

Esercizio Forense

Simulazione Esame

DOMANDE

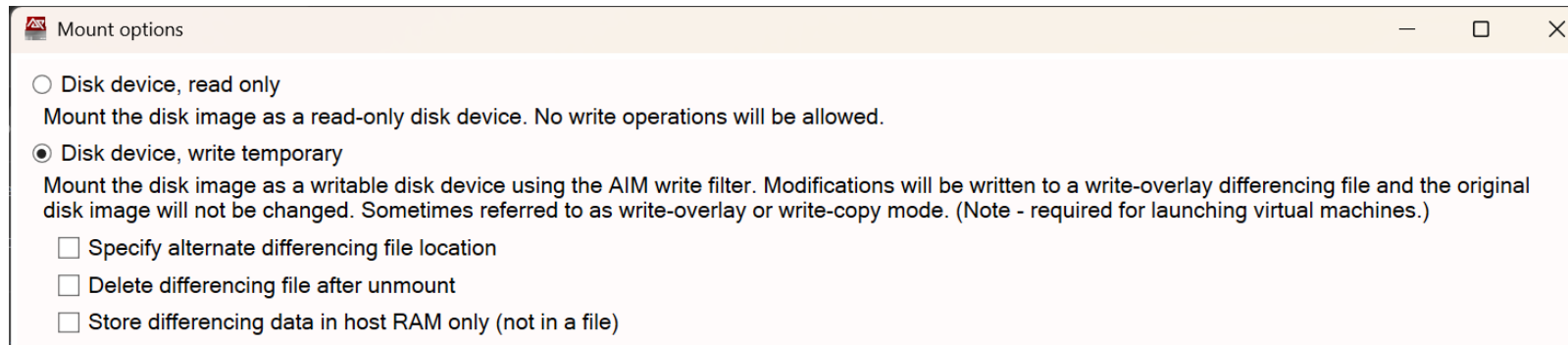
Dato il caso già indicizzato del programma Autospy chiamato PCClient, analizzarlo e rispondere ai seguenti quesiti

1. Quanti utenti ci sono nel PC
2. Qual è l'ultimo utente che ha effettuato l'accesso (Riportare la data)
3. Quale sistema operativo è in esecuzione sul PC e qual è il nome del PC
4. Quando è stato installato il S.O.
5. Sono presenti Client di Posta sul PC
6. Qual è il Timezone in uso sul PC
7. Sono stati installati programmi per catturare il traffico di rete, se si quali
8. Quante volte gli Utenti si sono loggati nel PC
9. Sono presenti email con degli allegati, elencare il nome del mittente e dell'allegato
10. Calcolare l'hash Md5 dei file allegati alle email
11. L'utente scarica l'allegato, dove è stato salvato e cosa contiene
12. Sono presenti connessioni remote al PC
13. Analizzando il PC ci sono dei processi in esecuzione sospetti, elencare quale e tutte le informazioni utili compresi eventuali connessioni.

Estrarre la VM denominata PCClient.zip ed importarla in VMWare.

NON ACCENDETELA

Aprire Arsenal Mount Image e caricare il disco che avete importato nella VM e selezione Disk device, Write temporary e cliccate su OK.



Una volta montato il disco, eseguite KAPE (eseguibile gkape) ed eseguite il triage per le analisi, prima la parte TARGET e successivamente la parte dei moduli. Per i Target e i Moduli da eseguire impostate tutto come la foto.

gkape v1.3.0.2

File Tools

☒ Use Target options

Target options

Target source:

Target destination:

☒ Flush ☐ Add %d ☐ Add %m

Targets (Double-click to edit a target)

Drag a column header here to group by that column

Selected	Name	Folder	Description
<input checked="" type="checkbox"/>	!c	!c	!c
<input checked="" type="checkbox"/>	!BasicCollection	Compound	Basic Collection
<input checked="" type="checkbox"/>	!SANS_Triage	Compound	SANS Triage Collection
<input checked="" type="checkbox"/>	KapeTriage	Compound	Kape Triage collections tha...

☒ Selected = ☐ Checked

☐ Process VSCs ☒ Deduplicate

Container: ☐ None ☒ VHDX ☐ VHD ☐ Zip

SHA-1 exclusions:

Base name:

☒ Zip container ☐ Transfer

Target variables **Transfer options**

☒ Use Module options

Module options

Module source:

Module destination:

☒ Flush ☐ Add %d ☐ Add %m ☐ Zip

Modules (Double-click to edit a module)

Drag a column header here to group by that column

Selected	Name	Folder	Category	Description
<input checked="" type="checkbox"/>	!c	!c	!c	!c
<input type="checkbox"/>	!!ToolSync	Compound	Sync	Sync for new Maps, B...
<input checked="" type="checkbox"/>	!EZParser	Compound	Modules	Eric Zimmerman Parsers
<input type="checkbox"/>	AmcacheParser	EZTools	ProgramExecution	AmcacheParser: extr...
<input type="checkbox"/>	AppCompatCacheParser	EZTools	ProgramExecution	AppCompatCachePar...
<input type="checkbox"/>	BitsParser	GitHub	GitHub	Tool to parse Window...
<input type="checkbox"/>	BMC-Tools_RDPBitmapCache...	GitHub	Remote Access	BMC-Tools: RDP Bitm...
<input type="checkbox"/>	bstrings	Compound	Modules	Run all bstrings Modul...
<input type="checkbox"/>	bstrings_AeonWallet	bstrings	KeywordSearches	Use bstrings to GREFP

Export format: ☒ Default ☐ CSV ☐ HTML ☐ JSON

Module variables:

Key:

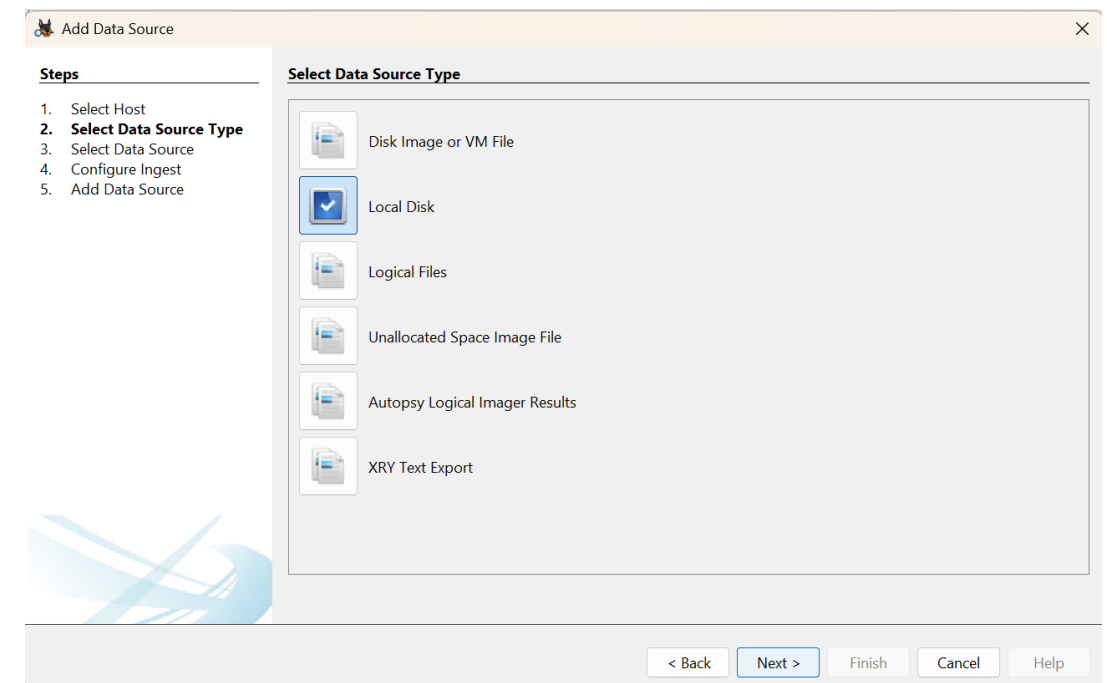
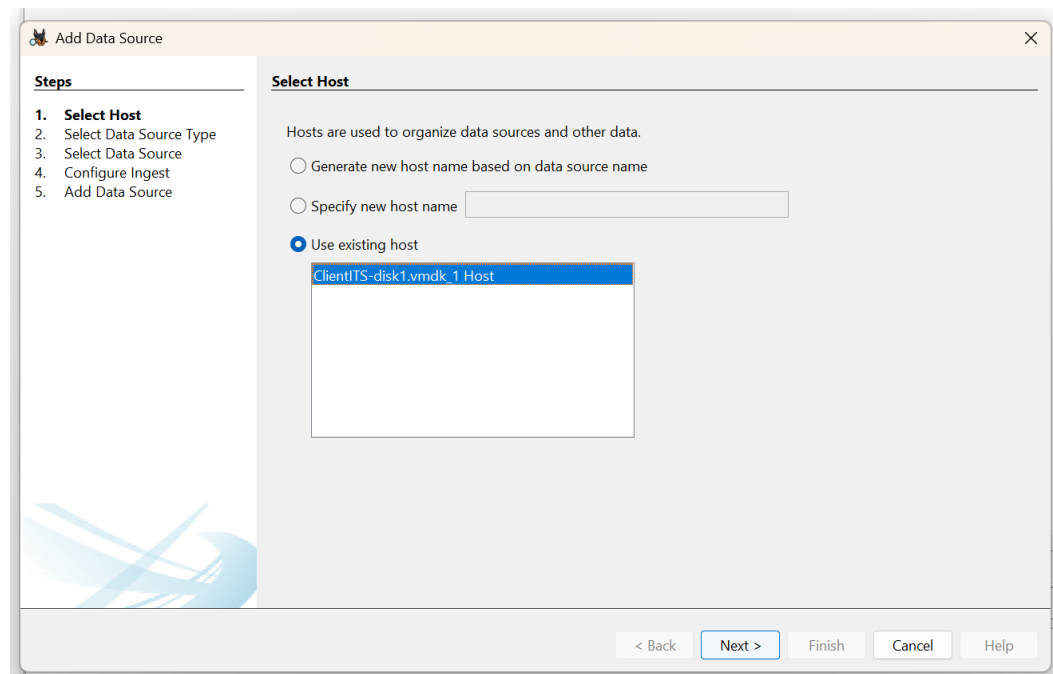
Value:

Successivamente create una cartella Autopsy Case ed estraete il contenuto dello zip denominato ClientITS.zip

Aprirete Autopsy con "esegui come **Amministratore**" e caricate il caso che è presente nella cartella Autopsy Case, vi chiederà la sorgente del disco dati cliccate **NO**.

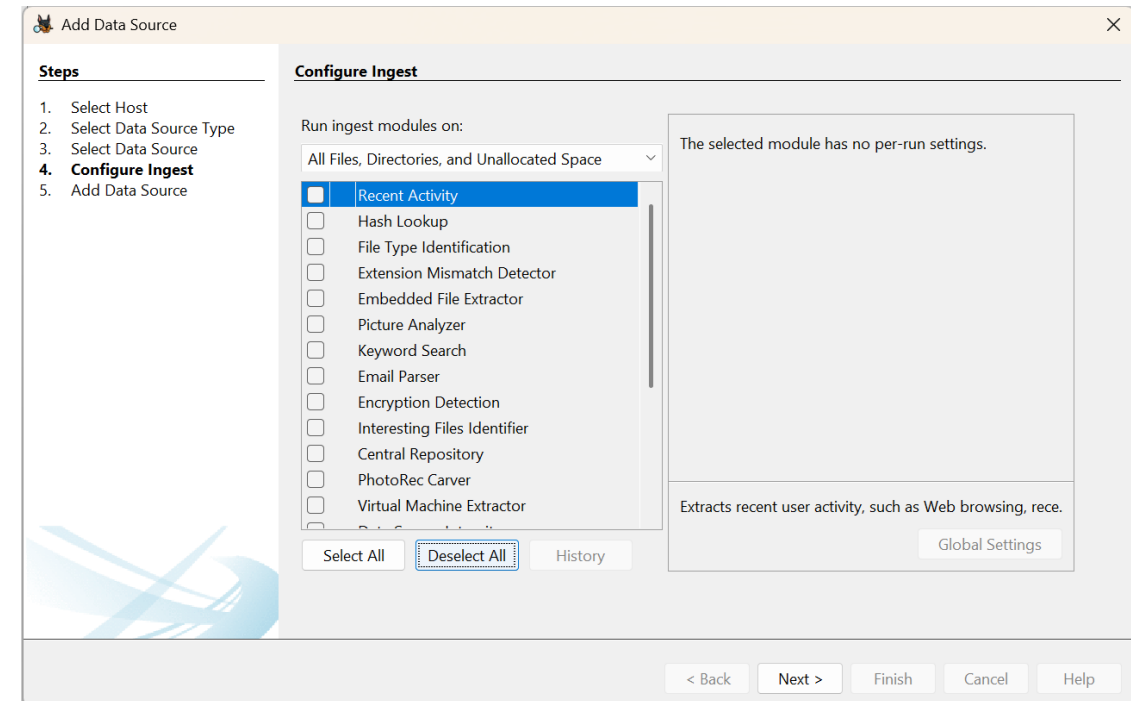
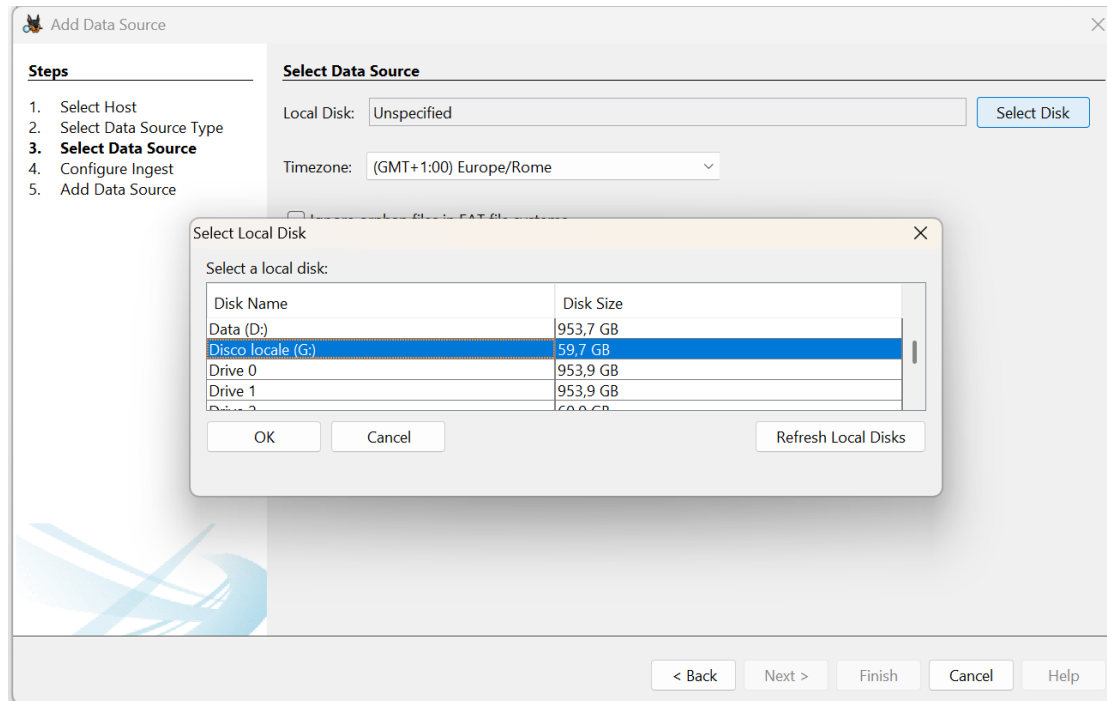
Una volta aperto Autopsy andate in Add Data Source, selezionare Use Existing Host e cliccate l'unico host presente.

