MRG Effitas efficacy assessment of ransomware protection by BackupAssist

2 Table of Contents

1 Introduction

The purpose of this independent report is to document our review of BackupAssist CryptoSafeGuard's backup protection and restore ability against various ransomware samples.

Endpoint backup has gone beyond a simple backup/restore process to a broader end-user data protection solution reducing and precluding various risks such as ransomware infection (the most imminent threat to an average user) against the possibility of even the smallest impact on one's productivity and convenience.

1.1 Executive Summary

This private efficacy assessment report is designed to serve as a reflection of protection against different ransomware families and personal data restoration.

Being the world's largest supplier of early-life malicious binaries and malicious URLs, and from our own experience in simulator development, we know that all endpoints can be infected, regardless of the security solution deployed. In this test we focused on discovering the capabilities of the product protection against both "In The Wild" ransomware and ransomware simulators. We also tested the restore backup functionality (both file restore and full system restore).

When conducting this test, we tried to simulate an average user's behavior. We are aware that a "Real World" test cannot be conducted by a team of professionals inside a laboratory, because we understand how certain types of ransomware attack and know how such attacks can be prevented. Simulating normal use means that we paid special attention to all alerts given by BackupAssist CryptoSafeGuard. It is very important to note that the best choice for typical use is to leave the CryptoSafeGuard settings in default, and we decided to choose the recommended suggestions.

As endpoints get compromised by Ransomware on an ever-greater scale, the ability to protect backups from being encrypted entirely and the prospect of restoring PC and user files after infection were the most important testing metric in this efficacy assessment.

1.2 Final results

BackupAssist's CryptoSafeGuard Detector and Shield had a 100% success rate against every ransomware strain we tested it against, including highly destructive strains of Locky, CryptoLocker, and TeslaCrypt. In every case, CryptoSafeGuard successfully identified the ransomware infection and ensured no backups were overwritten with encrypted files.

Ransomware:	Local backup:	SMB backup:	Infection:
CryptoMix	Protected	Protected	Detected
Osiris-Locky 2017	Protected	N/A	Detected
MafiaWare	Protected	N/A	Detected
CryptoLocker	Protected	Protected	Detected
CryptoShield 2.0	Protected	Protected	Detected
Spora	Protected	N/A	Detected
Cerber	Protected	N/A	Detected
Globe3	Protected	Protected	Detected
Havoc MK II	N/A	N/A	Detected
Dharma	Protected	Protected	Detected
Sage 2.0	Protected	N/A	Detected
Alphacrypt	Protected	Protected	Detected
TeslaCrypt	Protected	N/A	Detected
CTB Locker	Protected	N/A	Detected
Petya GoldenEye	System Backup protected	N/A	N/A
Not Petya	System Backup protected	N/A	N/A
Simluator 1	Protected	Protected	Detected
Simluator 2	Protected	Protected	Detected

* "SMB backup" column shows test results for backups located on Network shares

2 Test Details

2.1 Test application and version

BackupAssist 10.1.0 (t14)

2.2 Test conditions

BackupAssist was interested to achieve an independent review of the efficacy of their CryptoSafeGuard application and have provided the license and installer for the product to be tested.

2.3 Test specification

Discover the capabilities of BackupAssist with CryptoSafeGuard enabled, against "In The Wild" Execution ransomware, and test the restore and recovery functionality in order to rate the effectiveness of the application's backup functionality when protected by CryptoSafeGuard Shield.

Both backups to Network shares and Local backups must not fall to ransomware encryption and must remain unencrypted. CryptoSafeGuard must identify a ransomware infection on the next backup execution, and stop any further backups from running to preserve the existing backups' integrity.

Test restore functionality from Local or Network (SMB) backups, or after an MBR infection recovery from a System Backup (MBR restore).

2.4 Test environment

Upon testing we agreed to choose Windows 7 x64 based on fact that this version is the most commonly used environment:

- OS: Windows 7 x64
- CPU: Intel Core i5 2540M
- Memory: 8GB DDR3
- SSD: SATA 3 OCZ Agility

Even though BackupAssist is predominantly a Windows Server backup solution, Windows 7 x64 was chosen as the testing environment. This is because even though modern Operating Systems can be equally targeted and corrupted by ransomware, Windows 7 has the largest number of known exploits. By using the most vulnerable Windows Operating System available, this meant BackupAssist's CryptoSafeGuard was subjected to the most robust and comprehensive stress tests possible. Due to its design, CryptoSafeGuard will offer equal protection regardless of the Windows Operating System.

2.5 Test scenarios

To represent a detailed, relevant assessment about the product, we focused our attention on the following runtime ransomware attack scenarios. The analyzed scenarios represent typical user cases, where CryptoSafeGuard Shield needs to protect the backups in case of a ransomware infection and to determine whether the local and/or network backups are protected for a successful restore.

1. Local and network backup protection against ransomware attack.
   This test is the focus of our report. There are different cases of what can happen when a ransomware attacks a computer.
   i. The best case scenario is if the CryptoSafeGuard Shield solution stops the attack against the backup and it detects the Ransomware infection and stops any further backups happening.
2. System backup protection against ransomware attack.
   There are some Ransomware (Petya, Notpetya), that install a rootkit and attack the MFT. In case of such an attack the local backup will not be accessible and System restore is needed.
   i. The best case scenario is that the ransomware only attack the System drive MFT so the backups on other drives remain intact and MBR can be restored by BackupAssist..

3 Detailed results

3.1 Local and network backup protection against ransomware

In the first scenario, we tried to emulate a situation in which the user's computer has become infected with various types of ransomware families, and we collected data whether or not the backup solution gives protection in each case. The following table shows which backup solution was unaffected by which ransomware family.

Main Family:	Ransomware:	Local backup:	SMB backup:
CryptoMix	CryptoMix	Protected	Protected
Locky	Osiris-Locky 2017	Protected	N/A
Hidden Tear	MafiaWare	Protected	N/A
CryptoLocker	CryptoLocker	Protected	Protected
CryptoMix	CryptoShield 2.0	Protected	Protected
Spora	Spora	Protected	N/A
Cerber	Cerber	Protected	N/A
Globe	Globe3	Protected	Protected
HavocCrypt	Havoc MK II	N/A	N/A
CrySiS	Dharma	Protected	Protected
CryLocker	Sage 2.0	Protected	N/A
Alphacrypt	Alphacrypt	Protected	Protected
TeslaCrypt	TeslaCrypt	Protected	N/A
CTB Locker	CTB Locker	Protected	N/A
Petya	Petya GoldenEye	System Backup protected	N/A
Not Petya	Not Petya	System Backup protected	N/A
Simluator 1	Simluator 1	Protected	Protected
Simluator 2	Simluator 2	Protected	Protected

* "SMB backup" column shows test results for backups located on Network shares

The reason why some backup files were not attacked/encrypted is that the ransomware was not targeting the backup file types (marked as N/A). In case of Petya and Not Petya, the Local backup could not be reached due to the ransomware type, but the System Backup was protected and restorable.

