



Efficacy Assessment of Cb Defense Against Ransomware

September 2017

Table of Contents

1	Executive Summary	3
1.1	Test results	3
2	Introduction	5
2.1	Structure of this report	5
2.2	Overview	5
2.3	Ransomware as a business model	6
3	Ransomware families in scope	7
4	Detailed Results	10
5	Methodology	12
5.1	Infection methods.....	12
5.2	Result interpretation.....	12
6	Conclusion	13
7	Appendix – Examples of ransomware families used	14
7.1	WannaCry.....	14
7.2	CryptoMix.....	15
7.3	Locky	16
7.4	XYZWare (MafiaWare)	17
7.5	CryptoShield 2.0.....	18
7.6	Spora	19
7.7	Cerber.....	20
7.8	Globe3.....	21
7.9	Havoc MK II	22
7.10	Dharma.....	23
7.11	Sage 2.0.....	24
7.12	Petya GoldenEye	25
7.13	NotPetya	26
7.14	TeslaCrypt	27
7.15	MRG Effitas Python ransomware.....	28
7.16	MRG Effitas in-memory ransomware	29
8	Configuration policy for Cb Defense	30

1 Executive Summary

Carbon Black trusted MRG Effitas to conduct a security evaluation. A comprehensive set of fresh and prevalent commodity, master-boot infector, file-less and other type of ransomware samples were selected from 42 crypto-ransomware families.

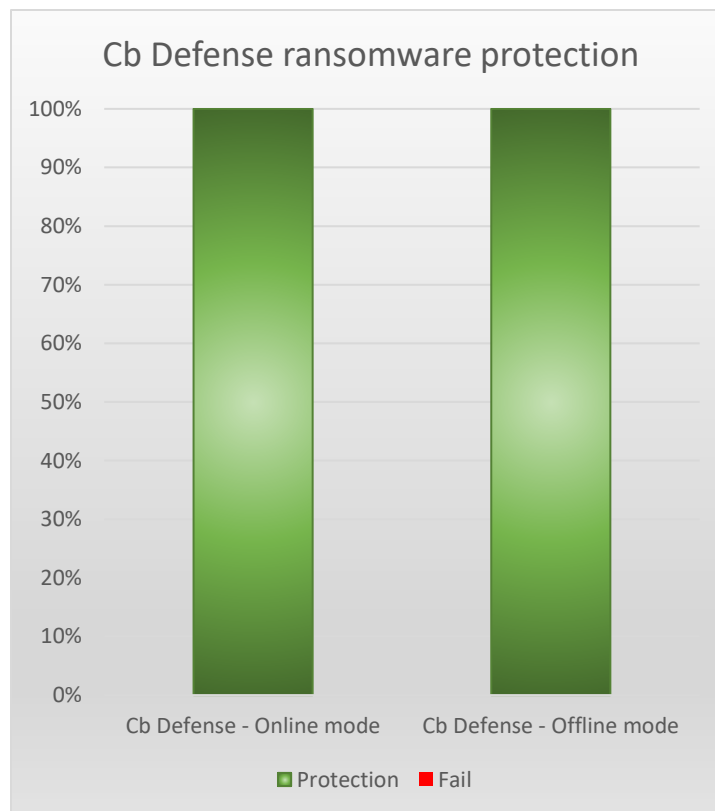
Crypto-ransomware is one of the most dangerous malware types, because if it infects a system, it can stop business processes for days or even weeks, in case no proper backup strategy was used. Crypto-ransomware attacking shared drives can affect multiple departments, not just a single computer in an 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. 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.

1.1 Test results

The testing was carried out between September 1, 2017 and September 9, 2017.

The following chart represents the results of the ransomware testing, consisting of 42 different ransomware families.



Carbon Black.

Based on the excellent protection, Cb Defense earned the MRG Effitas certified ransomware protection badge.



2 Introduction

Carbon Black trusted MRG Effitas to execute a non-biased efficacy assessment test, which aims on discovering capabilities of Cb Defense to protect against Ransomware – particularly Ransomware that contains new or unknown files, or no files at all. For testing purposes, we used numerous samples, representing all major ransomware families on the market (as of late 2016 - early 2017). The samples were collected in the wild, and a significant part of the tested samples were not older than 24 hours.

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 3 describes the ransomware families in scope. The detailed results can be read in Chapter 4. Chapter 5 provides a detailed description of the testing methodology, and finally Chapter 6 provides the conclusion.

2.2 Overview

Crypto ransomware denotes a type of malware, which performs malicious activity on the user's workstation by applying malicious operations that prevents user access to some extent. It then proposes an offer indicating access will be restored only when the victim pays a certain amount of ransom.

Most ransomware performs at least one of the following type of actions:

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

Crypto ransomware is a very special type of malware, because in most of the cases, the encrypted files cannot be recovered unless the ransom is paid. There are also cases where paying the ransom does not help either. In the past, most malware activities could have been rolled back easily, except in the case of information theft. Ransomware attacks cannot be rolled back unless a proper backup and restore procedure is in place.

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, flash drive, 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.

Following is a brief example of what ransomware can do to businesses:

In May 2017, Hospitals and GP surgeries in England and Scotland were among at least 16 health service organisations hit by a ransomware attack on Friday, using malware called Wanna Decryptor (a.k.a WannaCry) - with reports potentially dozens more were affected. Staff were forced to revert to pen and paper and use their own mobiles after the attack affected key systems, including telephones. Hospitals and doctors' surgeries in parts of England were forced to turn away patients and cancel appointments after they were infected with the ransomware, which scrambled data on computers and demanded payments

of \$300 to \$600 to restore access. People in affected areas were being advised to seek medical care only in emergencies. ¹

In June 2017, Maersk was hit by the NotPetya ransomware. The malware surfaced in Ukraine after being spread by a malicious update to MeDoc, the country's most popular accounting software. Maersk picked up an infection that hooked into its global network and shut down the shipping company, forcing it to halt operations at 76 port terminals around the world. "In the last week of the quarter we were hit by a cyber-attack, which mainly impacted Maersk Line, APM Terminals and Damco," CEO Soren Skou said in a statement. "Business volumes were negatively affected for a couple of weeks in July and as a consequence, our Q3 results will be impacted. We expect that the cyber-attack will impact results negatively by USD 200-300m." ²

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.