Selezionate come Data Source Local disk e cliccate su Next

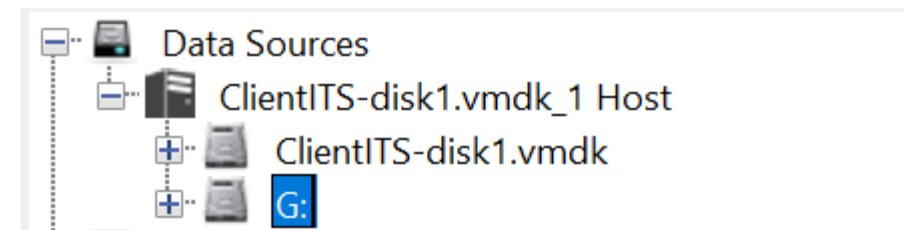


Nella schermata successiva cliccate su Local Disk si apre una finestra a tendina e selezione il disco che avete aperto precedentemente con Arsenal Mount Image, nel mio caso G: e cliccate su Next, se non avete aperto Autopsy come Amministratore non vedrete nessun disco.

In configure Ingest cliccate su Deselect All e andate avanti e appena fatto avrete il caso in Autopsy.









Se volete esportare i registri prendeteli nella source G:, i dischi sono uguali soltanto che solo G: permette l'export dei registri di Sistema.



1. Quanti utenti ci sono nel PC

Per rispondere alla domanda andare nel tab OS Accounts, da cui possiamo vedere un solo utente **Administrator** oppure nei registri estratti da KAPE nella cartella Registry, il file SAM da cui possiamo vedere che Administrator è l'unico account.

Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
 S-1-5-18				SYSTEM	ClientITS-...	Local	NT AUTHORITY	
 S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464			0		ClientITS-...	Local	NT SERVICE	
 S-1-5-21-69763590-1066019965-4026127357-500			0	Administrator	ClientITS-...	Domain		2024-11-06 15:54:16 CET
 S-1-5-20				NETWORK SERVICE	ClientITS-...	Local	NT AUTHORITY	
 S-1-5-19				LOCAL SERVICE	ClientITS-...	Local	NT AUTHORITY	
 S-1-5-21-69763590-1066019965-4026127357-501			0	Guest	ClientITS-...	Domain		2024-11-06 15:54:16 CET

```
samparse v.20220921
(SAM) Parse SAM file for user & group mbrshp info
User Information
-----
Username       : Administrator [500]
SID            : S-1-5-21-69763590-1066019965-4026127357-500
Full Name      :
User Comment   : Built-in account for administering the computer/domain
Account Type   : Default Admin User
Account Created : Wed Nov  6 14:54:16 2024 Z
Name           :
Last Login Date : Tue Nov 12 13:54:56 2024 Z
Pwd Reset Date  : Wed Nov  6 14:54:22 2024 Z
Pwd Fail Date   : Never
Login Count     : 19
```

2. Qual è l'ultimo utente che ha effettuato l'accesso (Riportare la data)

L'utente Administrator, ultimo login 12-11-2024 alle ore 13:54:56 Z

```
Last Login Date : Tue Nov 12 13:54:56 2024 Z
Pwd Reset Date  : Wed Nov 6 14:54:22 2024 Z
Pwd Fail Date   : Never
Login Count     : 19
```