The number one best practice to protect against ransomware is to have backups. In most cases users forget that ransomware can encrypt the backup files if these files are not offline, read-only or in the cloud, but as the above table shows, BackupAssist's CryptoSafeGuard solution gives 100% backup protection against the tested ransomware families.

3.2 Infection detection.

In this scenario, we tested the CryptoSafeGuard functionality that is designed to detect a possible ransomware infection, maintain the backup's integrity and inform the user about the infection. The following table shows which ransomware families were detected:

Main Family:	Ransomware:	Infection:
CryptoMix	CryptoMix	Detected
Locky	Osiris-Locky 2017	Detected
Hidden Tear	MafiaWare	Detected
CryptoLocker	CryptoLocker	Detected
CryptoMix	CryptoShield 2.0	Detected
Spora	Spora	Detected
Cerber	Cerber	Detected
Globe	Globe3	Detected
HavocCrypt	Havoc MK II	Detected
CrySiS	Dharma	Detected
CryLocker	Sage 2.0	Detected
Alphacrypt	Alphacrypt	Detected
TeslaCrypt	TeslaCrypt	Detected
CTB Locker	CTB Locker	Detected
Petya	Petya GoldenEye	N/A
Not Petya	Not Petya	N/A
Simluator 1	Simluator 1	Detected
Simluator 2	Simluator 2	Detected

Petya and Not-Petya target the MFT and lock the machine, therefore no infection detection can happen.

3.3 Restore functionality from local, system and network backup

In this case we tested the restore from Local backup, full system backup and network (SMB) backup

Main Family:	Ransomware:	Local / System Backup:	SMB Backup:
CryptoMix	CryptoMix	Restored / Restored	Restored
Locky	Osiris-Locky 2017	Restored / Restored	Restored
Hidden Tear	MafiaWare	Restored / Restored	Restored
CryptoLocker	CryptoLocker	Restored / Restored	Restored
CryptoMix	CryptoShield 2.0	Restored / Restored	Restored
Spora	Spora	Restored / Restored	Restored
Cerber	Cerber	Restored / Restored	Restored
Globe	Globe3	Restored / Restored	Restored
HavocCrypt	Havoc MK II	Restored / Restored	Restored
CrySiS	Dharma	Restored / Restored	Restored
CryLocker	Sage 2.0	Restored / Restored	Restored
Alphacrypt	Alphacrypt	Restored / Restored	Restored
TeslaCrypt	TeslaCrypt	Restored / Restored	Restored
CTB Locker	CTB Locker	Restored / Restored	Restored
Petya	Petya GoldenEye	N/A / Restored	N/A
Not Petya	Not Petya	N/A / Restored	N/A
Simluator 1	Simluator 1	Restored / Restored	Restored
Simluator 2	Simluator 2	Restored / Restored	Restored

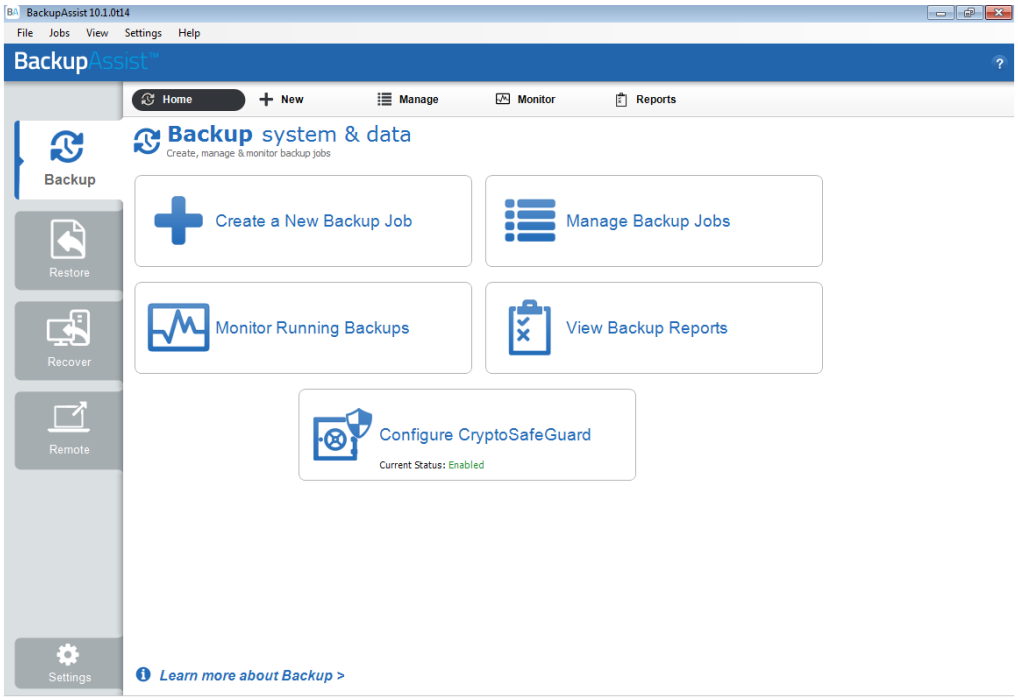
* “SMB backup” column shows test results for backups located on Network shares

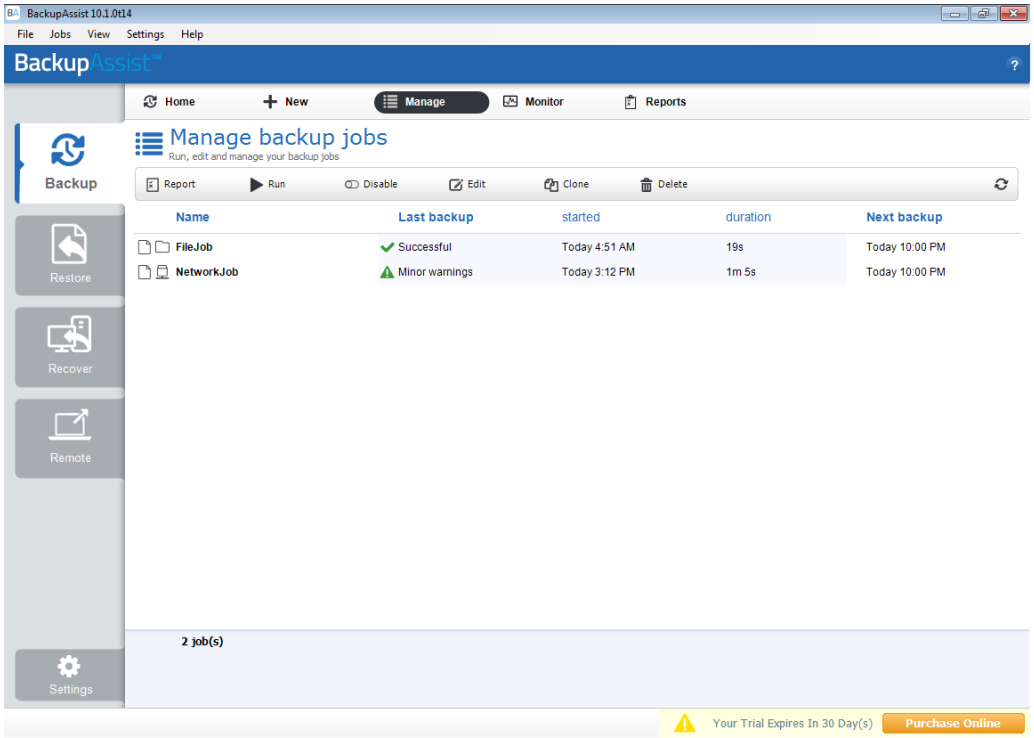
BackupAssist restore was successful from all available backups. Petya and Not Petya lock the machine, therefore the local and network backup/restore function is not available.

