**[INDUSTRY RESEARCH](https://securityscorecard.com/research?category=industry-research)**

# Avoslocker Ransomware Forensics

**Executive Summary of Avoslocker Ransomware**

AvosLocker is a variant of Ransomware that is operated as a ransomware-as-a-service (RaaS) model. It was initially observed in the middle of 2021, evolved over time and continued to operation into 2022.

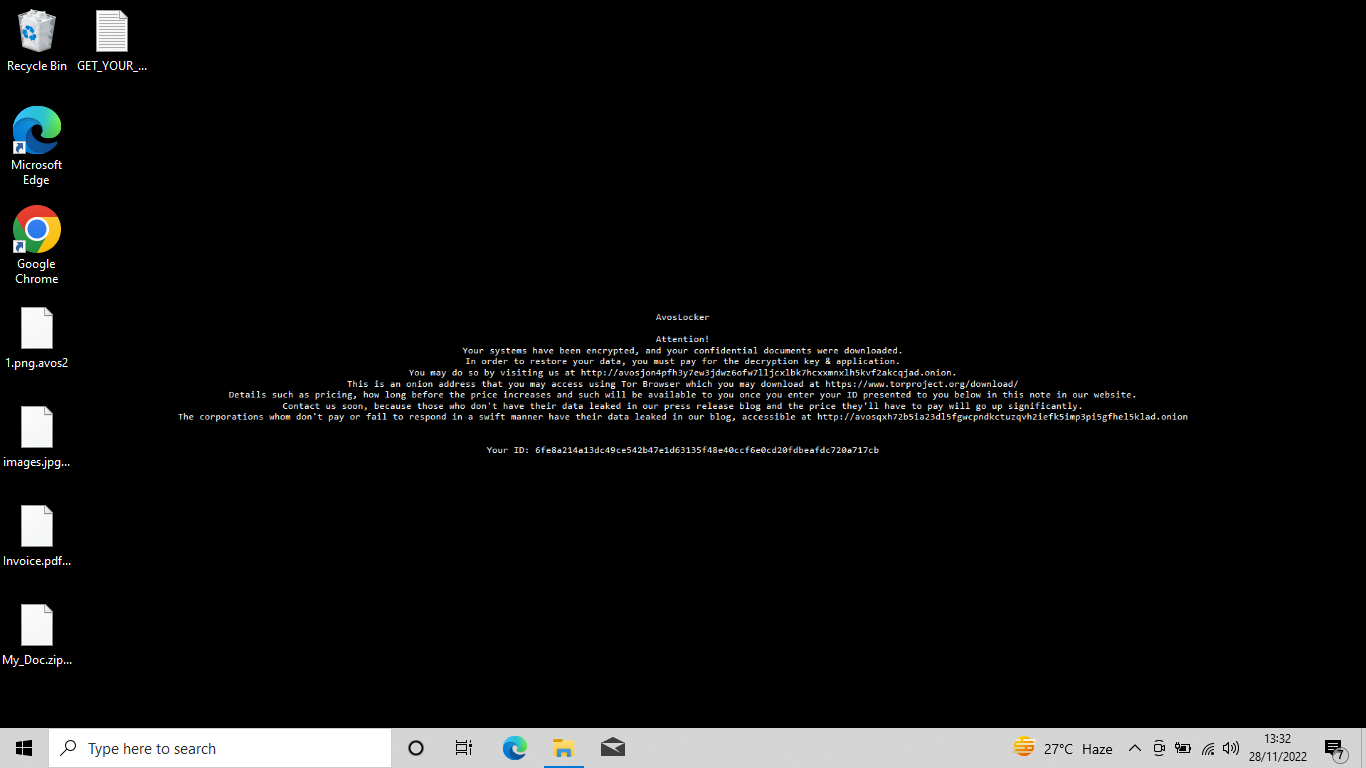
Avoslocker is written in C++. Its initially targeted Windows Operating Systems, however updated variants are also capable of targeting Linux system as well as ESXi virtual machines. The files are encrypted using combination of AES-256 and RSA-2048 algorithms. Encrypted files are appended with the “.avos” extension or “.avos2” extension for an updated variant, similarly in linux machine it appends with “.avoslinux” extension. A ransom note "GET\_YOUR\_FILES\_BACK.txt" is created in each encrypted directory after the file has been successfully encrypted , in linux environment the ransom note is named as “README\_FOR\_RESTORE”.

**Modus Operand**

Avoslocker ransomware’s attack vector could be spam emails consisting malicious attachment, trojans, backdoors, software download from untrusted source, malvertising, it can also Powershell to exploit the vulnerabilities of Microsoft exchange server to penetrate into the environment CVE-2021-31207, CVE-2021-31206, CVE-2021-34523, and CVE-2021-34473, and CVE-2021-26855. Avolocker uses tools such as PowerShell , windows command shell for execution & remote administration tool such as Anydesk to operate the compromise system.

