TOPIC:

Environment setup and Detection of Cerber Ransomware and it's Prevention

CSE3501: Information Analytics and Audit

Faculty: Prof. Subbulakshmi T

TEAM NAME: AZURE 11

TEAM MEMBERS:

19BAI1033	Suhail Ahmed
19BAI1089	Subramanian Venkittanarayanan
19BAI1098	Aaditya Hemant

VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

December 2021

Abstract:

Ransomwares is a form of malware that upon gaining access to a system, encrypts the various files and data stored on it. The encrypted files are then held hostage and the victim is asked to pay a ransom for the files to be decrypted. In particular, we take a look at CERBER ransomware which spreads through emails with malicious word documents attached to them which would download the malware and begin its execution. Initially the working and propagation of the malware was analyzed using the pcap files available on malware-traffic-analysis.net.. To improve understanding of the malware working, this was followed by execution in a controlled windows 7 virtual machine environment. We created decoy files to test the extent of the malware. Using tools such as Procmon and Wireshark we deeply analyzed the actions taken by the malware in real time. Preventive measures were also explored, such as using anti virus softwares like Avast, to detect the ransomware prior to its execution. For protecting our files we employed drive encryption technologies offered by BitLocker and Veracrypt. Finally, the .pcap file generated during malware execution was observed, to find the exact sites the ransomware connected to download the .exe file that would eventually encrypt our files.

Objectives:

- To view and analyze the method of propagation of the malware.
- To analyze the procedure in which the Cerber ransomware affects the availability of files stored in a target system
- To understand the procedure it uses to achieve the same.
- To track the execution of the malware through static and dynamic attack analysis
- To analyse the results of tools such as wireshark and procmon when used in tracking
- To explore methods through which the malware attack can be prevented
- To explore methods through which the malware attack can be mitigated

Procedure:

1. Set up a virtual machine using VMware or any other application.
2. Use Windows 7 as the VM operating system
3. Ensure that the virtual machine is not connected to the host machine through NAT.
4. Download wireshark on the virtual machine
5. Go to malware traffic analysis website and search for Cerber Ransomware.
6. Download the zip files at https://www.malware-traffic-analysis.net/2017/01/17/index.html. Specifically the file containing the .pcap file and the one containing the malware itself.
7. Take a snapshot of the system state after downloading the ransomware. This ensures we can revert back to it after malware execution.

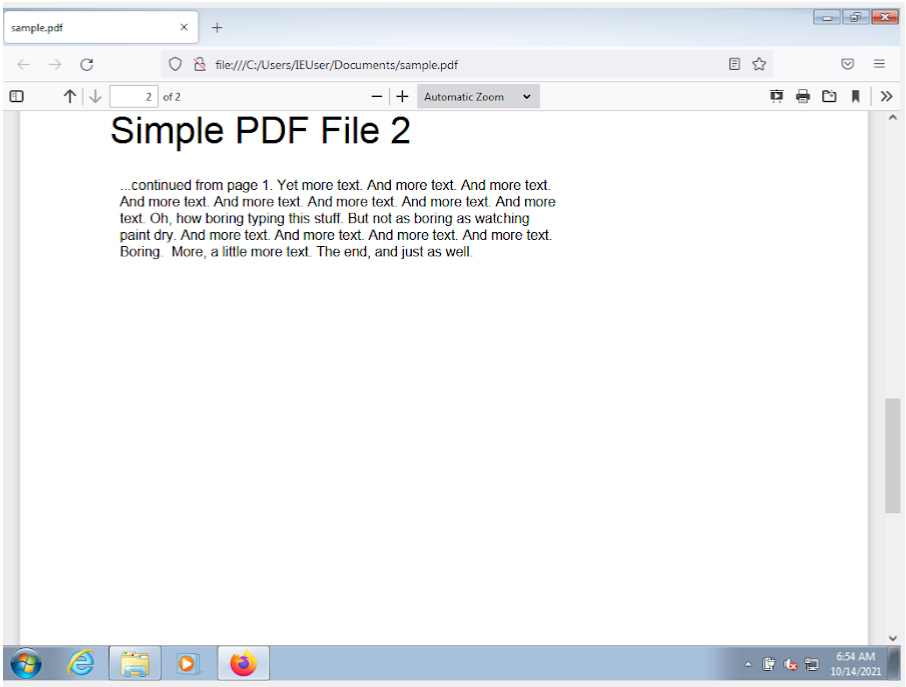
8. Open the .pcap file in wireshark and examine the contents. Look at the requests made by the malware and find out more about the attack.
9. Create a decoy file that will serve as a means to identify if the ransomware is affecting any local files.
10. Extract the contents of the downloaded zip file and run the executables.
11. This should run the ransomware and now all your files will be encrypted.
12. Document the major changes seen across the virtual machine including file renames, wallpaper changes and new files added.
13. Revert back to the previous snapshot.
14. Install procmon and set it up to track processes while the ransomware is executed.
15. Apply the appropriate filters to procmon and document all the operations performed by the ransomware software.
16. Revert back to the previous snapshot.
17. Setup wireshark to record the network traffic while the ransomware is run.
18. Document all the packet captures of interest from the pcap file.
19. Revert back to the previous snapshot.
20. Install and setup Avast antivirus software.
21. Run the ransomware and document the difference made by using Avast, if any.
22. Revert back to the previous snapshot.
23. Install and setup Veracrypt
24. Create a separate windows drive partition to store files in Drive ‘S’
25. Add a decoy file to the drive partition.
26. Open Veracrypt and create a new hidden ‘ Veracrypt Volume’
27. Select the drive partition to be encrypted and select encryption algorithms and set a secure password for the drive
28. Once this is done Drive S will become inaccessible.
29. To access files in the drive we open the drive using Veracrypt by providing the password. Which mounts the hidden volume as Drive ‘A’
30. Now we store our files in both Documents folder and in Drive A, run the ransomware and document the differences in execution.

Implementation and Results:

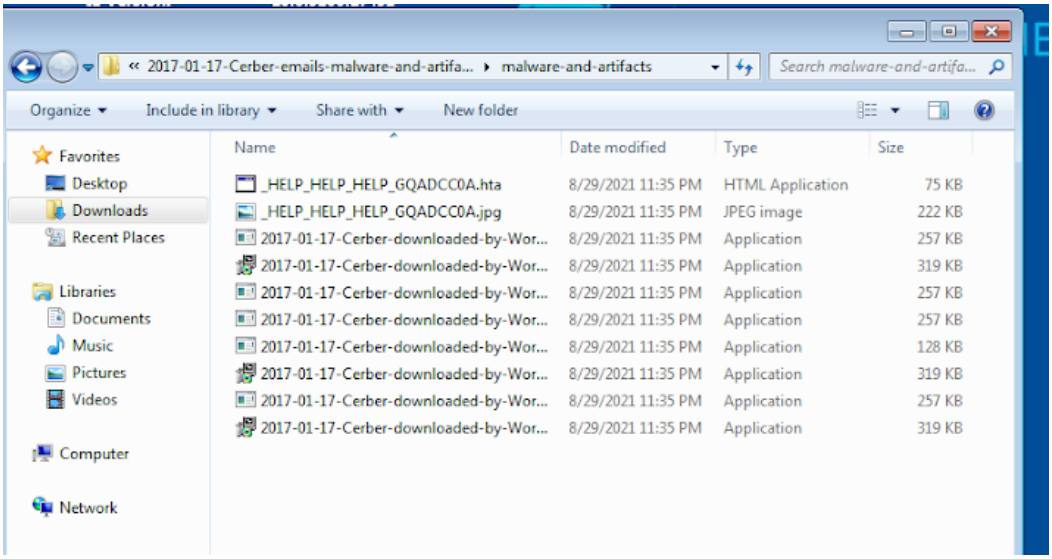
Implementation:

Attack Detection Screenshots:

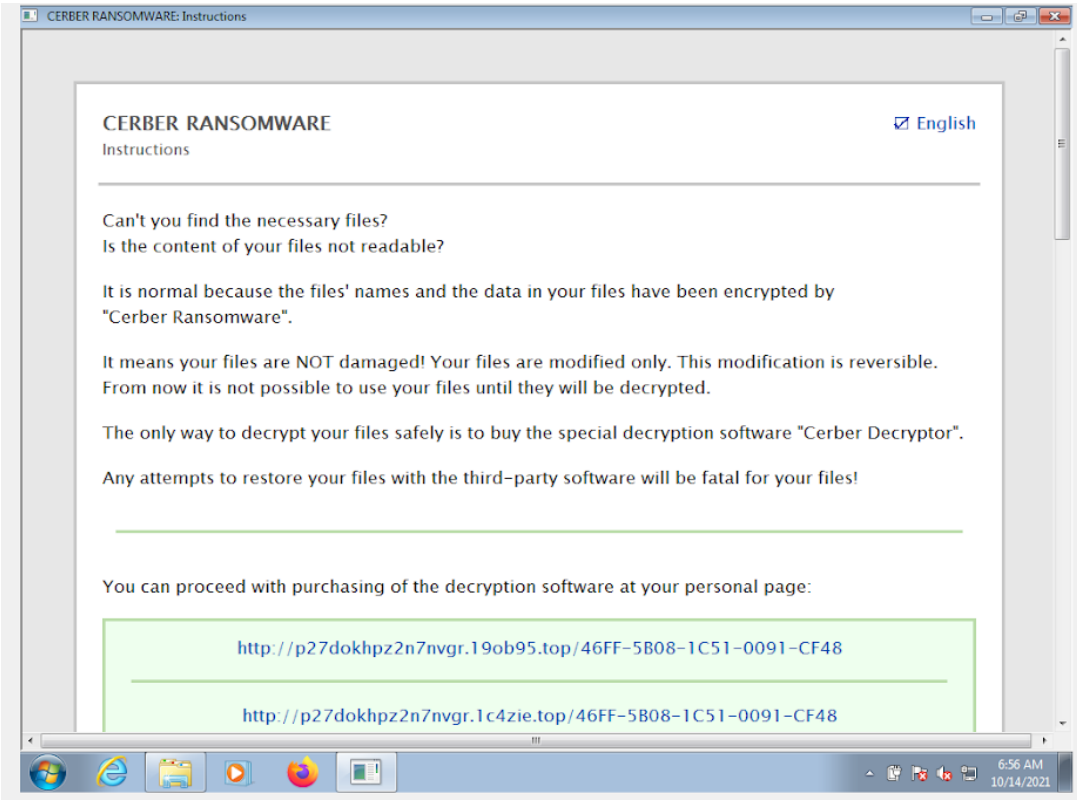
Initial state of VM (unaffected)