In addition, many ransomware distributors maintain a 'help desk' to aid victims in making the payment, for example: installing and setting up the TOR browser, buying Bitcoins etc. Counterintuitive as this might look, 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 are informed that in some cases (especially with the e-mail based contact model), even a negotiation of the ransom amount can also take place.

¹ <http://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/>

² https://www.theregister.co.uk/2017/08/16/notpetya_ransomware_attack_cost_us_300m_says_shipping_giant_maersk/

3 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 a significant part of the tested samples were not older than 24 hours.

In order to create a full spectrum of the samples in the test, during sample collection, we focused on the following:

- The more ransomware family is covered, the better
- The more prevalent and fresh the sample is, the better
- Test with packed sample of the ransomware, using Themida, UPX, SFX, Morpheus or Mpress
- Test with modified samples where only the hash of the file is changed
- Test with file-less ransomware
- Test with ransomware targeting MBR/MFT/boot record
- EXE, DLL, script based ransomware
- Unique samples dropped by exploit kits
- Ransomware targeting the Volume Shadow Copy (deleting it via vssadmin)

The following list represents the types of ransomware samples used in the test:

Ransomware type	Ransomware family
Commodity	BTCWare 2017
Commodity	Cancer
Commodity	Cerber
Commodity	ChinaYunLong
Commodity	Cryakl
Commodity	Cryptolocker
Commodity	CryptoMix
Commodity	CryptoShield
Commodity	CryptoTorLocker
Commodity	CryptoXXX
Commodity	Dharma
Commodity	Erebus
Commodity	Fenrir
Commodity	Globe3
Commodity	Havok2
Commodity	HiddenTear
Commodity	HydraCrypt
Commodity	Kirk
Commodity	Locky
Commodity	Mobef (Yakes)
Commodity	MRG Modified Commodity RW
Commodity	MRG Packed ransomware
Commodity	NoobCrypt
Commodity	Perseus
Commodity	PokemonGo
Commodity	Rokku
Commodity	Sage
Commodity	Satan
Commodity	Satana
Commodity	Spora
Commodity	Striked
Commodity	Symmi
Commodity	TeslaCrypt
Commodity	Troldesh
Commodity	Volume Shadow Copy manipulatc
Commodity	WannaCry
Commodity	XYZWare
Commodity	Zusy
Master-boot	NotPetya
Master-boot	Petya
Master-boot	Petya Goldeneye
Simulator	MRG Powershell ransomware
Simulator	MRG Python ransomware

For detailed information about some of the ransomware families used in the test, please refer to “

Carbon Black.

Appendix – Examples of ransomware families used”.

4 Detailed Results

Testing was carried out between September 1, 2017 and September 9, 2017.

Due to the specific nature of ransomware behaviour, we have tested Cb Defense in two configurations – online and offline. In online mode, the agent was able to communicate with the cloud. The cloud communication is used to blacklist known malware by sample hash. In the offline mode, the agent could not reach the cloud, thus hash based reputation was not working and Cb Defense needed to rely on other prevention mechanisms. Cb Defense performed 100% both in online and offline mode against the tested ransomware samples.

In some test cases, where the behaviour protection blocked the ransomware, a small number of files have been encrypted. Although this could be an inconvenience to the users, it is still significantly better compared to the case where all files on the disk are encrypted. For example the file-less MRG ransomware encrypted some files on the desktop before the behaviour protection blocked and killed the process.

Carbon Black.

Ransomware family	Full protection (Online)	Full protection (Offline)
BTCWare 2017	blocked	blocked
Cancer	blocked	blocked
Cerber	blocked	blocked
Cerber	blocked	blocked
Cerber	blocked	blocked
Cerber (MRG Modified)	blocked	blocked
ChinaYunLong	blocked	blocked
Cryakl	blocked	blocked
Cryakl	blocked	blocked
Cryptolocker	blocked	blocked
CryptoMix	blocked	blocked
CryptoShield 2.0	blocked	blocked
Cryptoshield	blocked	blocked
Cryptoshield	blocked	blocked
Cryptoshield (MRG Modified)	blocked	blocked
CryptoTorLocker	blocked	blocked
CryptoXXX	blocked	blocked
Dharma	blocked	blocked
Dharma (MRG Modified)	blocked	blocked
Erebus	blocked	blocked
Erebus (MRG Modified)	blocked	blocked
Fenrir	blocked	blocked
Globe3	blocked	blocked
Havok2	blocked	blocked
HiddenTear	blocked	blocked
HiddenTear	blocked	blocked
HiddenTear Viro	blocked	blocked
HydraCrypt	blocked	blocked
Kirk	blocked	blocked
Locky	blocked	blocked
Mobef (Yakes)	blocked	blocked
MRG Packed ransomware 1	blocked	blocked
MRG Packed ransomware 2	blocked	blocked
MRG Packed ransomware 3	blocked	blocked
MRG Packed ransomware 4	blocked	blocked
MRG Packed ransomware 5	blocked	blocked
MRG Powershell ransomware	blocked	blocked
MRG python ransomware	blocked	blocked
Naampa (VS Copy manipulator)	blocked	blocked
Nemesis (VS Copy manipulator)	blocked	blocked
NoobCrypt	blocked	blocked
NotPetya	blocked	blocked
Perseus	blocked	blocked
Petya	blocked	blocked
Petya Goldeneye	blocked	blocked
PokemonGo	blocked	blocked
Rokku	blocked	blocked
Sage 2.0	blocked	blocked
Sage 2.0	blocked	blocked
Sage 2.2	blocked	blocked
Satan	blocked	blocked
Satana	blocked	blocked
Spora	blocked	blocked
Spora	blocked	blocked
Striked	blocked	blocked
Symmi	blocked	blocked
TeslaCrypt	blocked	blocked
TeslaCrypt	blocked	blocked
Troldesh	blocked	blocked
WannaCry	blocked	blocked
WannaCry	blocked	blocked
XYZWare	blocked	blocked
Zusy	blocked	blocked