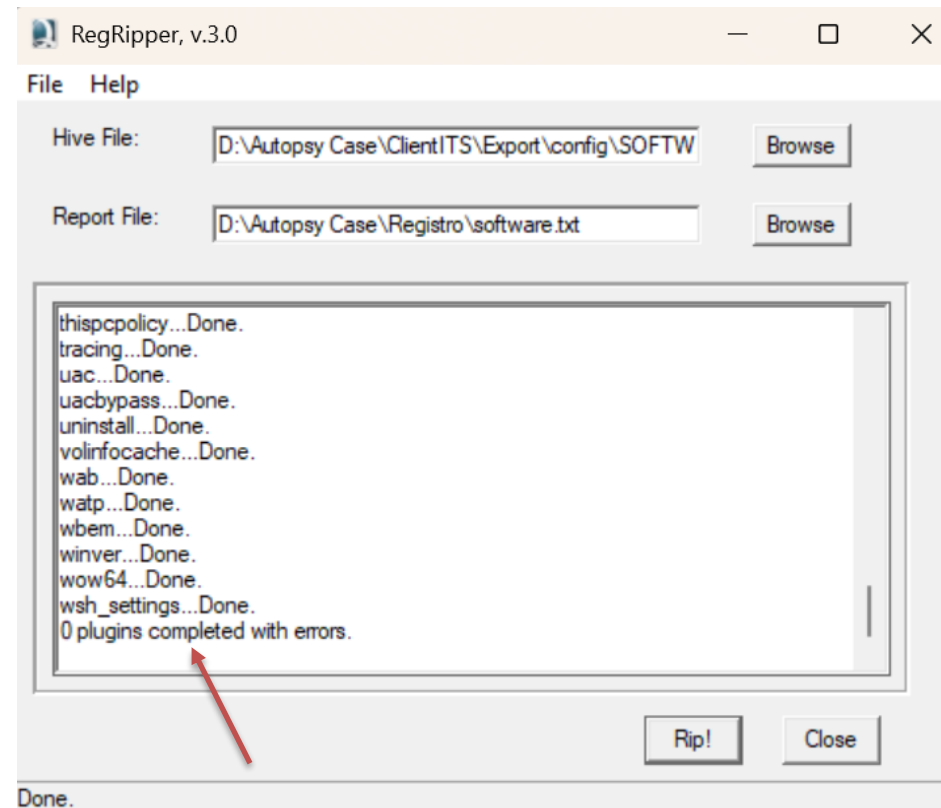
La risposta si trova nel registro Sam

Per rispondere alla domanda esportate i registri di sistema che sono in C:\Windows\System32\config e processateli con il programma RegRipper 3.0 che trovate nella cartella Tools lanciando il programma **rr.exe**

In Hive file mettete il registro, in questo caso SOFTWARE e in report mette il nome del registro corrispondete in questo caso software.txt, cliccate su Rip! ed il programma decodificherà il registro che possiamo aprire con un editor di testo.

Fate questa operazione per tutti i registri che vi occorrono

IMPORTANTE ricordatevi che i timestamp nei registri sono tutti in **UTC**, invece se li prendete da Autopsy li riporta nel fuso orario impostato nel caso.




Quando vedete la scritta completed, allora il programma ha terminato e potete passare al registro successivo

3. Quale sistema operativo è in esecuzione sul PC e qual è il nome del PC

Il S.O. è Windows Server 2012 R2 Standard Evaluation e il nome del PC è WIN-99KA9GD0I0G

Nel tab Operating System Information di Autopsy c'è la risposta

Source Name	S	C	O	Name	Program Name	Processor Architecture	Temporary Files Directory	Path
 ClientITS-disk1.vmdk				WIN-99KA9GD0I0G	Windows Server 2012 R2 Standard Evaluation	AMD64	%SystemRoot%\TEMP	C:\Windows

*Oppure vediamo i registri estratti da KAPE, nel registro SOFTWARE cerchiamo il plugin **winver**, per il nome del pc nel registro SYSTEM cerchiamo il plugin **compname***

```
winver v.20200525
(Software) Get Windows version & build info
ProductName      Windows Server 2012 R2 Standard Evaluation
BuildLab         9600.winblue_gdr.140221-1952
BuildLabEx       9600.17031.amd64fre.winblue_gdr.140221-1952
RegisteredOrganization
RegisteredOwner  Windows User
InstallDate      2024-11-06 14:54:23Z
```

Registro Software

```
compname v.20090727
(System) Gets ComputerName and Hostname values from System hive
ComputerName     = WIN-99KA9GD0I0G
TCP/IP Hostname  = WIN-99KA9GD0I0G
```

Registro System



4. Quando è stato installato il S.O.
Il S.O. installato il 06-11-2024
La risposta si trova nel registro SOFTWARE
*Sempre cercando il plugin **winver***

```
winver v.20200525
(Software) Get Windows version & build info
ProductName           Windows Server 2012 R2 Standard Evaluation
BuildLab              9600.winblue_gdr.140221-1952
BuildLabEx            9600.17031.amd64fre.winblue_gdr.140221-1952
RegisteredOrganization
RegisteredOwner       Windows User
InstallDate           2024-11-06 14:54:23Z
```

5. Sono presenti Client di Posta sul PC
Si è presente Mozilla Thunderbird
*La risposta si trova nel tab Installed Programs di Autopsy, ma potete vedere le applicazioni installate sul pc, cercando nel registro SOFTWARE il plugin **apppaths***

Source Name	S	C	O	Program Name	Date/Time	Data Source
SOFTWARE			0	7-Zip 23.01 (x64) v.23.01	2024-11-07 09:19:17 CET	ClientITS-disk1.vmdk
SOFTWARE			0	Mozilla Thunderbird (x64 it) v.115.16.2	2024-11-06 15:07:28 CET	ClientITS-disk1.vmdk
SOFTWARE			0	Mozilla Maintenance Service v.115.16.2	2024-11-06 15:07:28 CET	ClientITS-disk1.vmdk
SOFTWARE			0	VMware Tools 4.0.15.0370705	2024-11-06 15:07:28 CET	ClientITS-disk1.vmdk

```
apppaths v.20200511
(NTUSER.DAT,Software) Gets content of App Paths subkeys
2024-11-07 09:19:17Z
7zFM.exe - C:\Program Files\7-Zip\7zFM.exe
2024-11-06 15:07:28Z
thunderbird.exe - C:\Program Files\Mozilla Thunderbird\thunderbird.exe
```

7. Sono stati installati programmi per catturare il traffico di rete, se si quali

Si risulta installato il programma Wireshark

*La risposta si trova nel tab Installed Programs di Autopsy, ma potete vedere le applicazioni installate sul pc, cercando nel registro SOFTWARE il plugin **apppaths***

SOFTWARE	0	WIC	2013-08-22 14:48:11 CEST	ClientITS-disk1.vmdk
SOFTWARE	0	Microsoft Edge Update v.1.3.195.35	2024-11-12 13:07:20 CET	ClientITS-disk1.vmdk
SOFTWARE	0	Wireshark 4.0.16 64-bit v.4.0.16	2024-11-06 15:00:31 CET	ClientITS-disk1.vmdk
SOFTWARE	0	Npcap v.1.71	2024-11-06 15:00:25 CET	ClientITS-disk1.vmdk
SOFTWARE	0	Microsoft Visual C++ 2015-2022 Redistributable (x64) ...	2024-11-06 15:00:15 CET	ClientITS-disk1.vmdk

```
apppaths v.20200511
(NTUSER.DAT,Software) Gets content of App Paths subkeys
2024-11-07 09:19:17Z
  7zFM.exe - C:\Program Files\7-Zip\7zFM.exe
2024-11-06 15:07:28Z
  thunderbird.exe - C:\Program Files\Mozilla Thunderbird\thunderbird.exe
2024-11-06 15:00:28Z
  Wireshark.exe - C:\Program Files\Wireshark\Wireshark.exe
```

8. Quante volte gli Utenti si sono loggati nel PC



Utente Administrator si è loggato 19 volte

La risposta si trova nel registro SAM

```
Last Login Date : Tue Nov 12 13:54:56 2024 Z
Pwd Reset Date  : Wed Nov 6 14:54:22 2024 Z
Pwd Fail Date   : Never
Login Count     : 19
```

9. Sono presenti email con degli allegati, elencare il nome del mittente e dell'allegato
E' presente una sola email con allegato proveniente da attacker@malicious.com e il nome dell'allegato è Document_Confidential.zip

Nel tab E-mail messages di Autopsy troviamo la risposta, la potevate trovare anche nel registro NTUSER ma in quel caso dovevate estrarre l'email e controllare il contenuto, da Autopsy è più semplice.