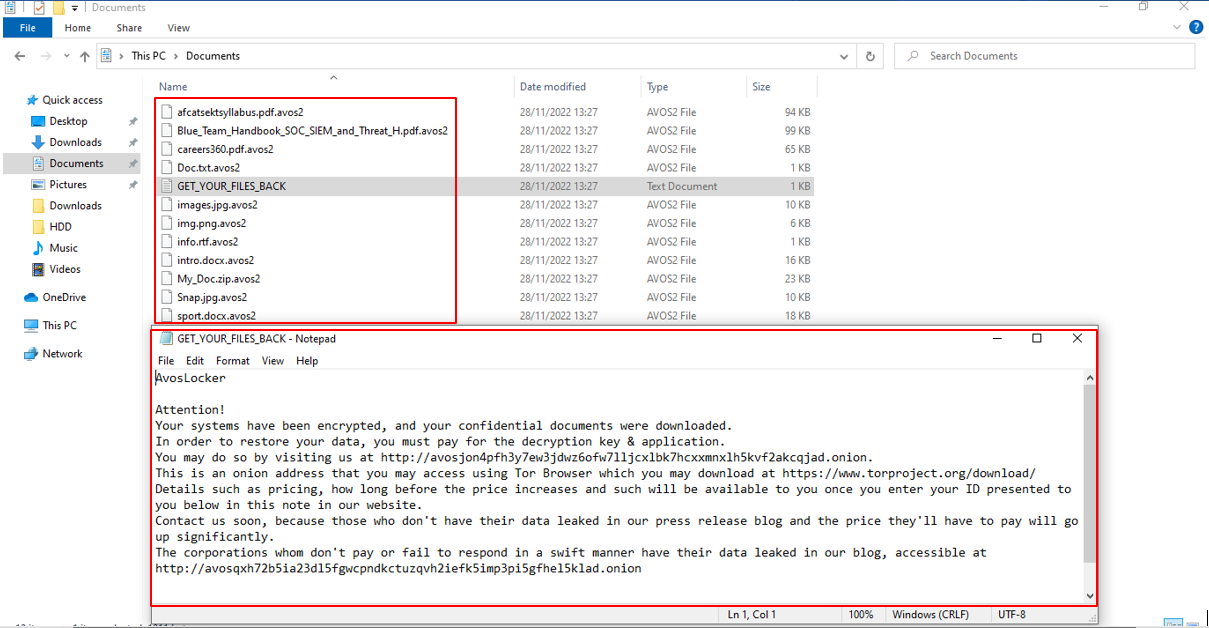
**Avoslocker Ransomware Analysis**

Files are encrypted with "**.avos2**" extension & desktop background gets replaced with a ransom note.



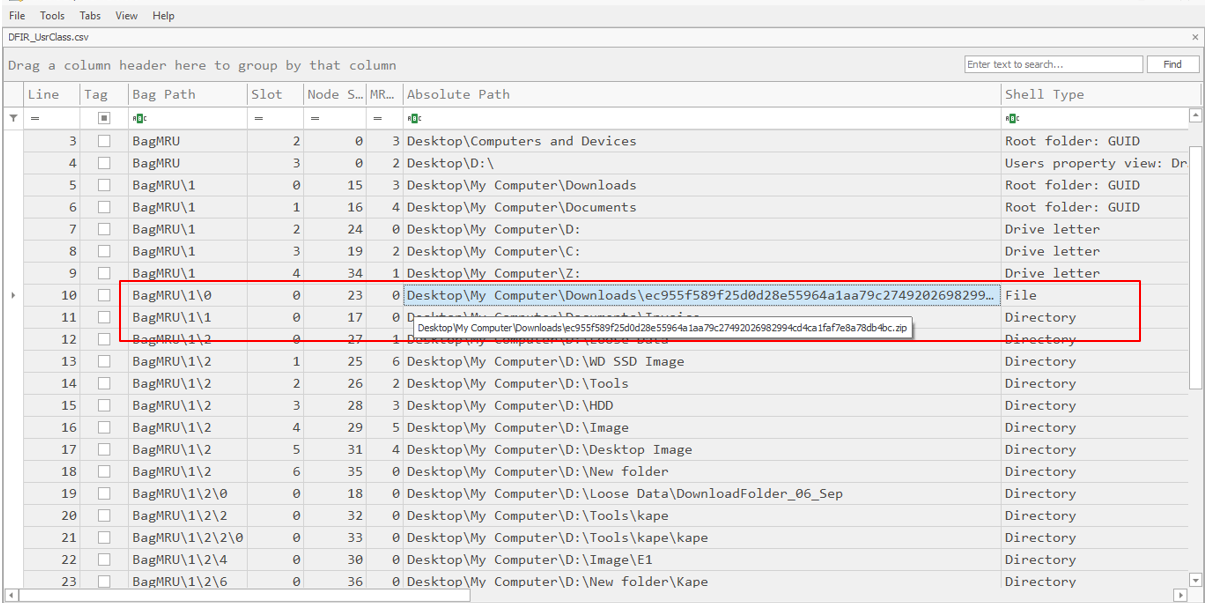
**Figure 1**

Ransome note "**GET\_YOUR\_FILES\_BACK.txt**" created in each infected folder.



