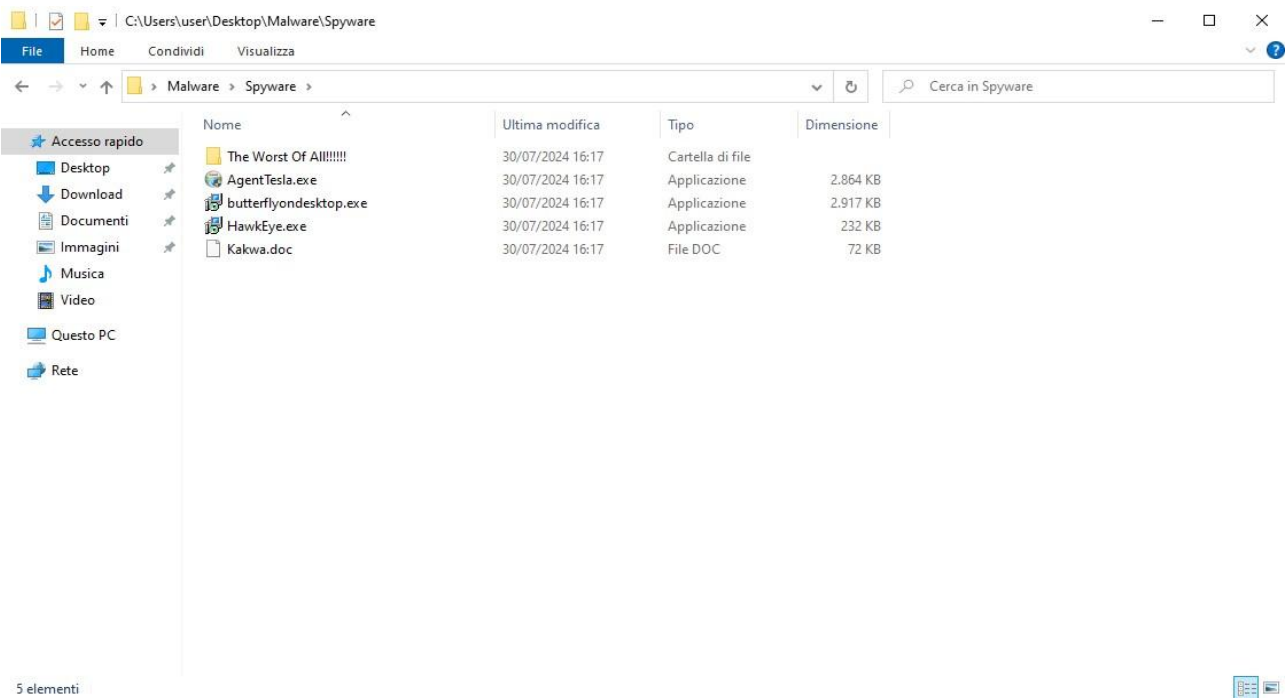


Relazione Analisi del Malware

Nella seguente immagine, abbiamo la Home Page di VirusTotal, un tool per la scansione ed analisi perimetrale del nostro **FILE**, **URL** o **HASH**:



Dopo aver caricato il nostro file, presunto Malware da analizzare, denominato **AgentTesla.exe**, su VirusTotal, nella prossima immagine, possiamo vedere l'analisi finale con il report che riporta il numero di elementi malevoli:



26

/ 72

Community Score

-8

26/72 security vendors flagged this file as malicious

Reanalyze

Similar

More

18aab0e981eee9e4ef8e15d4b003b14b3a1b0bfb7233fade8ee4b6a22a5abbb9

Size

2.80 MB

Last Analysis Date

5 days ago

AgentTesla.exe

peexe

direct-cpu-clock-access

runtime-modules

overlay

detect-debug-environment

nsis

Terminato la scansione con il tool VirusTotal, utilizziamo la **Sandbox Cuckoo**, per l’analisi profonda del Malware, con relativo report, che descrive gli elementi trovati all’interno dello stesso, come da immagini seguenti, procediamo con la ricerca del file infetto sul sito **MalwareBazaar** e successivamente con l’upload del file malevolo da analizzare, AgentTesla.exe:

MALWARE bazaar

by ABUSE[CH]

Browse

Upload

Hunting

API

Export

Statistics

FAQ

About

Login

MalwareBazaar

MalwareBazaar is a project from abuse.ch with the goal of sharing malware samples with the infosec community, AV vendors and threat intelligence providers.