4 Overview of BackupAssist

4.1 Overall usage of the program

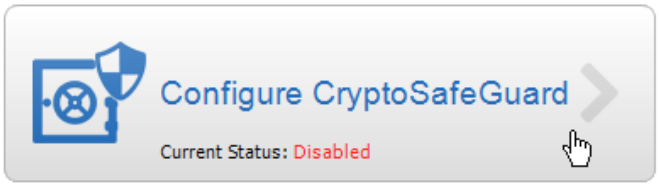
Working with the BackupAssist application was always intuitive. The menu items are well-placed and the recommendations in the application always guide the user to set up the best protection for their backups. The UI is well thought out, and has clear instructions.

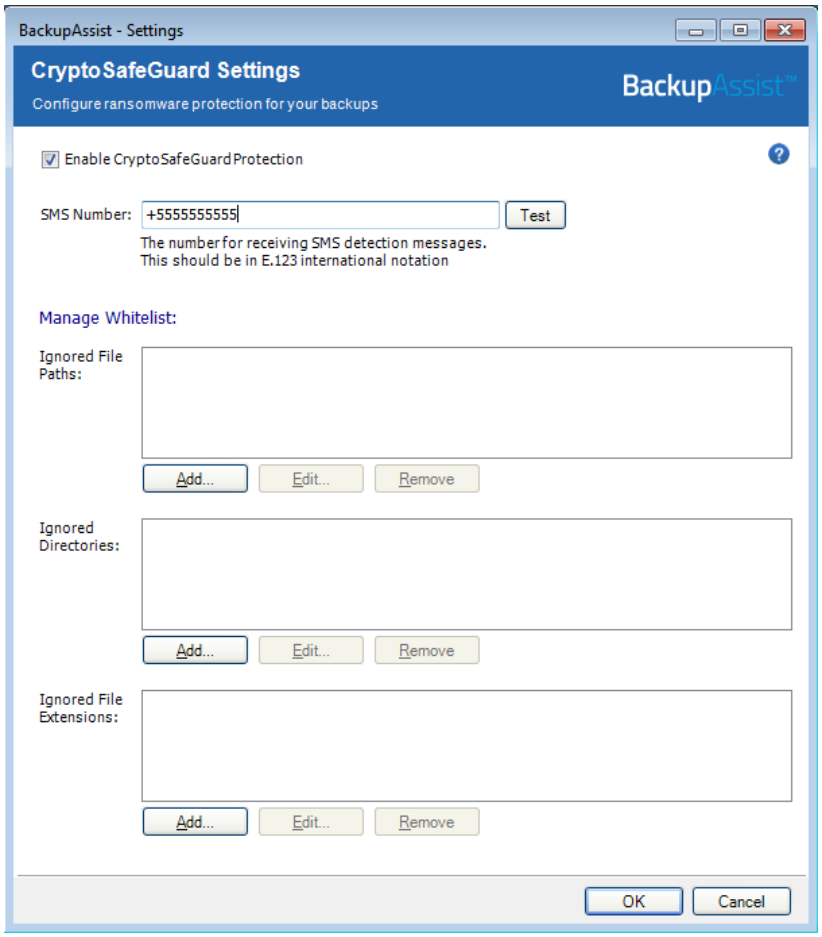




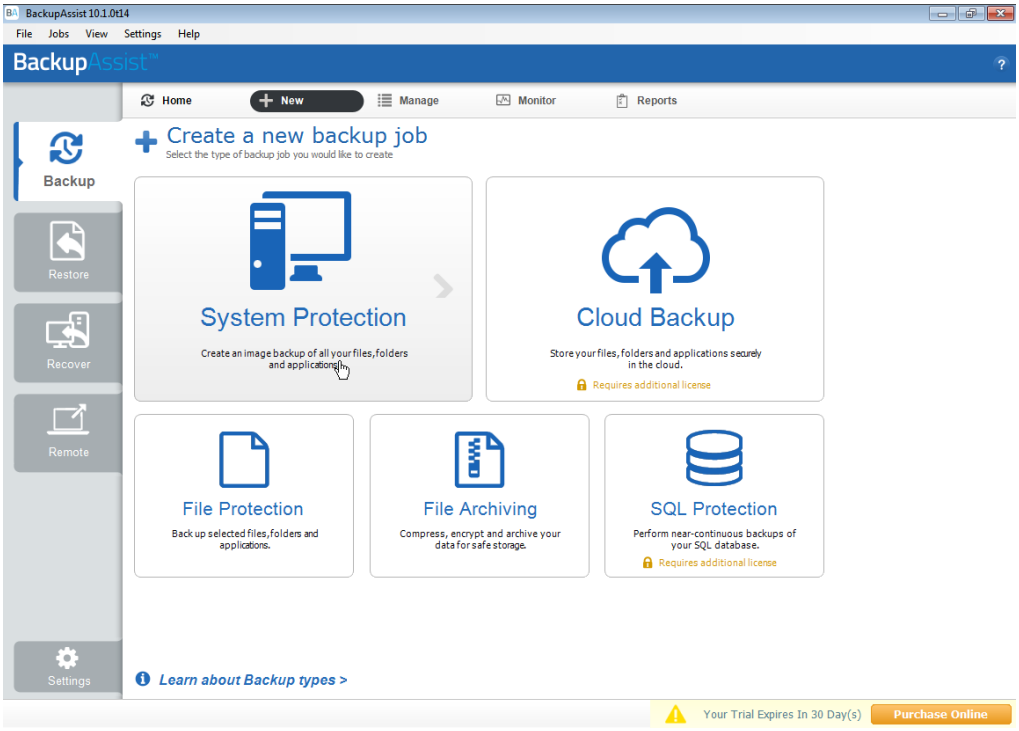
4.2 Screenshots about how to configure BackupAssist protection against ransomware.