**Figure 2**

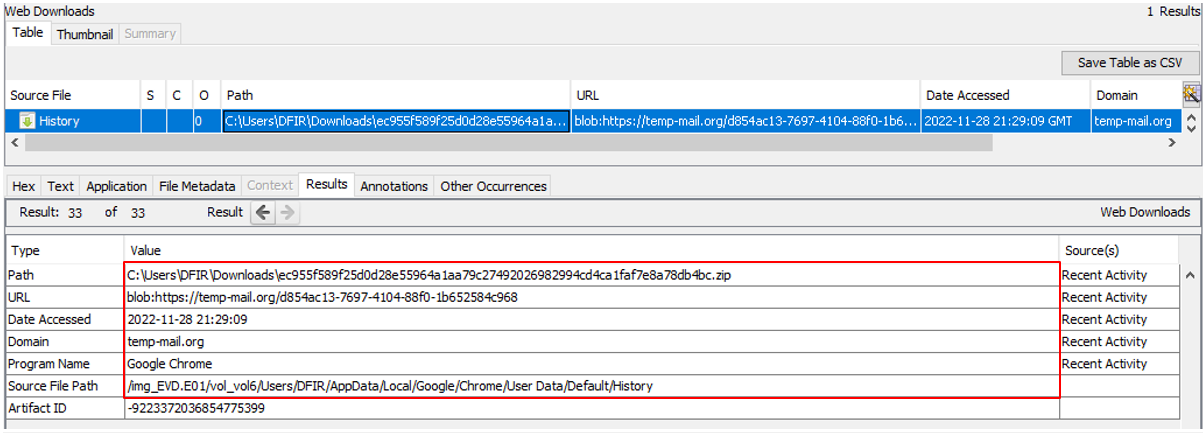
Noted instances of suspicious file “ec955f589f25d0d28e55964a1aa79c27492026982994cd4ca1faf7e8a78db4bc.zip” in the Download folder of DFIR User. (Artifact Source: Userclass.dat)

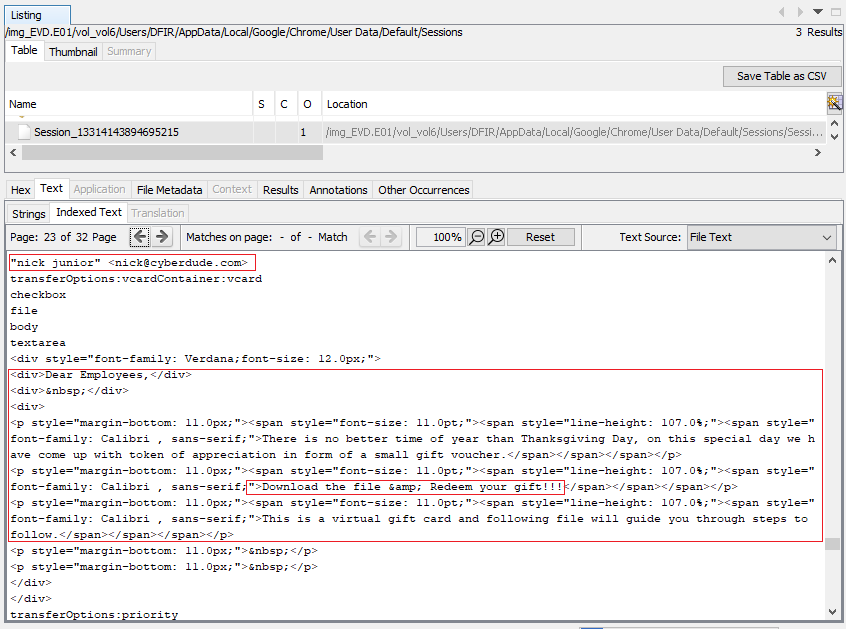


**Figure 3**

In our analysis we observed ransomware payload “C:\Users\DFIR\Downloads\ec955f589f25d0d28e55964a1aa79c27492026982994cd4ca1faf7e8a78db4bc.zip” is delivered using a phishing email at 28 November 2022 at 21:29:09 UTC.