MalwareBazaar database »

API

Integrate threat intel from MalwareBazaar into your SIEM using the API.

View details »

MalwareBazaar database

Get insights, browse MalwareBazaar database and find most recent additions.

View details »

Get involved

Share malware samples with the community, helping them to make the internet a safer place.

View details »

© abuse.ch 2024

File

Home

Condividi

Visualizza

C:\Users\user\Desktop\Malware\Spyware

Malware > Spyware

Cerca in Spyware

Accesso rapido

Desktop

Download

Documenti

Immagini

Musica

Video

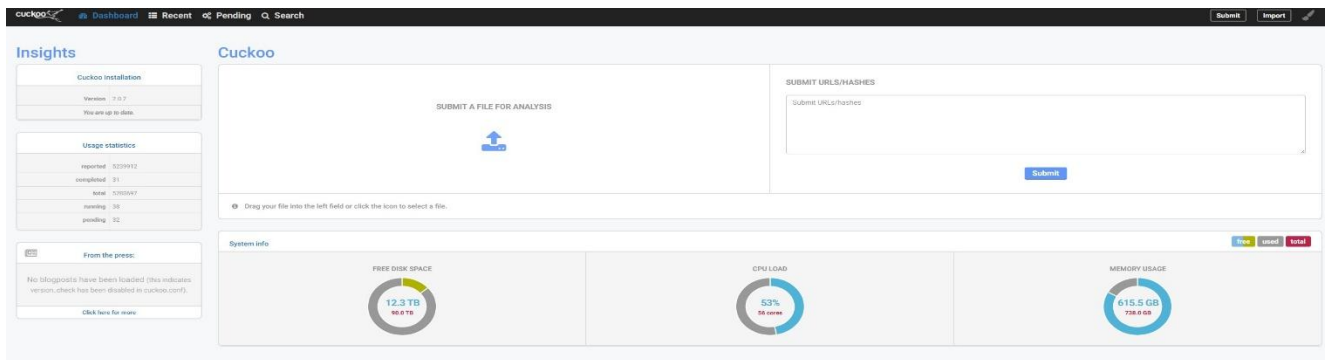
Questo PC

Rete

Nome	Ultima modifica	Tipo	Dimensione
The Worst Of All!!!!!!	30/07/2024 16:17	Cartella di file	
AgentTesla.exe	30/07/2024 16:17	Applicazione	2.864 KB
butterflyondesktop.exe	30/07/2024 16:17	Applicazione	2.917 KB
HawkEye.exe	30/07/2024 16:17	Applicazione	232 KB
Kakwa.doc	30/07/2024 16:17	File DOC	72 KB

5 elementi

Carichiamo sulla parte di sinistra della Sandbox **SUBMIT A FILE ANALYSIS**, **AgentTesla.exe**



Dopo aver caricato il file malevolo, attendiamo l'analisi da parte di Cuckoo, che ci indicherà sulla parte destra del file che sta scansionando, **in pending**.

Terminata l'analisi di **AgentTesla.exe**, sempre sulla destra, troviamo invece di **in pending**, in running, e possiamo successivamente cliccare in alto a sinistra su **Recent**, dove troviamo il nostro file, esaminato, e cliccando sul nome del file, possiamo vedere la pagina con tutti i dati relativi alla scansione di **AgentiTesla.exe**

Summary

File AgentTesla.exe

Summary

Size	2.8MB
Type	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
MD5	ccc184cab13569c8a2a4a7cae09187
SHA1	e4b8f4b0cab1899748f83e9fffd275ef5276199e
SHA256	18a0b0e981ee9e4ef8e1564b083b143a1b0bf07233f4de8ee4b5a22a5abb09
SHA512	Show SHA512
CRC32	5CEAB9ED
sdeep	None
Yara	<ul style="list-style-type: none">escalate_priv - Escalade privilegesscreenshot - Take screenshotwin_registry - Affect system registrieswin_token - Affect system tokenswin_files_operation - Affect private profile

Score

This file is very suspicious, with a score of 10 out of 10!

Please notice: The scoring system is currently still in development and should be considered an alpha feature.