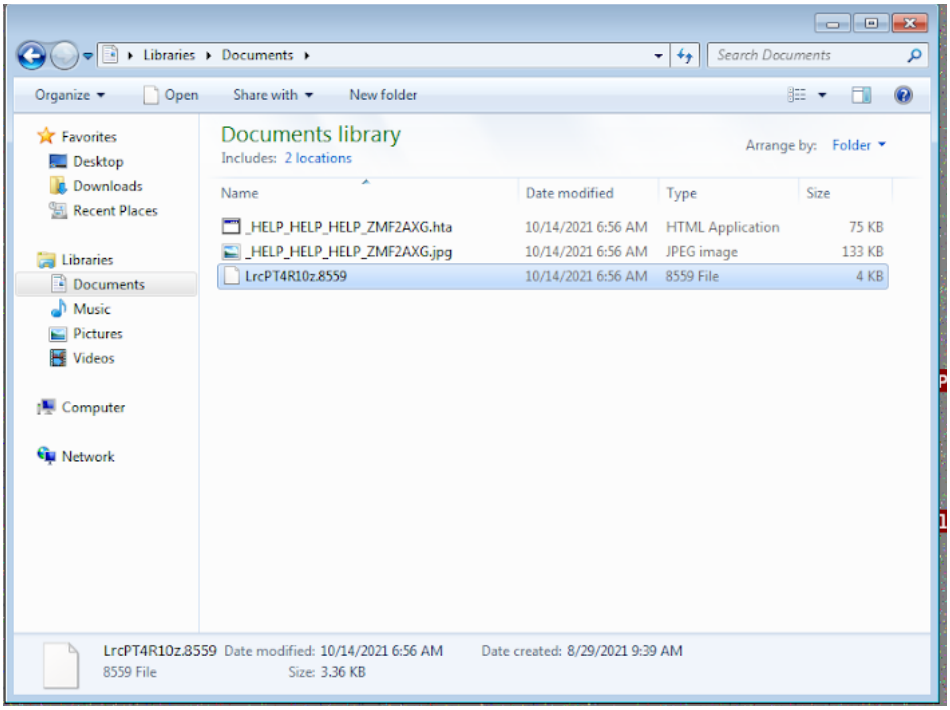
A saved file in the target machine's documents directory



The malware files

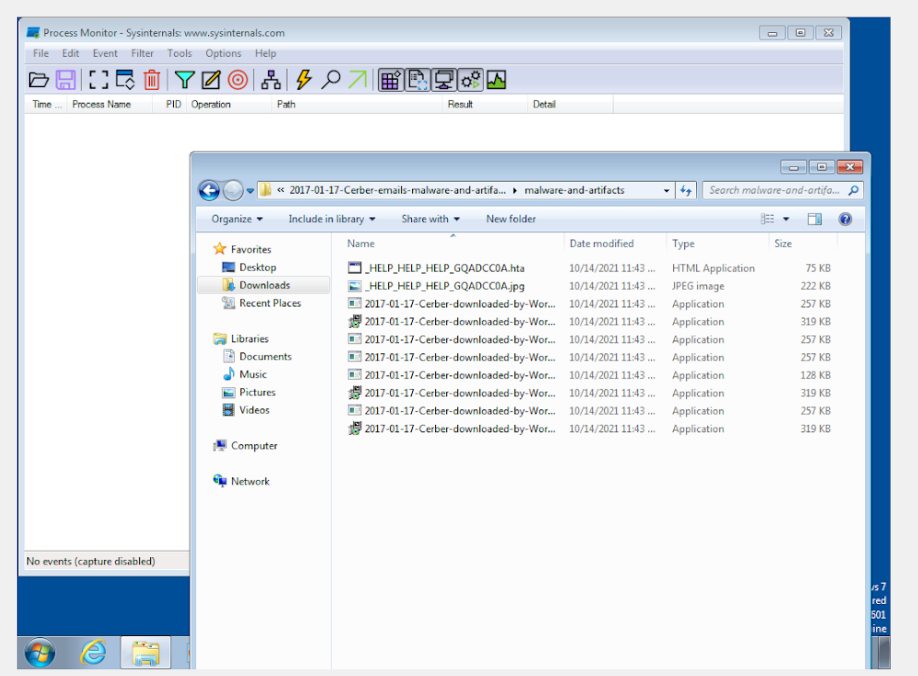


Ransom note with instructions

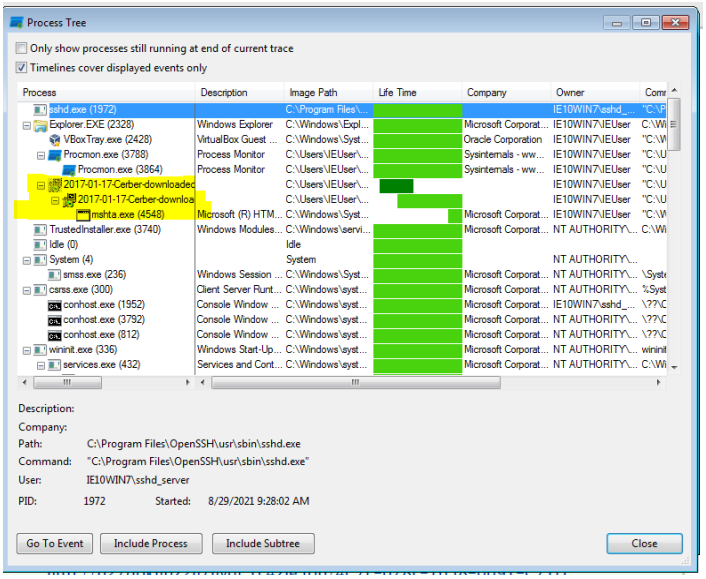


The saved file was encrypted

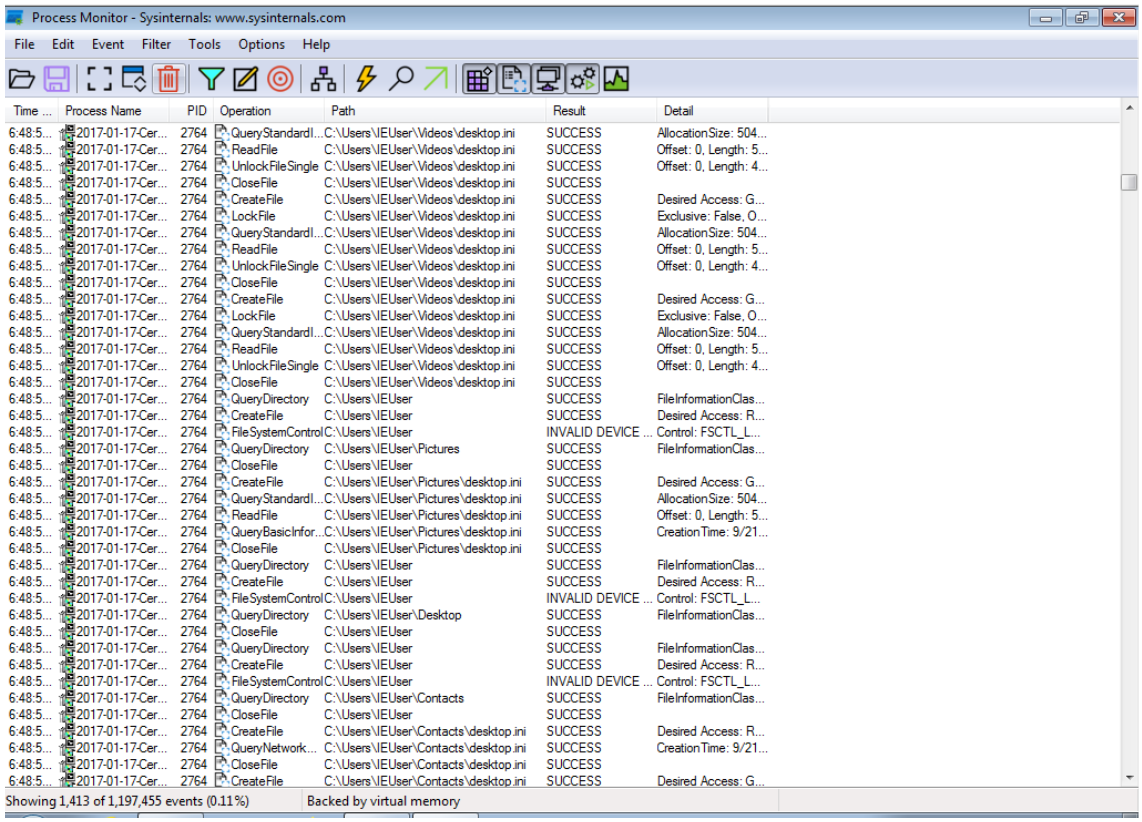
Monitoring processes when ransomware was run:



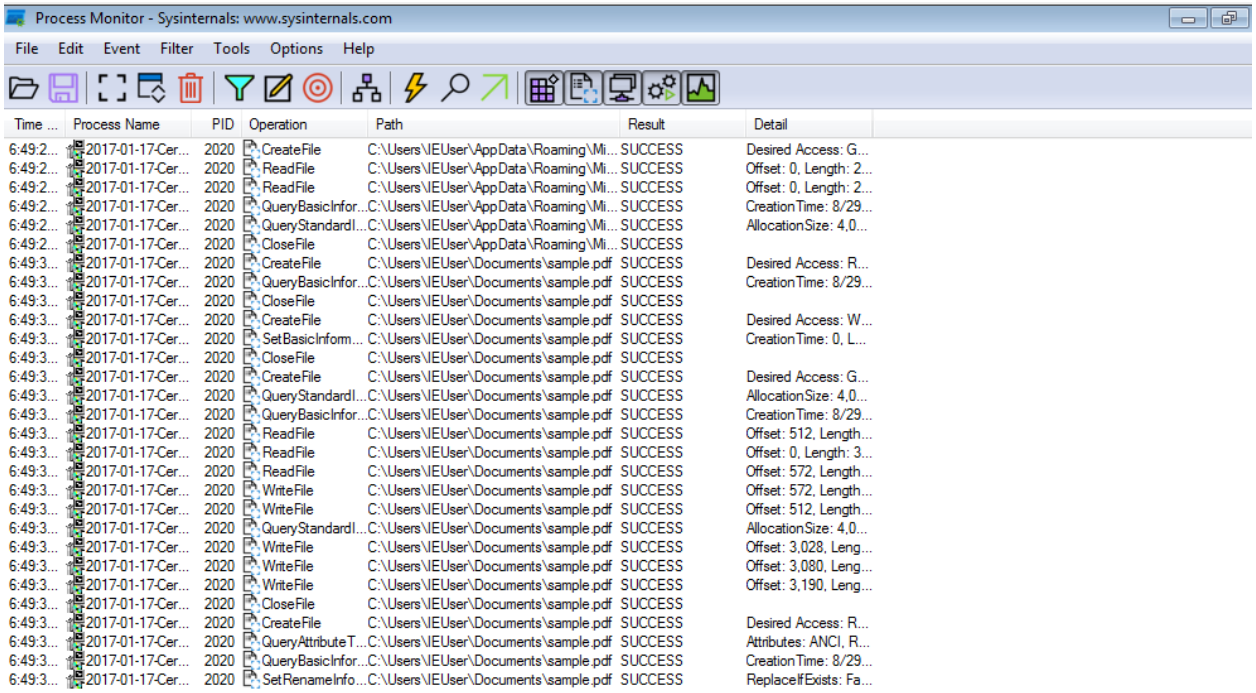
Setup procmon before executing malware



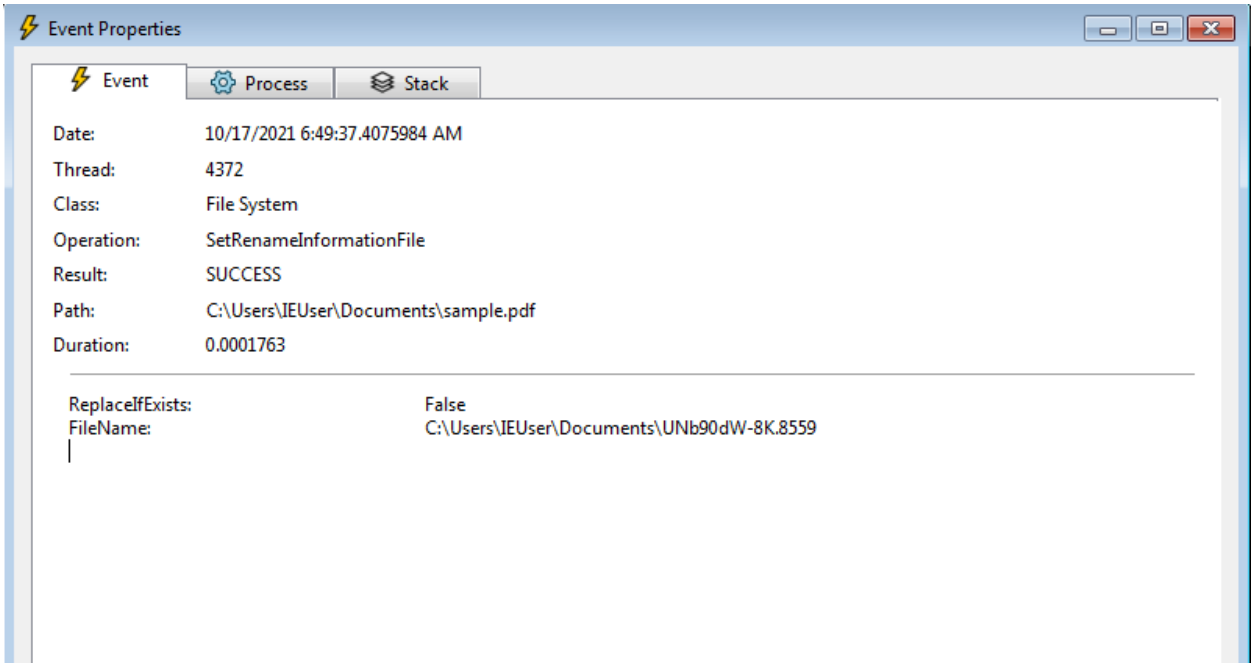
Post execution procmon Process Tree of Captured events shows the malware executing. We also see that mshta.exe is a subprocess started from the malware execution.



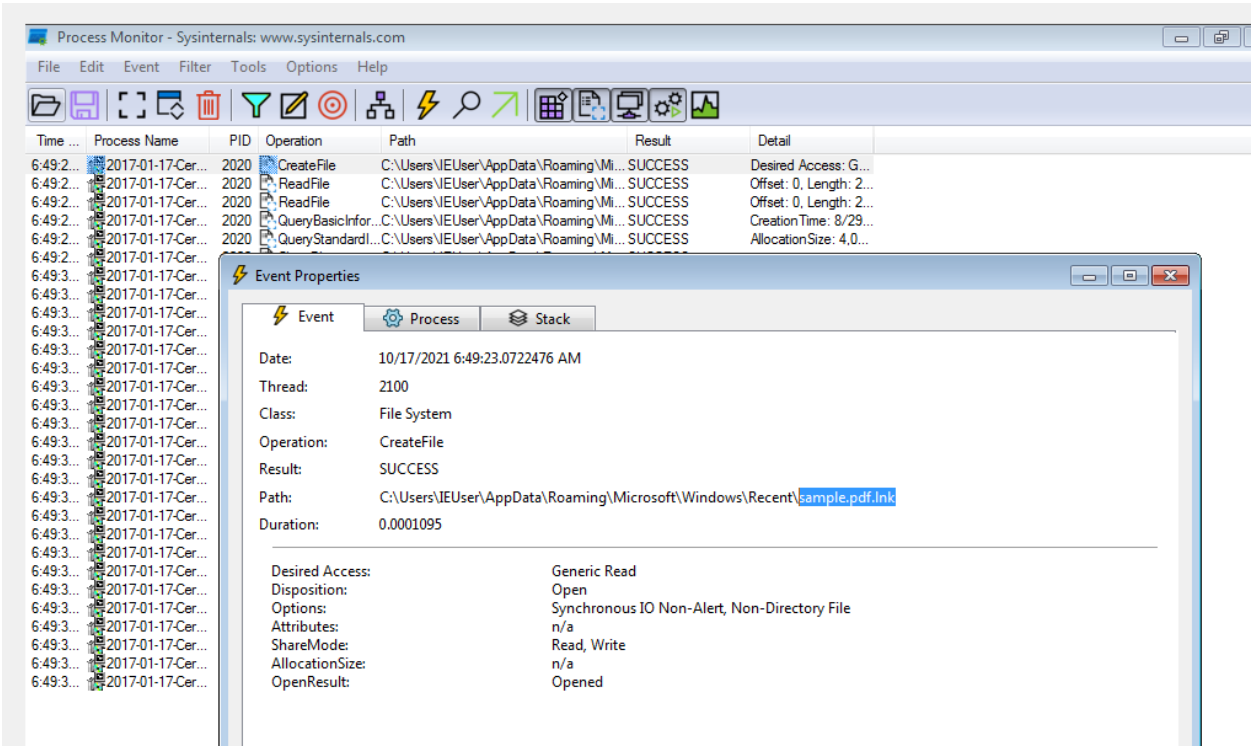
Here we can see the various directories the ransomware searches through, including Downloads, AppData, Searches, Videos, Pictures, Contacts, Favorites, Music, Documents, Links, Desktop and Recents.