To set up maximum protection, which is highly recommended, CryptoSafeGuard activation is essential:

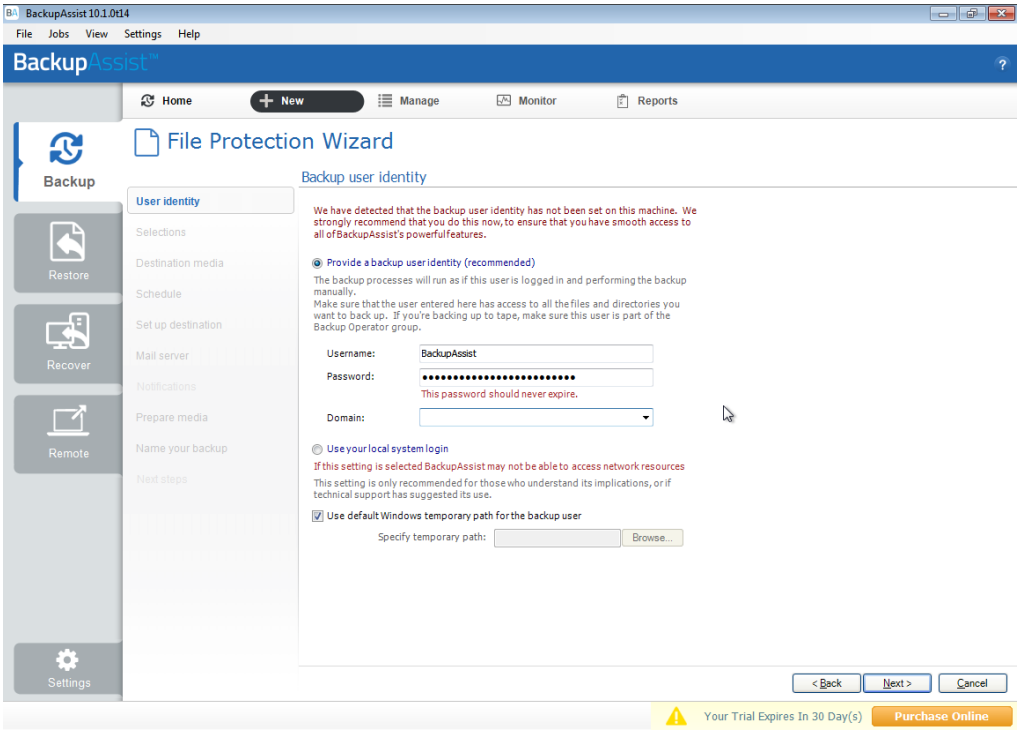




Once the CSG is activated, we can setup the backups. MRG Effitas' recommendation is to set up both a System and a File Protection. NB Cloud Backup (not used) has a built in "air gap" that is effective protection for backups against all known ransomware variants:



Setting the Backup user identity is a key element for the backups to be protected against a ransomware infection, as a dedicated backup account is a prerequisite for good backup security practices:



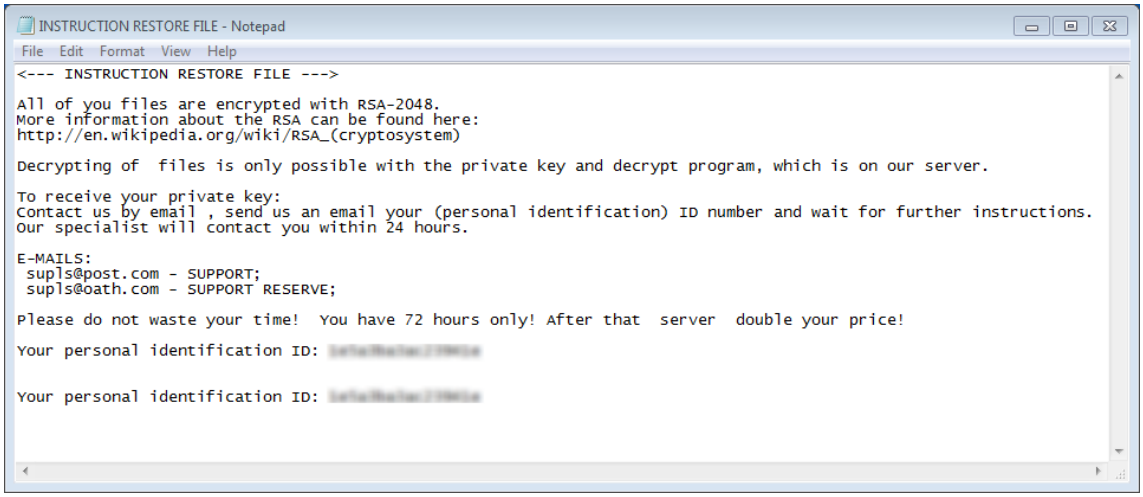
5 Conclusion

MRG Effitas found BackupAssist's CryptoSafeGuard solution to be a well-designed and well thought-out solution against ransomware infection. Not only did it provide complete protection for user's backup files against all ransomware infections in this assessment, but it also provided a System Recovery solution against MBR / MFT ransomwares like NotPetya and Petya GoldenEye.

6 Appendix A - Ransomware families used

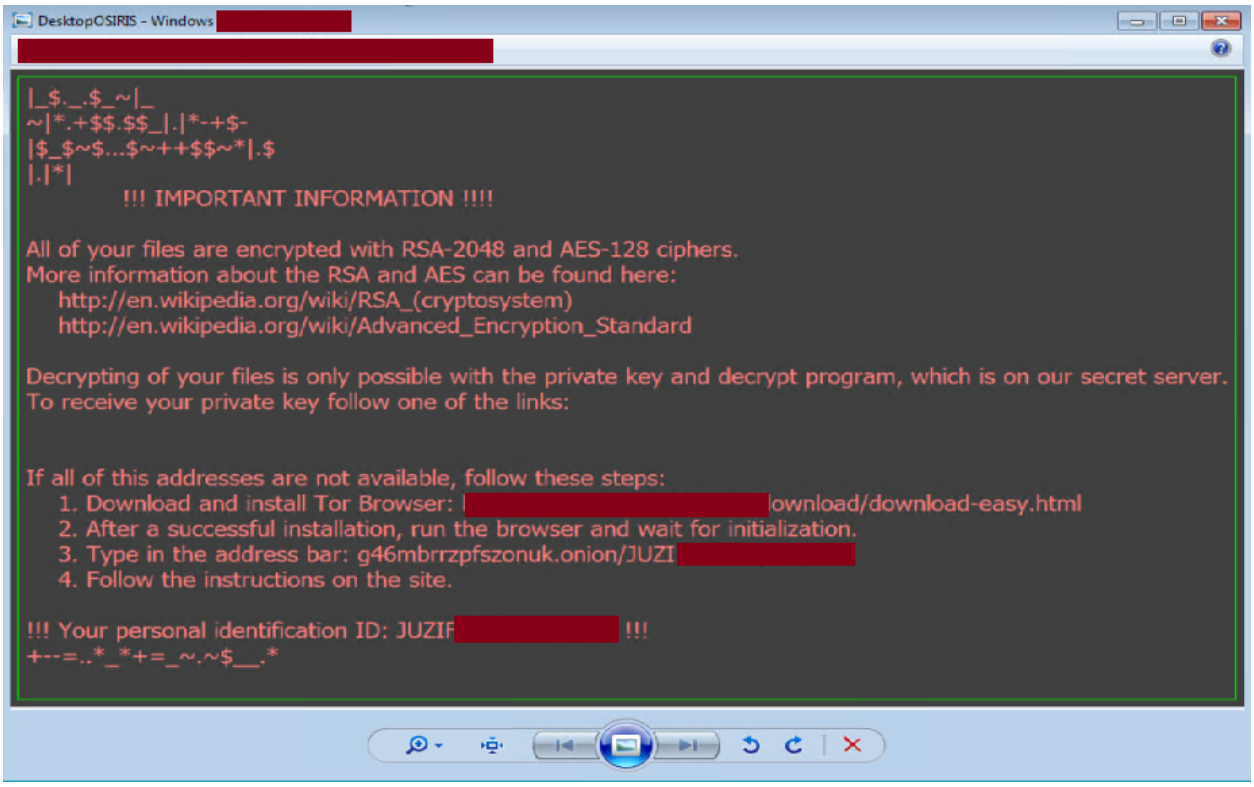
The following paragraph contains basic description about the ransomware families used in the test.

