Sysinternals Challenge

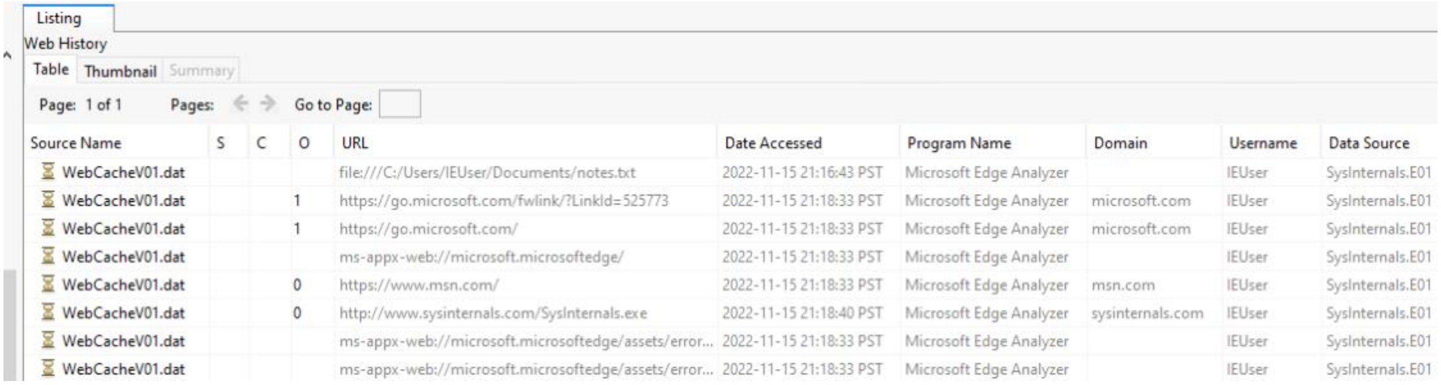
Scenario:

A user thought they were downloading the SysInternals tool suite and attempted to open it, but the tools did not launch and became inaccessible. Since then, the user has observed that their system has gradually slowed down and become less responsive.

As a soc analyst, analyze the artifacts and answer the questions.

Task 1:
What was the malicious executable file name that the user downloaded?

I opened the image file with Autopsy and checked the Data Artfiacts - Web Hisotry



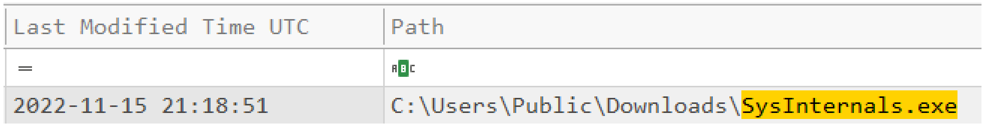
Source Name	S	C	O	URL	Date Accessed	Program Name	Domain	Username	Data Source
WebCacheV01.dat				file:///C:/Users/IEUser/Documents/notes.txt	2022-11-15 21:16:43 PST	Microsoft Edge Analyzer		IEUser	SysInternals.E01
WebCacheV01.dat			1	https://go.microsoft.com/fwlink/?LinkId=525773	2022-11-15 21:18:33 PST	Microsoft Edge Analyzer	microsoft.com	IEUser	SysInternals.E01
WebCacheV01.dat			1	https://go.microsoft.com/	2022-11-15 21:18:33 PST	Microsoft Edge Analyzer	microsoft.com	IEUser	SysInternals.E01
WebCacheV01.dat				ms-appx-web://microsoft.microsoftedge/	2022-11-15 21:18:33 PST	Microsoft Edge Analyzer		IEUser	SysInternals.E01
WebCacheV01.dat			0	https://www.msn.com/	2022-11-15 21:18:33 PST	Microsoft Edge Analyzer	msn.com	IEUser	SysInternals.E01
WebCacheV01.dat			0	http://www.sysinternals.com/SysInternals.exe	2022-11-15 21:18:40 PST	Microsoft Edge Analyzer	sysinternals.com	IEUser	SysInternals.E01
WebCacheV01.dat				ms-appx-web://microsoft.microsoftedge/assets/error...	2022-11-15 21:18:33 PST	Microsoft Edge Analyzer		IEUser	SysInternals.E01
WebCacheV01.dat				ms-appx-web://microsoft.microsoftedge/assets/error...	2022-11-15 21:18:33 PST	Microsoft Edge Analyzer		IEUser	SysInternals.E01

Answer: sysinternals.exe

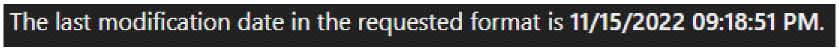
Task 2:
When was the last time the malicious executable file was modified? 12-hour format

