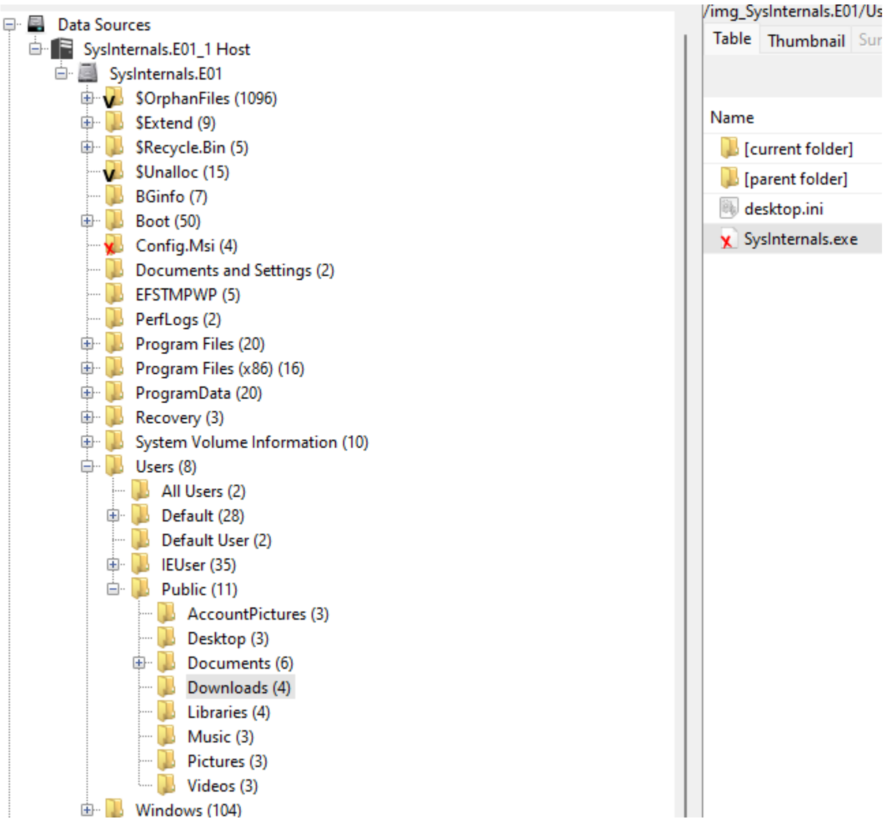
CyberDefenders: Sysinternals Lab

The following writeup is for Sysinternals Lab on CyberDefenders, it involves analysing a disk image (Encase Image File Format) using a series of tools, most notable Autopsy, AppCompatParser, AmCacheParser, and VirusTotal. I am extremely new to this sort of forensic work so I advise reading other people's writeups of this challenge rather than my own.

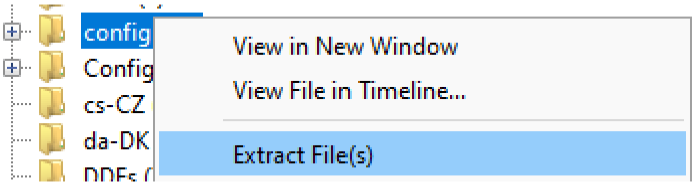
What was the malicious executable file name that the user downloaded?

To start my investigation, I launched Autopsy and added the data source. I kept everything as default, so due to the large number of ingest modules, it took a while to analyse. If we navigate to the Downloads folder for the Public user, we can see one executable:

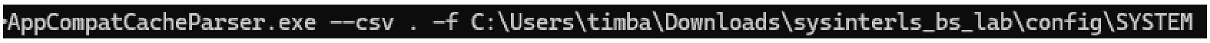


When was the last time the malicious executable file was modified? 12-hour format

To find when this executable was last modified, we can use the AppCompatCacheParser, which parses the AppCompatCache. This maintains a record of the application compatibility settings that have been applied to an executable. The AppCompatCache is located in SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache. The files that make up the Windows Registry can be found in Windows\System32\config, so let's export this directory:

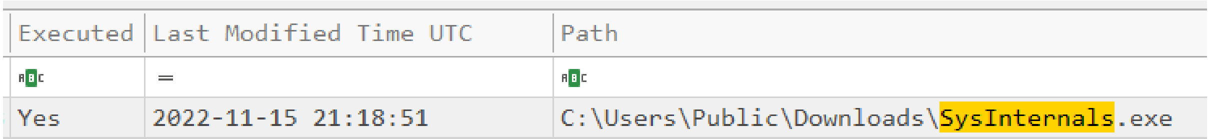


We can now parse the AppCompatCache using AppCompatCache Parser:



```
AppCompatCacheParser.exe --csv . -f C:\Users\timba\Downloads\sysinterls_bs_lab\config\SYSTEM
```