Source Name	S	C	O	E-Mail From	E-Mail To	Message (Plaintext)	Message ID	Has Attachments
 Mail.eml				attacker@malicious.com;	mario.rossi@prova.com;	Dear Mario Rossi,We have identified a critical issue wit...	Not available	Yes
 Mail.eml				attacker@malicious.com;	mario.rossi@prova.com;	Dear Mario Rossi,We have identified a critical issue wit...	Not available	Yes

Headers

Text

HTML

RTF


Attachments (1)

Accounts

Table

Thumbnail

Summary

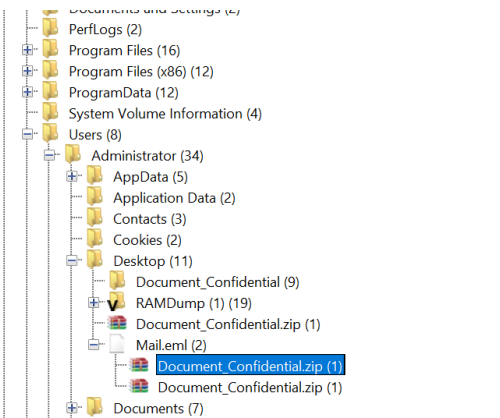
Location	Size	Mime type	Known
 /img_ClientITS-disk1.vmdk/vol_vol3/Users/Administrator/Desktop/Mail.eml/Document_Confidential.zip	1216574	application/zip	unknown

10. Calcolare l'hash Md5 dei file allegati alle email
- Il file allegato all'email è Document_Confidential.zip avente hash MD5*
- Document_Confidential.zip 595522000a4ad998815c05f764b702c1*

Se cliccate sull'email vi riporta all'email dal quale potete vedere l'hash MD5 dell'allegato

Location	MD5 Hash
/img_ClientITS-disk1.vmdk/vol_vol3/Users/Administrator/Desktop/Mail.eml/Document_Confidential.zip	595522000a4ad998815c05f764b702c1
/img_ClientITS-disk1.vmdk/vol_vol3/Users/Administrator/Desktop/Mail.eml/Document_Confidential.zip	595522000a4ad998815c05f764b702c1

11. L'utente scarica l'email e l'allegato, dove sono stati salvati e cosa contiene il contenuto dell'allegato
- L'allegato e l'email sono stati salvati nel Desktop e l'allegato Document_Confidential.zip contiene all'interno un file denominato Document.exe*



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
Document.exe			0	2024-11-06 15:12:15 CET	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	3266048	Allocated

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Result: of Result < >

12. Sono presenti connessioni remote al PC

*Analizzando gli eventi di sistema, non sono presenti connessioni remote, per cercare connessioni remote dobbiamo guardare gli Event Log estratti da KAPE e nello specifico quelli presenti nella cartella EventLogs, nel file *****EvtxECmd_Output.csv. Aprite il file tramite il tool Timeline Explorer e cercate tutti gli eventi **1149** (campo Event Id) che è l'evento che ci dice se ci sono state connessioni remote tramite il software Remote Desktop di Windows.*

IMPORTANTE

Negli eventi se cercate la parola RDP troverete sicuramente qualcosa soprattutto nei pc Server, quindi per evitare falsi positivi come in questo caso cercate solamente l'event ID 1149

Timeline Explorer v2.0.0.1									
File Tools Tabs View Help									
20241115154557_EvtxECmd_Output.csv									
Map Description ▲									
Line	Tag	Time Created	Record Number	Event Record Id	Event Id ▼	Level	Provider	Channel	
▼ =	<input type="checkbox"/>	=	=	=	=	Info	Microsoft-Windows-Termina...	Microsoft-Windows-Termin...	
▼ Map Description: RDP Begin session arbitration (Count: 7)									
1611	<input type="checkbox"/>	2024-11-12 13:54:56	128	128	41	Info	Microsoft-Windows-Termina...	Microsoft-Windows-Termin...	
1604	<input type="checkbox"/>	2024-11-12 13:28:16	121	121	41	Info	Microsoft-Windows-Termina...	Microsoft-Windows-Termin...	
1597	<input type="checkbox"/>	2024-11-12 13:18:25	114	114	41	Info	Microsoft-Windows-Termina...	Microsoft-Windows-Termin...	
1592	<input type="checkbox"/>	2024-11-12 13:13:02	109	109	41	Info	Microsoft-Windows-Termina...	Microsoft-Windows-Termin...	
1587	<input type="checkbox"/>	2024-11-12 12:56:23	104	104	41	Info	Microsoft-Windows-Termina...	Microsoft-Windows-Termin...	
1580	<input type="checkbox"/>	2024-11-08 08:17:59	97	97	41	Info	Microsoft-Windows-Termina...	Microsoft-Windows-Termin...	
1573	<input type="checkbox"/>	2024-11-07 13:23:36	90	90	41	Info	Microsoft-Windows-Termina...	Microsoft-Windows-Termin...	