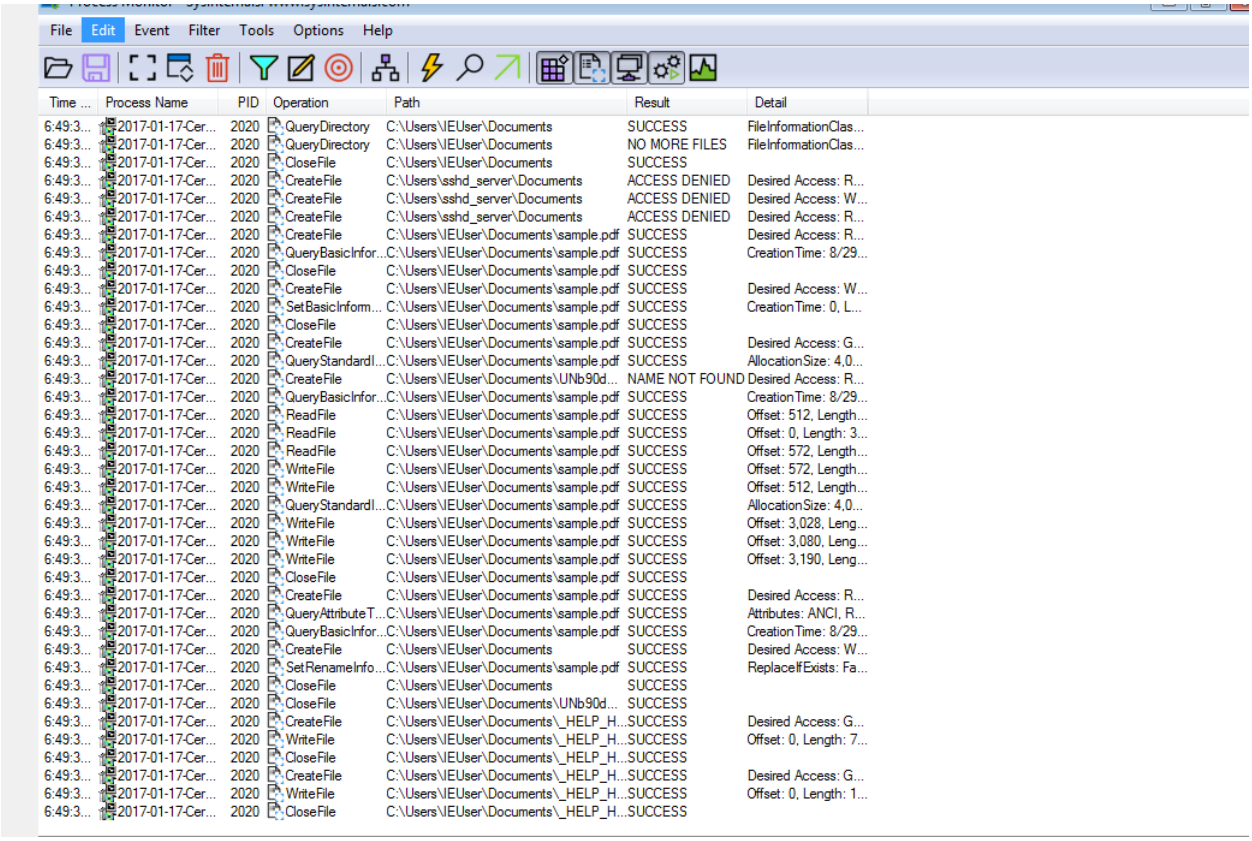
Events created that relate to our demo pdf which got encrypted



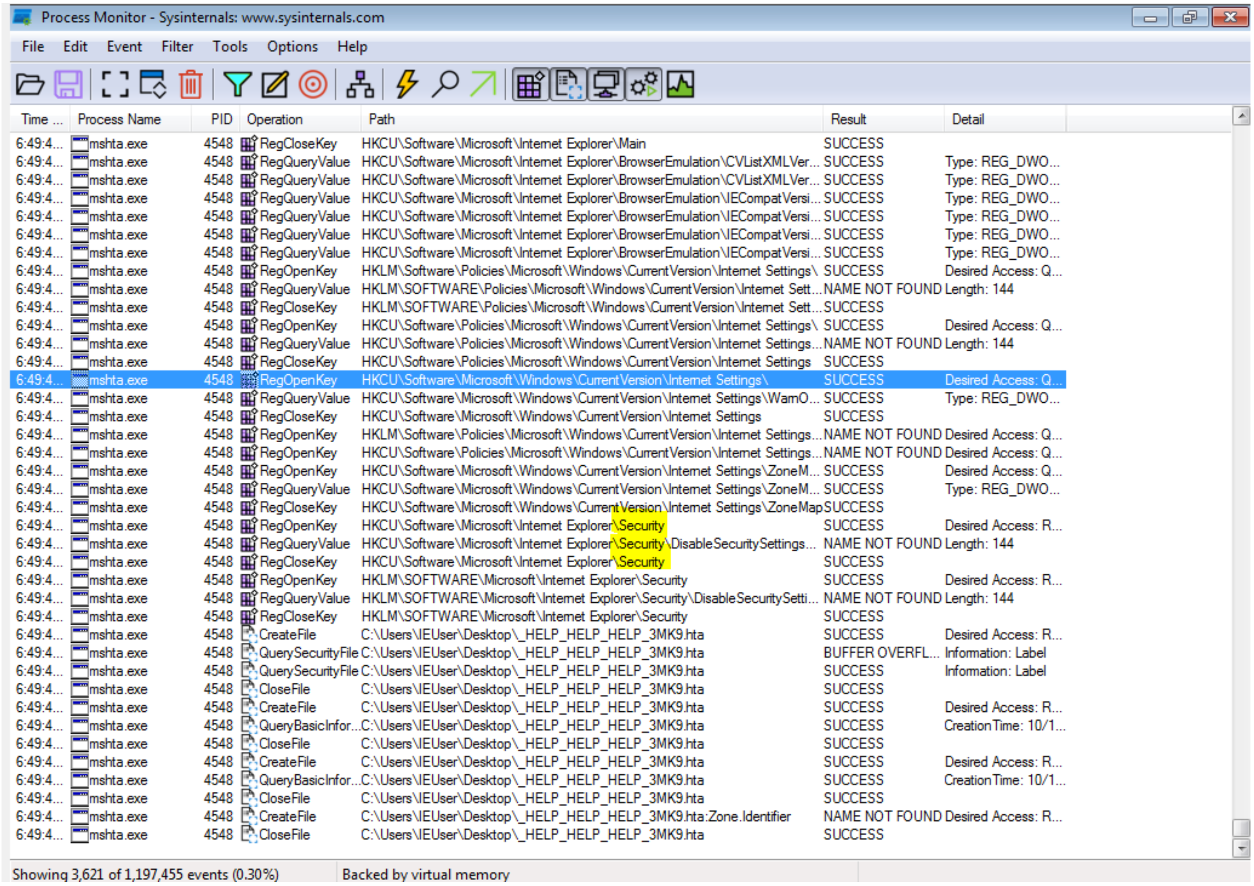
Last event from above filter which renames the file to how we found the encrypted file.



The ransomware found our sample.pdf file through the items in the Recent directory in the machine allowing it to target all the frequently used files easily.



Finds sample.pdf while going through the C:\Users\IEUser\Documents\ directory too.