Where --csv . indicates that I want the output to be saved in the current directory and -f is the file path to the SYSTEM hive. We can now import this csv into Excel or something like Timeline Explorer to find the last modification time:

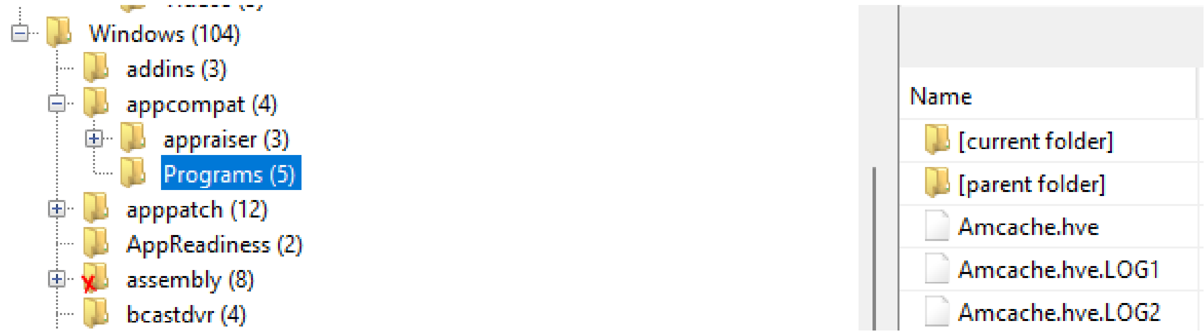


Executed	Last Modified Time UTC	Path
Yes	2022-11-15 21:18:51	C:\Users\Public\Downloads\SysInternals.exe

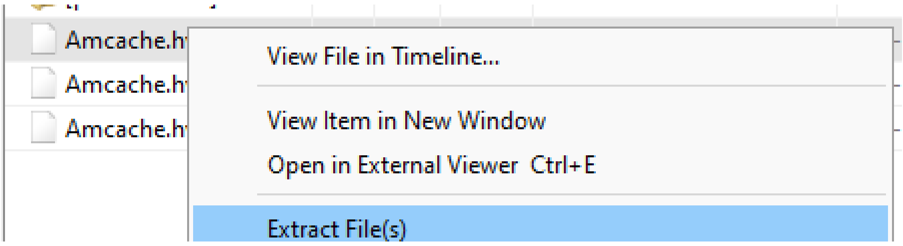
For some stupid reason you have to do a specific format for the answer: 11/15/2022 09:18:51 PM.

What is the SHA1 hash value of the malware?

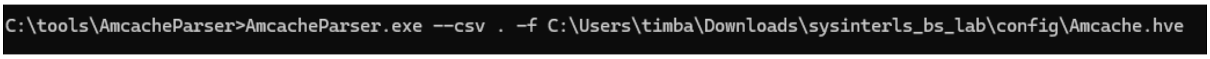
To find the SHA1 hash value of the binary and maintain non-repudiation, we can utilise the Amcache, which is a Window artifact that provides a repository of metadata about the execution of programs and other files. It is located in Windows\AppCompat\Programs\Amcache.hve:



Let’s extract the Amcache.hve file:

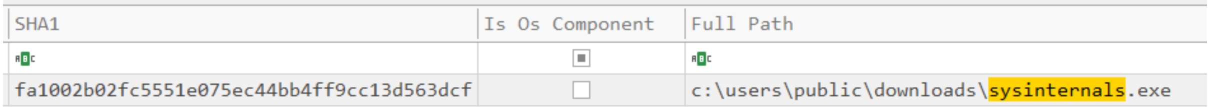


We can now utilise another Eric Zimmerman tool called AmCacheParser to parse the Amcache file:



```
C:\tools\AmcacheParser>AmcacheParser.exe --csv . -f C:\Users\timba\Downloads\sysinterls_bs_lab\config\Amcache.hve
```