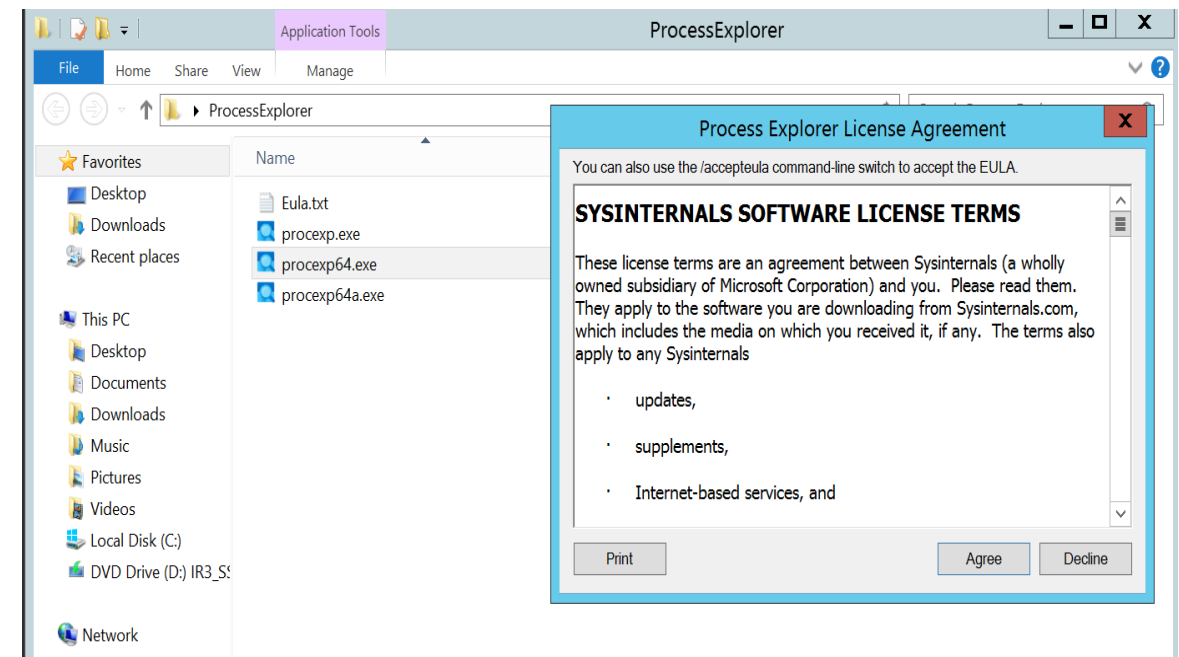
13. Analizzando il PC ci sono dei processi in esecuzione sospetti, elencare quale e tutte le informazioni utili compresi eventuali connessioni.

Per rispondere a questa domanda dobbiamo accendere la macchina virtuale e chiudere il programma **Arsenal Image Mounter**. La password della VM è **123try456**.

Installiamo due tools che ci servono per l'esercizio si tratta dei programmi **Autoruns** e **Process Explorer** che si trovano nella cartella Tools che vi abbiamo fornito.

Il primo programma da utilizzare sarà Process Explorer per vedere i processi in esecuzione.

Estraete il programma e cliccate su procexp64.exe e cliccate su Agree



Ci troviamo in questa schermata che ci da tutte le informazioni sui processi in esecuzione, in questo caso, troviamo un processo sospetto chiamato **Document.exe** con PID 684, descrizione del processo nome "Client" e company name "Xeno". Se clicchiamo sul processo sospetto si apre un'ulteriore finestra, dove possiamo vedere ulteriori informazioni interessanti sul processo.

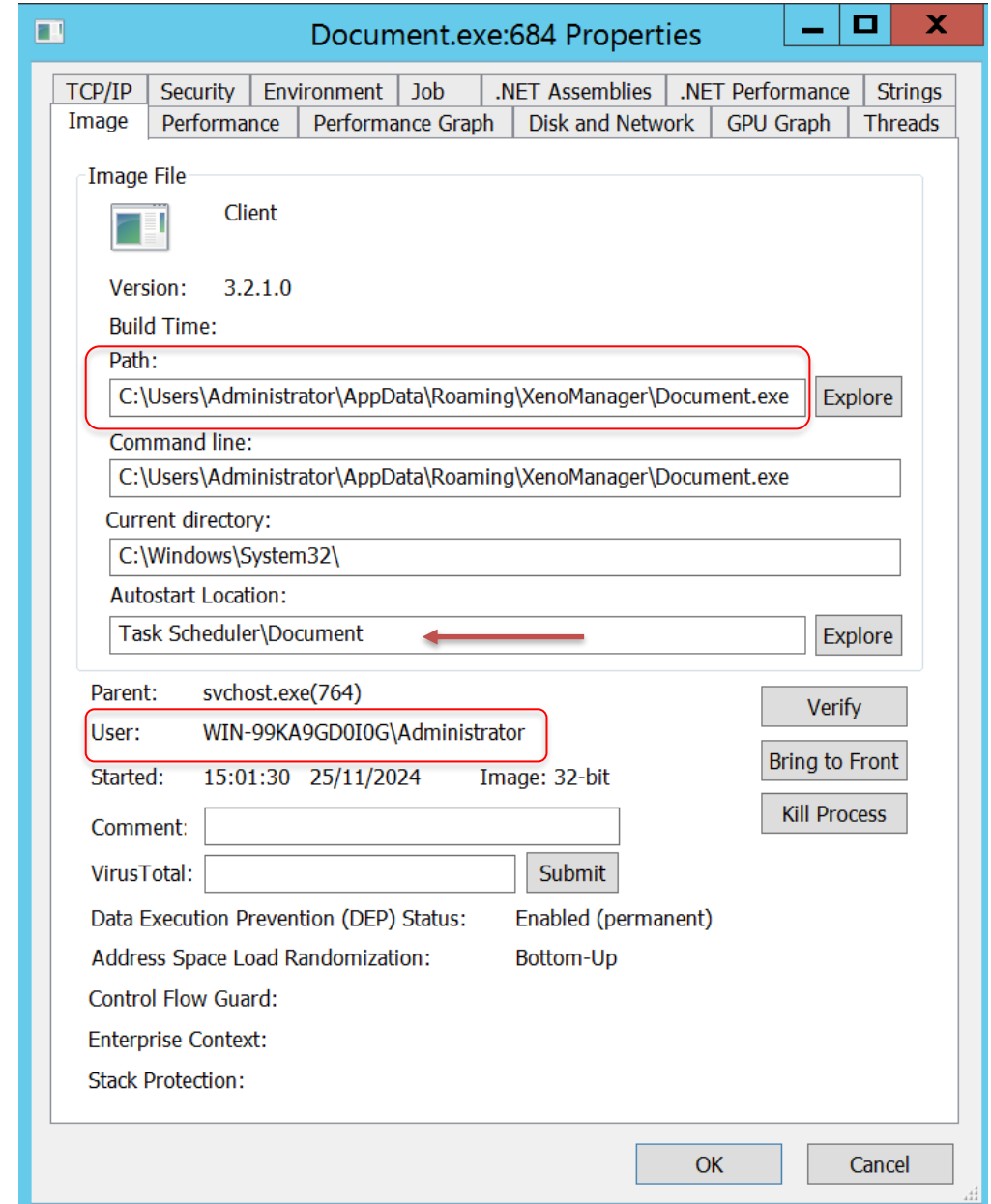
Il processo viene lanciato da svchost.exe che è un processo lecito di Windows progettato per eseguire e gestire servizi di sistema. Ogni istanza di svchost.exe può ospitare diversi servizi ed è utilizzato dai malware perché Svchost.exe viene eseguito con privilegi di sistema, il che significa che i malware che si infiltrano in questo processo possono ottenere accesso completo al sistema operativo.