Process Monitor - Sysinternals: www.sysinternals.com

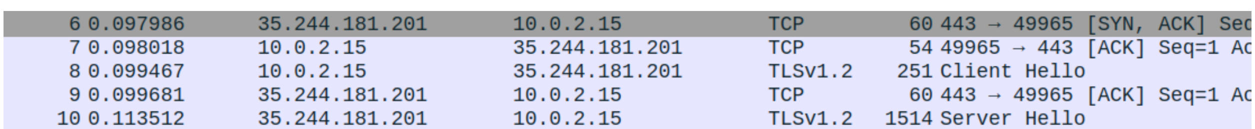
File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
6:49:4...	mshta.exe	4548	RegCloseKey	HKCU\Software\Microsoft\Internet Explorer\Main	SUCCESS	
6:49:4...	mshta.exe	4548	RegQueryValue	HKCU\Software\Microsoft\Internet Explorer\BrowserEmulation\CVListXMLVer...	SUCCESS	Type: REG_DWO...
6:49:4...	mshta.exe	4548	RegQueryValue	HKCU\Software\Microsoft\Internet Explorer\BrowserEmulation\CVListXMLVer...	SUCCESS	Type: REG_DWO...
6:49:4...	mshta.exe	4548	RegQueryValue	HKCU\Software\Microsoft\Internet Explorer\BrowserEmulation\IECompatVersi...	SUCCESS	Type: REG_DWO...
6:49:4...	mshta.exe	4548	RegQueryValue	HKCU\Software\Microsoft\Internet Explorer\BrowserEmulation\IECompatVersi...	SUCCESS	Type: REG_DWO...
6:49:4...	mshta.exe	4548	RegQueryValue	HKCU\Software\Microsoft\Internet Explorer\BrowserEmulation\IECompatVersi...	SUCCESS	Type: REG_DWO...
6:49:4...	mshta.exe	4548	RegQueryValue	HKCU\Software\Microsoft\Internet Explorer\BrowserEmulation\IECompatVersi...	SUCCESS	Type: REG_DWO...
6:49:4...	mshta.exe	4548	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\	SUCCESS	Desired Access: Q...
6:49:4...	mshta.exe	4548	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Sett...	NAME NOT FOUND	Length: 144
6:49:4...	mshta.exe	4548	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Sett...	SUCCESS	
6:49:4...	mshta.exe	4548	RegOpenKey	HKCU\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\	SUCCESS	Desired Access: Q...
6:49:4...	mshta.exe	4548	RegQueryValue	HKCU\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings...	NAME NOT FOUND	Length: 144
6:49:4...	mshta.exe	4548	RegCloseKey	HKCU\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	SUCCESS	
6:49:4...	mshta.exe	4548	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\	SUCCESS	Desired Access: Q...
6:49:4...	mshta.exe	4548	RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\WarnO...	SUCCESS	Type: REG_DWO...
6:49:4...	mshta.exe	4548	RegCloseKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings	SUCCESS	
6:49:4...	mshta.exe	4548	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings...	NAME NOT FOUND	Desired Access: Q...
6:49:4...	mshta.exe	4548	RegOpenKey	HKCU\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings...	NAME NOT FOUND	Desired Access: Q...
6:49:4...	mshta.exe	4548	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneM...	SUCCESS	Desired Access: Q...
6:49:4...	mshta.exe	4548	RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneM...	SUCCESS	Type: REG_DWO...
6:49:4...	mshta.exe	4548	RegCloseKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap	SUCCESS	
6:49:4...	mshta.exe	4548	RegOpenKey	HKCU\Software\Microsoft\Internet Explorer\Security	SUCCESS	Desired Access: R...
6:49:4...	mshta.exe	4548	RegQueryValue	HKCU\Software\Microsoft\Internet Explorer\Security\DisableSecuritySettings...	NAME NOT FOUND	Length: 144
6:49:4...	mshta.exe	4548	RegCloseKey	HKCU\Software\Microsoft\Internet Explorer\Security	SUCCESS	
6:49:4...	mshta.exe	4548	RegOpenKey	HKLM\SOFTWARE\Microsoft\Internet Explorer\Security	SUCCESS	Desired Access: R...
6:49:4...	mshta.exe	4548	RegQueryValue	HKLM\SOFTWARE\Microsoft\Internet Explorer\Security\DisableSecuritySetti...	NAME NOT FOUND	Length: 144
6:49:4...	mshta.exe	4548	RegCloseKey	HKLM\SOFTWARE\Microsoft\Internet Explorer\Security	SUCCESS	
6:49:4...	mshta.exe	4548	CreateFile	C:\Users\IEUser\Desktop_HELP_HELP_HELP_3MK9.hta	SUCCESS	Desired Access: R...
6:49:4...	mshta.exe	4548	QuerySecurityFile	C:\Users\IEUser\Desktop_HELP_HELP_HELP_3MK9.hta	BUFFER OVERFL...	Information: Label
6:49:4...	mshta.exe	4548	QuerySecurityFile	C:\Users\IEUser\Desktop_HELP_HELP_HELP_3MK9.hta	SUCCESS	Information: Label
6:49:4...	mshta.exe	4548	CloseFile	C:\Users\IEUser\Desktop_HELP_HELP_HELP_3MK9.hta	SUCCESS	
6:49:4...	mshta.exe	4548	CreateFile	C:\Users\IEUser\Desktop_HELP_HELP_HELP_3MK9.hta	SUCCESS	Desired Access: R...
6:49:4...	mshta.exe	4548	QueryBasicInfor...	C:\Users\IEUser\Desktop_HELP_HELP_HELP_3MK9.hta	SUCCESS	CreationTime: 10/1...
6:49:4...	mshta.exe	4548	CloseFile	C:\Users\IEUser\Desktop_HELP_HELP_HELP_3MK9.hta	SUCCESS	
6:49:4...	mshta.exe	4548	CreateFile	C:\Users\IEUser\Desktop_HELP_HELP_HELP_3MK9.hta	SUCCESS	Desired Access: R...
6:49:4...	mshta.exe	4548	QueryBasicInfor...	C:\Users\IEUser\Desktop_HELP_HELP_HELP_3MK9.hta	SUCCESS	CreationTime: 10/1...
6:49:4...	mshta.exe	4548	CloseFile	C:\Users\IEUser\Desktop_HELP_HELP_HELP_3MK9.hta	SUCCESS	
6:49:4...	mshta.exe	4548	CreateFile	C:\Users\IEUser\Desktop_HELP_HELP_HELP_3MK9.hta:Zone.Identifier	NAME NOT FOUND	Desired Access: R...
6:49:4...	mshta.exe	4548	CloseFile	C:\Users\IEUser\Desktop_HELP_HELP_HELP_3MK9.hta	SUCCESS	

Showing 3,621 of 1,197,455 events (0.30%) Backed by virtual memory

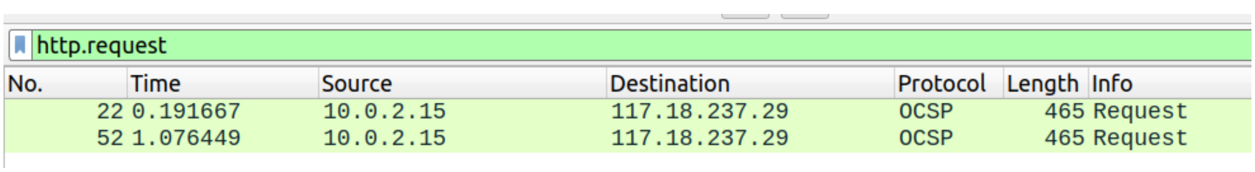
Mshta.exe attempts to disable various security settings by editing the registry.

Packet analysis during execution:



6	0.097986	35.244.181.201	10.0.2.15	TCP	60	443 → 49965 [SYN, ACK] Sec
7	0.098018	10.0.2.15	35.244.181.201	TCP	54	49965 → 443 [ACK] Seq=1 Ac
8	0.099467	10.0.2.15	35.244.181.201	TLSv1.2	251	Client Hello
9	0.099681	35.244.181.201	10.0.2.15	TCP	60	443 → 49965 [ACK] Seq=1 Ac
10	0.113512	35.244.181.201	10.0.2.15	TLSv1.2	1514	Server Hello

Client-Server "Hello"



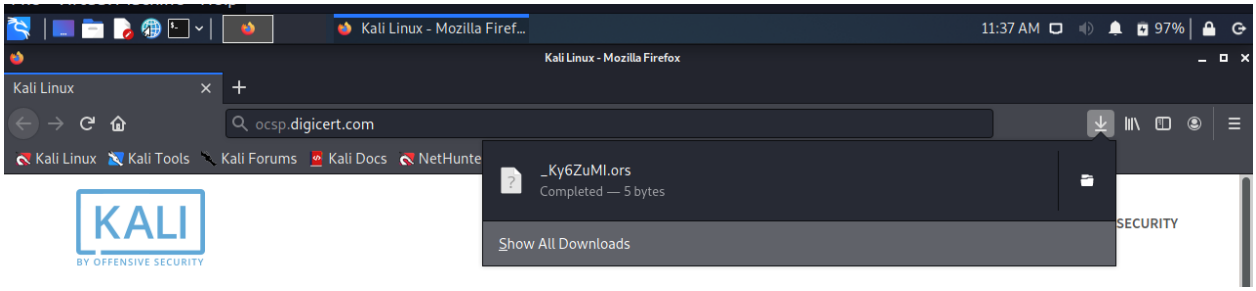
http.request

No.	Time	Source	Destination	Protocol	Length	Info
22	0.191667	10.0.2.15	117.18.237.29	OCSP	465	Request
52	1.076449	10.0.2.15	117.18.237.29	OCSP	465	Request