Figure 1 - Detailed result of the test

5 Methodology

5.1 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. This is a hardened virtualized environment which is not detected by malware. This test environment is crucial in tests where the malware is executed, and behavior protection is part of the test. Each product configuration has been installed, activated and updated with the latest 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)

5.2 Result interpretation

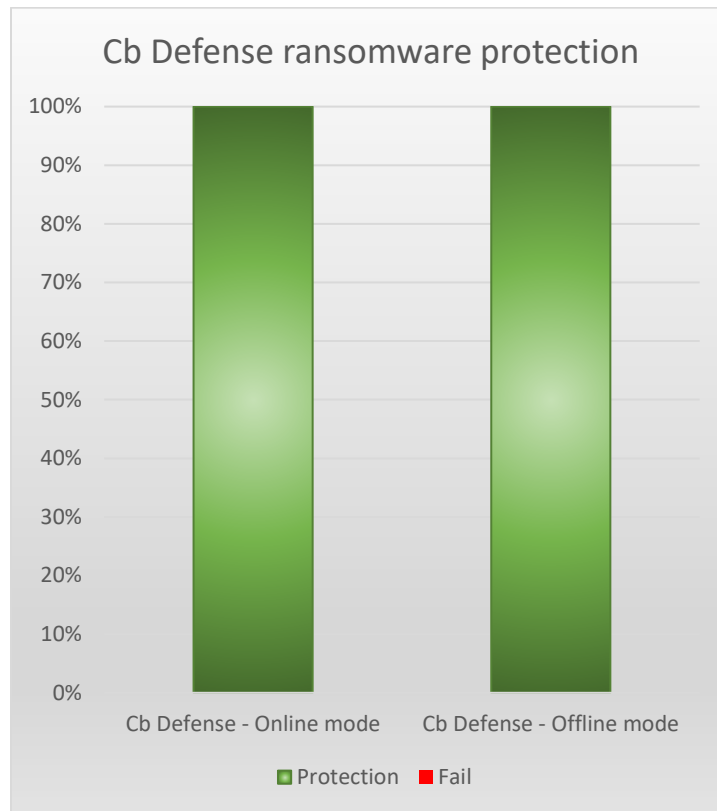
The scores of this test are results of a sample-based approach. Note that this approach has some inherent errors, which, despite all care, cannot be eliminated.

- 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.
- Cb Defense has a lots of configuration options and auxiliary features, which can be individually configured. The authors of this report were aided by the vendor to configure the product in an optimal fashion by selecting one of the alternative policies that ships out-of-the-box with Cb Defense. The details of the policy can be found in Appendix - Configuration policy for Cb Defense.
- The protection of security products in general 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 types 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 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 Conclusion

Through this assessment, MRG Effitas found Cb Defense as a reliable ransomware protection application. Cb Defense provided a strong protection, both in online and offline mode against not only well-known, but against 0-day ransomware too. Ransomwares like Petya, NotPetya and Petya Goldeneye, which targets the MBR / MFT were caught efficiently as well.



7 Appendix – Examples of ransomware families used

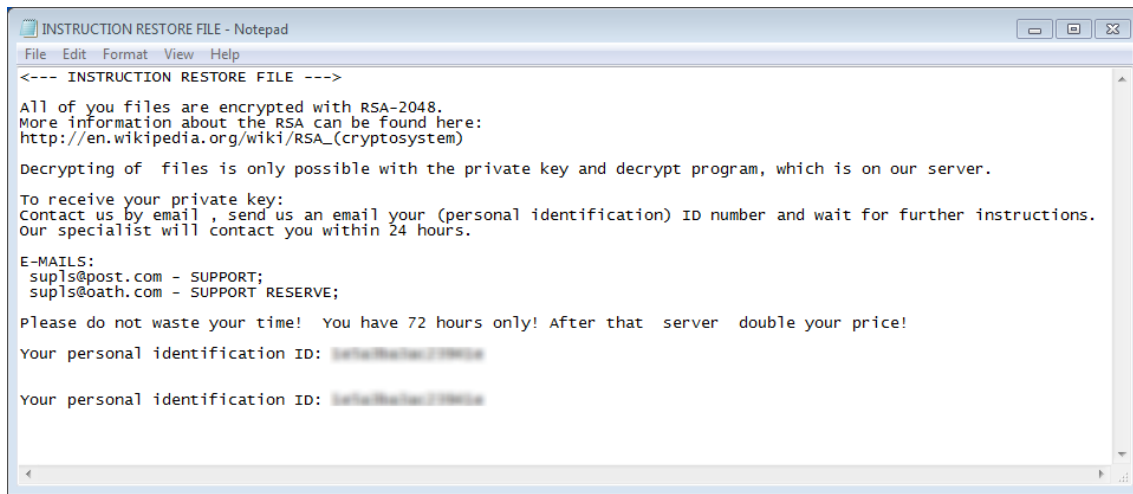
The following paragraphs contains basic descriptions about some of the ransomware families used in the test.