Source: Web Artifacts





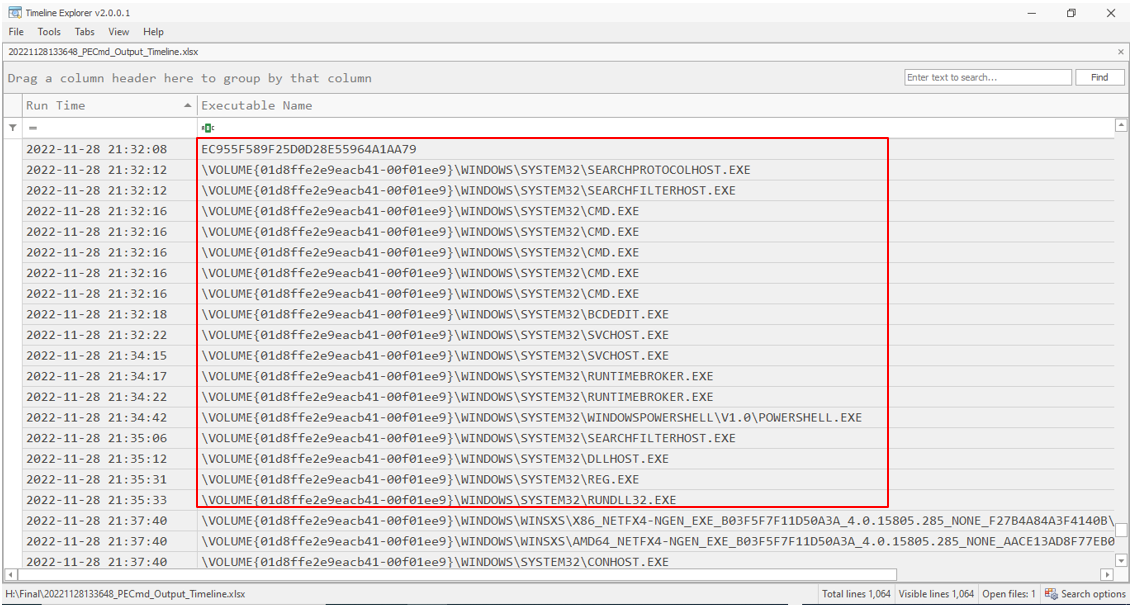
**Figure 4**

Defender



Execution of "ec955f589f25d0d28e55964a1aa79" at "28 November 2022 21:32:08 UTC" has been noted. Thereafter we noticed instances of cmd.exe, bcdedit.exe, and svchost.exe being executed. Further, at “"28 November 2022 21:34:42 UTC” noted instances of PowerShell being run.

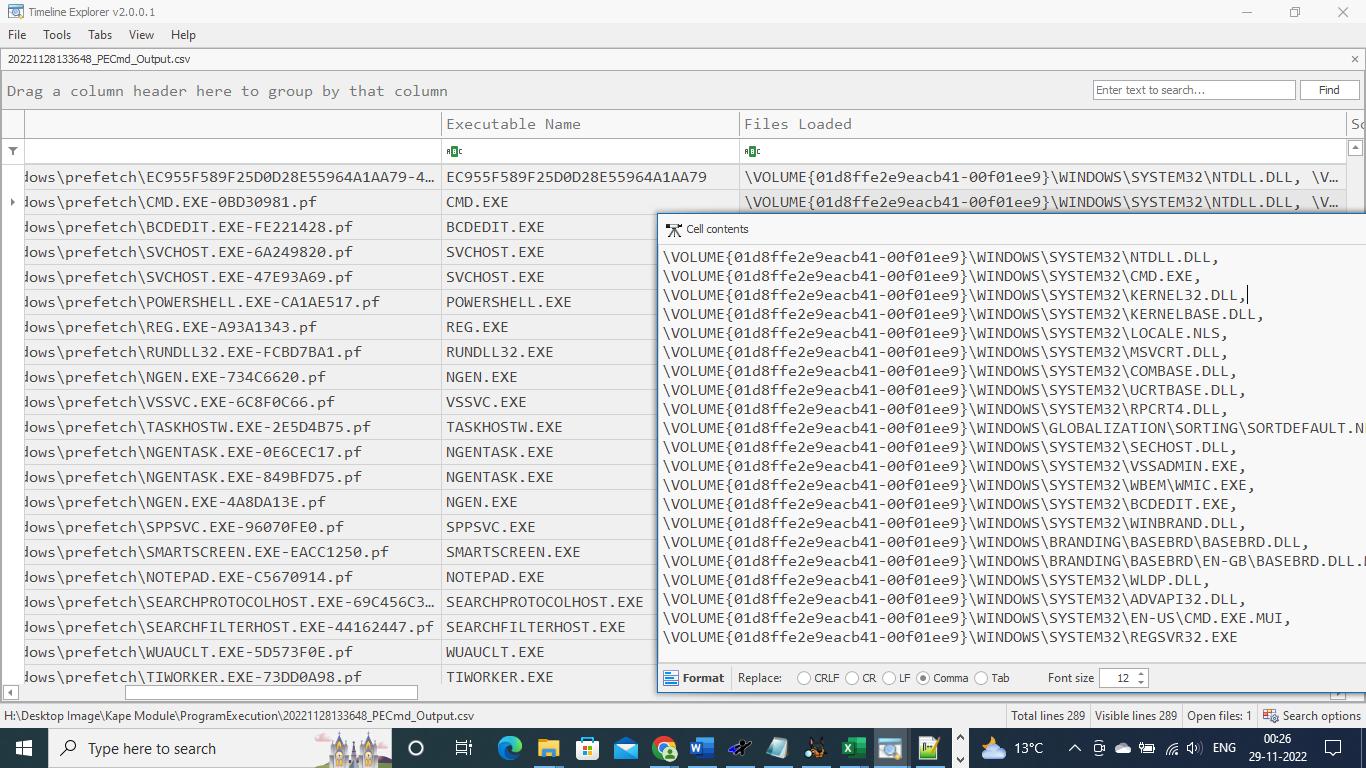
(Artifact source – Prefetch)