OCSP Request Made by the Malware

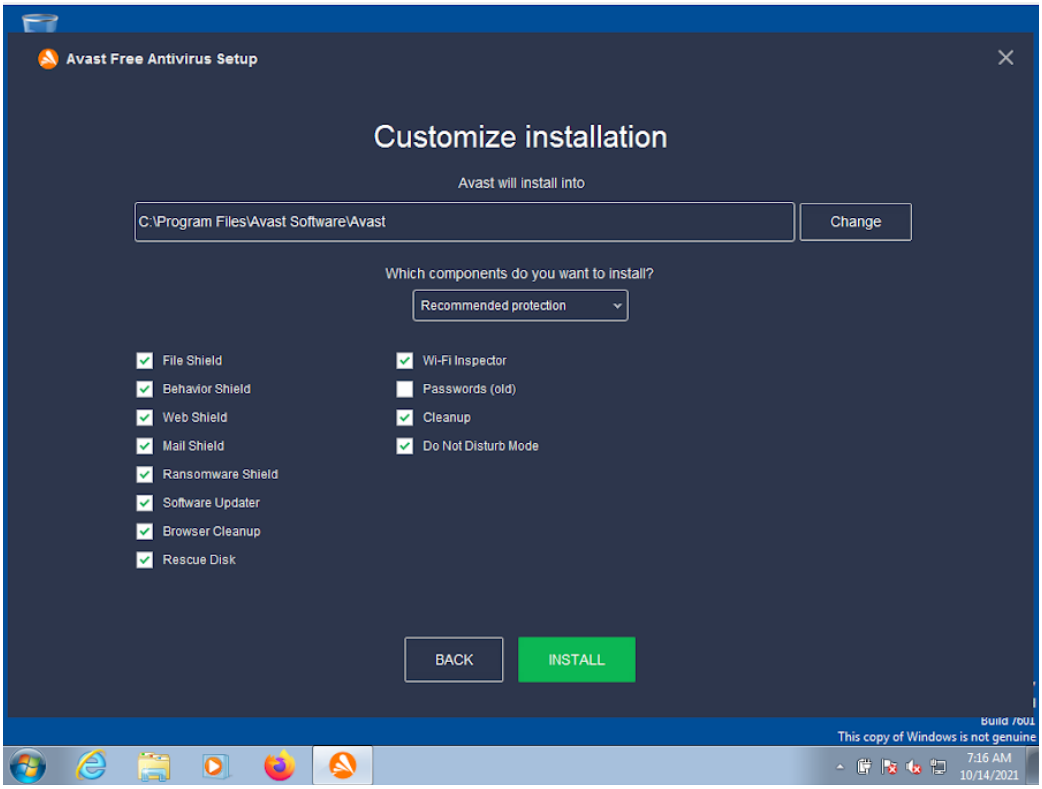
```
▾ Hypertext Transfer Protocol
  ▸ POST / HTTP/1.1\r\n
    Host: ocsp.digicert.com\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:94.0) Gecko/20100101 Firefox/94.0\r\n
    Accept: */*\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Content-Type: application/ocsp-request\r\n
  ▸ Content-Length: 83\r\n
```

HTTP Request Details

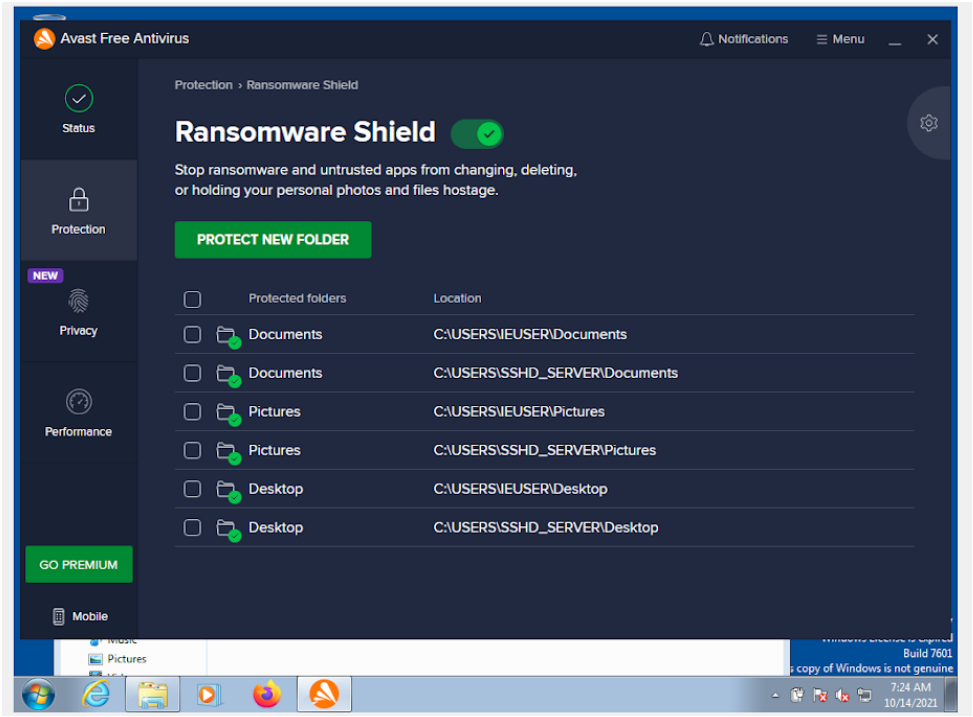


ORS File Downloaded by the Ransomware

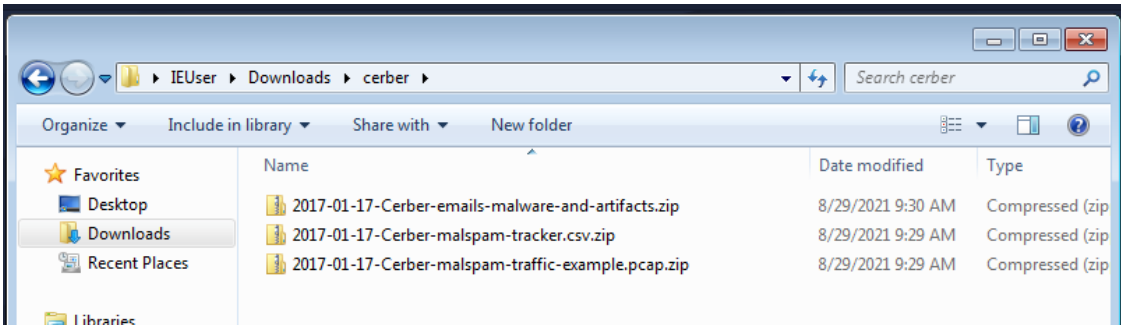
Setting up Avast Antivirus for prevention:



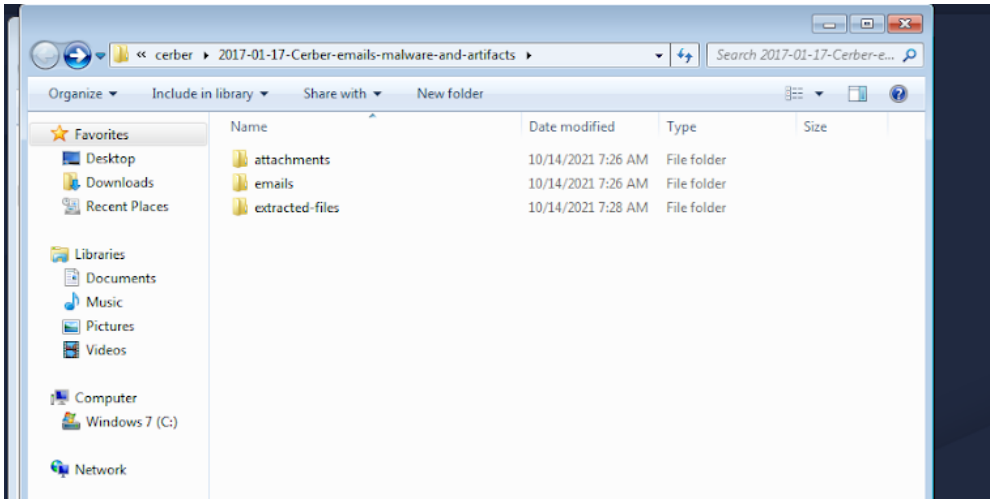
Avast Antivirus was installed



Ransomware shield was switched on and the documents folder was added to the protected folders list