Feedback

Expecting different results? Send us this analysis and we will inspect it. [Click here](#)

Information on Execution

Category	Started	Completed	Duration	Routing	Logs
FILE	Oct. 8, 2024, 4:35 p.m.	Oct. 8, 2024, 4:43 p.m.	440 seconds	internet	Show Analyzer Log Show Cuckoo Log

Signatures

Yara rules detected for file (5 events)

Checks amount of memory in system, this can be used to detect virtual machines that have a low amount of memory available (1 event)

The executable contains unknown PE section names indicative of a packer (could be a false positive) (1 event)

Queries the disk size which could be used to detect virtual machine with small fixed size or dynamic allocation (6 events)

File has been identified by 6 AntiVirus engine on IRMA as malicious (6 events)

File has been identified by 26 AntiVirus engines on VirusTotal as malicious (26 events)

Screenshots












Come passaggio finale, andiamo ad utilizzare il tool **Procmon** per visualizzare i movimenti e le azioni del Malware, all'interno dei processi del computer, come da seguenti immagini:



Nella seguente immagine, possiamo notare i processi in **protocollo UDP** di invio e ricezione delle comunicazioni:

Process Monitor - Sysinternals: www.sysinternals.com

FileEditEventFilterToolsOptionsHelp



Time ...	Process Name	PID	Operation	Path	Result	Detail
16:47:...	svchost.exe	1016	UDP Send	DESKTOP-KH6PO3M.home.arpas.dhcpv...	SUCCESS	Length: 95, sequ...
16:47:...	svchost.exe	1208	UDP Send	DESKTOP-KH6PO3M.home.arpas.55513...	SUCCESS	Length: 90, sequ...
16:47:...	svchost.exe	1208	UDP Receive	DESKTOP-KH6PO3M.home.arpas.55513...	SUCCESS	Length: 90, sequ...
16:47:...	svchost.exe	1208	UDP Send	DESKTOP-KH6PO3M.home.arpas.58131...	SUCCESS	Length: 90, sequ...
16:47:43,7858549	svchost.exe	1208	UDP Send	DESKTOP-KH6PO3M.home.arpas.58131...	SUCCESS	Length: 90, sequ...
16:47:...	svchost.exe	1208	UDP Send	DESKTOP-KH6PO3M.home.arpas.58131...	SUCCESS	Length: 90, sequ...
16:47:...	svchost.exe	1208	UDP Send	DESKTOP-KH6PO3M.home.arpas.58131...	SUCCESS	Length: 90, sequ...
16:47:...	svchost.exe	1208	UDP Send	DESKTOP-KH6PO3M.home.arpas.62592...	SUCCESS	Length: 43, sequ...
16:47:...	svchost.exe	1208	UDP Receive	DESKTOP-KH6PO3M.home.arpas.62592...	SUCCESS	Length: 70, sequ...
16:47:...	svchost.exe	1208	UDP Send	DESKTOP-KH6PO3M.home.arpas.51530...	SUCCESS	Length: 90, sequ...
16:47:...	svchost.exe	1208	UDP Send	DESKTOP-KH6PO3M.home.arpas.57260...	SUCCESS	Length: 42, sequ...
16:47:...	svchost.exe	1208	UDP Receive	DESKTOP-KH6PO3M.home.arpas.51530...	SUCCESS	Length: 90, sequ...
16:47:...	svchost.exe	1208	UDP Send	DESKTOP-KH6PO3M.home.arpas.58191...	SUCCESS	Length: 90, sequ...
16:47:...	svchost.exe	1208	UDP Send	DESKTOP-KH6PO3M.home.arpas.58191...	SUCCESS	Length: 90, sequ...
16:47:...	svchost.exe	1208	UDP Receive	DESKTOP-KH6PO3M.home.arpas.57260...	SUCCESS	Length: 42, sequ...
16:47:...	svchost.exe	1208	UDP Send	DESKTOP-KH6PO3M.home.arpas.55515...	SUCCESS	Length: 42, sequ...
16:47:...	svchost.exe	1208	UDP Send	DESKTOP-KH6PO3M.home.arpas.55515...	SUCCESS	Length: 42, sequ...
16:47:...	svchost.exe	1208	UDP Send	DESKTOP-KH6PO3M.home.arpas.58191...	SUCCESS	Length: 90, sequ...
16:47:...	svchost.exe	1208	UDP Send	DESKTOP-KH6PO3M.home.arpas.58191...	SUCCESS	Length: 90, sequ...