Followings are the file loaded by cmd.exe, run just after the execution of "ec955f589f25d0d28e55964a1aa79”. VSSADMINE.exe & WMIC.exe to deletes all Volume Shadow Copies.

BCEDIT.exe to disable Windows recovery feature

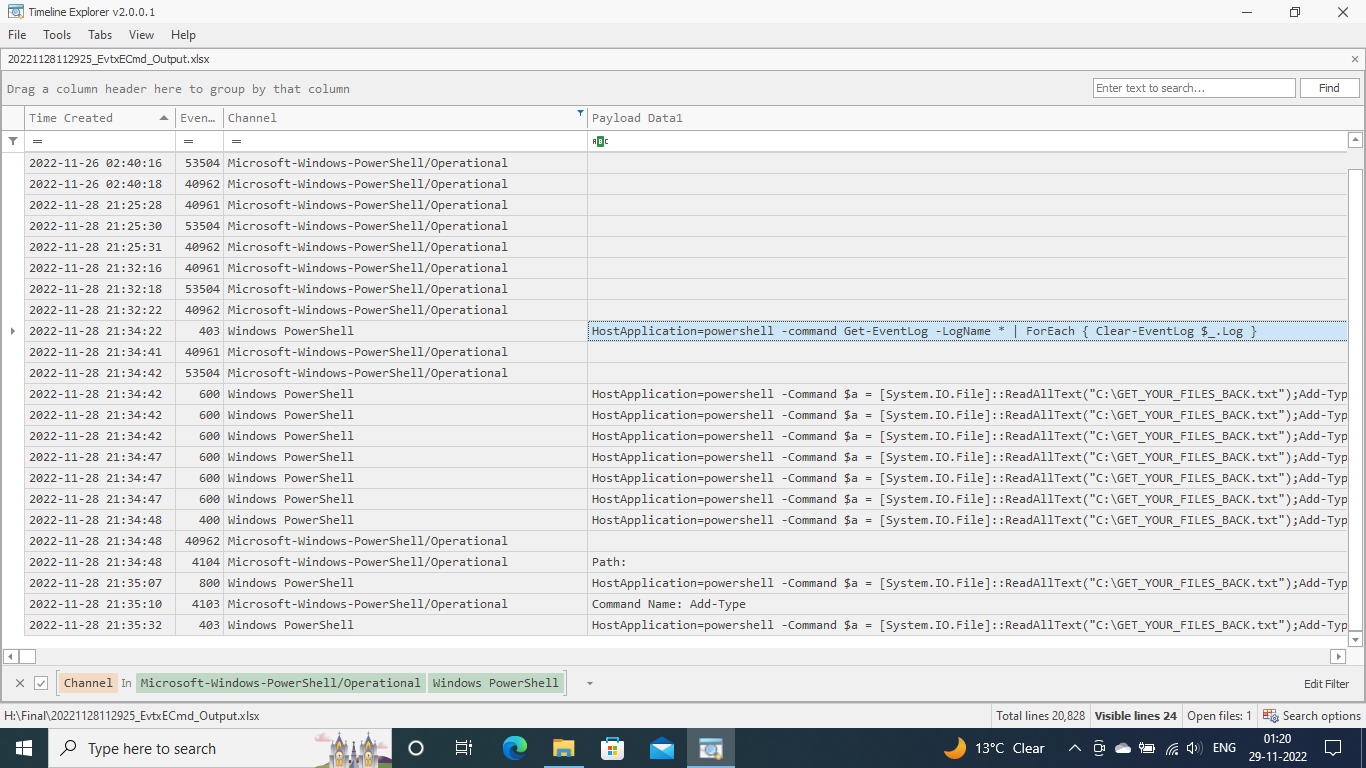
reg.exe to add a image on Desktop Wallpaper.