I used the hint for this task

I used the AppCompatCacheParser on the SYSTEM Hive and searched for the sysinternals.exe
And told ChatGPT to make it for the answer format



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

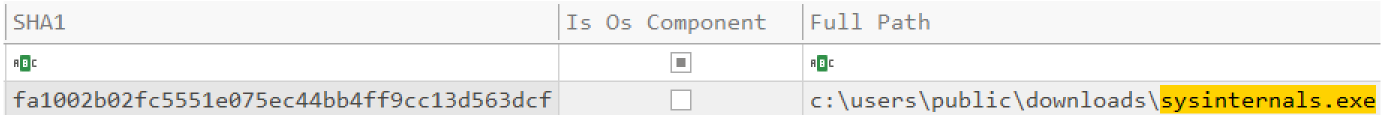


The last modification date in the requested format is **11/15/2022 09:18:51 PM.**

Answer: 11/15/2022 09:18:51 PM

Task 3:
What is the SHA1 hash value of the malware?

I checked the Amcache hive and searched for sysinternals.exe

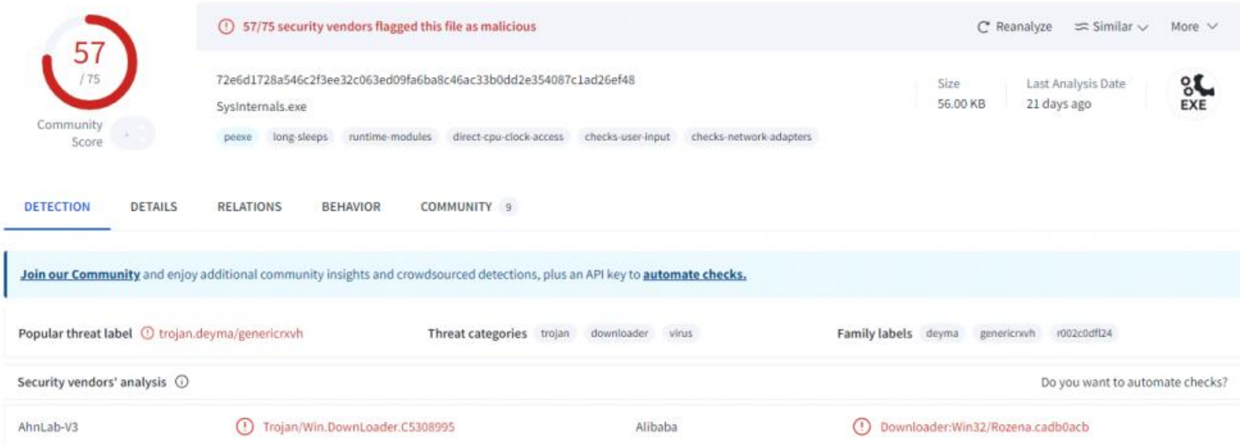


SHA1	Is Os Component	Full Path
ABC	■	ABC
fa1002b02fc5551e075ec44bb4ff9cc13d563dcf	□	c:\users\public\downloads\sysinternals.exe

Answer: fa1002b02fc5551e075ec44bb4ff9cc13d563dcf

Task 4:
What is the malware's family?

I checked the SHA1 in Virus Total and found the name by the Vendors detections



57 / 75 Community Score

57/75 security vendors flagged this file as malicious

72e6d1728a546c2f3ee32c063ed09fa6ba8c46ac33b0dd2e354087c1ad26ef48
SysInternals.exe

peexe long-sleeps runtime-modules direct-cpu-clock-access checks-user-input checks-network-adapters

Size 56.00 KB
Last Analysis Date 21 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.deyma/genericrxvh
Threat categories trojan downloader virus
Family labels deyma genericrxvh r002c0dfl24

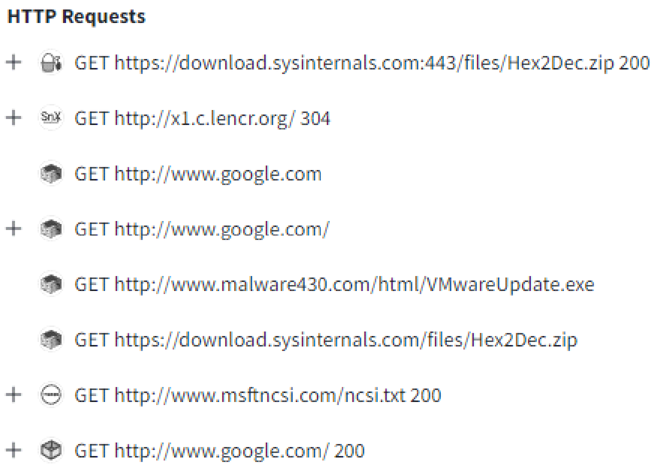
Security vendors' analysis
Do you want to automate checks?