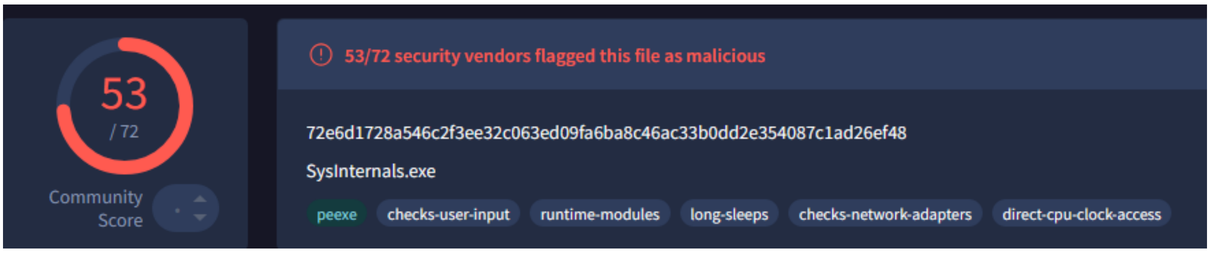
If you take a look at the UnassociatedFileEntries.csv file and filter for the binary, we can find its SHA1 hash:



SHA1	Is Os Component	Full Path
fa1002b02fc5551e075ec44bb4ff9cc13d563dcf	□	c:\users\public\downloads\sysinternals.exe

What is the malware's family?

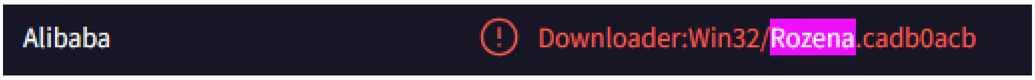
This is where tools such as VirusTotal come into play, as all we need to do is enter the SHA1 hash and boom we can see that its associated with Rozena:



53/72 security vendors flagged this file as malicious

72e6d1728a546c2f3ee32c063ed09fa6ba8c46ac33b0dd2e354087c1ad26ef48

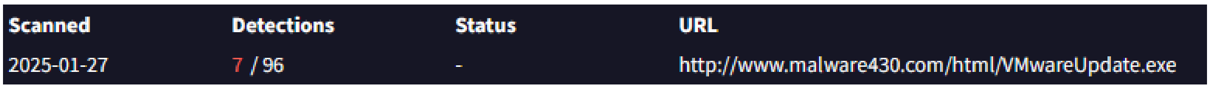
SysInternals.exe



Alibaba ⓘ Downloader:Win32/Rozena.cadb0acb

What is the first mapped domain's Fully Qualified Domain Name (FQDN)?

You can find contact URLs in the Relations tab on VirusTotal:

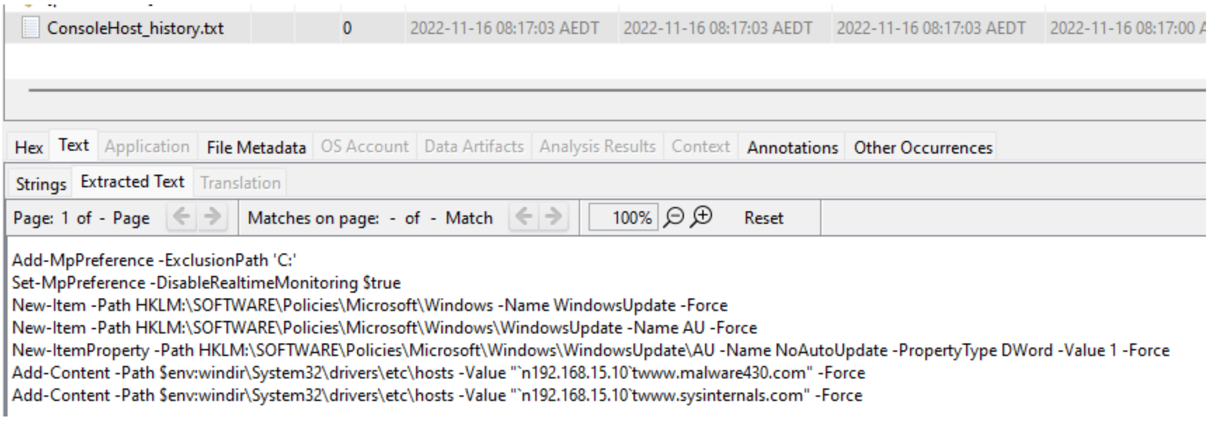


Scanned	Detections	Status	URL
2025-01-27	7 / 96	-	http://www.malware430.com/html/VMwareUpdate.exe

The first mapped domain in this instance is www.malware430.com.

The mapped domain is linked to an IP address. What is that IP address?