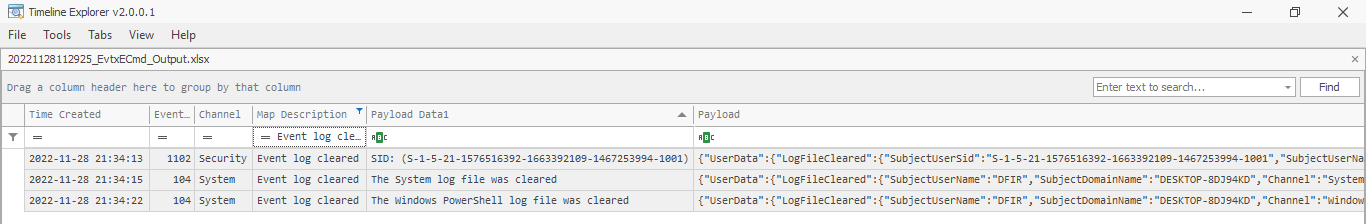
Powershell

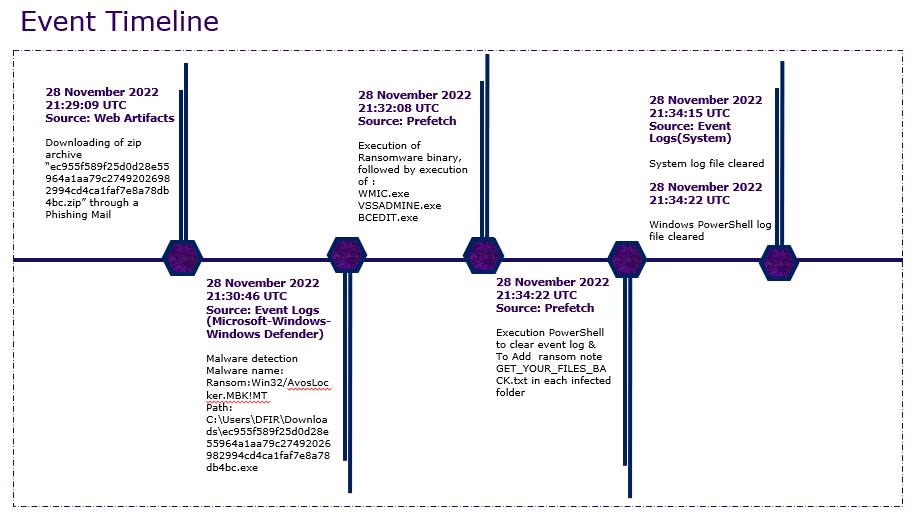
HostApplication=powershell -command Get-EventLog -LogName \* | ForEach { Clear-EventLog $\_.Log }

Host Application = powershell -Command $a = [System.IO.File]::ReadAllText("C:\GET\_YOUR\_FILES\_BACK.txt");Add-Type -AssemblyName System.Drawing;$filename = "$env:temp\$(Get-Random).png";$bmp = new-object System.Drawing.Bitmap 1920,1080;$font = new-object System.Drawing.Font Consolas,10;$brushBg = [System.Drawing.Brushes]::Black;$brushFg = [System.Drawing.Brushes]::White;$format = [System.Drawing.StringFormat]::GenericDefault;$format.Alignment = [System.Drawing.StringAlignment]::Center;$format.LineAlignment = [System.Drawing.StringAlignment]::Center;$graphics = [System.Drawing.Graphics]::FromImage($bmp);$graphics.FillRectangle($brushBg,0,0,$bmp.Width,$bmp.Height);$graphics.DrawString($a,$font,$brushFg,[System.Drawing.RectangleF]::FromLTRB(0, 0, 1920, 1080),$format);$graphics.Dispose();$bmp.Save($filename);reg add "HKEY\_CURRENT\_USER\Control Panel\Desktop" /v Wallpaper /t REG\_SZ /d $filename /f;Start-Sleep 1;rundll32.exe user32.dll, UpdatePerUserSystemParameters, 0, $false;