7.1 WannaCry



WannaCry was the first and famous ransomworm, which started in May 2017. It spread through the leaked EternalBlue SMB exploit, with the help of the DoublePulsar backdoor. Within a day it was reported to have infected more than 230,000 computers in over 150 countries. Cybersecurity companies have both said the code has some similarities with that previously used by the Lazarus Group (believed to have carried out the cyberattack on Sony Pictures in 2014 and a Bangladesh bank heist in 2016—and linked to North Korea). Experts advised against paying the ransom due to no reports of people getting their data back after payment and as high revenues would encourage more of such campaigns. The ransomworm affected basically all types of businesses around the world.

7.2 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:
sup1s@post.com - SUPPORT;
sup1s@oath.com - SUPPORT RESERVE;

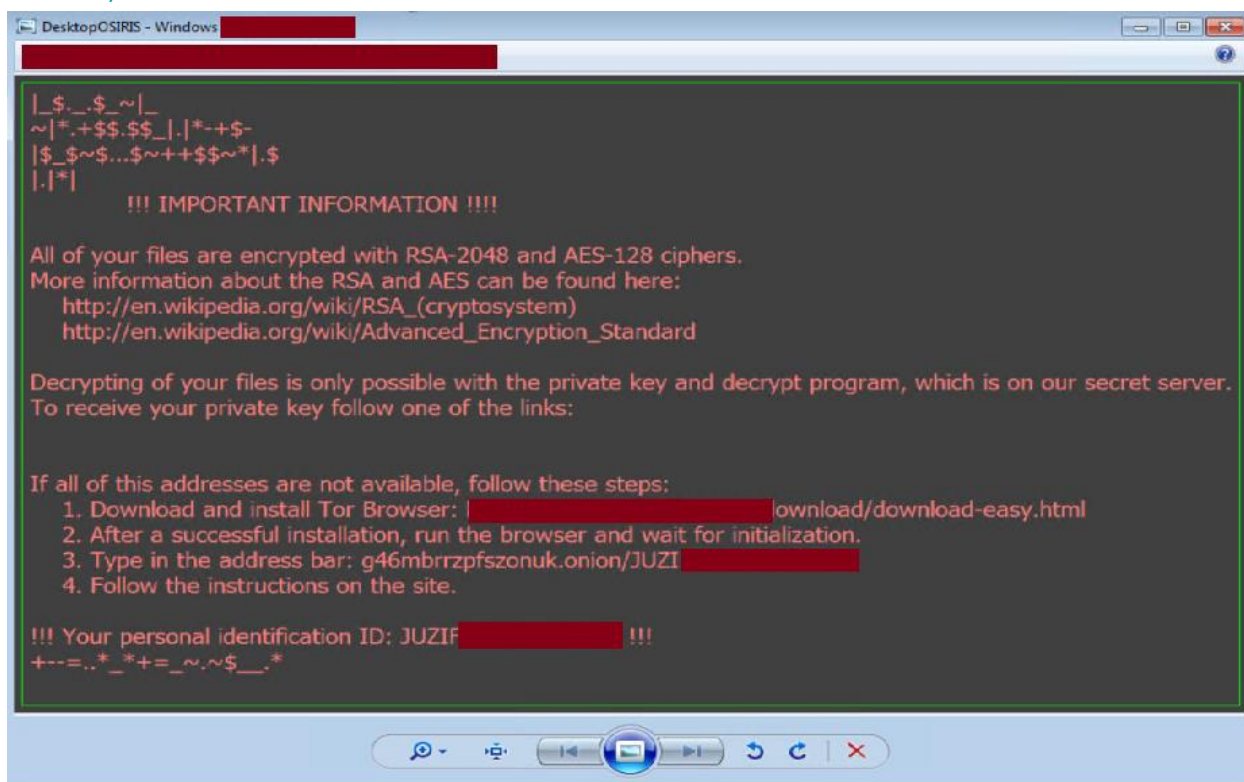
Please do not waste your time! You have 72 hours only! After that server double your price!

