

Windows Memory Dump

Windows Memory Dump

Windows Memory

Our friend fell victim to a suspicious crack tool. But it seems it didn't go in the right path so investigate it to find any evidence.

Top 10 Scoreboard - Windows Memory Dump

Rank	User	Country	Completion date
1	 Melfice60		10:07 AM 03 Jan 2024
2	 abdul.jadid		03:17 PM 03 Jan 2024
3	 jad		02:46 PM 22 Jan 2024
4	 ramirezs4		07:46 PM 07 Feb 2024

Volatility - CheatSheet.....	3
Búsqueda	3
Nota	11
¿Cuántos usuarios hay en la máquina?	11
¿Qué usuario es el infectado?	11
¿Qué archivo obtuvo el ransomware?.....	11
¿Cómo ese archivo descargo el ransomware [URL]?	11
¿Cuál es la direccion offset de ese ransomware?.....	11
El ransomware editó una de las claves de registro del administrador de hash principal. Busque la clave que se modificó.	11
¿Cuál es la credencial del AdminRecovery?	11

Volatility - CheatSheet

<https://book.hacktricks.xyz/generic-methodologies-and-resources/basic-forensic-methodology/memory-dump-analysis/volatility-cheatsheet>

Búsqueda

Volatility3 tiene diferentes complementos que permiten el análisis de los procesos activos, usaremos varias para ver algunas diferencias.

Nota: Se fijarán que al usar un complemento de volatily3 usare ">" para crear un documento de texto con la salida del complemento, de esta forma nos ahorramos tener que ejecutar y esperar que procese la información nuevamente, también nos permite realizar búsquedas de forma más rápido.

Iniciamos viendo los procesos activos en el equipo:

1) Pstree

El comando quedaría así

```
python3 /root/Desktop/volatility3/vol.py -f vLP.vmem windows.pstree > pstree.txt
```