Event log cleared

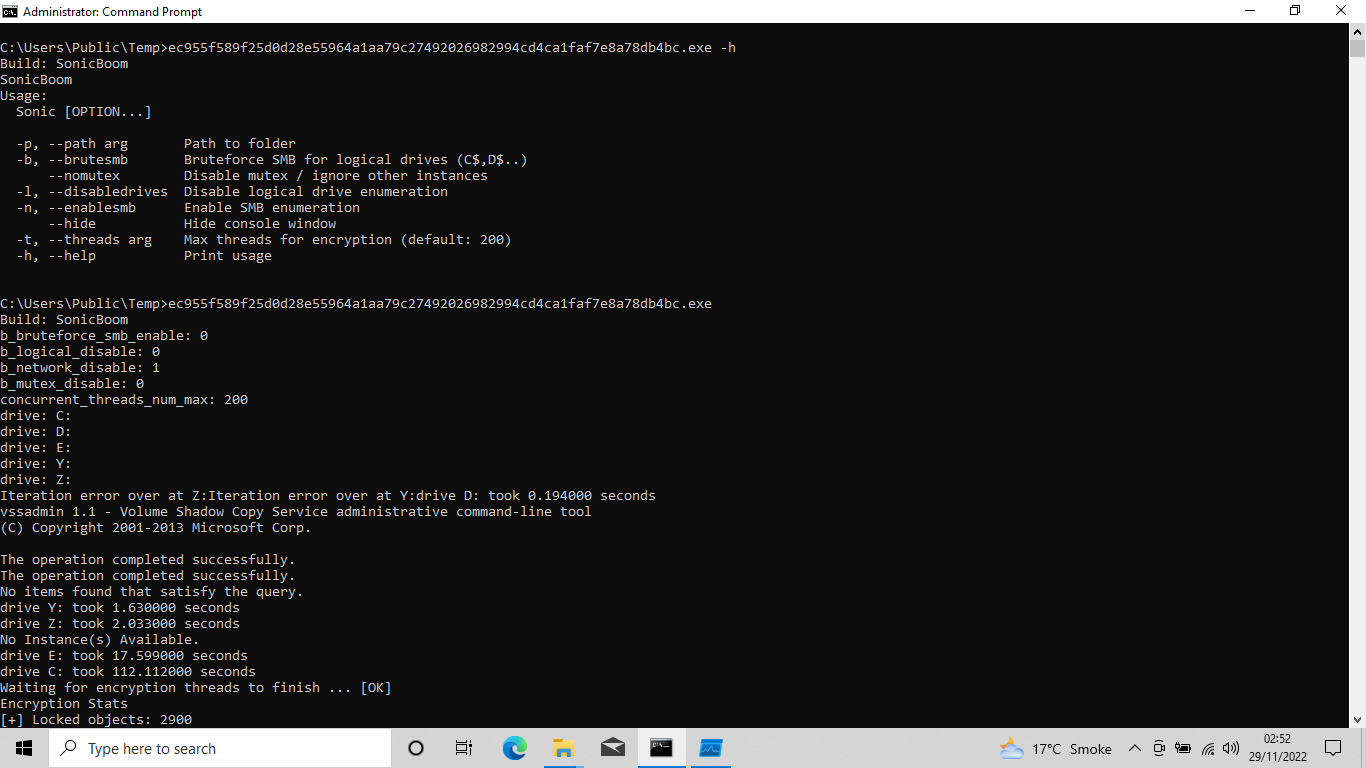




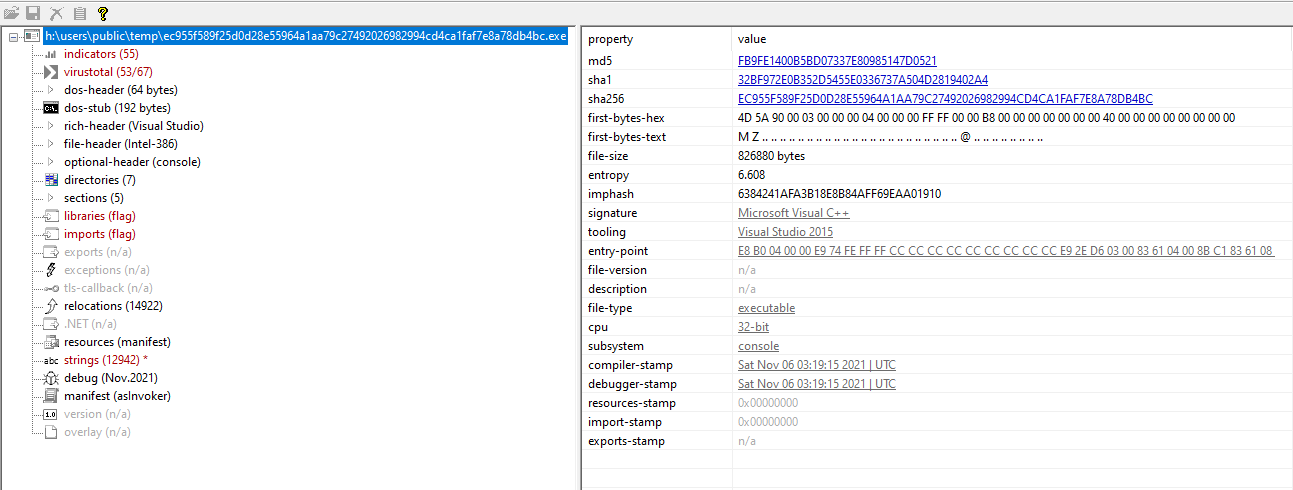
**Basic Malware Analysis of Avoslocker**