16:47:...	svchost.exe	1208	UDP Send	DESKTOP-KH6PO3M.home.arpas.55515...	SUCCESS	Length: 42, sequ...
16:47:...	svchost.exe	1208	UDP Send	DESKTOP-KH6PO3M.home.arpas.55515...	SUCCESS	Length: 42, sequ...
16:47:...	svchost.exe	1208	UDP Send	DESKTOP-KH6PO3M.home.arpas.59762...	SUCCESS	Length: 32, sequ...
16:47:...	svchost.exe	1208	UDP Send	DESKTOP-KH6PO3M.home.arpas.59762...	SUCCESS	Length: 32, sequ...
16:47:...	svchost.exe	1208	UDP Receive	DESKTOP-KH6PO3M.home.arpas.59762...	SUCCESS	Length: 32, sequ...
16:48:...	svchost.exe	1208	UDP Send	DESKTOP-KH6PO3M.home.arpas.63883...	SUCCESS	Length: 41, sequ...
16:48:...	svchost.exe	1208	UDP Receive	DESKTOP-KH6PO3M.home.arpas.63883...	SUCCESS	Length: 41, sequ...
16:48:...	svchost.exe	1208	UDP Send	DESKTOP-KH6PO3M.home.arpas.50290...	SUCCESS	Length: 45, sequ...
16:48:...	svchost.exe	1208	UDP Receive	DESKTOP-KH6PO3M.home.arpas.50290...	SUCCESS	Length: 104, sequ...
16:48:...	svchost.exe	1208	UDP Send	DESKTOP-KH6PO3M.home.arpas.54068...	SUCCESS	Length: 45, sequ...
16:48:...	svchost.exe	1208	UDP Send	DESKTOP-KH6PO3M.home.arpas.54068...	SUCCESS	Length: 45, sequ...
16:48:...	svchost.exe	1208	UDP Send	DESKTOP-KH6PO3M.home.arpas.54068...	SUCCESS	Length: 45, sequ...
16:48:...	svchost.exe	1208	UDP Send	DESKTOP-KH6PO3M.home.arpas.54068...	SUCCESS	Length: 45, sequ...
16:48:...	msedge.exe	920	UDP Send	DESKTOP-KH6PO3M.home.arpas.65042...	SUCCESS	Length: 36, sequ...
16:48:...	msedge.exe	920	UDP Send	DESKTOP-KH6PO3M.home.arpas.62861...	SUCCESS	Length: 36, sequ...
16:48:...	svchost.exe	1208	UDP Send	DESKTOP-KH6PO3M.home.arpas.58848...	SUCCESS	Length: 32, sequ...
16:48:...	svchost.exe	1208	UDP Receive	DESKTOP-KH6PO3M.home.arpas.58848...	SUCCESS	Length: 32, sequ...
16:48:...	msedge.exe	920	UDP Receive	DESKTOP-KH6PO3M.home.arpas.65042...	SUCCESS	Length: 36, sequ...
16:48:...	msedge.exe	920	UDP Receive	DESKTOP-KH6PO3M.home.arpas.62861...	SUCCESS	Length: 36, sequ...
16:48:...	msedge.exe	920	UDP Send	DESKTOP-KH6PO3M.home.arpas.55280...	SUCCESS	Length: 36, sequ...
16:48:...	msedge.exe	920	UDP Send	DESKTOP-KH6PO3M.home.arpas.57178...	SUCCESS	Length: 36, sequ...
16:48:...	msedge.exe	920	UDP Receive	DESKTOP-KH6PO3M.home.arpas.57178...	SUCCESS	Length: 36, sequ...
16:48:...	msedge.exe	920	UDP Receive	DESKTOP-KH6PO3M.home.arpas.55280...	SUCCESS	Length: 36, sequ...
16:48:...	svchost.exe	1208	UDP Send	DESKTOP-KH6PO3M.home.arpas.55577...	SUCCESS	Length: 36, sequ...
16:48:...	svchost.exe	1208	UDP Receive	DESKTOP-KH6PO3M.home.arpas.55577...	SUCCESS	Length: 36, sequ...
16:48:...	msedge.exe	920	UDP Send	DESKTOP-KH6PO3M.home.arpas.63438...	SUCCESS	Length: 36, sequ...
16:48:...	msedge.exe	920	UDP Send	DESKTOP-KH6PO3M.home.arpas.59315...	SUCCESS	Length: 36, sequ...
16:48:...	msedge.exe	920	UDP Receive	DESKTOP-KH6PO3M.home.arpas.63438...	SUCCESS	Length: 36, sequ...
16:48:...	msedge.exe	920	UDP Send	DESKTOP-KH6PO3M.home.arpas.58559...	SUCCESS	Length: 36, sequ...
16:48:...	msedge.exe	920	UDP Receive	DESKTOP-KH6PO3M.home.arpas.58559...	SUCCESS	Length: 36, sequ...
16:48:...	msedge.exe	920	UDP Receive	DESKTOP-KH6PO3M.home.arpas.59315...	SUCCESS	Length: 36, sequ...
16:48:...	msedge.exe	920	UDP Send	DESKTOP-KH6PO3M.home.arpas.56293...	SUCCESS	Length: 36, sequ...

