Endpoint Forensics Incident Documentation: Sysinternals

Case: Sysinternals Endpoint Compromise
Analyst: *Nizar Aderbaz*
Date: *02/08/2026*

1. Executive Summary

The SOC opened **an investigation** into a threat on one of the systems **after unusual system activity was detected**. **The threat occurred** because **a user was socially engineered** to run a **malware program** that was disguised to look like a **legitimate system management** program named **sysinternals.exe**.

Once executed, **the malware** initializes **its payload** via a call to the Windows operating system's executable, **cmd.exe**, **which runs a secondary executable**, **vmtoolsIO.exe**, while **gaining persistence** through **the creation of an automatic system service**, simply called **VMwareIOHelperService**. An examination of **the host's files** successfully determined the identity of the **attacker's infrastructure**, resolving the domain identity of **www.malware430.com** to an IP address of **192.168.15.10**

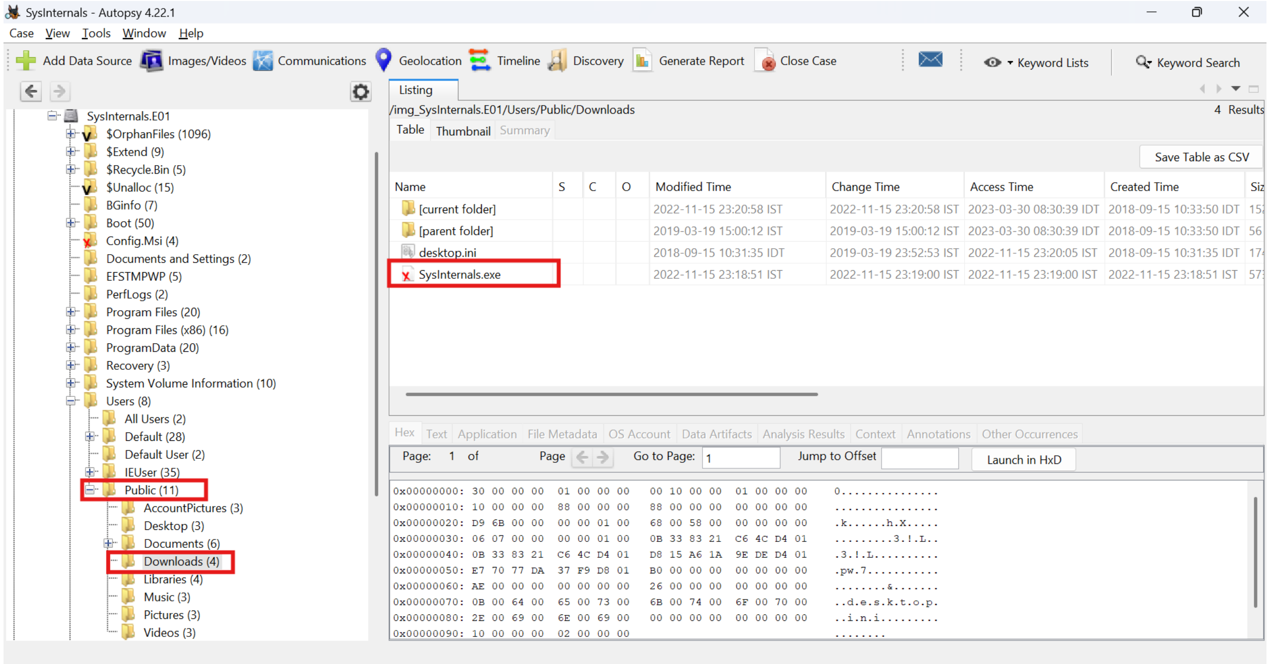
2. Tools

Tool	Purpose
Arsenal Image Mounter	To mount disk images as **virtual drives** for easy access and forensic analysis
VirusTotal	Scans **files** and **URLs** for malware using **multiple antivirus engines** and provides threat analysis.
Timeline Explorer	Reviewing **CSV exports** of forensic artifacts for chronological analysis.
AutoPsy	Analyzes **digital media** and **forensic data** to investigate and recover evidence.
MFTECmd	Parses and analyzes the **NTFS** Master File Table **(MFT)** for Windows forensic investigations.

3. Questions & Answers

1. What is the malicious executable file name that the user downloaded ?

I started the investigation by reviewing **the browser history**, specifically focusing on **Microsoft Edge**, but it did **NOT** yield any useful activity. I also confirmed that **Google Chrome** was **NOT** present on the system. Next, I checked the main user **"IEUser"** and searched in the **Downloads folder**, but again found **nothing**. I then moved on to other users to see if I could find something useful and found a binary called **"Sysinternals.exe"** inside the **Downloads folder** under the **Public user**.



SysInternals.E01
- $OrphanFiles (1096)
- $Extend (9)
- $Recycle.Bin (5)
- $Unalloc (15)
- BGinfo (7)
- Boot (50)
- Config.Msi (4)
- Documents and Settings (2)
- EFSTMPWP (5)
- PerfLogs (2)
- Program Files (20)
- Program Files (x86) (16)
- ProgramData (20)
- Recovery (3)
- System Volume Information (10)
- Users (8)
  - All Users (2)
  - Default (28)
  - Default User (2)
  - IEUser (35)
  - Public (11)
    - AccountPictures (3)
    - Desktop (3)
    - Documents (6)
    - Downloads (4)
    - Libraries (4)
    - Music (3)
    - Pictures (3)
    - Videos (3)

/img_SysInternals.E01/Users/Public/Downloads

4 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Siz
[current folder]				2022-11-15 23:20:58 IST	2022-11-15 23:20:58 IST	2023-03-30 08:30:39 IDT	2018-09-15 10:33:50 IDT	15
[parent folder]				2019-03-19 15:00:12 IST	2019-03-19 15:00:12 IST	2023-03-30 08:30:39 IDT	2018-09-15 10:33:50 IDT	56
desktop.ini				2018-09-15 10:31:35 IDT	2019-03-19 23:52:53 IST	2022-11-15 23:20:05 IST	2018-09-15 10:31:35 IDT	17
SysInternals.exe				2022-11-15 23:18:51 IST	2022-11-15 23:19:00 IST	2022-11-15 23:19:00 IST	2022-11-15 23:18:51 IST	57