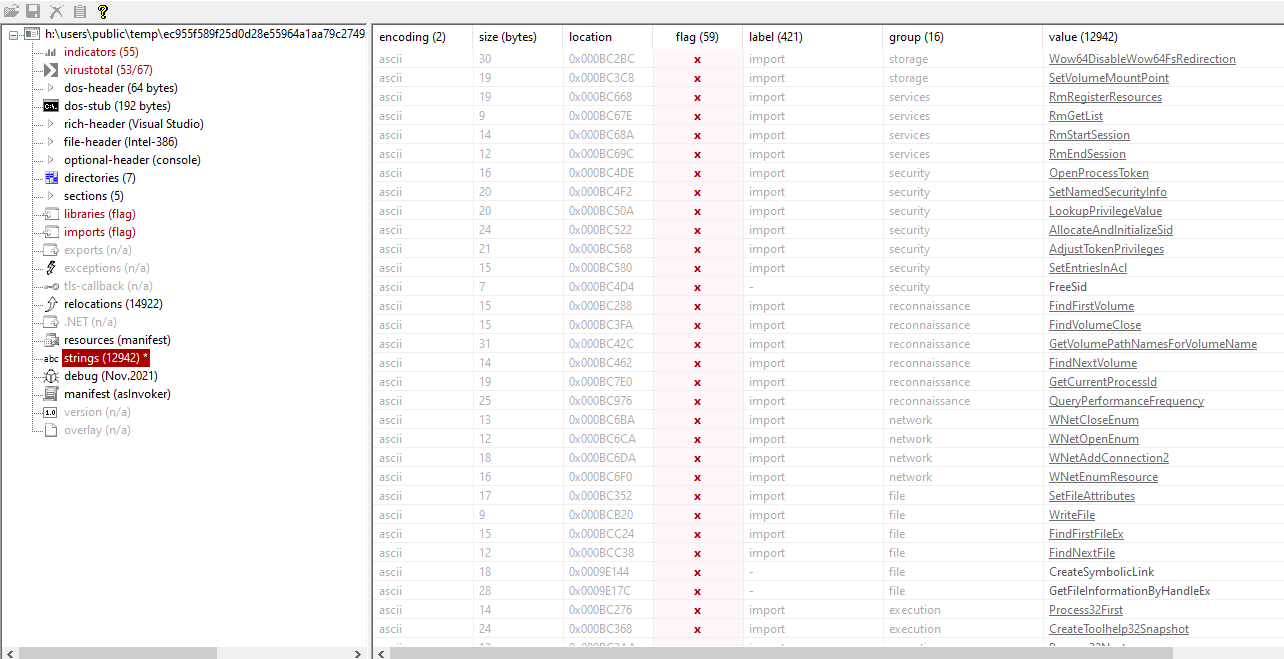
Extracted the malicious file present in Download folder to perform malware analysis.

Following figure represent options available for the command line execution.

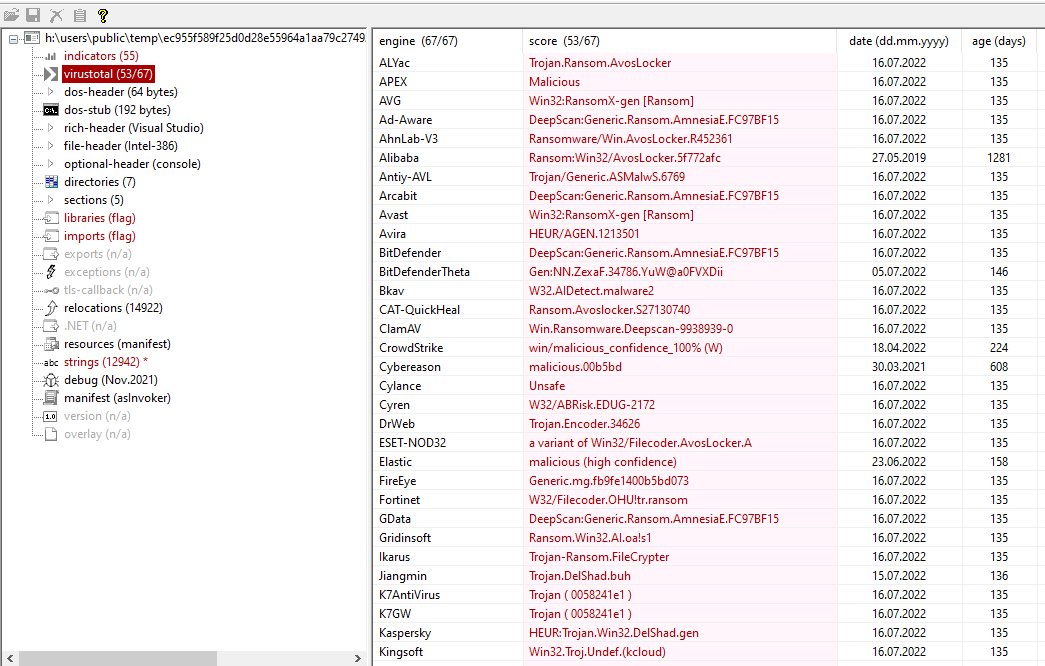


Binary Details





Fig



Following are the process tree generated after extecution of ec955f589f25d0d28e55964a1aa79c27492026982994cd4ca1faf7e8a78db4bc.exe