Your personal identification ID: 1a1f0a7b0a0c11981a

Your personal identification ID: 1a1f0a7b0a0c11981a
```

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. 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 decide to pay up.

7.3 Locky



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” extensions, 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 and 1 Bitcoin.

7.4 XYZWare (MafiaWare)

XYZWare is based on the almost ready solution MafiaWare Ransomware. While the original MafiaWare RansomWare is developed in Python environment, XYZWare is developed in Visual Studio 2012. The Ransomware uses RSA-2048 and AES-128 to encrypt data and add a “.XYZWare” extension. It has a weakness because it starts the infection from the folder where it executed, and if it comes to a file/folder that is either NTFS protected or cannot be accessed for any other reason (Backup folder with write protection), the ransomware crashes with a .NET framework error.

7.5 CryptoShield 2.0

NOT YOUR LANGUAGE? USE <http://translate.google.com>

What happens to you files?
All of your files encrypted by a strong encryption with RSA - 2048 using **CryptoShield 2.0**.
DANGEROUS.
More information about the encryption keys using RSA-2048 can be found here:
[en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

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.
ALL YOUR FILES ARE ENCRYPTED AND LOCKED, YOU CAN NOT DELETE THEM, MOVE OR DO SOMETHING WITH THEM. HURRY TO GET BACK ACCESS FILES.

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:
res_sup@india.com - SUPPORT;
res_sup@computer4u.com - SUPPORT RESERVE FIRST;

The bulk of this ransomware family's activity occurred in the first half of February 2017. It focuses on English-speaking users, which of course does not prevent it spreading around the world. This ransomware encrypts user data with AES-256, and then requires a redemption to return the files. It adds an extra extension pattern to the encrypted files, such as: [RES_SUP@INDIA.COM].ID [2D64A0776C78A9C3]. .CRYPTOSHIELD. The price it demands varies, and communication is via email.

7.6 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

US6CC- XXXXXXXXXX

[Авторизация](#)

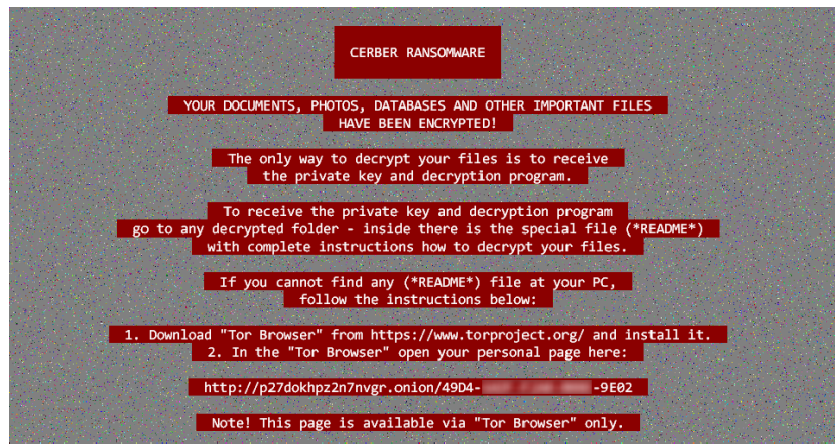
Что случилось?

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, затем Вам продаст его с наценкой.

Если Вы не смогли синхронизировать аккаунт (*.KEY), нажмите здесь:
• СИНХРОНИЗАЦИЯ •

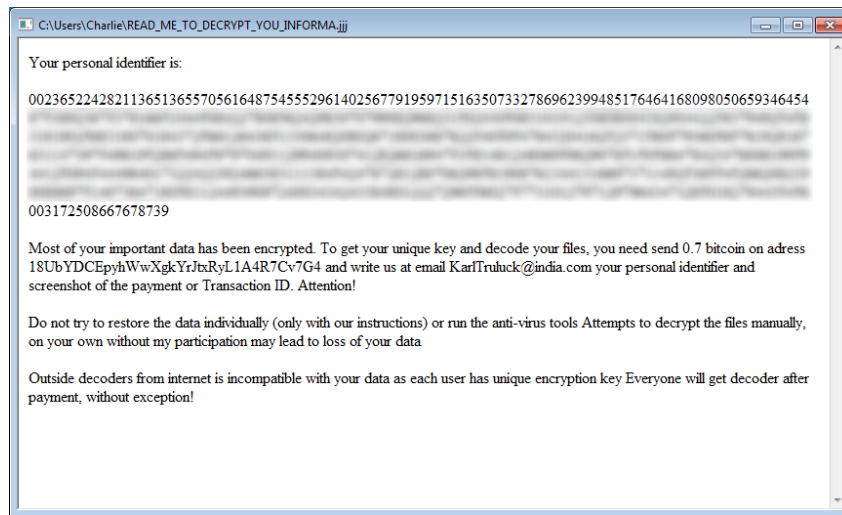
This Multilanguage ransomware was first seen at the beginning of January 2017 using AES + RSA to encrypt user data and modify the folder structure. Unlike many modern ransomware, Spora works offline and does not generate any network traffic. It does not generate extra file extensions.

7.7 Cerber



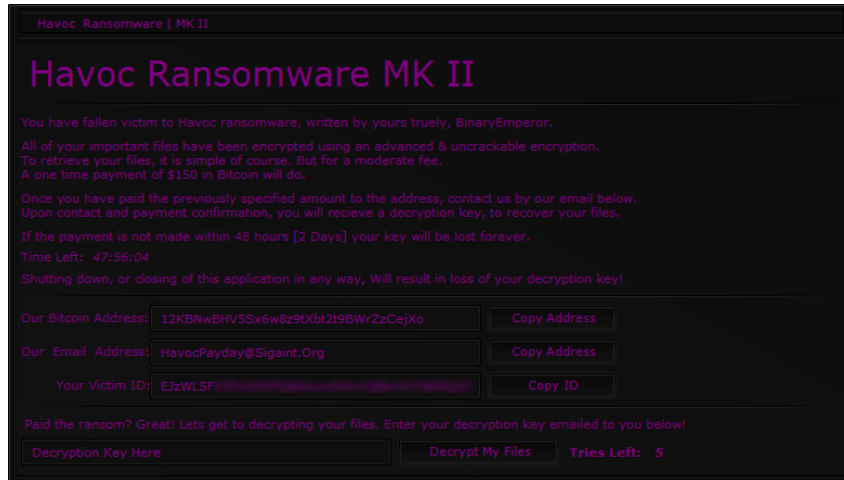