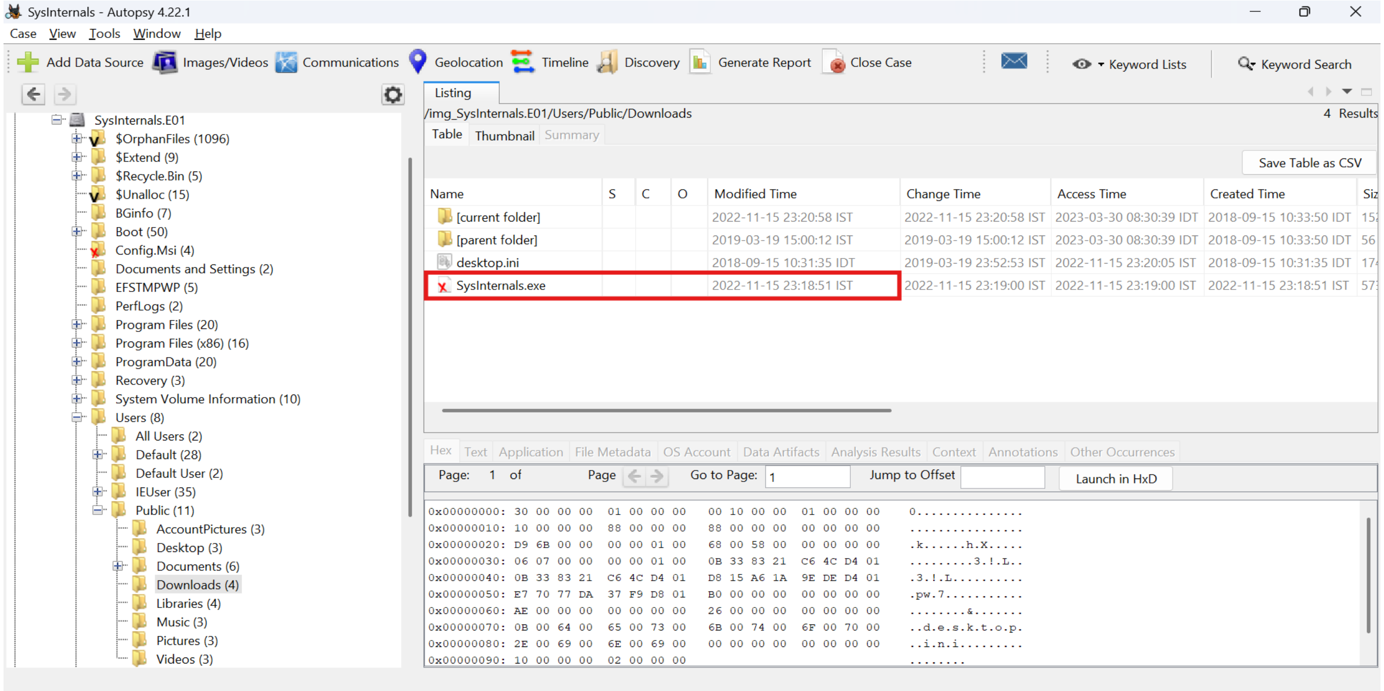
```
0x00000000: 30 00 00 00  01 00 00 00   00 10 00 00  01 00 00 00    0...............
0x00000010: 10 00 00 00  88 00 00 00   88 00 00 00  00 00 00 00    ................
0x00000020: D9 6B 00 00  00 00 01 00   68 00 58 00  00 00 00 00    .k......h.X.....
0x00000030: 06 07 00 00  00 00 01 00   0B 33 83 21  C6 4C D4 01    .........3.!.L..
0x00000040: 0B 33 83 21  C6 4C D4 01   D8 15 A6 1A  9E DE D4 01    .3.!.L..........
0x00000050: E7 70 77 DA  37 F9 D8 01   B0 00 00 00  00 00 00 00    .pw.7...........
0x00000060: AE 00 00 00  00 00 00 00   26 00 00 00  00 00 00 00    ........&.......
0x00000070: 0B 00 64 00  65 00 73 00   6B 00 74 00  6F 00 70 00    ..d.e.s.k.t.o.p.
0x00000080: 2E 00 69 00  6E 00 69 00   00 00 00 00  00 00 00 00    ..i.n.i.........
0x00000090: 10 00 00 00  02 00 00 00                               ........
```

Autopsy file system view showing "Sysinternals.exe" located in C:\Users\Public\Downloads

2. When was the last time the malicious executable file was modified ?

I wanted to figure out when **the malicious file** was **last changed**. So I looked at **the file system** using **AutoPsy** and the **MFT table** artifact to find this out. The results from **Autopsy** say the **malicious file** was last changed on **2022-11-15** at **21:18.** Because the program is set to **Istanbul time** it shows **23:18** which is actually the same time as **21:18** for **the malicious file**.

The **MFT table** artifact **"Parses, extracts, and analyzes NTFS Master File Table (MFT) records to reconstruct file system activity and timelines during Windows forensic investigations".**