Process Explorer - Sysinternals: www.sysinternals.com [WIN-99KA9GD0I0G]

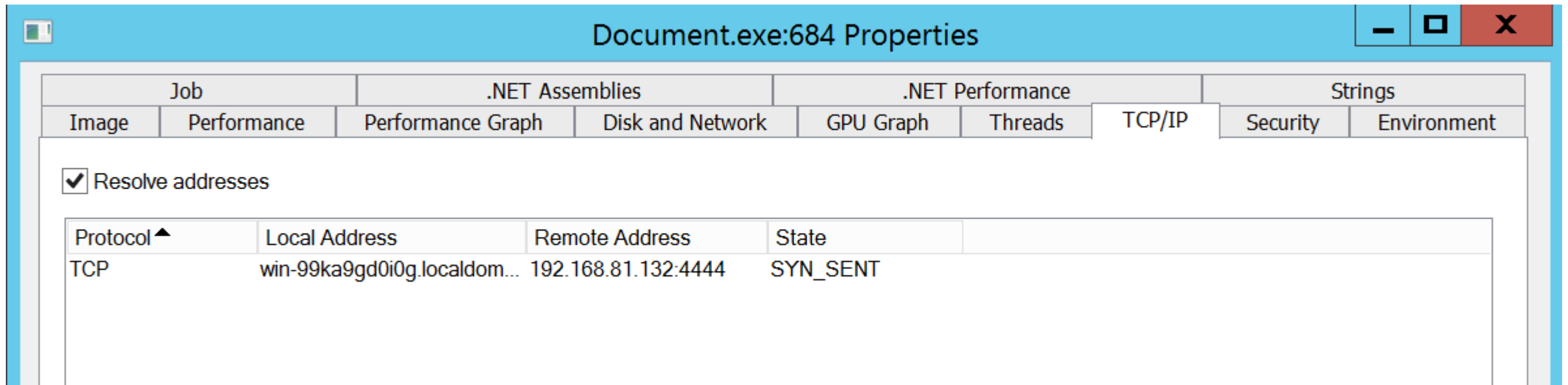
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	16.93	0 K	4 K	0		
System	< 0.01	108 K	276 K	4		
Interrupts	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		288 K	1.064 K	232		
csrss.exe		1.688 K	3.764 K	320		
wininit.exe		668 K	3.576 K	412	Windows Start-Up Application	Microsoft Corporation
services.exe		2.140 K	5.516 K	512		
svchost.exe		4.860 K	10.288 K	580	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe		10.256 K	18.752 K	1912	WMI Provider Host	Microsoft Corporation
WmiPrvSE.exe		15.964 K	22.016 K	2028	WMI Provider Host	Microsoft Corporation
TiWorker.exe		49.948 K	45.804 K	2400	Windows Modules Installer W...	Microsoft Corporation
svchost.exe		2.964 K	7.168 K	608	Host Process for Windows S...	Microsoft Corporation
svchost.exe		14.568 K	17.144 K	708	Host Process for Windows S...	Microsoft Corporation
svchost.exe		25.384 K	35.584 K	764	Host Process for Windows S...	Microsoft Corporation
Document.exe		11.572 K	3.920 K	684	Client	Xeno
taskhost.exe		1.528 K	5.944 K	3056	Host Process for Windows Ta...	Microsoft Corporation
taskhost.exe		1.296 K	4.492 K	2316	Host Process for Windows Ta...	Microsoft Corporation
taskhost.exe		12.248 K	11.636 K	2712	Host Process for Windows Ta...	Microsoft Corporation
taskeng.exe		984 K	4.288 K	2796	Task Scheduler Engine	Microsoft Corporation
svchost.exe		5.436 K	11.056 K	808	Host Process for Windows S...	Microsoft Corporation
svchost.exe		6.640 K	15.636 K	868	Host Process for Windows S...	Microsoft Corporation
svchost.exe		8.356 K	10.288 K	1004	Host Process for Windows S...	Microsoft Corporation
spoolsv.exe		2.952 K	8.848 K	592	Spooler SubSystem App	Microsoft Corporation
svchost.exe		7.776 K	10.560 K	916	Host Process for Windows S...	Microsoft Corporation
VGAAuthService.exe		1.992 K	8.252 K	1032	VMware Guest Authenticatio...	VMware, Inc.
vm3dservice.exe	< 0.01	1.128 K	3.888 K	1076	VMware SVGA Helper Service	VMware, Inc.
vm3dservice.exe	< 0.01	1.228 K	4.456 K	1112	VMware SVGA Helper Service	VMware, Inc.
vmtoolsd.exe	< 0.01	8.252 K	17.000 K	1096	VMware Tools Core Service	VMware, Inc.
wlms.exe		468 K	2.604 K	1164	Windows License Monitoring ...	Microsoft Corporation
svchost.exe		988 K	4.296 K	1576	Host Process for Windows S...	Microsoft Corporation
dllhost.exe		3.108 K	9.896 K	1672	COM Surrogate	Microsoft Corporation
msdtc.exe		2.228 K	6.620 K	1800	Microsoft Distributed Transac...	Microsoft Corporation
TrustedInstaller.exe		1.356 K	4.648 K	1140	Windows Modules Installer	Microsoft Corporation
svchost.exe		492 K	2.556 K	1964	Host Process for Windows S...	Microsoft Corporation
lsass.exe		3.584 K	9.152 K	524	Local Security Authority Proc...	Microsoft Corporation
csrss.exe	< 0.01	1.944 K	39.180 K	420		
winlogon.exe		1.708 K	7.672 K	456	Windows Logon Application	Microsoft Corporation
dwm.exe	< 0.01	50.624 K	87.476 K	696	Desktop Window Manager	Microsoft Corporation
explorer.exe	< 0.01	35.904 K	94.068 K	1052	Windows Explorer	Microsoft Corporation
vmtoolsd.exe	< 0.01	15.460 K	26.004 K	2536	VMware Tools Core Service	VMware, Inc.
procexp64.exe	< 0.01	19.388 K	43.668 K	2260	Sysinternals Process Explorer	Sysinternals - www.sysinter...

Da questa nuova finestra possiamo vedere che il processo è stato lanciato dall'utente Administrator, il path ci dice dov'è il programma legato al processo e se parte in automatico, in questo caso si vede il tab "Autostart Location".