AhnLab-V3	Trojan/Win.DownLoader.C5308995	Alibaba	Downloader:Win32/Rozena.cadb0acb

Answer: rozena

Task 5:
What is the first mapped domain's Fully Qualified Domain Name (FQDN)?

I checked the Behavior tab in Virus Total



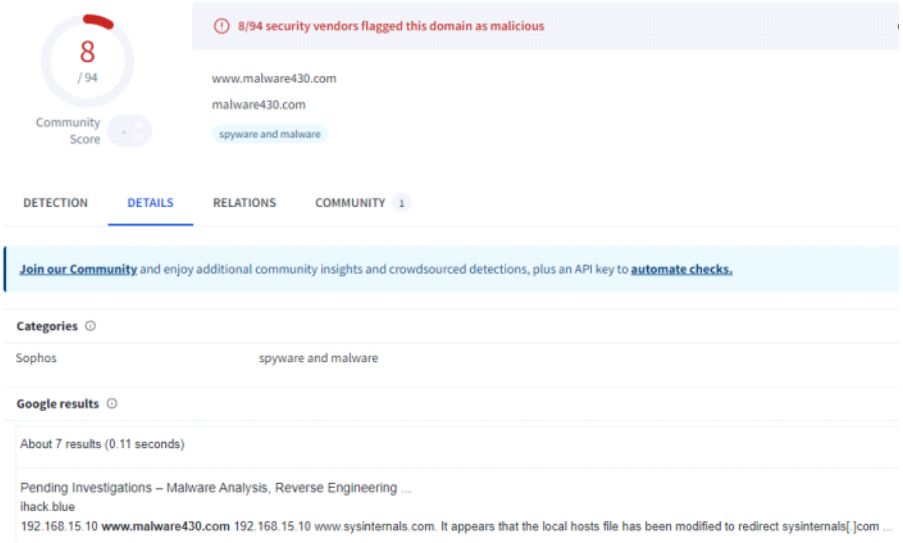
HTTP Requests

```
+ GET https://download.sysinternals.com:443/files/Hex2Dec.zip 200
+ GET http://x1.c.lencr.org/ 304
  GET http://www.google.com
+ GET http://www.google.com/
  GET http://www.malware430.com/html/VMwareUpdate.exe
  GET https://download.sysinternals.com/files/Hex2Dec.zip
+ GET http://www.msftncsi.com/ncsi.txt 200
+ GET http://www.google.com/ 200
```

Answer: www.malware430.com

Task 6:
The mapped domain is linked to an IP address. What is that IP address?