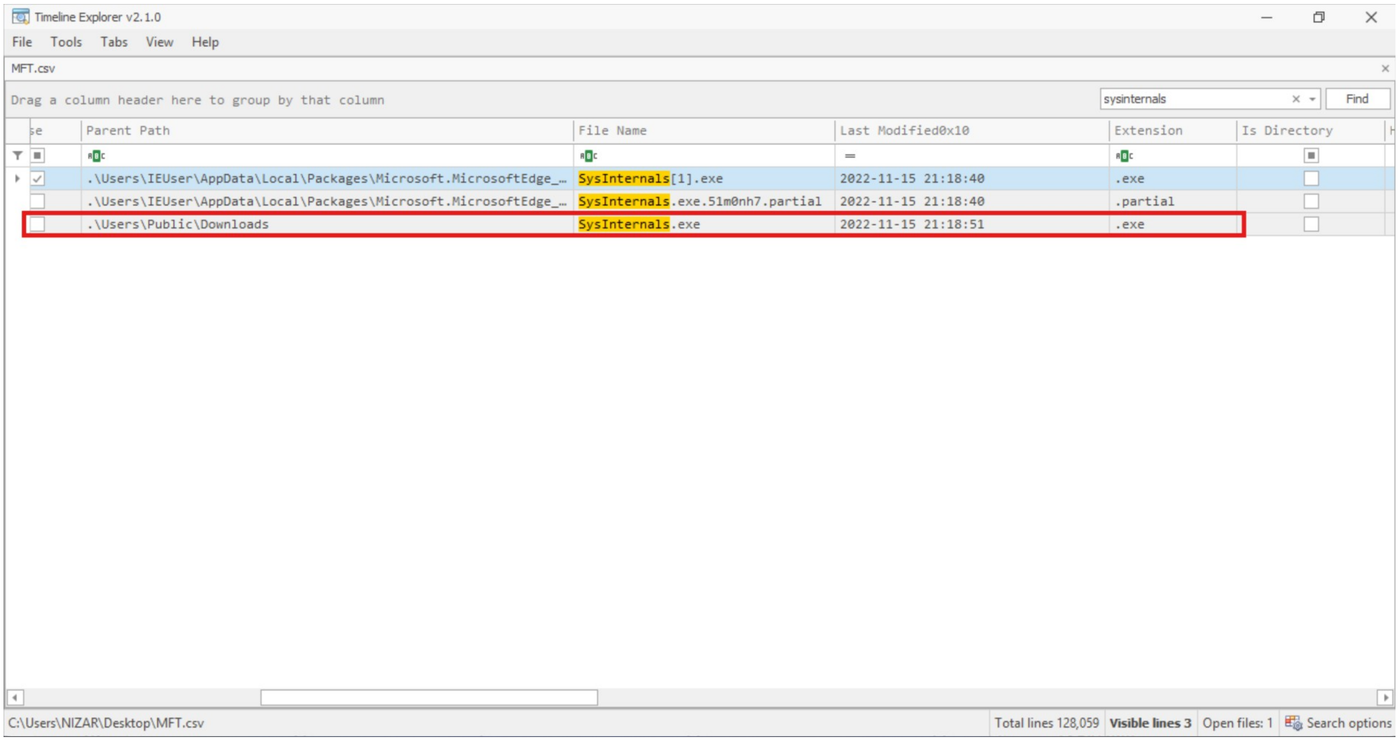
/img_SysInternals.E01/Users/Public/Downloads   4 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Siz
[current folder]				2022-11-15 23:20:58 IST	2022-11-15 23:20:58 IST	2023-03-30 08:30:39 IDT	2018-09-15 10:33:50 IDT	15
[parent folder]				2019-03-19 15:00:12 IST	2019-03-19 15:00:12 IST	2023-03-30 08:30:39 IDT	2018-09-15 10:33:50 IDT	56
desktop.ini				2018-09-15 10:31:35 IDT	2019-03-19 23:52:53 IST	2022-11-15 23:20:05 IST	2018-09-15 10:31:35 IDT	17
SysInternals.exe				2022-11-15 23:18:51 IST	2022-11-15 23:19:00 IST	2022-11-15 23:19:00 IST	2022-11-15 23:18:51 IST	57

Page: 1 of   Page   Go to Page: 1   Jump to Offset

```
0x00000000: 30 00 00 00  01 00 00 00   00 10 00 00  01 00 00 00    0...............
0x00000010: 10 00 00 00  88 00 00 00   88 00 00 00  00 00 00 00    ................
0x00000020: D9 6B 00 00  00 00 01 00   68 00 58 00  00 00 00 00    .k......h.X.....
0x00000030: 06 07 00 00  00 00 01 00   0B 33 83 21  C6 4C D4 01    .........3.!.L..
0x00000040: 0B 33 83 21  C6 4C D4 01   D8 15 A6 1A  9E DE D4 01    .3.!.L..........
0x00000050: E7 70 77 DA  37 F9 D8 01   B0 00 00 00  00 00 00 00    .pw.7...........
0x00000060: AE 00 00 00  00 00 00 00   26 00 00 00  00 00 00 00    ........&.......
0x00000070: 0B 00 64 00  65 00 73 00   6B 00 74 00  6F 00 70 00    ..d.e.s.k.t.o.p.
0x00000080: 2E 00 69 00  6E 00 69 00   00 00 00 00  00 00 00 00    ..i.n.i.........
0x00000090: 10 00 00 00  02 00 00 00                               ........
```

Autopsy file system metadata showing the modification time for "Sysinternals.exe" as 2022-11-15 21:18 (displayed as 23:18 due to Istanbul time configuration).