6.1 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. 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.

6.2 Osiris-Locky 2017



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.

6.3 XYZWare (MafiaWare)

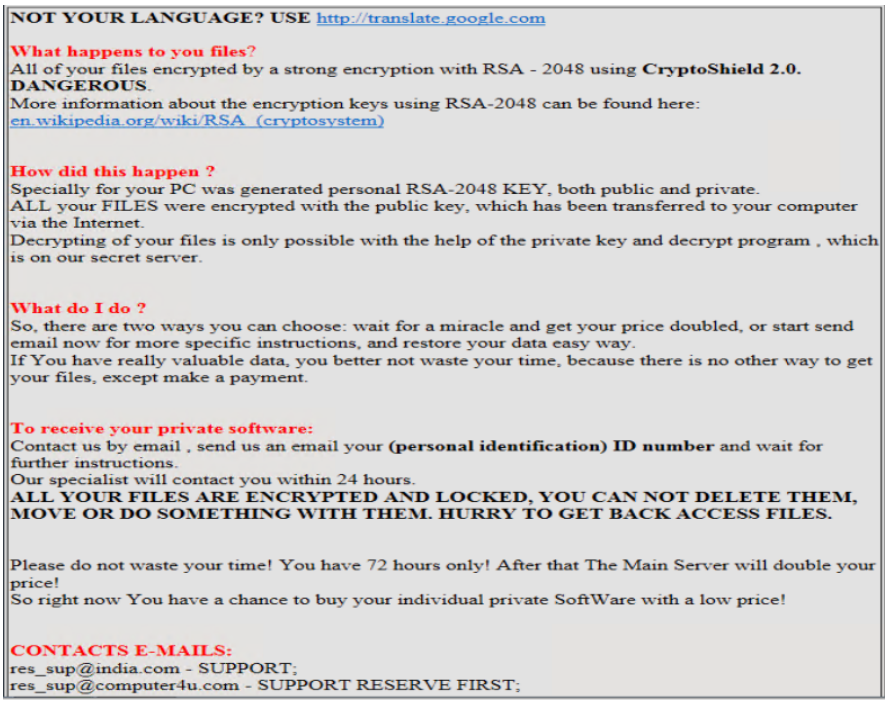
XYZWare is based on the almost ready solution MafiaWare Ransomware. While the original RansomWare is developed in Python environment, XYZWare is developed in Visual Studio 2012. The Ransomware uses RSA-2048 and AES-128 to encrypt data and add a ".XYZWare" extension. It has a weakness because it starts 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.

6.4 CryptoLocker

Cryptolocker was first seen back in September 2013 and since then many versions have been created. It infects the computer like normal malware, placing its files in Windows directories, and creating registry entries that allow it to restart when you reboot. It then also tries to contact its command and control (C&C) server. The malware uses a random domain name generation algorithm to try and find a current C&C server, such as jkamevbxhupg.co.uk or uvpevldfpfhoipn.info.

Once Cryptolocker contacts its C&C, it generates a public/private cryptographic key for your specific computer, using very strong RSA-2048-bit encryption. It also adds the ".cryptolocker" or ".crypt0l0cker" (depending on the ransomware variation) extension. The private key is only stored on the attacker's C&C servers, but the public key is saved in a registry entry on your computer.

6.5 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)

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.

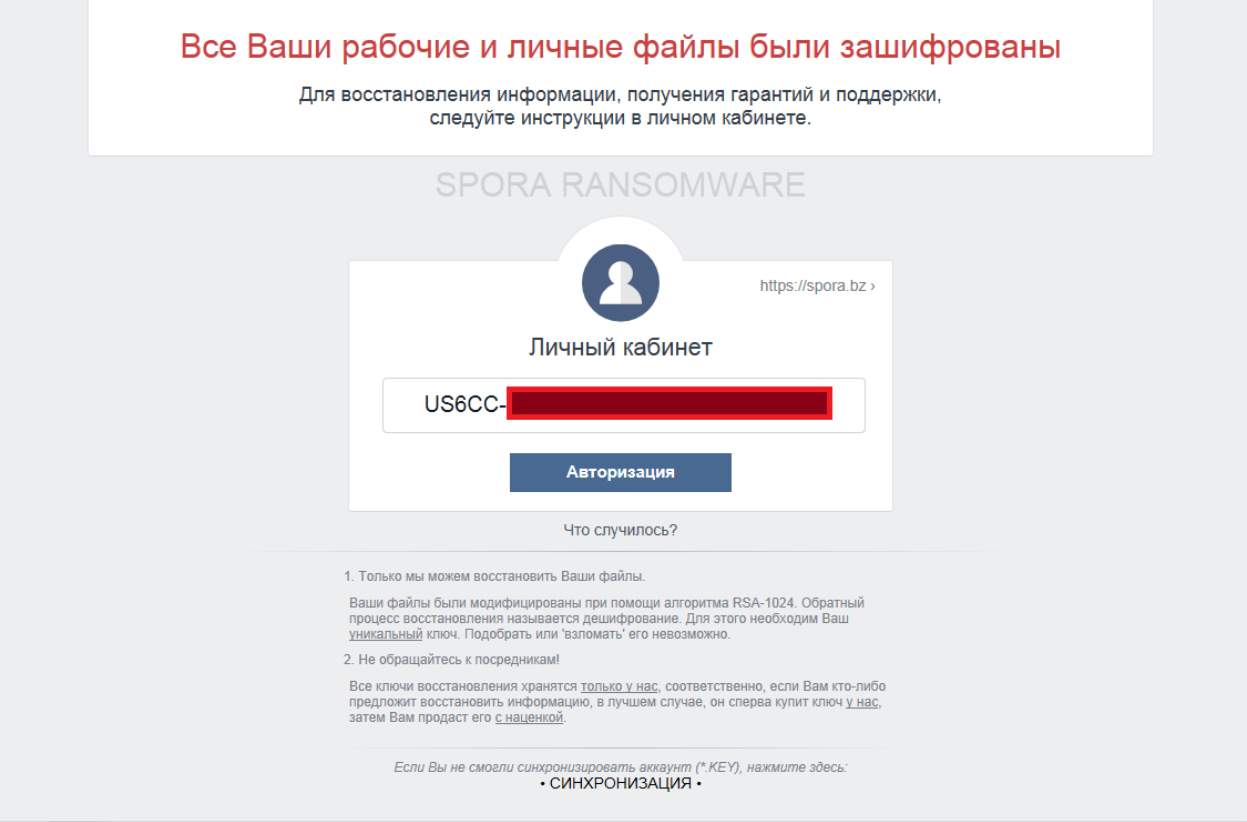
To receive your private software:
Contact us by email , send us an email your **(personal identification) ID number** and wait for further instructions.
Our specialist will contact you within 24 hours.
ALL YOUR FILES ARE ENCRYPTED AND LOCKED, YOU CAN NOT DELETE THEM, MOVE OR DO SOMETHING WITH THEM. HURRY 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;