I checked the domain in Virus Total



8/94 security vendors flagged this domain as malicious

www.malware430.com

malware430.com

spyware and malware

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Categories

Sophos	spyware and malware

Google results

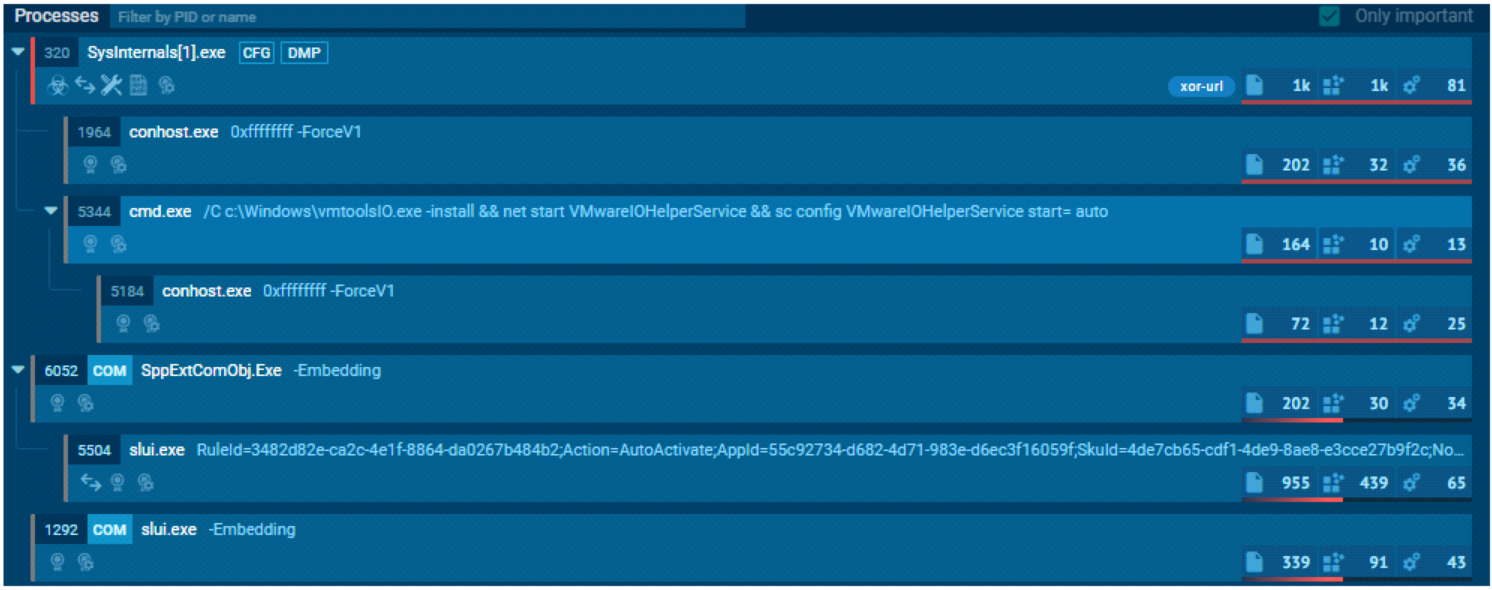
About 7 results (0.11 seconds)

Pending Investigations – Malware Analysis, Reverse Engineering ...
ihack.blue
192.168.15.10 **www.malware430.com** 192.168.15.10 www.sysinternals.com. It appears that the local hosts file has been modified to redirect sysinternals[.]com ...

Answer: 192.168.15.10

Task 7:
What is the name of the executable dropped by the first-stage executable?

I checked for the hash on Google and found a link to AnyRun which this malware was executed so I took the malware and executed it again and found the process

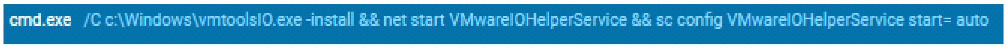


```
320  SysInternals[1].exe  CFG  DMP                                                        1k   1k   81
  1964  conhost.exe  0xffffffff -ForceV1                                                  202   32   36
  5344  cmd.exe  /C c:\Windows\vmtoolsIO.exe -install && net start VMwareIOHelperService && sc config VMwareIOHelperService start= auto   164   10   13
    5184  conhost.exe  0xffffffff -ForceV1                                                 72   12   25
6052  COM  SppExtComObj.Exe  -Embedding                                                   202   30   34
  5504  slui.exe  RuleId=3482d82e-ca2c-4e1f-8864-da0267b484b2;Action=AutoActivate;AppId=55c92734-d682-4d71-983e-d6ec3f16059f;SkuId=4de7cb65-cdf1-4de9-8ae8-e3cce27b9f2c;No...   955   439   65
1292  COM  slui.exe  -Embedding                                                           339   91   43
```

Answer: vmtoolsIO.exe

Task 8:
What is the name of the service installed by 2nd stage executable?

Same as task 7



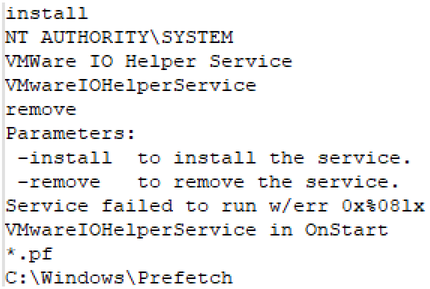
```
cmd.exe  /C c:\Windows\vmtoolsIO.exe -install && net start VMwareIOHelperService && sc config VMwareIOHelperService start= auto
```

Answer: VMwareIOHelperService

Task 9:
What is the extension of files deleted by the 2nd stage executable?

From the AnyRun I saw the 2nd stage is located at C:\Windows\vmtoolsIO.exe so I navigated to this directory with FTK Imager and then exported the file.
Then I used Strings on this file and saved it to a txt file.

I checked the strings file and noticed the extension



```
install
NT AUTHORITY\SYSTEM
VMWare IO Helper Service
VMwareIOHelperService
remove
Parameters:
 -install  to install the service.
 -remove   to remove the service.
Service failed to run w/err 0x%08lx
VMwareIOHelperService in OnStart
*.pf
C:\Windows\Prefetch
```

Answer: pf