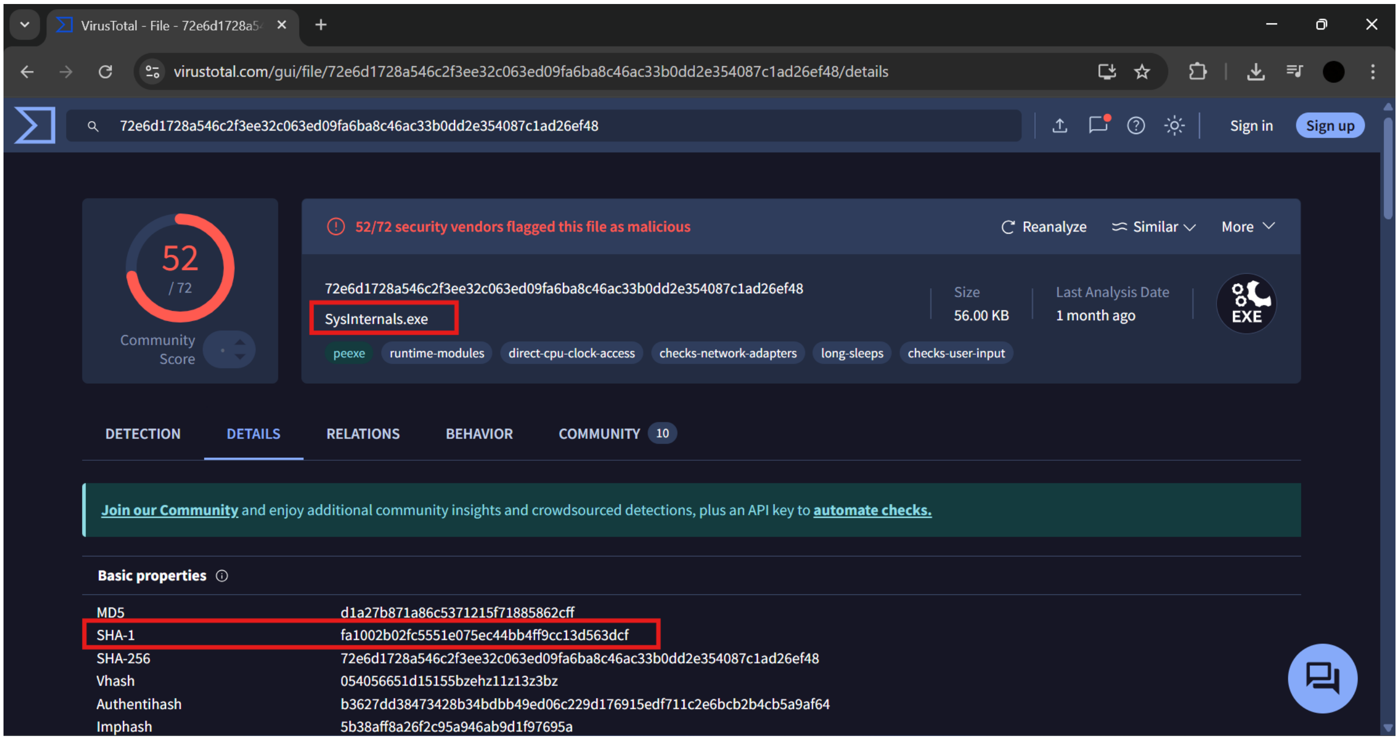
ꜱe	Parent Path	File Name	Last Modified0x10	Extension	Is Directory
☑	.\Users\IEUser\AppData\Local\Packages\Microsoft.MicrosoftEdge_…	SysInternals[1].exe	2022-11-15 21:18:40	.exe	□
□	.\Users\IEUser\AppData\Local\Packages\Microsoft.MicrosoftEdge_…	SysInternals.exe.51m0nh7.partial	2022-11-15 21:18:40	.partial	□
□	.\Users\Public\Downloads	SysInternals.exe	2022-11-15 21:18:51	.exe	□

Timeline Explorer view of the MFT artifact confirming the modification time for "Sysinternals.exe"

3. What is the SHA1 hash value of the malware?

To identify the malware, I extracted the file and uploaded it to **VirusTotal**. This helped me create a unique **file fingerprint** and compare it with **known threats**.

The malware's SHA1 hash is: fa1002b02fc5551e075ec44bb4ff9cc13d563dcf



52/72 security vendors flagged this file as malicious

72e6d1728a546c2f3ee32c063ed09fa6ba8c46ac33b0dd2e354087c1ad26ef48
SysInternals.exe

Size: 56.00 KB
Last Analysis Date: 1 month ago

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

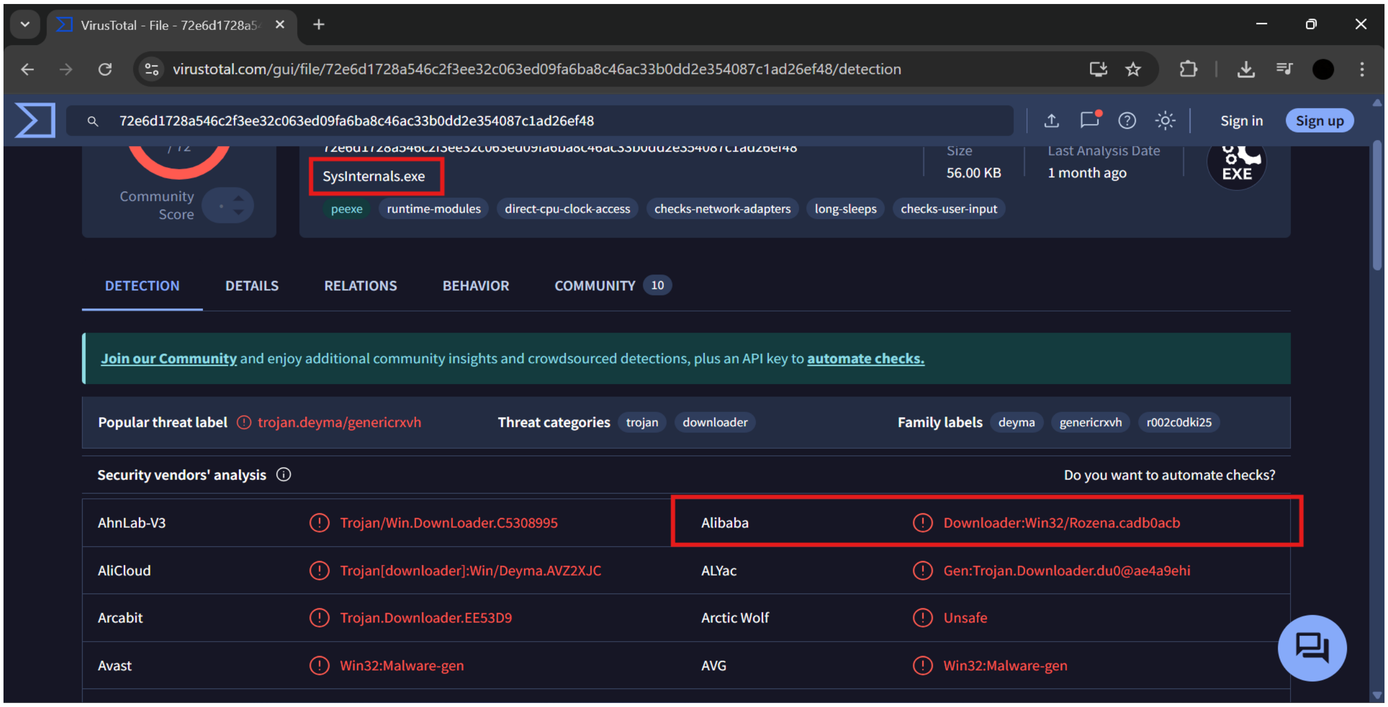
Basic properties

MD5	d1a27b871a86c5371215f71885862cff
SHA-1	fa1002b02fc5551e075ec44bb4ff9cc13d563dcf
SHA-256	72e6d1728a546c2f3ee32c063ed09fa6ba8c46ac33b0dd2e354087c1ad26ef48
Vhash	054056651d15155bzehz11z13z3bz
Authentihash	b3627dd38473428b34bdbb49ed06c229d176915edf711c2e6bcb2b4cb5a9af64
Imphash	5b38aff8a26f2c95a946ab9d1f97695a

VirusTotal analysis results confirming the SHA1 hash and malicious reputation of the extracted binary.