Cerber ransomware, much like many other encryption-type malware, is known to encrypt files with AES-256 encryption on the infected computer. It creates random filenames and appends the extension “.CERBER” or “.B126” and holds those files for a substantial ransom fee. As it encrypts the victim's files, it creates TXT, HTML, and VBS files named 'DECRYPT MY FILES' with instructions on how to pay. It has an 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 ransom via a TOR browser within one week or the amount is doubled.

7.8 Globe3



The main targets of the Globe Ransomware are small businesses but it causes damage to any computer it infects. This crypto Trojan encrypts user data using AES-256 + RSA and adds a “.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 a “How to restore your files.hta” ransom note which advises the user about the 0.7 Bitcoin ransom fee and contains instructions on how to pay to recover the encrypted files.

7.9 Havoc MK II



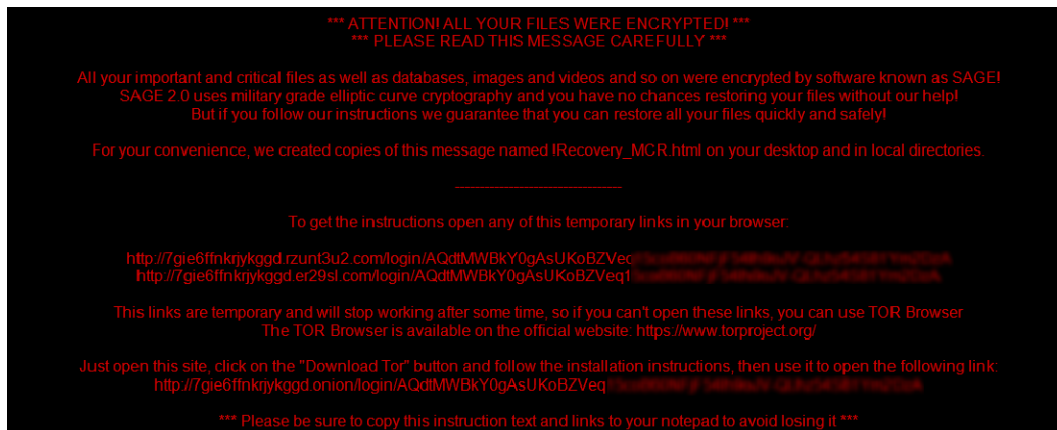
The Havoc MK II Ransomware's bright violet ransom note first appeared in public in January 2017. It uses RSA256 encryption and ".havokcrypt" extensions to lock the victim's files, targeting a wide variety of files that can include video and audio files, text files, databases, images, and numerous other commonly-used file types. However, Havoc Ransomware will only target specific folders and 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 a 0.15 Bitcoin ransom fee to restore the data or the restore key is deleted.

7.10 Dharma



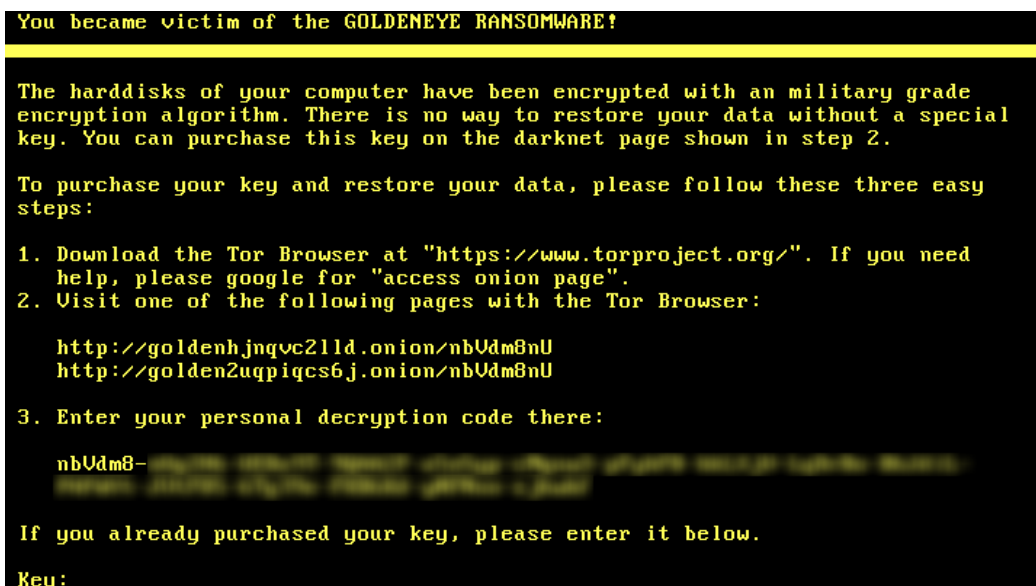
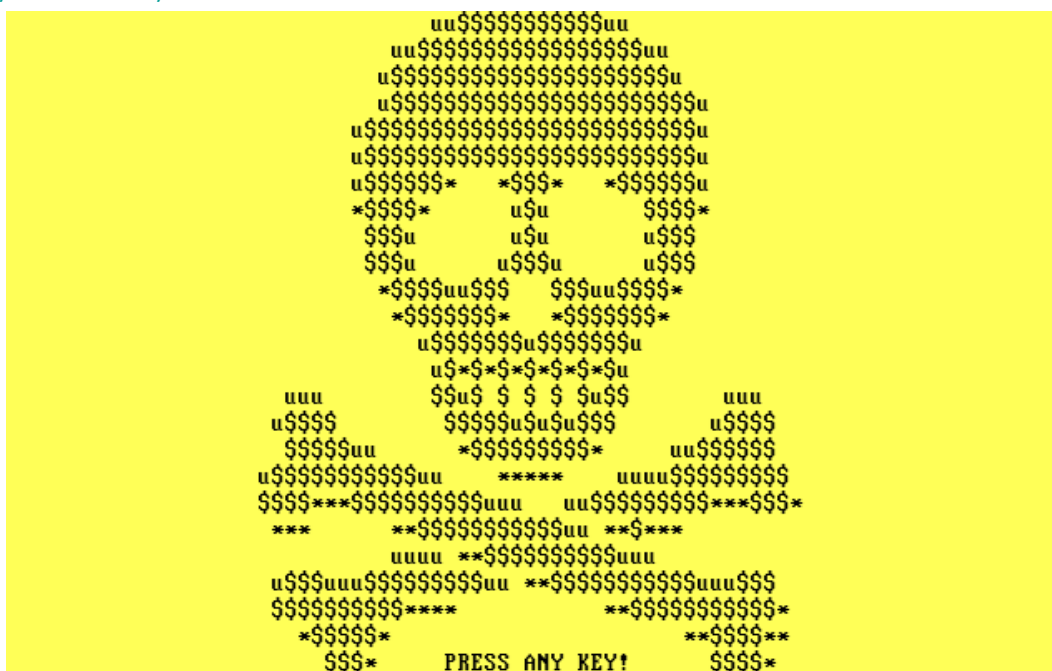
Dharma is a variant of Crysis - a high-risk ransomware-type malware. Following successful infiltration, Dharma encrypts stored files using AES. In addition, this file-encoder usually appends the “[webmafia@asia.com]. wallet” “[webmafia@asia.com]. dharma” or “[webmafia@asia.com].zzzzz” extension and encrypts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

7.11 Sage 2.0



Sage Ransomware belongs to the TeslaCrypt family. This crypto ransomware encrypts user data using AES-256 and RSA-1024 ciphers and adds the “.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 ransom – which is doubled after 7 days – and get instructions on how to restore files.

7.12 Petya GoldenEye



The GoldenEye Ransomware is an improved version of the Petya Ransomware, which surfaced in March 2016. GoldenEye followed its predecessor openly in December 2016. It encrypts local drives using an AES-256 cipher and adds a random 8-character extension to the file names. However, it avoids directories that contain system data (Windows, Program Data, Program Files, Program Files (x86), Volume Information). If GoldenEye manages to elevate its system privileges, it installs a rootkit which locks the access to the computer entirely by encrypting the drive's MFT disguising its progress as a fake check disk scan. Then the custom boot screen is loaded on the screen. The ransom fee to undo the encryption is about 1.4 Bitcoins.

7.13 NotPetya