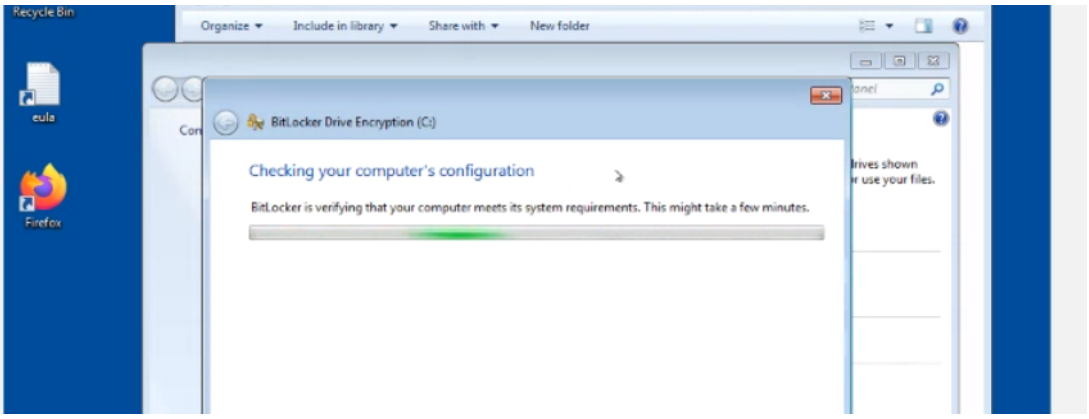


The unzipped malware executables were deleted by Avast Antivirus

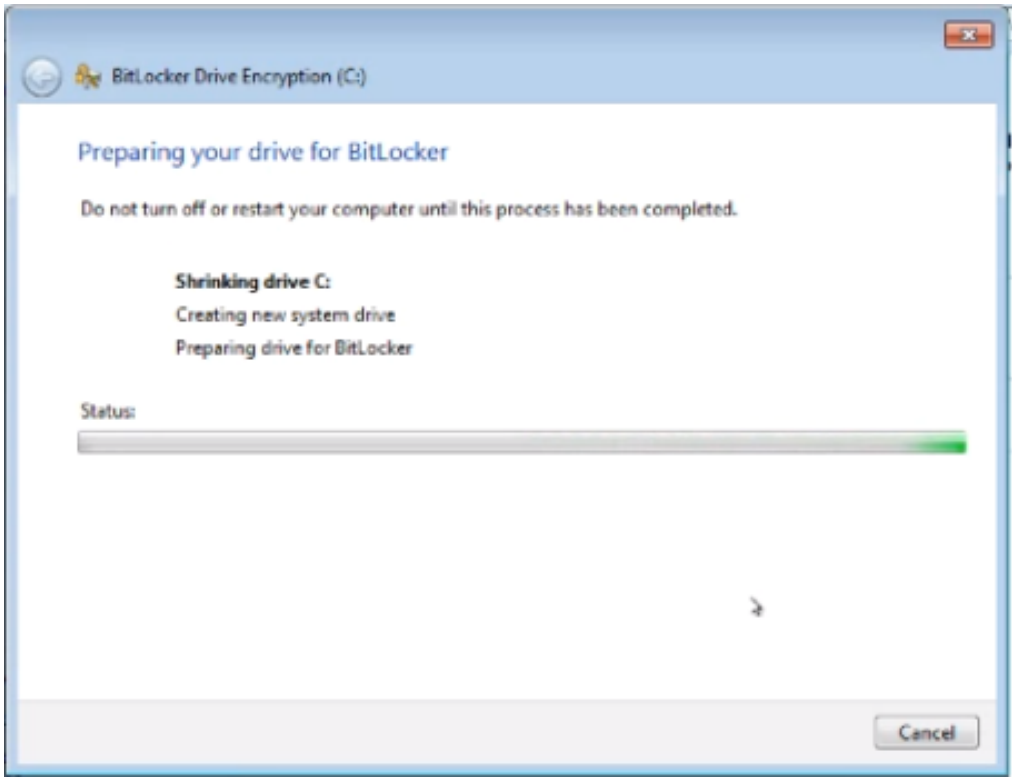


Trying to unzip the malware files causes avast to flag and immediately delete them

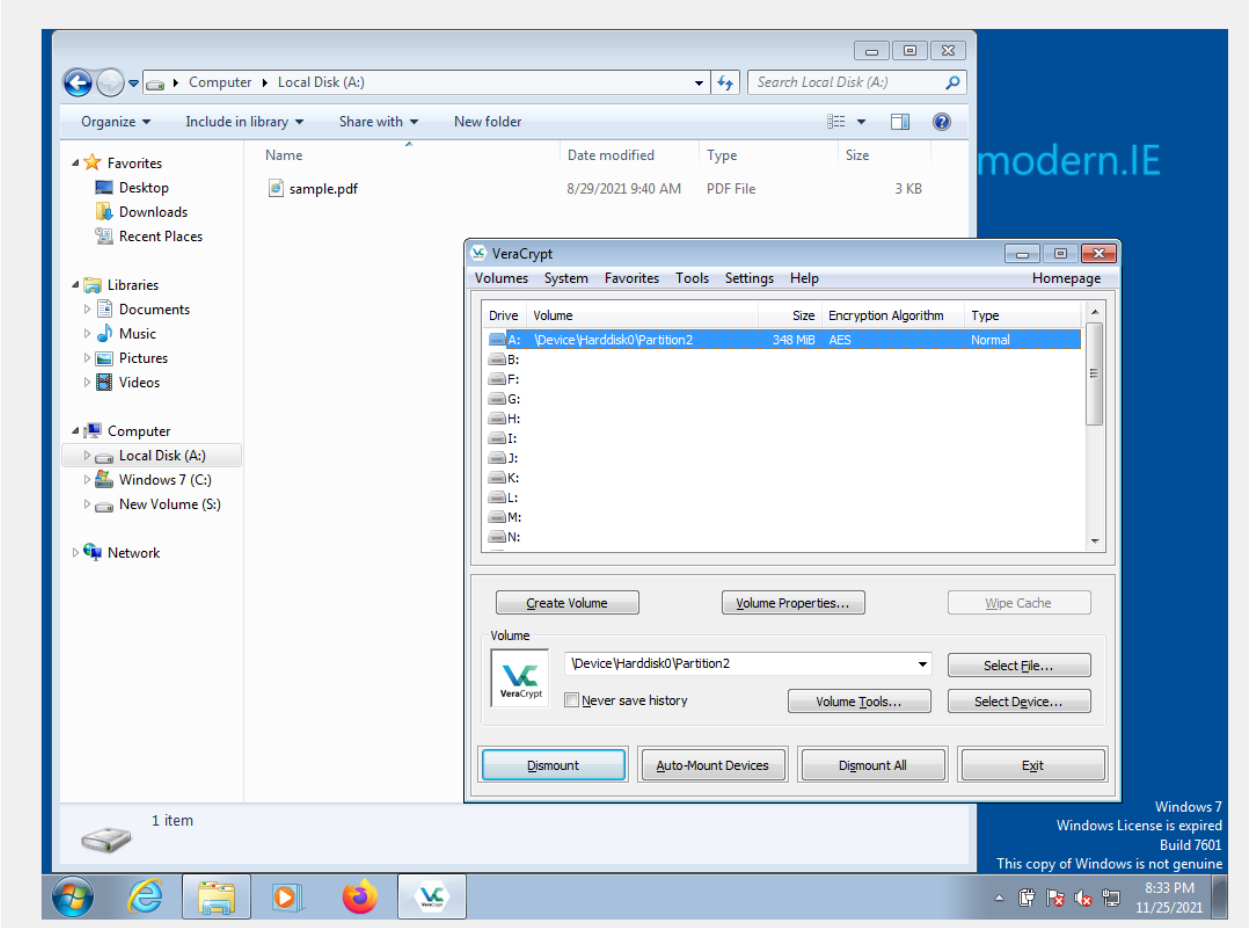
Protection methods:



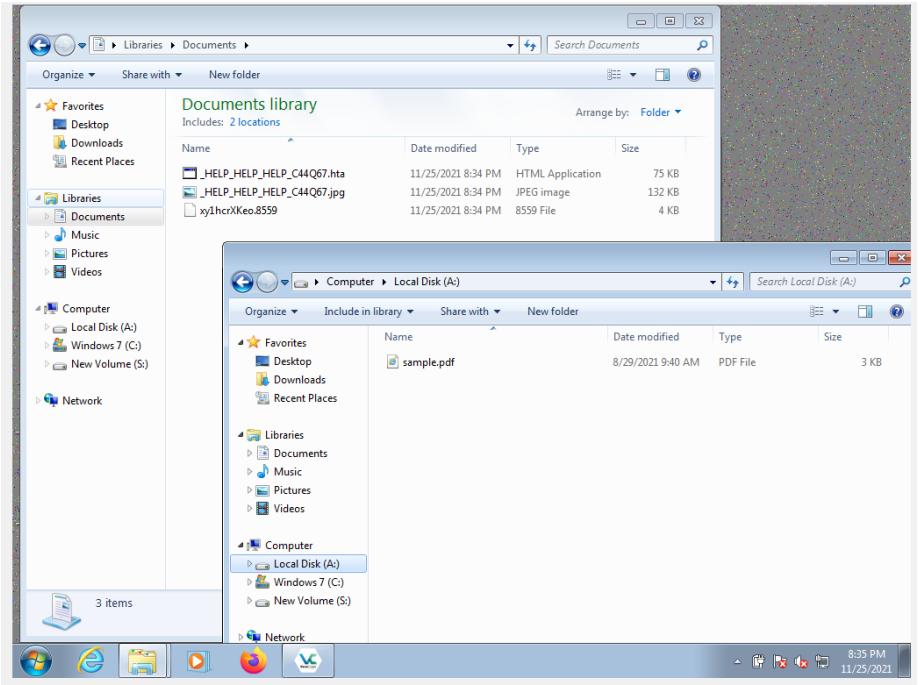
Bitlocker setup



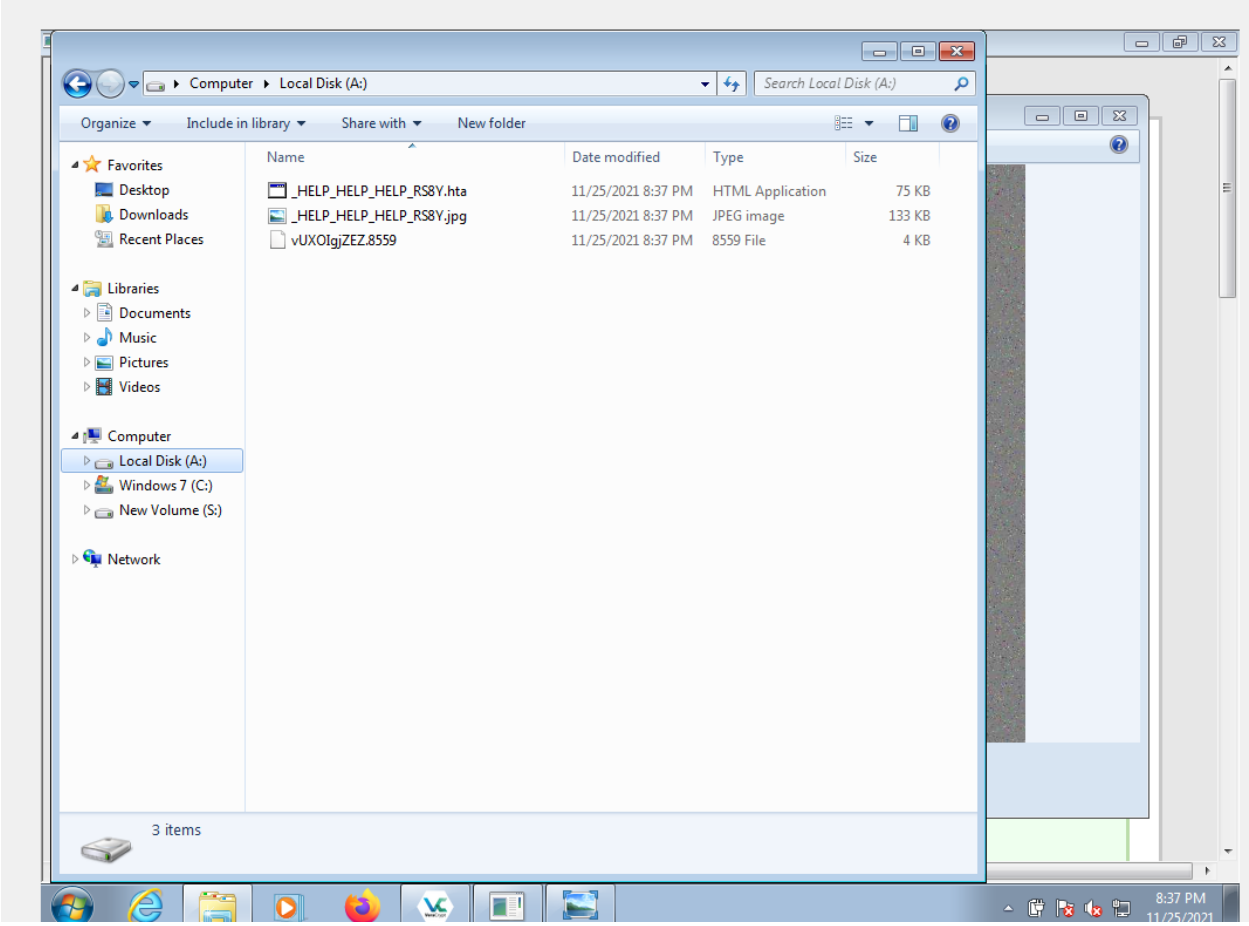
Bitlocker attempting to encrypt C drive



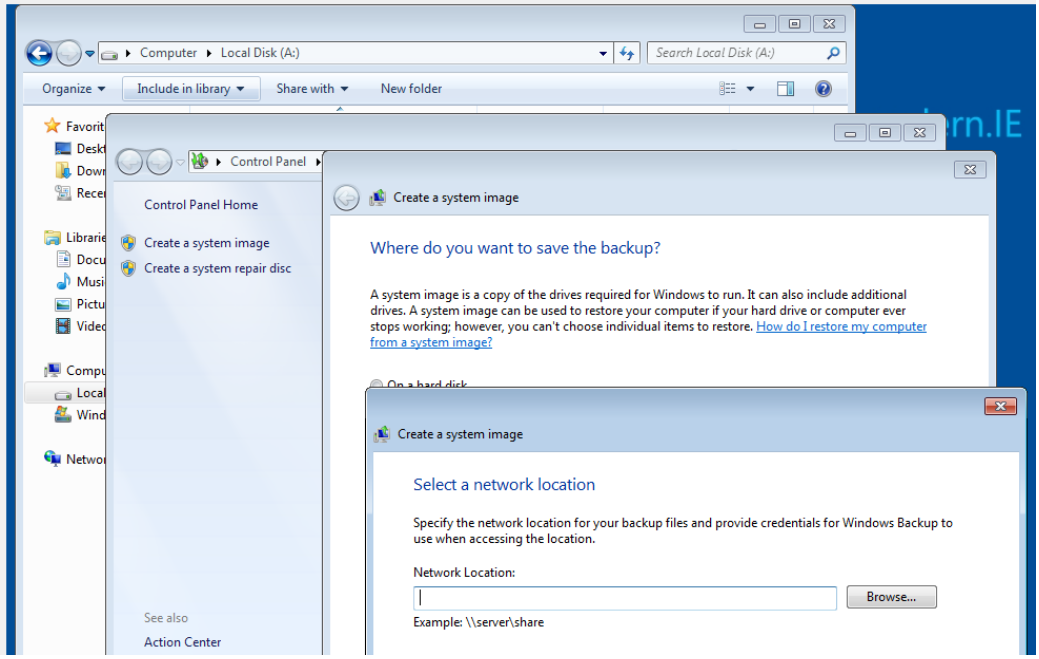
Selecting the drive to encrypt using veracrypt.



Running the ransomware executable while veracrypt is running in the background.



When the ransomware is executed and the drive isn't encrypted.



System image backup using windows.

Implementation and Results Description:

We used wireshark to analyze .pcap files of malware propagation. We know that Cerber ransomware infects windows machines using malspam emails sent out by the blank slate attack campaign. The Blank slate campaign is a spam campaign that gets its name from the uniquely empty body and messy subject that usually contains random numbers. The mail doesn't give away any information on the attachment. They also spoof the email addresses. Spoofing is making the email seem like it originated from a secure source. In the pcap file we can see where the download of the malware artifacts occurs from http://aloepolera.top/read.php? . The attachment is usually a zip that encloses another zip which contains a javascript file or a word document. The word document contains malicious macros and the javascript is an obfuscated malicious script. We were able to successfully test the malware by executing the files that are downloaded by the mail spam attack as provided.

To see the effect of the ransomware we created a sample.pdf file to test encryption. Upon execution of the malware artifact we first see that the desktop background changes to the cerber image. An html application file opens which details the method the affected victim can use. Files located in directories such as Photos and Documents are encrypted. Attempting to open sample.pdf finds that the file has been replaced with another file which cannot be opened and has been encrypted. The .hta will ask the user to redirect to a website through which the user can pay a predetermined amount of money using cryptocurrency to then have their files decrypted.

We used Procmon which is a system monitoring software for windows to capture system events occurring during the execution of the Cerber ransomware. Through this we were able to identify many of the actions taken by the malware. The malware execution took around 1.5 minutes. The malware initially edits various registry files to allow different actions. Some of these include files related to Windows Security and browser security which will now allow the malware to interact with a global server to connect for payments and will allow the malware to run unhindered on the target system. The ransomware will scan through various directories in a system such as Downloads, AppData, Searches, Videos, Pictures, Contacts, Favorites, Music, Documents, Links, Desktop and Recents which are likely to have important data for a user. By looking at the Procmon output and System event we can see that the sample.pdf demo file we created for testing was found in both documents and Recents folder. Once this was done the process executed various operations such as Open, read Write to modify contents of the pdf and encrypt its information and then renamed the file. Another process called mshta.exe was generated by the malware. This process also modified security related registry files and added cerber ransomware payment and decryption details next to any information which was encrypted. Thus we were able to see a more detailed view and analysis of the execution of the ransomware using procmon.

Performing Wireshark analysis during malware execution allowed us to understand the working of the ransomware in depth. The host system first connects to a remote server - evidenced by the “Client Hello” and “Server Hello” records. We can also see a client key exchange and an encrypted handshake confirming the connection. The point of interest in this exchanges is the HTTP request that the malware forces the machine to make, ocsp.digicert.com (do not open), which downloads an executable file onto the computer. This executable file is then responsible for the encryption of files by the ransomware.

Usage of an antivirus was able to prevent the malware. Avast antivirus detected the malware files and would quarantine and delete them automatically. Attempting to unzip the compressed file would result in the malware artifacts not being loaded. In the event of the virus executing successfully, it is near impossible to recover the information through decryption. However, the data can be recovered if a system backup was taken prior. Windows allows for the system to be backed up as an image file, which can then later be used to restore the state of the machine before the malware attack.

Veracrypt was used to successfully protect our important files. Veracrypt is a file and drive encryption tool. We created a hidden volume partition on our drive that can only be accessed through veracrypt after providing a password. On virus execution with drive hidden CERBER was unable to access our files. In comparison, running the malware while the drive is not hidden results in files being encrypted. Thereby proper usage of veracrypt tools drive encryption enabled us to protect our files from a ransomware attack.

Conclusion:

The experiment helped us understand how ransomware functions and helped us understand how to better protect our system from such threats and helped us realise the importance of taking regular backups of data. We analyzed the initial propagation of CERBER and its working. We performed a deeper analysis of the malware execution using Procmon and Wireshark. Using Antivirus and Drive encryption methods we incorporated prevention methods and successfully protected our files and performed damage mitigation through use of backups.

References:

1. Imaji, Asibi. (2019). Ransomware Attacks: Critical Analysis, Threats, and Prevention methods.
2. A K Maurya et al (2018) Ransomware Evolution, Target and Safety Measures
3. Segun I Popoola (2017) Ransomware: Current Trend, Challenges, and Research Directions
4. Detection and Analysis Cerber Ransomware Based on Network Forensics Behavior (2018), Ade Kurniawan and Imam Riadi