4. Based on the Alibaba vendor, what is the malware's family?

To further identify the threat, I navigated to the **Detection section** on **VirusTotal**, where the **Alibaba engine** explicitly identifies the malware family as **Rozena**. This specific classification helps in understanding **the malware's likely behavior** and the necessary remediation steps.



VirusTotal - File - 72e6d1728a5

virustotal.com/gui/file/72e6d1728a546c2f3ee32c063ed09fa6ba8c46ac33b0dd2e354087c1ad26ef48/detection

72e6d1728a546c2f3ee32c063ed09fa6ba8c46ac33b0dd2e354087c1ad26ef48

/ 72

Community Score

72e6d1728a546c2f3ee32c063ed09fa6ba8c46ac33b0dd2e354087c1ad26ef48

SysInternals.exe

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

Size 56.00 KB

Last Analysis Date 1 month 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

Family labels deyma genericrxvh r002c0dki25

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Trojan/Win.DownLoader.C5308995	Alibaba	Downloader:Win32/Rozena.cadb0acb
AliCloud	Trojan[downloader]:Win/Deyma.AVZ2XJC	ALYac	Gen:Trojan.Downloader.du0@ae4a9ehi
Arcabit	Trojan.Downloader.EE53D9	Arctic Wolf	Unsafe
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen

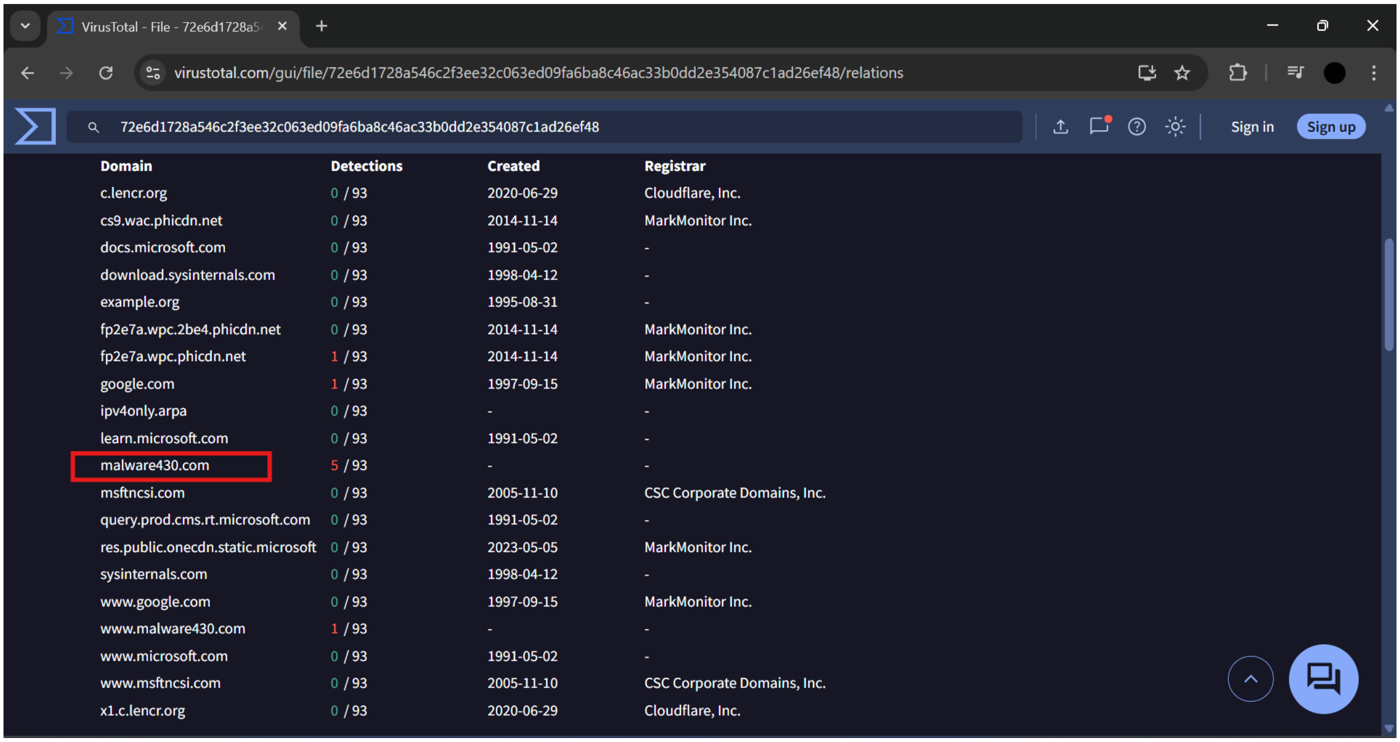
VirusTotal detection tab highlighting the "Rozena" malware family classification by the Alibaba security engine

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

By navigating to the **Relations tab** in **VirusTotal**, we can identify the **network infrastructure** associated with the **malware**. This tab lists **external resources** the binary interacts with, such as **contacted domains** and **IP addresses**.

The first mapped Fully Qualified Domain Name (FQDN) linked to this **Rozena malware** sample is: **www.malware430.com**

This domain likely serves as **the command-and-control (C2)** server where the malware sends **exfiltrated data** or **receives further instructions**.