```
Repairing file system on C:

The type of the file system is NTFS.
One of your disks contains errors and needs to be repaired. This process
may take several hours to complete. It is strongly recommended to let it
complete.

WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD
DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED
IN!

CHKDSK is repairing sector 17600 of 147424 (11%)
```

```
Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted. Perhaps you are busy looking for a way to recover your
files, but don't waste your time. Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily. All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

1Mz71 [REDACTED]

2. Send your Bitcoin wallet ID and personal installation key to e-mail
wowsmith123456@posteo.net. Your personal installation key:

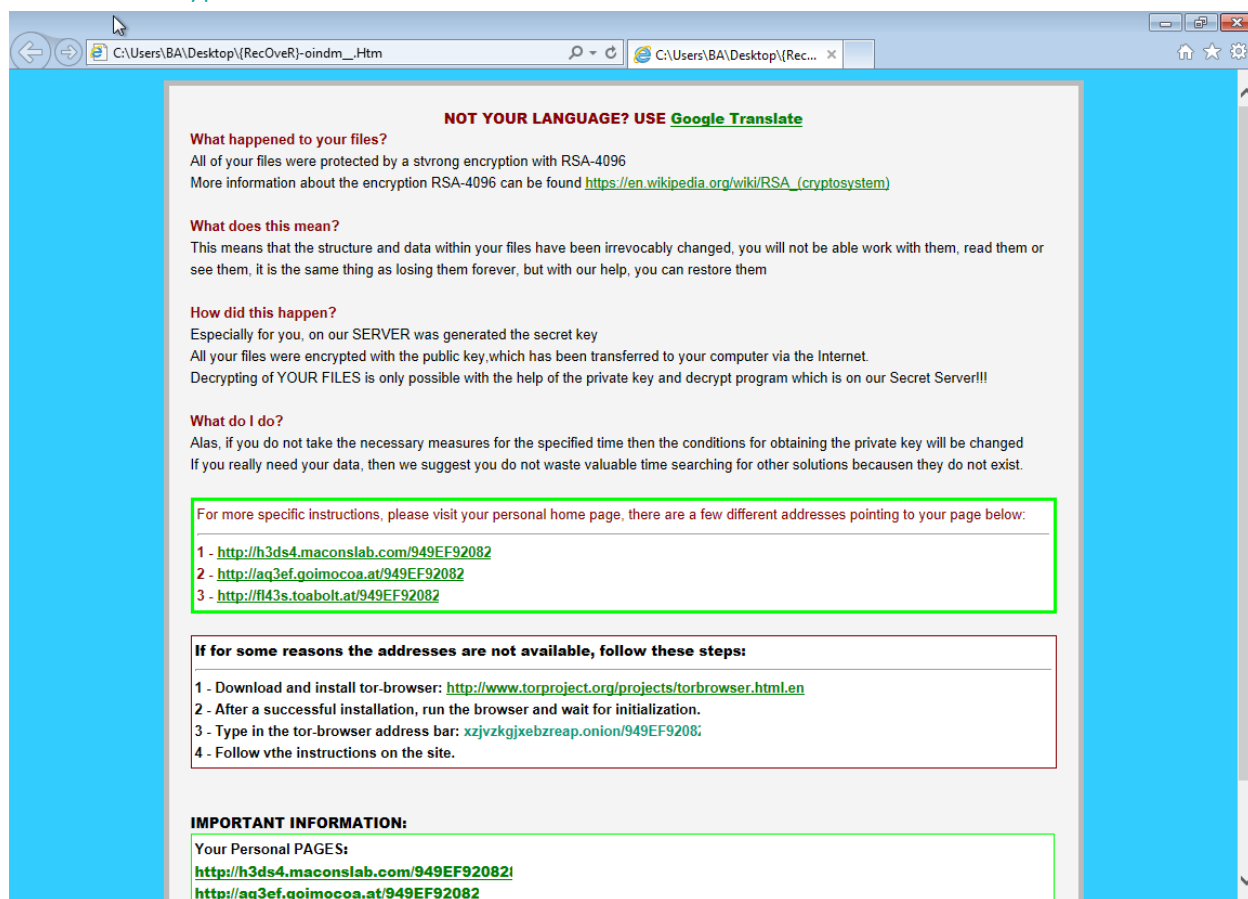
F23faM-Y [REDACTED]