An alternative method to answering the previous question and finding the IP address linked to the domain we just found is to inspect the ConsoleHost_history.txt file found in /Users/[username]/AppData/Roaming/Microsoft/Windows/PowerShell/PSReadLine:



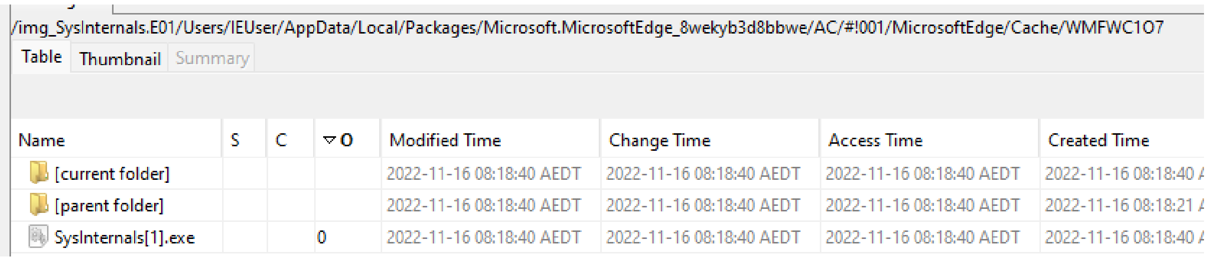
ConsoleHost_history.txt	0	2022-11-16 08:17:03 AEDT	2022-11-16 08:17:03 AEDT	2022-11-16 08:17:03 AEDT

```
Add-MpPreference -ExclusionPath 'C:'
Set-MpPreference -DisableRealtimeMonitoring $true
New-Item -Path HKLM:\SOFTWARE\Policies\Microsoft\Windows -Name WindowsUpdate -Force
New-Item -Path HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate -Name AU -Force
New-ItemProperty -Path HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU -Name NoAutoUpdate -PropertyType DWord -Value 1 -Force
Add-Content -Path $env:windir\System32\drivers\etc\hosts -Value "`n192.168.15.10`twww.malware430.com" -Force
Add-Content -Path $env:windir\System32\drivers\etc\hosts -Value "`n192.168.15.10`twww.sysinternals.com" -Force
```

We can see that the IP address associated with malware430[.]com is 192.168.15.10.

What is the name of the executable dropped by the first-stage executable?

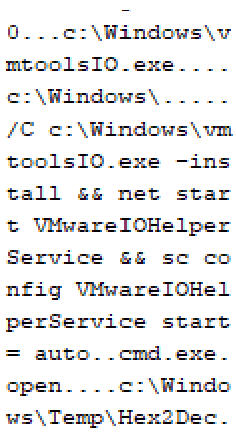
I tried to just export the sysinternals.exe binary found in the downloads directory, but it seems like the file is corrupted in some way. Alternatively, we can see if the file has been cached by the browser, and fortunately enough it has been:



/img_SysInternals.E01/Users/IEUser/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/AC/#!001/MicrosoftEdge/Cache/WMFWC1O7

Name	S	C	▽ O	Modified Time	Change Time	Access Time	Created Time
[current folder]				2022-11-16 08:18:40 AEDT	2022-11-16 08:18:40 AEDT	2022-11-16 08:18:40 AEDT	2022-11-16 08:18:40 A
[parent folder]				2022-11-16 08:18:40 AEDT	2022-11-16 08:18:40 AEDT	2022-11-16 08:18:40 AEDT	2022-11-16 08:18:21 A
SysInternals[1].exe			0	2022-11-16 08:18:40 AEDT	2022-11-16 08:18:40 AEDT	2022-11-16 08:18:40 AEDT	2022-11-16 08:18:40 A

Looking at the hex view, we can see a reference to C:\Windows\vmtoolsIO.exe:



```
0...c:\Windows\v
mtoolsIO.exe....
c:\Windows\.....
/C c:\Windows\vm
toolsIO.exe -ins
tall && net star
t VMwareIOHelper
Service && sc co
nfig VMwareIOHel
perService start
= auto..cmd.exe.
open....c:\Windo
ws\Temp\Hex2Dec.
```

Along with a series of other suspicious commands. Due to not being in a sandboxed environment, I am avoiding downloading this binary locally.

What is the name of the service installed by the 2nd stage executable?

As per the image seen in the previous question, we can see that a command is being issued to start the VMwareIOHelperService.

What is the extension of files deleted by the 2nd stage executable?

pf