VirusTotal - File - 72e6d1728a5
virustotal.com/gui/file/72e6d1728a546c2f3ee32c063ed09fa6ba8c46ac33b0dd2e354087c1ad26ef48/relations
72e6d1728a546c2f3ee32c063ed09fa6ba8c46ac33b0dd2e354087c1ad26ef48

Domain	Detections	Created	Registrar
c.lencr.org	0 / 93	2020-06-29	Cloudflare, Inc.
cs9.wac.phicdn.net	0 / 93	2014-11-14	MarkMonitor Inc.
docs.microsoft.com	0 / 93	1991-05-02	-
download.sysinternals.com	0 / 93	1998-04-12	-
example.org	0 / 93	1995-08-31	-
fp2e7a.wpc.2be4.phicdn.net	0 / 93	2014-11-14	MarkMonitor Inc.
fp2e7a.wpc.phicdn.net	1 / 93	2014-11-14	MarkMonitor Inc.
google.com	1 / 93	1997-09-15	MarkMonitor Inc.
ipv4only.arpa	0 / 93	-	-
learn.microsoft.com	0 / 93	1991-05-02	-
malware430.com	5 / 93	-	-
msftncsi.com	0 / 93	2005-11-10	CSC Corporate Domains, Inc.
query.prod.cms.rt.microsoft.com	0 / 93	1991-05-02	-
res.public.onecdn.static.microsoft	0 / 93	2023-05-05	MarkMonitor Inc.
sysinternals.com	0 / 93	1998-04-12	-
www.google.com	0 / 93	1997-09-15	MarkMonitor Inc.
www.malware430.com	1 / 93	-	-
www.microsoft.com	0 / 93	1991-05-02	-
www.msftncsi.com	0 / 93	2005-11-10	CSC Corporate Domains, Inc.
x1.c.lencr.org	0 / 93	2020-06-29	Cloudflare, Inc.

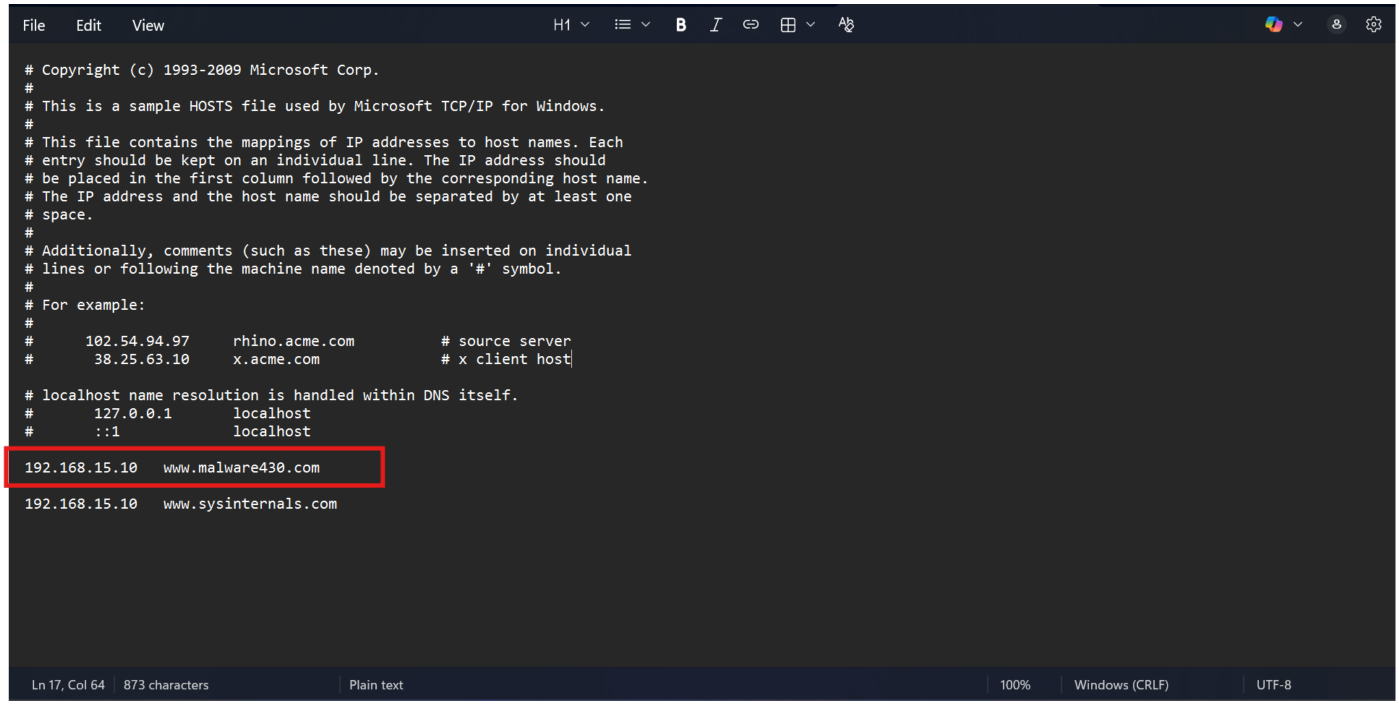
VirusTotal "Relations" tab showing the "Contacted Domains" section, where the FQDN "www.malware430.com" is identified as a network indicator associated with the malware.

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

To confirm the specific **IP address** **the malware** intends to communicate with, we should examine the **hosts file** on the **infected system**. In forensic investigations, **the hosts file** is a **critical artifact** because it can be used **to redirect traffic by mapping domain names to specific IP addresses.**

By reviewing the system's hosts file **(typically located at C:\Windows\System32\drivers\etc\hosts)**,

The IP address linked to the domain **"www.malware430.com"** in this case is: **192.168.15.10**