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime
4	0	System	0xe4870649d040	138	-	N/A	False	2023-08-16 11:21:05.000000	N/A
* 1224	4	MemCompression	0xe48706add8800	82	-	N/A	False	2023-08-16 11:21:39.000000	N/A
* 92	4	Registry	0xe487064e8800	4	-	N/A	False	2023-08-16 11:20:48.000000	N/A
* 324	4	smss.exe	0xe487060e2040	2	-	N/A	False	2023-08-16 11:21:05.000000	N/A
6772	6728	csrss.exe	0xe48706c2a040	10	-	2	False	2023-08-16 11:24:12.000000	N/A
7280	6728	winlogon.exe	0xe48706c35000	3	-	2	False	2023-08-16 11:24:12.000000	N/A
* 2084	7280	fontdrvhost.exe	0xe4870605f5140	5	-	2	False	2023-08-16 11:24:13.000000	N/A
* 6540	7280	dwm.exe	0xe48706d19a000	15	-	2	False	2023-08-16 11:24:12.000000	N/A
* 6940	7280	LogonUI.exe	0xe48706b49e340	8	-	2	False	2023-08-16 11:26:06.000000	N/A
* 6596	7280	userinit.exe	0xe48706e47c300	0	-	2	False	2023-08-16 11:24:20.000000	2023-08-16 11:24:53.000000
** 2844	6596	explorer.exe	0xe48706e470000	58	-	2	False	2023-08-16 11:24:20.000000	N/A
*** 8844	2844	SecurityHealth	0xe48706d7df000	2	-	2	False	2023-08-16 11:24:48.000000	N/A
5704	7724	msedge.exe	0xe48706d03000	0	-	2	False	2023-08-16 11:24:27.000000	2023-08-16 11:24:28.000000
7012	8280	msiexec.exe	0xe48706d1a0000	24	-	2	True	2023-08-16 11:25:46.000000	N/A
3104	2152	csrss.exe	0xe48706b50c340	9	-	4	False	2023-08-16 11:26:06.000000	N/A
3816	2152	winlogon.exe	0xe48706c26000	5	-	4	False	2023-08-16 11:26:06.000000	N/A
* 4728	3816	fontdrvhost.exe	0xe48706b0e000	5	-	4	False	2023-08-16 11:26:07.000000	N/A
* 6580	3816	dwm.exe	0xe48706b69000	15	-	4	False	2023-08-16 11:26:07.000000	N/A
* 8668	3816	LogonUI.exe	0xe48706eb6e2c0	6	-	4	False	2023-08-16 11:26:27.000000	N/A
* 3196	3816	userinit.exe	0xe48706c2000	0	-	4	False	2023-08-16 11:26:09.000000	2023-08-16 11:26:36.000000
** 4104	3196	explorer.exe	0xe48706baf1000	1	-	4	False	2023-08-16 11:26:09.000000	N/A
*** 424	4104	SecurityHealth	0xe48706bf1b2c0	1	-	4	False	2023-08-16 11:26:28.000000	N/A
**** 440	424	csrss.exe	0xe487069683140	10	-	0	False	2023-08-16 11:21:23.000000	N/A
**** 516	424	wininit.exe	0xe48706a5cb000	1	-	0	False	2023-08-16 11:21:25.000000	N/A
**** 648	516	services.exe	0xe48706a5c1000	8	-	0	False	2023-08-16 11:21:26.000000	N/A
***** 772	648	svchost.exe	0xe48706999d240	13	-	0	False	2023-08-16 11:21:32.000000	N/A
***** 1152	772	StartMenuExper	0xe48706c51d000	26	-	4	False	2023-08-16 11:26:15.000000	N/A
***** 8968	772	TextInputHost	0xe48706dd5c000	11	-	2	False	2023-08-16 11:24:38.000000	N/A
***** 11528	772	StartMenuExper	0xe48706fb88000	9	-	6	False	2023-08-16 11:32:04.000000	N/A
***** 3468	772	dllhost.exe	0xe48706ecc32c0	6	-	4	False	2023-08-16 11:26:12.000000	N/A
***** 10764	772	dllhost.exe	0xe48706f00000	2	-	6	False	2023-08-16 11:27:58.000000	N/A
***** 8208	772	SearchApp.exe	0xe48706d7d9300	24	-	4	False	2023-08-16 11:26:16.000000	N/A
***** 9184	772	RuntimeBroker	0xe48710693000	5	-	6	False	2023-08-16 11:27:34.000000	N/A
***** 4636	772	RuntimeBroker	0xe48706e93c200	7	-	2	False	2023-08-16 11:24:33.000000	N/A
***** 2592	772	dllhost.exe	0xe48706e0e000	6	-	6	False	2023-08-16 11:25:05.000000	N/A
***** 8484	772	dllhost.exe	0xe48706dd0f000	5	-	5	False	2023-08-16 11:26:33.000000	N/A
***** 5928	772	dllhost.exe	0xe48706d932c0	3	-	2	False	2023-08-16 11:24:59.000000	N/A
***** 7208	772	TextInputHost	0xe48706fe25240	11	-	5	False	2023-08-16 11:26:55.000000	N/A
***** 5420	772	WmiPrvSE.exe	0xe48706c50e280	6	-	0	False	2023-08-16 11:22:12.000000	N/A
***** 5048	772	RuntimeBroker	0xe48706e94f280	1	-	2	False	2023-08-16 11:24:44.000000	N/A
***** 10168	772	RuntimeBroker	0xe48706fc3c2c0	1	-	5	False	2023-08-16 11:26:47.000000	N/A
***** 7224	772	RuntimeBroker	0xe48706e0ea000	4	-	2	False	2023-08-16 11:27:19.000000	N/A
***** 4028	772	ShellExperience	0xe48706a5c2c0	11	-	2	False	2023-08-16 11:24:44.000000	N/A
***** 9276	772	ShellExperience	0xe48706fa5a000	10	-	5	False	2023-08-16 11:26:39.000000	N/A
***** 7488	772	RuntimeBroker	0xe48706cac32c0	6	-	5	False	2023-08-16 11:26:37.000000	N/A
***** 840	772	RuntimeBroker	0xe48706e653000	8	-	4	False	2023-08-16 11:26:16.000000	N/A
***** 3916	772	TextInputHost	0xe48706e0f000	10	-	4	False	2023-08-16 11:26:24.000000	N/A
***** 460	772	StartMenuExper	0xe48706c75e000	22	-	5	False	2023-08-16 11:26:36.000000	N/A
***** 8144	772	RuntimeBroker	0xe48706dce1280	4	-	2	False	2023-08-16 11:24:31.000000	N/A

La salida se vería así la particularidad que tiene es que nos muestra unos asteriscos al frente de cada proceso de esta forma nos ayuda a ver a simple vista una jerarquía en el inicio de los procesos.