Ci sono ulteriori tab interessanti, quello più importante è il tab TCP/IP per vedere se il processo comunica con eventuali pc in rete o su internet



Nel Tab TCP/IP vediamo che il processo tenta di comunicare "SYN_SENT" con un pc remoto attestato sull'indirizzo 192.168.81.132 sulla porta 4444



Document.exe:684 Properties

Job		.NET Assemblies		.NET Performance			Strings	
Image	Performance	Performance Graph	Disk and Network	GPU Graph	Threads	TCP/IP	Security	Environment
<input checked="" type="checkbox"/> Resolve addresses								
Protocol ▲	Local Address	Remote Address	State					
TCP	win-99ka9gd0i0g.localdom...	192.168.81.132:4444	SYN_SENT					

Con il programma Autoruns possiamo vedere se il processo sospetto si garantisce la persistenza, inserendo nello Scheduled Tasks un job che gli permette di riavviarsi ogni volta che la macchina si riavvia.

Autoruns - Sysinternals: www.sysinternals.com (Administrator) [WIN-99KA9GD010G\Administrator]						
File Search Entry User Options Category Help						
Quick Filter						
Print Monitors LSA Providers Network Providers WMI Office						
Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute Image Hijacks Applnit Known DLLs Winlogon Winsock Providers						
Autoruns Entry	Description	Publisher	Image Path	Timestamp	Virus Total	
HKLM\Software\Classes\Folder\ShellEx\ContextMenuHandlers				Thu Nov 7 10:19:17 2024		
<input checked="" type="checkbox"/> 7-Zip	7-Zip Shell Extension	(Not Verified) Igor Pav...	C:\Program Files\7-Zip\7-zip.dll	Tue Jun 20 10:00:00 2023		
Internet Explorer						
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects				Wed Nov 6 15:59:05 2024		
<input checked="" type="checkbox"/> IEToEdge BHO	IEToEdge BHO	(Verified) Microsoft C...	C:\Program Files (x86)\Microsoft\Edge\Application\109.0.1518.140\BHO\ie...	Thu Sep 14 11:39:20 2023		
HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects				Wed Nov 6 15:59:05 2024		
<input checked="" type="checkbox"/> IEToEdge BHO	IEToEdge BHO	(Verified) Microsoft C...	C:\Program Files (x86)\Microsoft\Edge\Application\109.0.1518.140\BHO\ie...	Thu Sep 14 11:39:08 2023		
Scheduled Tasks						
Task Scheduler						
<input checked="" type="checkbox"/> \Document	Client	(Not Verified) Xeno	C:\Users\Administrator\AppData\Roaming\XenoManager\Document.exe	Tue Nov 12 15:08:02 2024		
<input checked="" type="checkbox"/> \Microsoft\Windows\Server Manager\Cl...	Microsoft ® Console Base...	(Verified) Microsoft W...	C:\Windows\system32\cscrip.exe	Fri Mar 21 19:49:12 2014		
<input type="checkbox"/> \Microsoft\Windows\Software Inventory...	Microsoft ® Console Base...	(Verified) Microsoft W...	C:\Windows\system32\cscrip.exe	Fri Mar 21 19:49:12 2014		
<input type="checkbox"/> \Microsoft\Windows\WS\License Validati...	Windows Store License Ver...	(Verified) Microsoft W...	C:\Windows\system32\rundll32.exe	Thu Aug 22 13:03:41 2013		
<input checked="" type="checkbox"/> \MicrosoftEdgeUpdateTaskMachineCore[...	Mantiene aggiornato il soft...	(Verified) Microsoft C...	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	Wed Nov 6 15:58:57 2024		
<input checked="" type="checkbox"/> \MicrosoftEdgeUpdateTaskMachineUA[D...	Mantiene aggiornato il soft...	(Verified) Microsoft C...	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	Wed Nov 6 15:58:57 2024		
<input checked="" type="checkbox"/> \npcapwatchdog	Ensure Npcap service is co...	(Not Verified)	C:\Program Files\Npcap\CheckStatus.bat	Thu Aug 18 19:49:28 2022		
<input checked="" type="checkbox"/> \Quasar Client Startup			File not found: C:\Users\Administrator\AppData\Roaming\SubDir\Client.exe			
Services						
HKLM\System\CurrentControlSet\Services				Mon Nov 25 15:07:07 2024		
<input checked="" type="checkbox"/> edgeupdate	Servizio Aggiornamento M...	(Verified) Microsoft C...	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	Wed Nov 6 15:58:57 2024		
<input checked="" type="checkbox"/> edgeupdateam	Servizio Aggiornamento M...	(Verified) Microsoft C...	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	Wed Nov 6 15:58:57 2024		
<input checked="" type="checkbox"/> MicrosoftEdgeElevationService	Microsoft Edge Elevation S...	(Verified) Microsoft C...	C:\Program Files (x86)\Microsoft\Edge\Application\109.0.1518.140\elevati...	Thu Sep 14 11:39:31 2023		
<input checked="" type="checkbox"/> MozillaMaintenance	Mozilla Maintenance Servic...	(Verified) Mozilla Corp...	C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe	Thu Oct 17 07:07:35 2024		
<input type="checkbox"/> NetTcpPortSharing	Net.Tcp Port Sharing Serv...	(Verified) Microsoft C...	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMsvHost.exe	Thu Nov 7 12:28:38 2024		
<input checked="" type="checkbox"/> VgAuthService	VMware Alias Manager and...	(Verified) Broadcom Inc	C:\Program Files\VMware\VMware Tools\VMware VgAuthService.e...	Thu May 2 03:29:06 2024		
<input checked="" type="checkbox"/> VMTTools	VMware Tools: Provides su...	(Verified) Broadcom Inc	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	Thu May 2 04:07:06 2024		
Drivers						
HKLM\System\CurrentControlSet\Services				Mon Nov 25 15:07:07 2024		
<input checked="" type="checkbox"/> cht4vbd	Chelsio T4 Virtual Bus Drive...	(Not Verified) Chelsio ...	C:\Windows\System32\drivers\cht4vx64.sys	Tue Jun 18 16:45:17 2013		
<input checked="" type="checkbox"/> iaStorAV	Intel(R) SATA RAID Control...	(Verified) Intel Corpor...	C:\Windows\System32\drivers\iaStorAV.sys	Sat Aug 10 02:39:30 2013		
<input checked="" type="checkbox"/> npcap	Npcap Packet Driver (NPCA...	(Verified) Insecure.Co...	C:\Windows\system32\DRIVERS\npcap.sys	Fri Aug 19 21:09:22 2022		
Codecs						
Boot Execute						

Nello scheduled task è presente un task denominato Document pubblicato da un ente non verificato di nome Xeno che richiama un file al percorso C:\Users\Administrator\AppData\Roaming\XenoManager\Document.exe creato in data 12/11/24 alle ore 15:08.

Sempre nello scheduled task è presente un task denominato Quasar Client Startup che richiama un file non più presente al percorso C:\Users\Administrator\AppData\Roaming\SubDir\Client.exe

Tutti e due i processi risultano sospetti