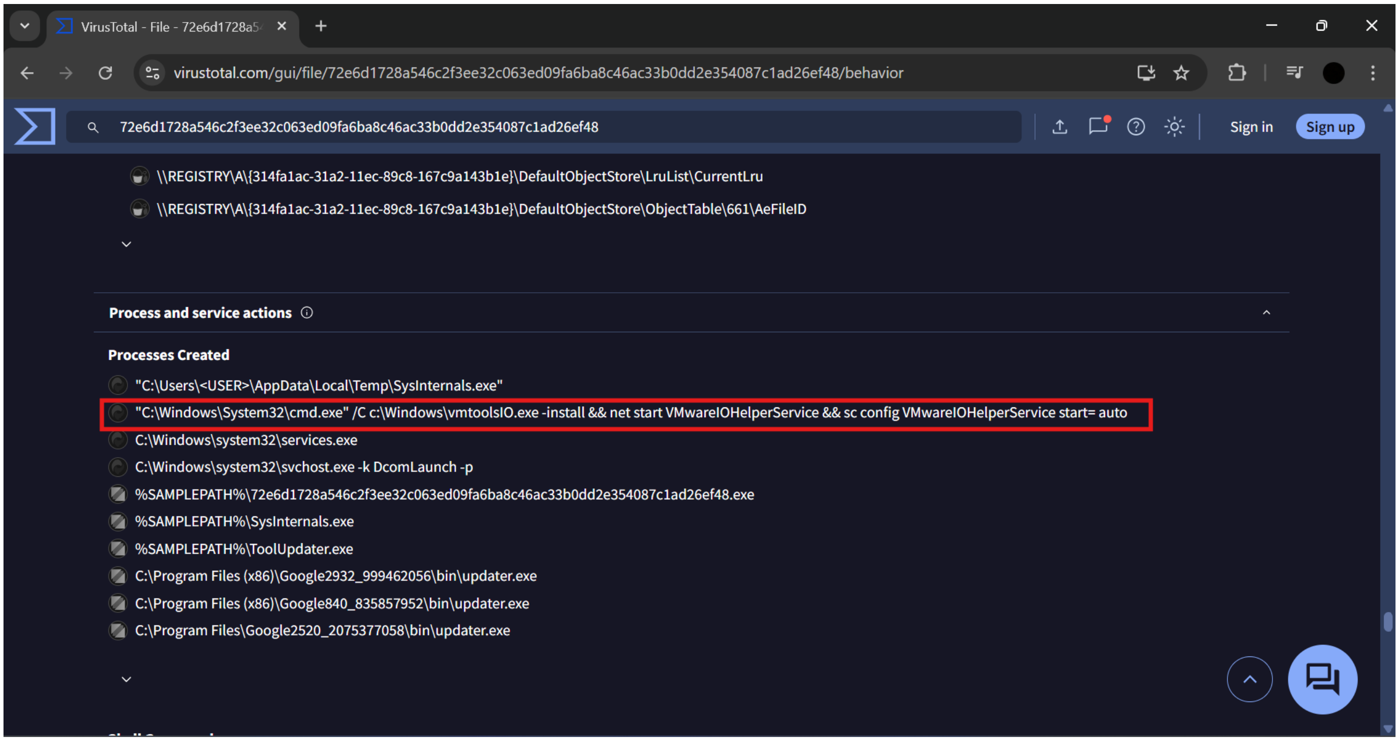
```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost

192.168.15.10   www.malware430.com

192.168.15.10   www.sysinternals.com
```

System hosts file displaying the static mapping of the domain "www.malware430.com" to the malicious IP address 192.168.15.10

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

To investigate **the specific actions** taken by the malware **during execution**, we navigate to the **Behavior tab** in **VirusTotal**. This section **allows us** to inspect the **Process Tree**, which visually maps out the **parent-child relationships** between **different processes** launched by the sample.

Once executed, we can see clearly that **the malware initialises a command line** interface via **cmd.exe**. Following this, it executes a binary named **vmtoolsIO.exe**. This sequence spawning a **command shell** to **launch a specific executable** is a **classic behavior** used by **the Rozena family** to establish **its presence** and begin **its malicious operations.**


VirusTotal - File - 72e6d1728a5
virustotal.com/gui/file/72e6d1728a546c2f3ee32c063ed09fa6ba8c46ac33b0dd2e354087c1ad26ef48/behavior
72e6d1728a546c2f3ee32c063ed09fa6ba8c46ac33b0dd2e354087c1ad26ef48
Sign in
Sign up

```
\\REGISTRY\A\{314fa1ac-31a2-11ec-89c8-167c9a143b1e}\DefaultObjectStore\LruList\CurrentLru
\\REGISTRY\A\{314fa1ac-31a2-11ec-89c8-167c9a143b1e}\DefaultObjectStore\ObjectTable\661\AeFileID
```