If you already purchased your key, please enter it below.
Key: _
```

NotPetya is a modified version of the Petya Ransomware, which uses the AES-128 cipher. The key difference is that it can spread through the local subnet by using a modified version of the NSA's stolen and leaked EternalBlue SMB exploit, previously used by WannaCry to infect other systems by injecting malicious code into other processes. It also uses a credential reuse technique to spread to other systems which are patched against EternalBlue.

It also installs a rootkit which locks the access to the computer entirely by encrypting the drive's MFT during reboot, disguising its progress as a fake check disk scan.

7.14 TeslaCrypt



TeslaCrypt was first released 2 months earlier than AlphaCrypt around the end of February 2015. It uses an RSA-4096 encryption to infect the personal file types like: compressed, audio, video, picture document. When the infection has finished it will also delete all the Shadow Volume Copies that are on the affected computer. It does this so that the user cannot use the shadow volume copies to restore the encrypted files.

7.15 MRG Effitas Python ransomware

MRG Effitas 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, has no C&C at all but encrypts the following file types recursively in a specified directory: .pdf,.jpg,.docx, .txt, .xlsx, .png. First it creates the encrypted copy of the original file, then overwrites the original file with zeroes, and deletes it.

The simulator was also tested as a stand-alone Python script, with the same results (counted only once in the results).

7.16 MRG Effitas in-memory ransomware

This simulator is an in-memory Meterpreter extension. The DLL is loaded from the server and injected into the host process without touching the disk. First it scans for the files which will be processed, and it encrypts the files with AES-256 one by one. The original files are overwritten by zeroes before it is deleted. The Meterpreter session is started from Powershell.

8 Configuration policy for Cb Defense

We used Cb Defense's Advanced Policy to conduct our testing. While not the default policy, this policy is one of the out-of-the-box policies that ships with Cb Defense.

POLICY
Use policies to define and prioritize rules for how applications can behave on groups of devices

+ NEW POLICY X DELETE POLICY DUPLICATE POLICY SAVE

NAME	DEVICES
Monitored	0
Standard	0
Advanced	2
quarantine	0
Behavior Only	1

Cb DEFENSE SETTINGS LOCAL SCAN SETTINGS

Policy Name: Advanced (LOCKED POLICY)

Policy Description (optional): Strong defense, but not suitable as a starting policy for most endpoints

Target Value: Medium

Quarantine Message: Quarantine devices in this policy. Device has been quarantined by your computer administrator.

Sensor UI Message:

LOCAL SCAN SETTINGS

- Allow Executable Uploads for Scans
- Show Sensor UI
- Allow User to Disable Protection
- Private Logging Level
- Run background scan
- Scan files on network drives
- Scan execute on network drives
- Delay Execute for Cloud Scan
- Hash MDS
- Use Windows Security Center
- Enable Live Response

Blocking and Isolation + NEW RULE

APPLICATION	OPERATION	ACTION
When known malware that has a verified signature	Tries to run o...	Terminate pr... X
When applications that appear on the company blacklist	Tries to run o...	Terminate pr... X
When suspected malware	Tries to run o...	Terminate pr... X
When adware or a potentially unwanted program	Tries to run o...	Terminate pr... X
When an unknown application (ex. new application when offline)	Tries to scrap...	Deny operati... X
When an unknown application (ex. new application when offline)	Tries to inject...	Terminate pr... X
When an unknown application (ex. new application when offline)	Tries to invok...	Deny operati... X
When a not listed application	Tries to scrap...	Deny operati... X
When a not listed application	Tries to inject...	Terminate pr... X
When a not listed application	Tries to invok...	Deny operati... X
When an application at path: **\powerpnt.exe	Tries to scrap...	Deny operati... X
When an application at path: **\powerpnt.exe	Tries to inject...	Terminate pr... X
When an application at path: **\powerpnt.exe	Tries to invok...	Deny operati... X
When an application at path: **\excel.exe	Tries to scrap...	Deny operati... X
When an application at path: **\excel.exe	Tries to inject...	Terminate pr... X
When an application at path: **\excel.exe	Tries to invok...	Deny operati... X
When an application at path: **\winword.exe	Tries to scrap...	Deny operati... X
When an application at path: **\winword.exe	Tries to inject...	Terminate pr... X
When an application at path: **\winword.exe	Tries to invok...	Deny operati... X

When an application at path: **\powershell*.exe	Tries to scrap...	Deny operati...	X
When an application at path: **\powershell*.exe	Tries to inject...	Terminate pr...	X
When an application at path: **\powershell*.exe	Tries to invoc...	Deny operati...	X
When an application at path: **\cscript.exe	Tries to scrap...	Deny operati...	X
When an application at path: **\cscript.exe	Tries to inject...	Terminate pr...	X
When an application at path: **\cscript.exe	Tries to invoc...	Deny operati...	X
When an application at path: **\wscript.exe	Tries to scrap...	Deny operati...	X
When an application at path: **\wscript.exe	Tries to inject...	Terminate pr...	X
When an application at path: **\wscript.exe	Tries to invoc...	Deny operati...	X
When an application at path: **/python	Tries to scrap...	Deny operati...	X
When an application at path: **/python	Tries to inject...	Terminate pr...	X
When an application at path: **/python	Tries to invoc...	Deny operati...	X
When an application at path: **/Microsoft PowerPoint.app/**	Tries to scrap...	Deny operati...	X
When an application at path: **/Microsoft PowerPoint.app/**	Tries to inject...	Terminate pr...	X
When an application at path: **/Microsoft PowerPoint.app/**	Tries to invoc...	Deny operati...	X
When an application at path: **/Microsoft Excel.app/**	Tries to scrap...	Deny operati...	X
When an application at path: **/Microsoft Excel.app/**	Tries to inject...	Terminate pr...	X
When an application at path: **/Microsoft Excel.app/**	Tries to invoc...	Deny operati...	X
When an application at path: **/Microsoft Word.app/**	Tries to scrap...	Deny operati...	X
When an application at path: **/Microsoft Word.app/**	Tries to inject...	Terminate pr...	X
When an application at path: **/Microsoft Word.app/**	Tries to invoc...	Deny operati...	X
When an application at path: **	Performs ran...	Terminate pr...	X

Permissions (Takes precedence over blocking and isolation) + NEW RULE

APPLICATION	OPERATION	ACTION
-------------	-----------	--------

No permissions set. Add a [new rule](#).

Uploads + NEW RULE

PATH	UPLOAD
------	--------

No override rules defined. Add a [new rule](#).

SAVE