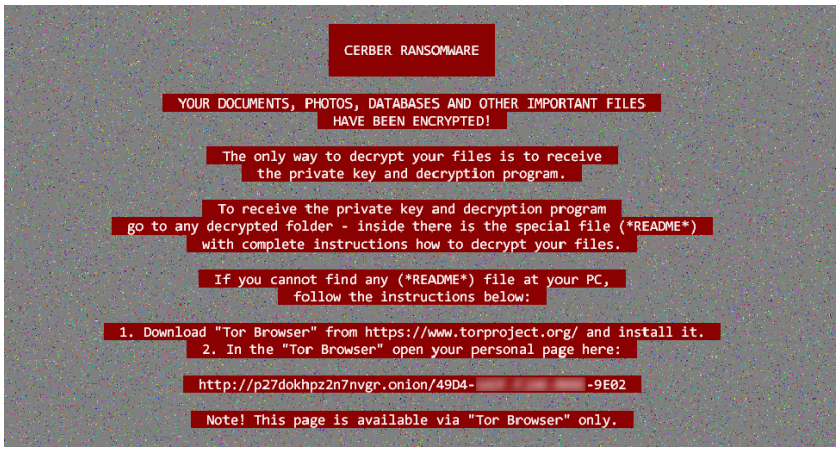
The bulk of this ransomware family's activity occurred in the first half of February 2017. It focuses on English-speaking users, which of course does not prevent it spreading around the world. This ransomware encrypts user data with AES-256, and then requires a redemption to return the files. It adds 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.

6.6 Spora



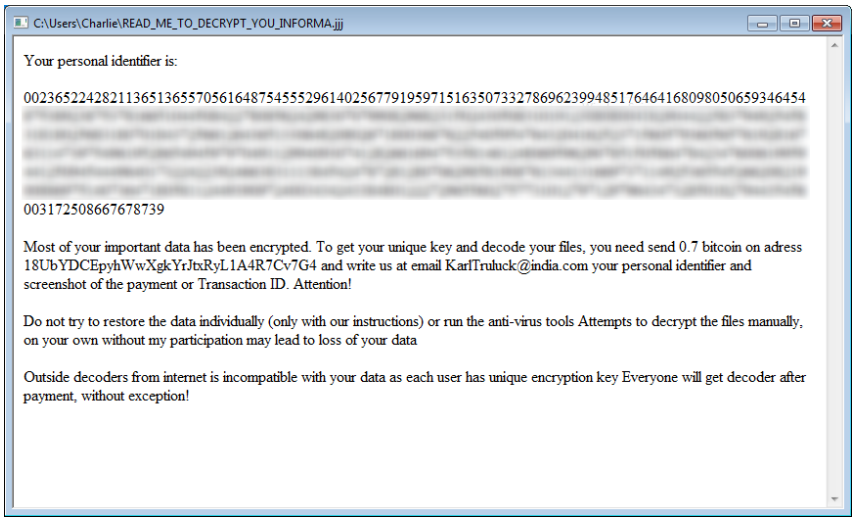
This Multilanguage ransomware was first seen at the beginning of January 2017 using AES + RSA to encrypt user data and modify the folder structure. Unlike many modern ransomware, Spora works offline and does not generate any network traffic. It does not generate extra file extensions.

6.7 Cerber



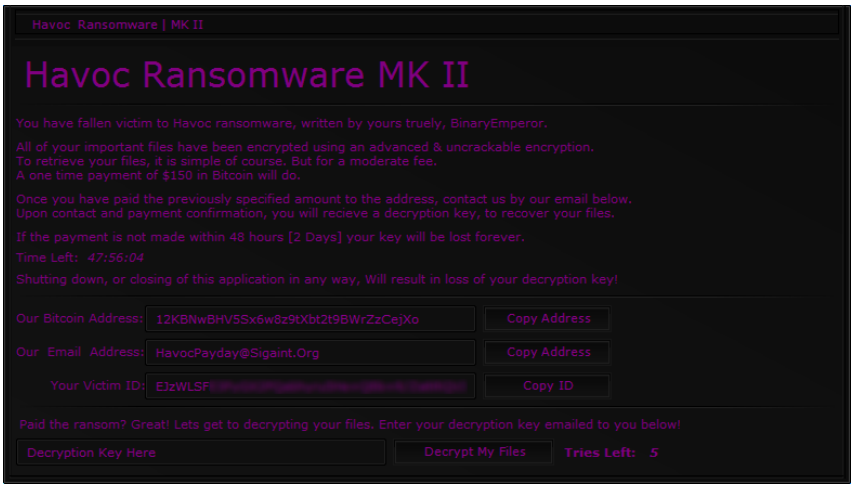
Cerber ransomware, much like many other encryption-type malware, is known to encrypt files with AES-256 encryption on the infected computer. It creates random filenames and appends the extension ".CERBER" or ".B126" and holds those files for a substantial ransom fee. As it encrypts the victim's files, 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.

6.8 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.

6.9 Havoc MK II

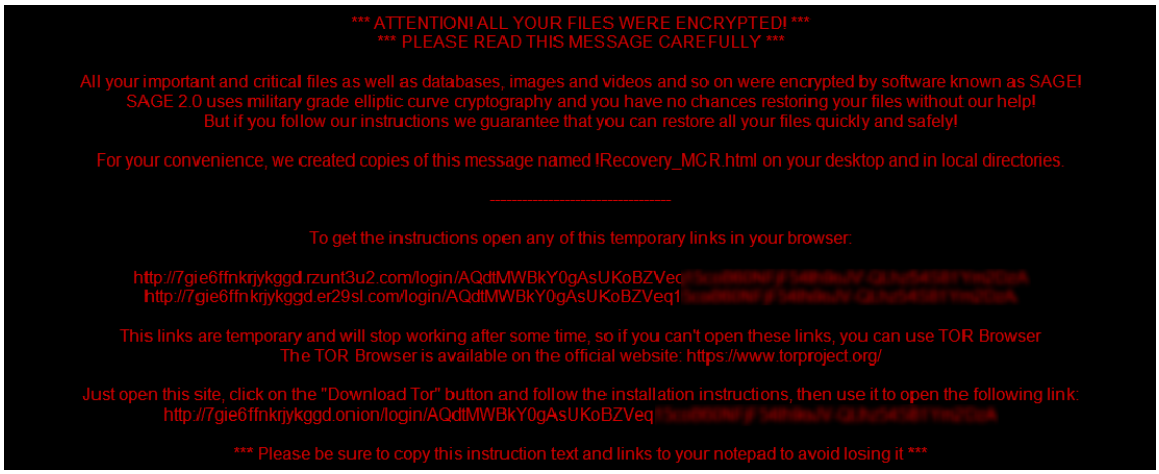


The Havoc MK II Ransomware's bright violet ransom note first appeared in public in January 2017. It uses RSA256 encryption and ".havokcrypt" extensions to lock the victim's files, targeting a wide variety of files that can include video and audio files, text files, databases, images, and numerous other 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.