Revisamos las relaciones entre los procesos y podemos anotar uno que otro que consideremos sospechosos, por ejemplo:

Veo 4 procesos winlogon y 4 explorer y 5 userinit.

```
root@ip-172-31-1-142:~/Desktop/ChallengeFile# grep "init" pstree.txt
* 6596 7280 userinit.exe 0xe4870e47c300 0 - 2 False 2023-08-16 11:24:20.000000 2023-08-16 11:24:53.000000
* 3196 3816 userinit.exe 0xe4870bc62000 0 - 4 False 2023-08-16 11:26:09.000000 2023-08-16 11:26:36.000000
**** 516 424 wininit.exe 0xe4870a5cb000 1 - 0 False 2023-08-16 11:21:25.000000 N/A
* 4668 6488 userinit.exe 0xe4870bcb2000 0 - 5 False 2023-08-16 11:26:30.000000 2023-08-16 11:26:57.000000
* 10820 6208 userinit.exe 0xe487107aa240 0 - 6 False 2023-08-16 11:27:05.000000 2023-08-16 11:27:41.000000
root@ip-172-31-1-142:~/Desktop/ChallengeFile# ^C
root@ip-172-31-1-142:~/Desktop/ChallengeFile# grep "winlogon" pstree.txt
7280 6728 winlogon.exe 0xe4870cb35000 3 - 2 False 2023-08-16 11:24:12.000000 N/A
3816 2152 winlogon.exe 0xe4870c26b000 5 - 4 False 2023-08-16 11:26:06.000000 N/A
6488 7312 winlogon.exe 0xe4870cida2c0 3 - 5 False 2023-08-16 11:26:27.000000 N/A
6208 10072 winlogon.exe 0xe4870fee20c0 3 - 6 False 2023-08-16 11:26:59.000000 N/A
root@ip-172-31-1-142:~/Desktop/ChallengeFile# grep "explorer" pstree.txt
** 2844 6596 explorer.exe 0xe4870e470000 58 - 2 False 2023-08-16 11:24:20.000000 N/A
** 4104 3196 explorer.exe 0xe4870baf1000 38 - 4 False 2023-08-16 11:26:09.000000 N/A
** 6428 4668 explorer.exe 0xe4870d7f0000 37 - 5 False 2023-08-16 11:26:30.000000 N/A
* 11420 6208 explorer.exe 0xe4870d1a2000 71 - 6 False 2023-08-16 11:32:01.000000 N/A
```

Utilizo el complemento cmdline para ver si se ejecutó algún comando, pero no veo nada.

```
python3 /root/Desktop/volatility3/vol.py -f vLP.vmem windows.cmdline > cmdline.txt
```

Debido al alto número de procesos activos más la información de los procesos winlogon puedo asumir que 4 usuarios están logeados en la máquina, y se dificulta el análisis de procesos no viendo de forma clara un proceso extraño aun analizando el árbol de procesos, voy a hacer un pequeño giro en la forma de búsqueda de este caso.

Busco en los archivos si encuentro algo relacionado con un crack, uso el complemento filescan

```
python3 /root/Desktop/volatility3/vol.py -f vLP.vmem windows.filescan > filescan.txt
```

```
root@ip-172-31-1-142:~/Desktop/ChallengeFile# grep "crack" filescan.txt
root@ip-172-31-1-142:~/Desktop/ChallengeFile# grep "Crack" filescan.txt
0xe4870d72ebf0 \Users\flapjack\Downloads\Windows10Crack.exe 216
0xe4870d7301d0 \Users\flapjack\Downloads\Windows10Crack.exe 216
root@ip-172-31-1-142:~/Desktop/ChallengeFile#
```

Encuentro dos archivos podemos ver que tienen diferentes direcciones virtuales (offset), pero esto responde la pregunta 2 y 3.