Process and service actions

Processes Created

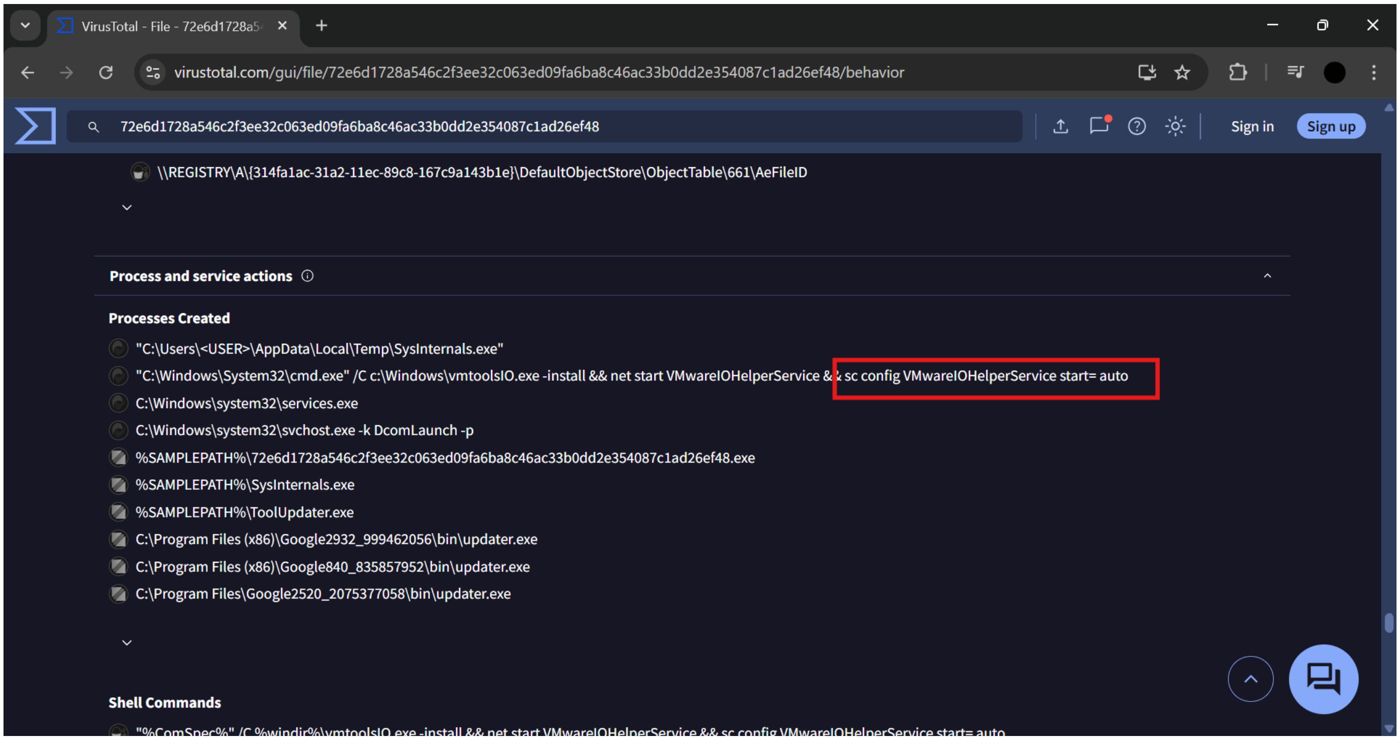
```
"C:\Users\<USER>\AppData\Local\Temp\SysInternals.exe"
"C:\Windows\System32\cmd.exe" /C c:\Windows\vmtoolsIO.exe -install && net start VMwareIOHelperService && sc config VMwareIOHelperService start= auto
C:\Windows\system32\services.exe
C:\Windows\system32\svchost.exe -k DcomLaunch -p
%SAMPLEPATH%\72e6d1728a546c2f3ee32c063ed09fa6ba8c46ac33b0dd2e354087c1ad26ef48.exe
%SAMPLEPATH%\SysInternals.exe
%SAMPLEPATH%\ToolUpdater.exe
C:\Program Files (x86)\Google2932_999462056\bin\updater.exe
C:\Program Files (x86)\Google840_835857952\bin\updater.exe
C:\Program Files\Google2520_2075377058\bin\updater.exe
```

VirusTotal "Behavior" tab showcasing the process tree, where the malware spawns "cmd.exe" which then executes the "vmtoolsIO.exe" binary

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

At the end of the executed command string, it is clearly visible that a **new service** is being **configured** and **launched**.
The name of **the service** installed by **the second-stage executable** is **VmwareIOHelperService.**

The malware sets this service to **start automatically**, ensuring that its malicious components **remain active even after a system reboot.**


VirusTotal - File - 72e6d1728a5
virustotal.com/gui/file/72e6d1728a546c2f3ee32c063ed09fa6ba8c46ac33b0dd2e354087c1ad26ef48/behavior
72e6d1728a546c2f3ee32c063ed09fa6ba8c46ac33b0dd2e354087c1ad26ef48
Sign in
Sign up

```
\\REGISTRY\A\{314fa1ac-31a2-11ec-89c8-167c9a143b1e}\DefaultObjectStore\ObjectTable\661\AeFileID
```

Process and service actions

Processes Created

```
"C:\Users\<USER>\AppData\Local\Temp\SysInternals.exe"
"C:\Windows\System32\cmd.exe" /C c:\Windows\vmtoolsIO.exe -install && net start VMwareIOHelperService && sc config VMwareIOHelperService start= auto
C:\Windows\system32\services.exe
C:\Windows\system32\svchost.exe -k DcomLaunch -p
%SAMPLEPATH%\72e6d1728a546c2f3ee32c063ed09fa6ba8c46ac33b0dd2e354087c1ad26ef48.exe
%SAMPLEPATH%\SysInternals.exe
%SAMPLEPATH%\ToolUpdater.exe
C:\Program Files (x86)\Google2932_999462056\bin\updater.exe
C:\Program Files (x86)\Google840_835857952\bin\updater.exe
C:\Program Files\Google2520_2075377058\bin\updater.exe
```

Shell Commands

```
"%ComSpec%" /C %windir%\vmtoolsIO.exe -install && net start VMwareIOHelperService && sc config VMwareIOHelperService start= auto
```

VirusTotal process analysis revealing the command execution used to install and start the "VMwareIOHelperService" for system persistence

3. Conclusion

The analysis of the Rozena malware incident confirms **a multi-stage compromise** designed to establish **persistent remote access**. The attacker demonstrated clear intent to **evade detection** and **maintain a long-term foothold** by:

- **Evasion:** Masquerading as a legitimate administrative tool named sysinternals.exe. Upon execution, the malware initiates a command-line sequence via **cmd.exe** to launch the secondary binary vmtoolsIO.exe, effectively hiding the **malicious process** within common system management activity.

- **Persistence:** Installing a dedicated system service named **VMwareIOHelperService**. By configuring this service to **start automatically**, the malware ensures it remains active on the system across reboots.

- **Command & Control (C2) :** Utilizing the local **hosts file** to link **the domain** **www.malware430.com** to **the IP address** **192.168.15.10.** This mapping confirms **the network infrastructure,** the malware is programmed to communicate with for its control **operations**.

4. Recommendations

- **Network Defense:** Immediately **block traffic** to the domain **www.malware430.com** and the IP address **192.168.15.10** at **the firewall** and **web gateway.**

- **Service Audit:** Scan the environment for the **VMwareIOHelperService** or **any services mimicking legitimate vendors** like **VMware** that are set to **"Automatic" start**.

- **Process Monitoring:** Set up alerts for **suspicious process chains**, specifically instances where **a command shell (cmd.exe)** launches **unknown binaries** from the **Downloads** or **Public directories.**

- **Verified Sources Policy:** Enforce **a policy** that administrative tools like the **Sysinternals Suite** must **only be downloaded** from **official Microsoft sources** and **verify their digital signatures** before execution.