6.10 Dharma

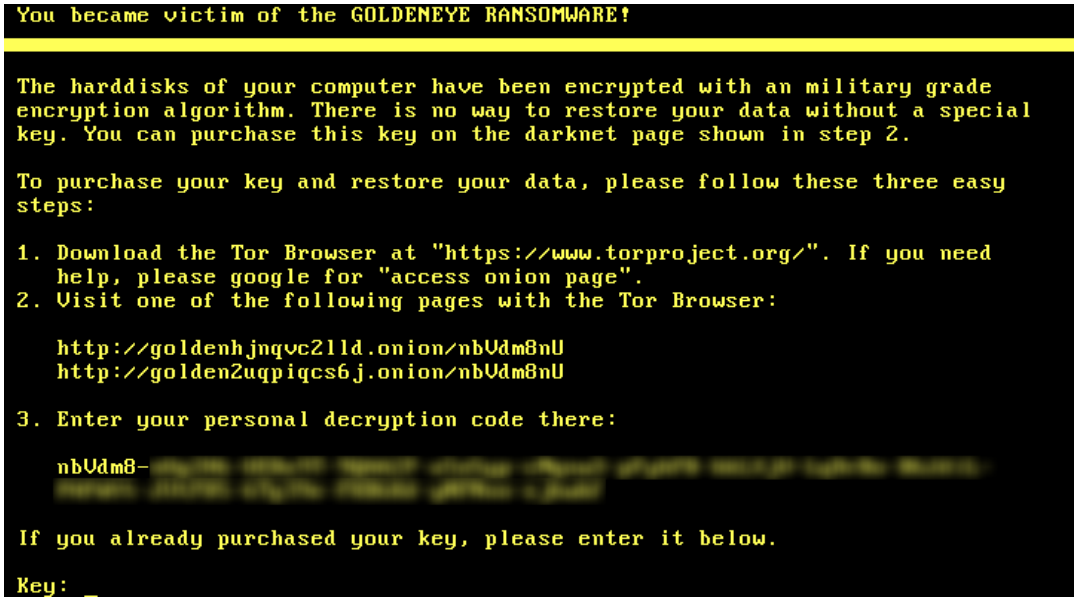
Dharma is a variant of Crysis - a high-risk ransomware-type malware. Following successful infiltration, Dharma encrypts stored files using AES. In addition, this file-encoder usually appends the ".[webmafia@asia.com]. wallet" ".[webmafia@asia.com]. dharma" or ".[webmafia@asia.com].zzzzz" extension and 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.

6.11 Sage 2.0



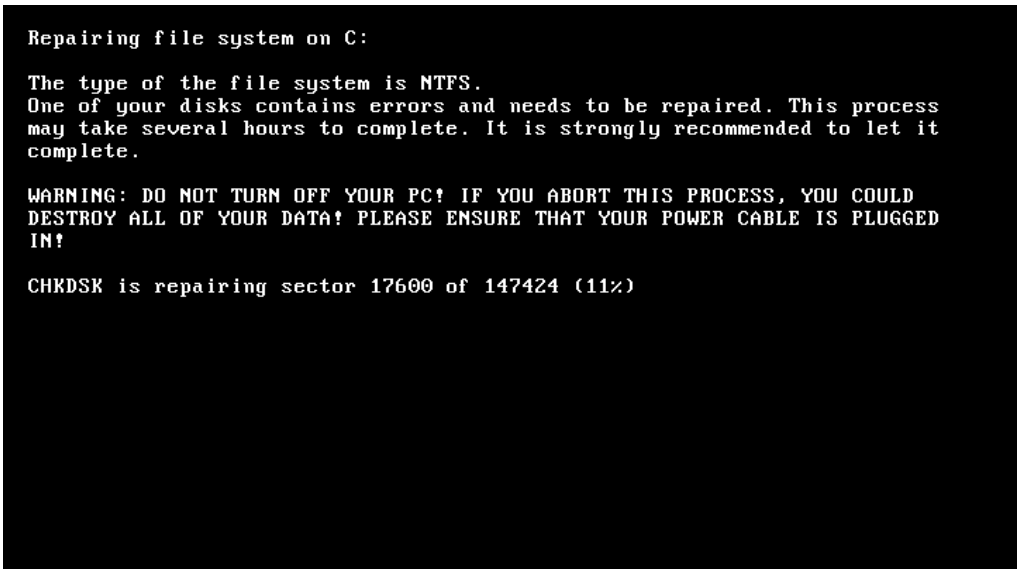
Sage Ransomware belongs to the TeslaCrypt family. This crypto ransomware encrypts user data using AES-256 and RSA-1024 ciphers and adds the ".sage" file extension to them. After encrypting, Sage delivers its ransom note as a text file on the victim's Desktop and opens an HTML file in the default browser. 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.

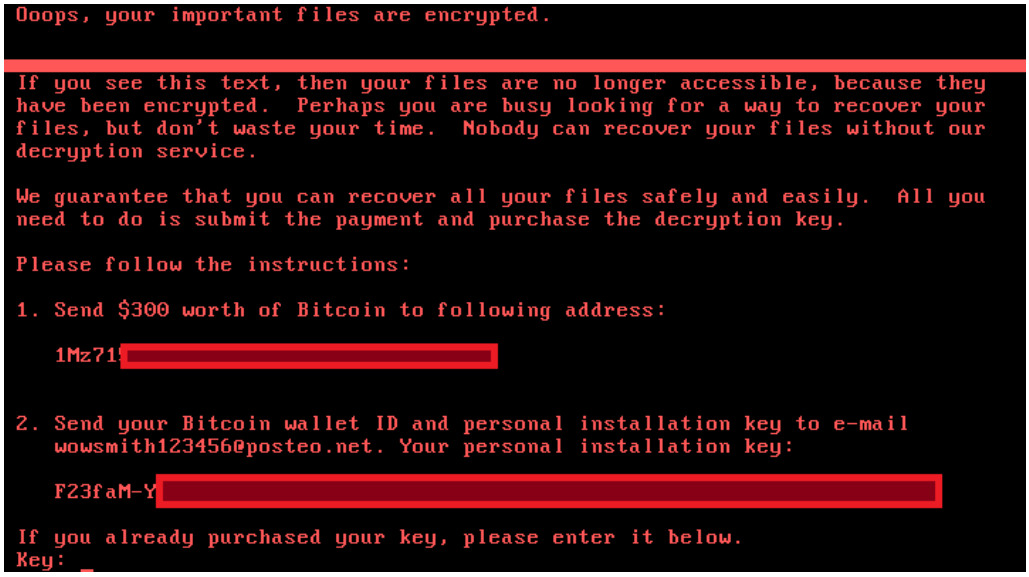
6.12 Petya GoldenEye



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.