Intento extraer los archivos:

```
python3 /root/Desktop/volatility3/vol.py -f vLP.vmem windows.dumpfiles --virtaddr 0xe4870d72ebf0
```

```
python3 /root/Desktop/volatility3/vol.py -f vLP.vmem windows.dumpfiles --virtaddr 0xe4870d7301d0
```

```
root@ip-172-31-1-142:~/Desktop/ChallengeFile# python3 /root/Desktop/volatility3/vol.py -f vLP.vmem windows.dumpfiles --virtaddr 0xe4870d72ebf0
Volatility 3 Framework 2.5.2
WARNING: volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a
WEM file. These should be placed in the same directory with the same file name, e.g. vLP.vmem and vLP.vms.
Progress: 100.00 PDB scanning finished
Cache FileObject FileName Result
ImageSectionObject 0xe4870d72ebf0 Windows10Crack.exe file.0xe4870d72ebf0.0xe4870dcd8010.ImageSectionObject.Windows10Crack.exe.img
root@ip-172-31-1-142:~/Desktop/ChallengeFile# python3 /root/Desktop/volatility3/vol.py -f vLP.vmem windows.dumpfiles --virtaddr 0xe4870d7301d0
Volatility 3 Framework 2.5.2
WARNING: volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a
WEM file. These should be placed in the same directory with the same file name, e.g. vLP.vmem and vLP.vms.
Progress: 100.00 PDB scanning finished
Cache FileObject FileName Result
ImageSectionObject 0xe4870d7301d0 Windows10Crack.exe file.0xe4870d7301d0.0xe4870dcd8010.ImageSectionObject.Windows10Crack.exe.img
root@ip-172-31-1-142:~/Desktop/ChallengeFile# ls
cmdline.txt filescan.txt vLP.vmem
file.0xe4870d72ebf0.0xe4870dcd8010.ImageSectionObject.Windows10Crack.exe.img psscan.txt
file.0xe4870d7301d0.0xe4870dcd8010.ImageSectionObject.Windows10Crack.exe.img pstree.txt
root@ip-172-31-1-142:~/Desktop/ChallengeFile#
```

Ya extraídos obtengo el hash de ambos, de esta forma verifico que sean el mismo archivo.

e58a2947b29b4b691e4011204d59ff52

Tomo uno de los archivos y le cambio la extensión para intentar ejecutarlo o hacerle ingeniería inversa.

mv

file.0xe4870d7301d0.0xe4870dcd8010.ImageSectionObject.Windows10Crack.exe.img

file.0xe4870d7301d0.0xe4870dcd8010.ImageSectionObject.Windows10Crack.exe

Además, lo busco en virus total

4 / 72

4 security vendors and no sandboxes flagged this file as malicious

Reanalyze Similar More

2b18d203b39dd8fb809fd22d1b8fad52cd9bebe29044467b23...
win10crack.exe

Size: 976.00 KB | Last Analysis Date: a moment ago

peexe 64bits overlay

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

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

Security vendors' analysis ⓘ Do you want to automate checks?




CrowdStrike Falcon	ⓘ Win/malicious_confidence_90% (W)	Cynet	ⓘ Malicious (score: 100)
Google	ⓘ Detected	Ikarus	ⓘ SuspectFile

En este encuentro la url de donde se descarga el ransomware lo cual responde la pregunta 4.

Memory Pattern Domains

 48.147.154.231

Memory Pattern Urls

 http://48.147.154.231/XGUbdem0hd.exe
 http://48.147.154.231/XGUbdem0hd.exeCracking
 http://48.147.154.231/XGUbdem0hd.exendows

Pero podemos usar otra técnica para ver el código sin tener que realizar todo un proceso de ingeniería inversa para esto usaremos la herramienta “strings”, esta herramienta permite extraer cadenas de texto de cualquier archivo, sumado a “grep” nos permitirá buscar la url si esta está en formato leíble.

El comando quedaría así:

```
strings  
file.0xe4870d72ebf0.0xe4870dcd8010.ImageSectionObject.Windows10Crack.exe.img |  
grep "http"
```

```
root@ip-172-31-24-38:~/Desktop/ChallengeFile# strings file.0xe4870d72ebf0.0xe4870dcd8010.ImageSectionObject.Windows10Crack.exe.img | grep "http"  
http://gh  
http://48.147.154.231/XGUbdem0hd.exe
```

Como podemos ver se pudo extraer de forma correcta la url sin necesidad de usar una plataforma de análisis de terceros.