In questa immagine finale, possiamo notare come il file infetto AgentTesla, sta prendendo il controllo degli elementi all'interno del nostro computer

Process Monitor - Sysinternals: www.sysinternals.com					
File Edit Event Filter Tools Options Help					
Time ...	Process Name	PID	Operation	Path	Result
16:47:...	Explorer.EXE	3404	RegQueryValue	HKLM\SOFTWARE\Microsoft\PolicyM...	NAME NOT FOUND
16:47:...	Explorer.EXE	3404	RegQueryValue	HKLM\SOFTWARE\Microsoft\PolicyM...	NAME NOT FOUND
16:47:...	Explorer.EXE	3404	RegQueryValue	HKLM\SOFTWARE\Microsoft\PolicyM...	NAME NOT FOUND
16:47:...	Explorer.EXE	3404	RegQueryValue	HKLM\SOFTWARE\Microsoft\PolicyM...	NAME NOT FOUND
16:47:...	Explorer.EXE	3404	RegQueryValue	HKLM\SOFTWARE\Microsoft\PolicyM...	NAME NOT FOUND
16:47:...	Explorer.EXE	3404	RegQueryValue	HKLM\SOFTWARE\Microsoft\PolicyM...	NAME NOT FOUND
16:47:...	Explorer.EXE	3404	RegQueryValue	HKLM\SOFTWARE\Microsoft\PolicyM...	NAME NOT FOUND
16:47:...	Explorer.EXE	3404	RegCloseKey	HKLM\SOFTWARE\Microsoft\PolicyM...	SUCCESS
16:47:...	Explorer.EXE	3404	RegOpenKey	HKLM\SOFTWARE\Microsoft\PolicyManag...	NAME NOT FOUND
16:47:...	Explorer.EXE	3404	RegOpenKey	HKLM\SOFTWARE\Microsoft\PolicyManag...	SUCCESS
16:47:...	Explorer.EXE	3404	RegOpenKey	HKLM\SOFTWARE\Microsoft\PolicyManag...	NAME NOT FOUND
16:47:...	Explorer.EXE	3404	RegOpenKey	HKCU\Software\Microsoft\Input\TSF.T...	SUCCESS
16:47:...	Explorer.EXE	3404	RegOpenKey	HKCU\Software\Microsoft\Input\TSF.T...	NAME NOT FOUND
16:47:...	Explorer.EXE	3404	RegOpenKey	HKCU\Software\Microsoft\Input\TSF.T...	SUCCESS
16:47:...	Explorer.EXE	3404	RegOpenKey	HKCU\Software\Microsoft\Input\TSF.T...	SUCCESS
16:47:...	Explorer.EXE	3404	ReadFile	C:\Windows\System32\AppResolver.dll	SUCCESS
16:47:...	Explorer.EXE	3404	RegOpenKey	HKCU\Software\Classes	SUCCESS
16:47:...	Explorer.EXE	3404	RegOpenKey	HKCU\Software\Classes	SUCCESS
16:47:...	Explorer.EXE	3404	RegOpenKey	HKCU\Software\Classes	SUCCESS
16:47:...	Explorer.EXE	3404	RegOpenKey	HKCU\Software\Classes\CLSID\{56AD...	NAME NOT FOUND
16:47:...	Explorer.EXE	3404	RegOpenKey	HKCR\CLSID\{56AD4C5D-B908-4F85-...	NAME NOT FOUND
16:47:...	Explorer.EXE	3404	RegOpenKey	HKCU\Software\Classes	SUCCESS
16:47:...	Explorer.EXE	3404	RegOpenKey	HKCU\Software\Classes	SUCCESS
16:47:...	Explorer.EXE	3404	RegOpenKey	HKCU\Software\Classes	SUCCESS
16:47:...	Explorer.EXE	3404	RegOpenKey	HKCU\Software\Classes	SUCCESS
16:47:...	Explorer.EXE	3404	RegOpenKey	HKCU\Software\Classes\CLSID\{56AD...	NAME NOT FOUND
16:47:...	Explorer.EXE	3404	RegOpenKey	HKCR\CLSID\{56AD4C5D-B908-4F85-...	NAME NOT FOUND
16:47:...	Explorer.EXE	3404	QueryNameInfo...	C:\Users\user\AppData\Local\Temp\I...	SUCCESS
16:47:...	Explorer.EXE	3404	CreateFile	C:\Users\user\AppData\Local\Temp\I...	SUCCESS
16:47:...	Explorer.EXE	3404	QueryBasicInfo...	C:\Users\user\AppData\Local\Temp\I...	SUCCESS
16:47:...	Explorer.EXE	3404	CloseFile	C:\Users\user\AppData\Local\Temp\I...	SUCCESS
16:47:...	Explorer.EXE	3404	CreateFile	C:\Users\user\AppData\Local\Temp\I...	SUCCESS
16:47:...	Explorer.EXE	3404	QueryDirectory	C:\Users\user\AppData\Local\Temp\I...	SUCCESS
16:47:...	Explorer.EXE	3404	CreateFile	C:\Users\user\AppData\Local\Temp\I...	SUCCESS
16:47:...	Explorer.EXE	3404	QueryDirectory	C:\Users\user\AppData\Local\Temp\I...	SUCCESS
16:47:...	Explorer.EXE	3404	CreateFile	C:\Users\user\AppData\Local\Temp\I...	SUCCESS
16:47:...	Explorer.EXE	3404	QueryDirectory	C:\Users\user\AppData\Local\Temp\I...	SUCCESS
16:47:...	Explorer.EXE	3404	CreateFile	C:\Users\user\AppData\Local\Temp\I...	SUCCESS
16:47:...	Explorer.EXE	3404	QueryDirectory	C:\Users\user\AppData\Local\Temp\I...	SUCCESS
16:47:...	Explorer.EXE	3404	CreateFile	C:\Users\user\AppData\Local\Temp\I...	SUCCESS
16:47:...	Explorer.EXE	3404	QueryDirectory	C:\Users\user\AppData\Local\Temp\I...	SUCCESS
16:47:...	Explorer.EXE	3404	CreateFile	C:\Users\user\AppData\Local\Temp\I...	SUCCESS
16:47:...	Explorer.EXE	3404	QueryDirectory	C:\Users\user\AppData\Local\Temp\I...	SUCCESS