6.13 NotPetya





NotPetya is a modified version of the Petya Ransomware, which uses the AES-128 cipher. The key difference is that it can spread trough 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 credential reuse technique to spread to other systems which are patched against EternalBlue.

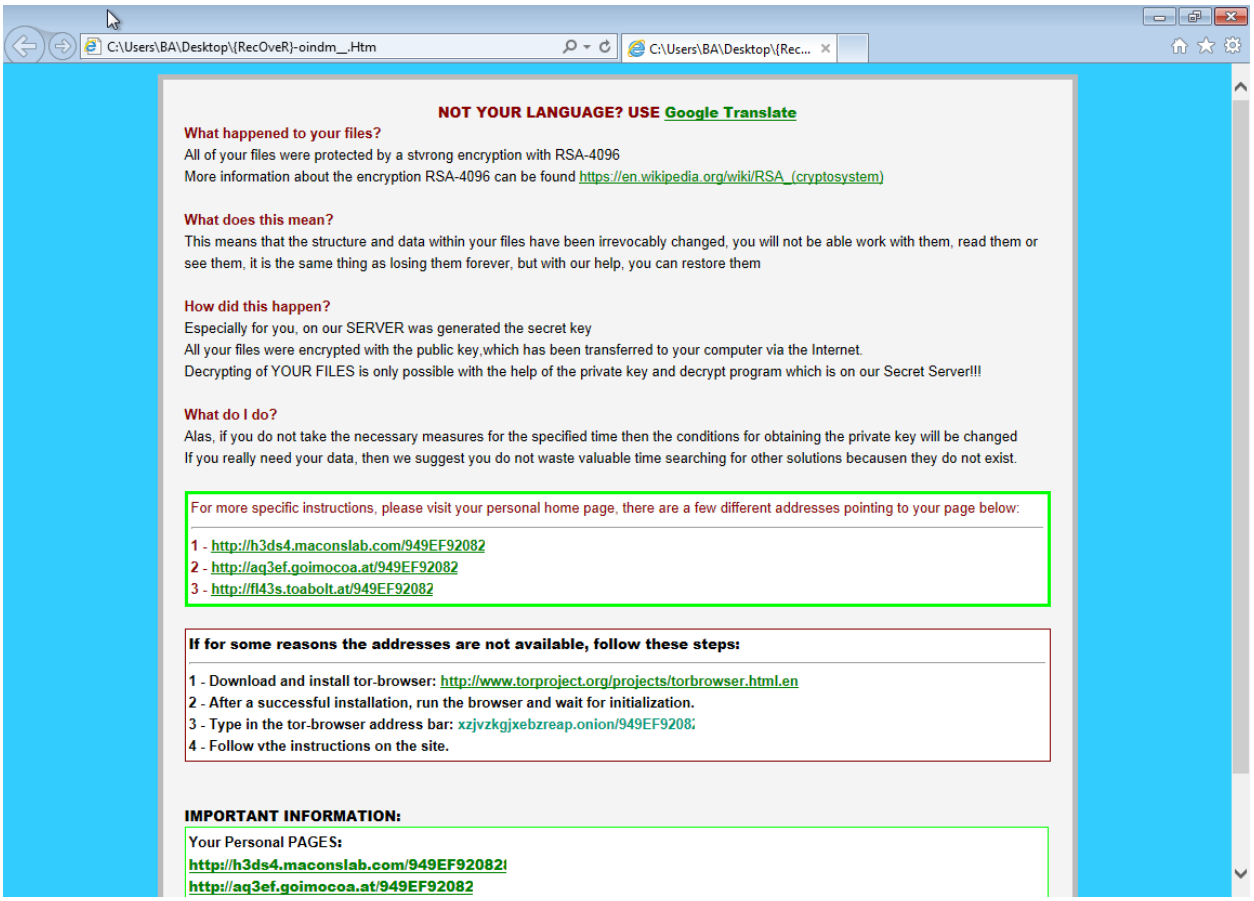
It also installs a rootkit which locks the access to the computer entirely by encrypting the drive's MFT during reboot, disguising its progress as a fake check disk scan.

6.14 AlphaCrypt

AlphaCrypt was released at the end of April 2015. After infection, AlphaCrypt will scan your computer for data files and encrypt them using AES-2048 encryption and add a ".ezz" extension so they can no longer be opened. Once the infection has encrypted the data files on all your computer drive letters it will display an application that contains instructions on how to get your files back. Ransomware also create a text file ransom note on the Windows desktop and in each folder in which a file has been encrypted.

These instructions include a link to a Decryption Service site, which will inform you of the current ransom amount, the number of files encrypted, and instructions on how to make your payment. The ransom cost starts at around $500 USD and is payable via bitcoins. The bitcoin address that you submit payment to is different for every victim.

6.15 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.

6.16 CTB Locker

The name of the ransomware, CTB, comes from its main advantages: Curve-Tor-Bitcoin. Once the machine is compromised it will install CTB Locker on the system which encrypts the personal files and adds extensions like ".zrvswok", also encrypting system data with "Elliptic Curve Encryption". A warning is presented on the screen with instructions on how to pay for the decryption key in bitcoin.

6.17 MRG Effitas ransomware simulators

Simulator 1

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.

Simulator 2

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.

7 Appendix B - Methodology used in the assessment

1. Install Windows 7 64 bit operating system on a hardened virtual box machine and apply all OS updates.
2. Installed the BackupAssist build 10.1.0t14.
3. Create and execute a “File Job to local” to back up the personal documents/files.
   The Local backup is placed under: “C:\!Backups\FileJob\” folder
4. Create and execute a “File Job to network” to back up the personal documents/files to a windows NTFS network share.
   The Network backup is mounted to “Z:\” letter
5. Create and execute a “System Job” to back up the entire system drive (necessary for disaster recovery).
   The System backup placed on a separate disk, mounted to: “D:\”
6. Create a separate “Detector Job” to back up the same files as in the “File Job”, but to a different location for later analysis.
   Detector Backup job was pointing to: “C:\!Backups\DetectorJob\” folder
7. Apply the infection.
8. Monitor attack activity to obtain definitive results of whether the local backups and/or network backup are attacked.
9. Test CryptoSafeGuard’s “Shield” functionality by checking that the ransomware unsuccessfully attacked the backups.
10. Test CryptoSafeGuard’s “Detector” functionality by running the “Detector Job”. The detection scan runs as a prerequisite of the backup job.