Con el nombre del ejecutable lo buscamos en los archivos.

```
grep "XGUbdem0hd.exe" filesan.txt
```

```
root@ip-172-31-1-142:~/Desktop/ChallengeFile# grep "XGUbdem0hd.exe" filesan.txt  
0xe4870d737578 \Users\flapjack\AppData\Local\Temp\XGUbdem0hd.exe 216
```

Encontramos el archivo como pudieron ver y así respondemos la pregunta 5.

```
python3 /root/Desktop/volatility3/vol.py -f vLP.vmem windows.dumpfiles --virtaddr 0xe4870d737570
```

```
root@ip-172-31-1-142:~/Desktop/ChallengeFile# python3 /root/Desktop/volatility3/vol.py -f vLP.vmem windows.dumpfiles --virtaddr 0xe4870d737570
Volatility 3 Framework 2.5.2
WARNING: volatility3.framework.layers.vmem: No metadata file found alongside VMEM file. A VMSS or VMSSN file may be required to correctly process a
VMEM file. These should be placed in the same directory with the same file name, e.g. vLP.vmem and vLP.vmemss.
Progress: 100.00 PDB scanning finished
Cache FileObject FileName Result
ImageSectionObject 0xe4870d737570 XGUbden0hd.exe file.0xe4870d737570.0xe4870fc51d00.ImageSectionObject.XGUbden0hd.exe.img
```

La máquina del laboratorio se reinició, pero retomaremos desde aquí

Obtengo el hash del ejecutable bde56933af564b982eea620666e01f9f

54 / 72

54 security vendors and 1 sandbox flagged this file as malicious

Reanalyze Similar More

2b96baa58402a24a21ea2bdfee7f18aa3bfe6cbe082866ed486a... Size 2.57 MB Last Analysis Date a moment ago

file.0xe4870d737570.0xe4870fc51d00.ImageSectionObject.XG... EXE

peexe idle detect-debug-environment

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 5

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

Popular threat label virus.expiro/blackcat Threat categories virus ransomware trojan Family labels expiro blackcat xpirat

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Virus/Win.Expiro.X2160	Alibaba	Virus:Win32/Expiro.57cd2c79
ALYac	Win32.Expiro.Gen.6	Antiy-AVL	Virus/Win32.Expiro.ndg
Arcabit	Win32.Expiro.Gen.6	Avast	Win32:Xpirat-C [Inf]

Vamos al apartado de "" y encontramos las modificaciones a los registros y con esto la respuesta 6.

- ⊞ HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
- ⊞ HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Windows
- ⊞ HKEY_LOCAL_MACHINE\Software\WOW6432Node\Policies\Microsoft\MUI\Settings
- ⊞ HKEY_LOCAL_MACHINE\Software\WOW6432Node\Policies\Microsoft\Windows\Display
- ⊞ HKEY_LOCAL_MACHINE\Software\WOW6432Node\Policies\Microsoft\Windows\Safe\CodeIdentifiers
- ⊞ HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem\
- ⊞ HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa
- ⊞ HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy
- ⊞ HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\MUI\Settings\LanguageConfiguration
- ⊞ HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\MUI\UILanguages
- ⊞ HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\MUI\UILanguages\PendingDelete
- ⊞ HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\NLS\Language
- ⊞ HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale
- ⊞ HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale
- ⊞ HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Sorting\Versions
- ⊞ HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SafeBoot\Option
- ⊞ HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager
- ⊞ HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SrplGPIDLL
- ⊞ HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server
- ⊞ HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters

Sobre LanmanWorkstation puedo decir que este servicio es parte del conjunto de servicios de red de Windows y está relacionado con la funcionalidad de trabajo en red y uso compartido de archivos y recursos en entornos Windows. Esta específicamente controla parámetros lo cual puede estar relacionado con intento de propagación en la local del equipo infectado.

Ahora continuamos a las acciones detectadas “Highlighted actions”:

Decoded Text

```
{ "config_id": "", "public_key":
"MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAt9uYkHzaizNXg/S11ncTTLybkMtqrKW8gg6TyzbGWhRNROi9O+IVZBLGOxiMt1mZbuSt8Lt31vIkMa92kgLjN+UfKmq3KhBheN2uMmROWpwV83kceVRr
"extension": "sykffle", "note_file_name": "RECOVER-$(EXTENSION)-FILES.txt", "note_full_text": ">> Introduction\n\nImportant files on your system was ENCRYPTED and now they have have \"$(EXTENSION)\" exten
including credentials for local and remote services.\n- Financial information including clients data, bills, budgets, annual reports, bank statements.\n- Complete datagrams/schemas/drawings for manufacturing
NOT MODIFY FILES YOURSELF.\nDO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.\nYOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.\nYOUR DATA IS STRONGLY ENCI
http://mu75ltv3lxd4dbu6gtvmwybecigs5auki7fces437xvflzva2nqd.onion/?access-key=$(ACCESS_KEY)", "note_short_text": "Important files on your system was ENCRYPTED.\nSensitive data on your system
[\"KELLERSUPPLY\\AdminRecovery\", \"K3ller$Supply\"], [\".\\Administrator\", \"d@gw00d\"], [\".\\Administrator\", \"K3ller$Supply\"]], \"kill_services\": [\"mepocs\", \"memtas\", \"veeam\", \"svc$\", \"backup\", \"sql\", \"vss\", \"msexchan
\"ocautoupds\", \"dbsnmp\", \"msaccess\", \"tbirdconfig\", \"ocssd\", \"mydesktopservice\", \"visio\", \"sq*\"], \"exclude_directory_names\": [\"system volume information\", \"intel\", \"$windows-~ws\", \"application data\", \"$recycle.bi
\"thumbs.db\", \"boot.ini\", \"ntuser.dat\", \"iconcache.db\", \"bootfont.bin\", \"ntuser.ini\", \"ntuser.dat.log\"], \"exclude_file_extensions\": [\"themepack\", \"nls\", \"diagpkg\", \"msi\", \"lnk\", \"exe\", \"cab\", \"scr\", \"bat\", \"drv\", \"rtp\", \"msp\", \"pr
\"enable_network_discovery\": true, \"enable_self_propagation\": false, \"enable_set_wallpaper\": true, \"enable_esxi_vm_kill\": true, \"strict_include_paths\": []]
```

Les dejare un recuadro con el texto decodificado por Virus Total.

```
{ "config_id": "", "public_key":
"MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAt9uYkHzaizNXg/S11ncTTLybkMtqrKW8gg
```

```

6TyzbGWnRNROI9O+11VZBLG0xiMt1mZbuStl8Lt3l1vlkMa92kgLjN+UfKmq3KhBEheN2uMmR0WpwV/
83kceVRmzr5lug4RyQ/xA6/OXK4NptDIT4L6CUTBWMyk2mmY0Cq9HyyrjdnHeAXWAcQGFEac7W4jT
jONZql+lgScPewS+cPFnz1hAD0IAqzj5X2mZVSfFGR3tDole42jw5wb6W2yi8zb3mgKrGtTBbw0Ppj0Ug
KrmndN5iFmfUQHLEzKAakDggLcBtrW1o5+4WMaZOLw8maU5byvjXu3F3i3GdQe8SKTYcVK5OQIDA
QAB", "extension": ".sykffle", "note_file_name": "RECOVER-#{EXTENSION}-FILES.txt",
"note_full_text": ">> Introduction\n\nImportant files on your system was ENCRYPTED and now they
have have \"#{EXTENSION}\" extension.\n\nIn order to recover your files you need to follow instructions
below.\n\n>> Sensitive Data\n\nSensitive data on your system was DOWNLOADED and it will be
PUBLISHED if you refuse to cooperate.\n\nData includes:\n- Employees personal data, CVs, DL,
SSN.\n- Complete network map including credentials for local and remote services.\n- Financial
information including clients data, bills, budgets, annual reports, bank statements.\n- Complete
datagrams/schemas/drawings for manufacturing in solidworks format\n- And more...\n\nPrivate preview
is published here:
http://zuigzbu5y64xbmvc42addp4lxkoosb4tslf5mehnh7pvqjpwxn5gokyd.onion/b21e1fb6-ff88-425b-
8339-
3523179a1e3e/886cf430a907bbe9a3fd38fb704d524dbd199c1b042ad6f65dc72ad78704e21\n\n\n>>
CAUTION\n\nDO NOT MODIFY FILES YOURSELF.\n\nDO NOT USE THIRD PARTY SOFTWARE TO
RESTORE YOUR DATA.\n\nYOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT
DATA LOSS.\n\nYOUR DATA IS STRONGLY ENCRYPTED, YOU CAN NOT DECRYPT IT WITHOUT
CIPHER KEY.\n\n>> Recovery procedure\n\nFollow these simple steps to get in touch and recover
your data:\n1) Download and install Tor Browser from: https://torproject.org/\n2) Navigate to:
http://mu75ltv3lxd24dbyu6gtvmnwbybecigs5auki7fces437xvflzva2nqd.onion/?access-
key=#{ACCESS_KEY}", "note_short_text": "Important files on your system was
ENCRYPTED.\nSensitive data on your system was DOWNLOADED.\nTo recover your files and
prevent publishing of sensitive information follow instructions in \"#{NOTE_FILE_NAME}\" file.",
"default_file_mode": {"SmartPattern": [31457280, 10]}, "default_file_cipher": "Best", "credentials":
[["KELLERSUPPLY\\Administrator", "d@gw00d"], ["KELLERSUPPLY\\AdminRecovery",
"K3llr!$Supp1y"], [".\\Administrator", "d@gw00d"], [".\\Administrator", "K3llr!$Supp1y"]],
"kill_services": ["mepocs", "memtas", "veeam", "svc$", "backup", "sql", "vss", "msexchange", "sql*"],
"kill_processes": ["encsvc", "thecat", "mydesktopqos", "xfssvccon", "firefox", "infopath", "winword",
"steam", "synctime", "notepad", "ocomm", "onenote", "mspub", "thunderbird", "agntsvc", "sql", "excel",
"powerpnt", "outlook", "wordpad", "dbeng50", "isqlplussvc", "sqbcoreservice", "oracle", "ocautoupds",
"dbsnmp", "msaccess", "tbirdconfig", "ocssd", "mydesktopservice", "visio", "sql*"],
"exclude_directory_names": ["system volume information", "intel", "$windows.~ws", "application data",
"$recycle.bin", "mozilla", "program files (x86)", "program files", "$windows.~bt", "public", "msocache",
"windows", "default", "all users", "tor browser", "programdata", "boot", "config.msi", "google", "perflogs",
"appdata", "windows.old"], "exclude_file_names": ["desktop.ini", "autorun.inf", "ntldr", "bootsect.bak",
"thumbs.db", "boot.ini", "ntuser.dat", "iconcache.db", "bootfont.bin", "ntuser.ini", "ntuser.dat.log"],
"exclude_file_extensions": ["themepack", "nls", "diagpkg", "msi", "lnk", "exe", "cab", "scr", "bat", "drv",
"rtp", "msp", "prf", "msc", "ico", "key", "ocx", "diagcab", "diagcfg", "pdb", "wpx", "hlp", "icns", "rom", "dll",
"msstyles", "mod", "ps1", "ics", "hta", "bin", "cmd", "ani", "386", "lock", "cur", "idx", "sys", "com",
"deskthemepack", "shs", "ldf", "theme", "mpa", "nimedia", "spl", "cpl", "adv", "icl", "msu"],
"exclude_file_path_wildcard": [], "enable_network_discovery": true, "enable_self_propagation": false,
"enable_set_wallpaper": true, "enable_esxi_vm_kill": true, "strict_include_paths": []}