Detail
Length: 12
Length: 12
Length: 12
Length: 12
Length: 12
Length: 12
Length: 12
Type: REG_DWORD, Length: 4, Data: 0
Query: Handle Tags, Handle Tags: 0x0
Desired Access: Read
Query: Handle Tags, Handle Tags: 0x0
Desired Access: Read
Query: Handle Tags, Handle Tags: 0x0
Desired Access: Query Value
Offset: 530,944, Length: 15,360, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
Query: Name
Query: Handle Tags, Handle Tags: 0x0
Query: Handle Tags, Handle Tags: 0x0
Desired Access: Read
Desired Access: Read
Query: Name
Query: Handle Tags, Handle Tags: 0x0
Query: Handle Tags, Handle Tags: 0x0
Desired Access: Read
Desired Access: Read
Name: \Users\user\AppData\Local\Temp\Procmon64.exe
Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: Read, Write, Delete, AllocationSiz...
Creation Time: 08/10/2024 16:47:05, LastAccessTime: 08/10/2024 16:47:05, LastWriteTime: 08/10/2024 16:47:05, ChangeTime: 08/10/2024 1...
Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, ShareM...
FileInformationClass: FileBothDirectoryInformation, Filter: Users, 2: Users
Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, ShareM...
FileInformationClass: FileBothDirectoryInformation, Filter: user, 2: user
Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, ShareM...
FileInformationClass: FileBothDirectoryInformation, Filter: AppData, 2: AppData
Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, ShareM...
FileInformationClass: FileBothDirectoryInformation, Filter: Local, 2: Local
Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, ShareM...
FileInformationClass: FileBothDirectoryInformation, Filter: Temp, 2: Temp