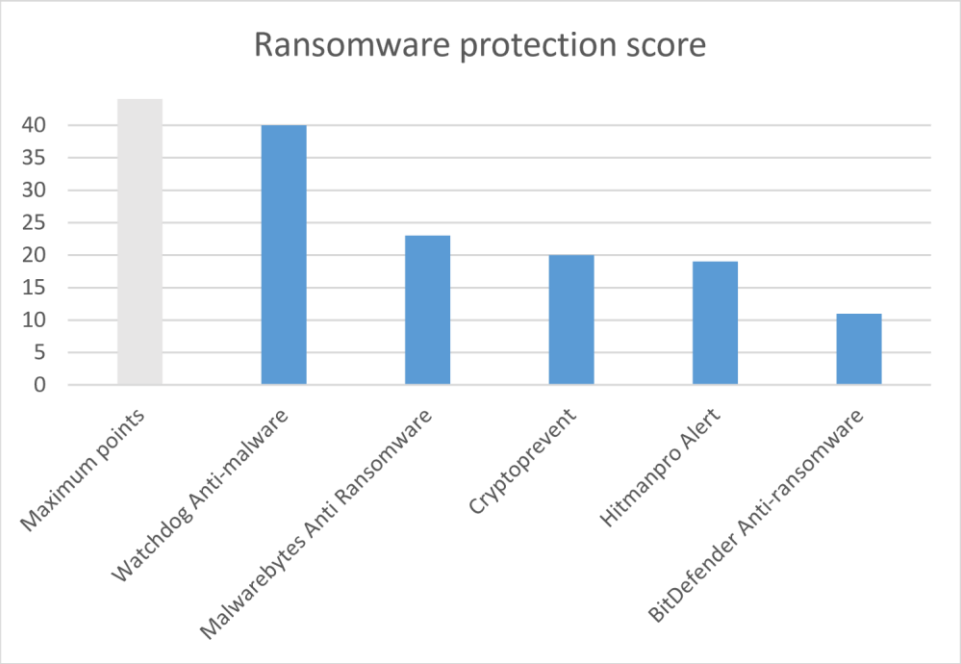
We developed a sample ransomware simulator in Python, and compiled it to an EXE file via Py2EXE. Due to the sensitive nature of ransomware, we will not release the code to the public. As it is only a sample to test generic protection, it uses a fixed key, AES encryption, encrypts the following file types recursively in a specified directory: .pdf,.jpg,.docx, .txt, .xlsx, .png, and has no C&C at all. First it creates the encrypted copy of the original file, then overwrites the original file with zeroes, and deletes it.

Test results

	Watchdog Anti-Malware	**Bitdefender Antiransomware**	**Cryptoprevent**	**Hitmanpro Alert**	**MalwareBytes Anti Ransomware**
Score	**0**	**0**	**0**	**0**	**0**

3 Final results

	Watchdog Anti-Malware	Bitdefender Antiransomware	Cryptoprevent	Hitmanpro Alert	MalwareBytes Anti Ransomware
Score	**40**	**11**	**20**	**19**	**23**



Based on this report, Watchdog Anti-Malware proved to be the best ransomware protection among the tested products during the test. These scores are not normalized with the prevalence of the ransomware samples. Usually, the most prevalent samples are included in these generic protections, but as always, life (and IT Security) is never simple.