```

Aquí vemos una clave pública.

Vemos el cuerpo de una nota de rescate común de un ransomware, con enlaces, carteras entre otros datos.

Y las credenciales del AdminRecovery

```
"credentials": [{"KELLERSUPPLY\\Administrator", "d@gw00d"}, {"KELLERSUPPLY\\AdminRecovery", "K3ll3r!$Supp1y"}, {".\\Administrator", "d@gw00d"}, {".\\Administrator", "K3ll3r!$Supp1y"}]
```

Nota

Vemos que la primera parte del malware tuvo exitoso vemos le crack el cual sabemos que se ejecutó debido al otro archivo ejecutable del ransomware encontrado en el sistema. Adicional estos desafíos podemos resolver de diferentes formas, no vimos necesario realizar ingeniería inversa debido a que encontramos la información, pero en muchos casos si es necesario realizar todo el proceso.

¿Cuántos usuarios hay en la máquina?

4

¿Qué usuario es el infectado?

flapjack

¿Qué archivo obtuvo el ransomware?

Windows10Crack.exe

¿Cómo ese archivo descargó el ransomware [URL]?

<http://48.147.154.231/XGUbdem0hd.exe>

¿Cuál es la dirección offset de ese ransomware?

0xe4870d737570

El ransomware editó una de las claves de registro del administrador de hash principal. Busque la clave que se modificó.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters

¿Cuál es la credencial del AdminRecovery?

K3ll3r!\$Supp1y



Windows Memory Dump

Elias Ramirez has completed the "Windows Memory Dump" challenge

[Explore Achievement](#)

Badge Name

Windows Memory Dump

Completed At

Feb, 07, 2024, 10:46 PM