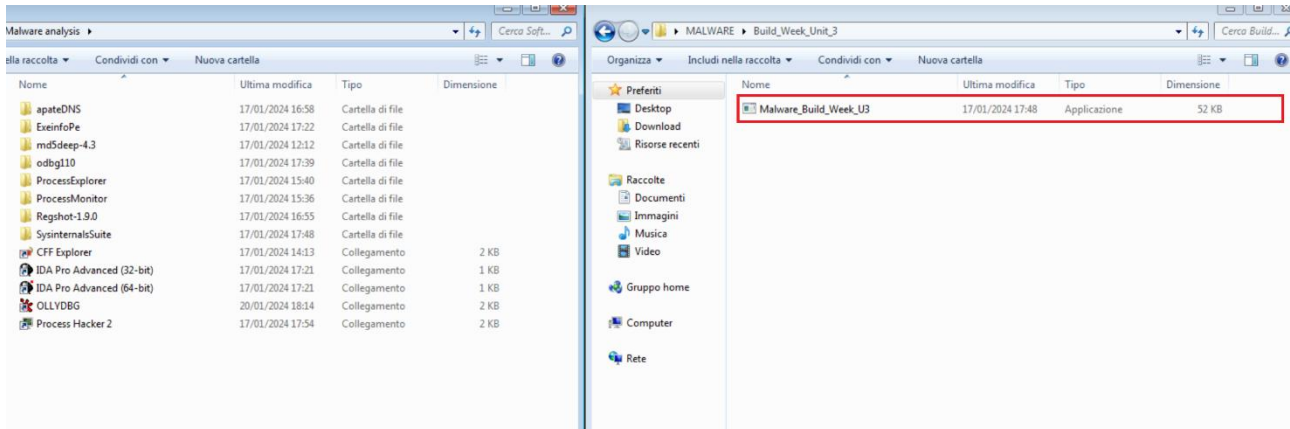


Progetto Modulo 6

Malware Analysis

Il Malware da analizzare è presente nella cartella Build_Week_Unit_3 sul desktop della macchina virtuale dedicata.



Durante l'analisi del malware , incontreremo due tecniche principali di studio:

- Analisi statica: fornisce tecniche e strumenti per analizzare il malware senza necessità di eseguirlo

- Analisi dinamica: presuppone l'esecuzione del malware in ambiente controllato

Durante la prima fase di analisi statica sfrutteremo il tool di md5deep per estrapolare hash del malware per poi confrontarlo su Virustotal, dove già avremo un primo riscontro e viene categorizzato come Trojan.

```
C:\Windows\system32\cmd.exe

C:\Users\user>cd "Desktop\Software Malware analysis\md5deep-4.3"
C:\Users\user\Desktop\Software Malware analysis\md5deep-4.3>dir
Il volume nell'unità C non ha etichetta.
Numero di serie del volume: 88D2-1ECE

Directory di C:\Users\user\Desktop\Software Malware analysis\md5deep-4.3
17/01/2024 13:12 <DIR>      .
17/01/2024 13:12 <DIR>      ..
17/01/2024 13:12 <DIR>      md5deep-4.3
                   0 File      0 byte
                   3 Directory 26.384.367.616 byte disponibili

C:\Users\user\Desktop\Software Malware analysis\md5deep-4.3>cd md5deep-4.3
C:\Users\user\Desktop\Software Malware analysis\md5deep-4.3\md5deep-4.3>dir
Il volume nell'unità C non ha etichetta.
Numero di serie del volume: 88D2-1ECE

Directory di C:\Users\user\Desktop\Software Malware analysis\md5deep-4.3\md5deep-4.3
17/01/2024 13:12 <DIR>      .
```

```
C:\Windows\system32\cmd.exe

17/01/2024 13:12      800.256 sha256deep.exe
17/01/2024 13:12      988.160 sha256deep64.exe
17/01/2024 13:12      800.256 tigerdeep.exe
17/01/2024 13:12      988.160 tigerdeep64.exe
17/01/2024 13:12      800.256 whirlpooldeep.exe
17/01/2024 13:12      988.160 whirlpooldeep64.exe
      17 File      10.796.902 byte
      2 Directory 26.384.367.616 byte disponibili

C:\Users\user\Desktop\Software Malware analysis\md5deep-4.3>md5deep
C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3
md5deep: WARNING: You are running a 32-bit program on a 64-bit system.
md5deep: You probably want to use the 64-bit version of this program.
C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3: Is a directory

C:\Users\user\Desktop\Software Malware analysis\md5deep-4.3>md5deep
C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\Malware_Build_Week_U3.exe
md5deep: WARNING: You are running a 32-bit program on a 64-bit system.
md5deep: You probably want to use the 64-bit version of this program.
a9c55bb87a7c5c3c923c4fa12940e719 C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\Malware_Build_Week_U3.exe

C:\Users\user\Desktop\Software Malware analysis\md5deep-4.3>
```

52
/ 71

52/71 security vendors and no sandboxes flagged this file as malicious

Reanalyze Similar More

57d8d248a8741176348b5d12dcf29f34c8f48ede0ca13c30d12e5ba0384096d7

Size 52.00 KB Last Modification Date 15 hours ago

Lab11-01.exe

Community Score

peexe spreader armadillo checks-user-input

DETECTION DETAILS RELATIONS BEHAVIOR TELEMETRY COMMUNITY 10

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

Popular threat label trojan.doina/totbrick Threat categories trojan Family labels doina totbrick genericncq

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Trojan/Win32.Agent.C39204	Alibaba	Trojan:Win32/Totbrick.db39e83f
AllCloud	Backdoor	ALYac	Gen:Variant.Doina.65814
Antiy-AVL	Trojan/Win32.Agent	Arcabit	Trojan.Doina.D10116
Avast	Win32:Trojan-gen	AVG	Win32:Trojan-gen
Avira (no cloud)	TR/Agent.53248.465	BitDefender	Gen:Variant.Doina.65814
BitDefenderTheta	Gen:NN.ZedlaF.36802.aq4@a0clrOb	Bkav Pro	W32.AIDetectMalware
ClamAV	Win.Trojan.Agent-595082	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsafe	Cynet	Malicious (score: 99)
DeepInstinct	MALICIOUS	DrWeb	BackDoor.Siggen2.1689
Elastic	Malicious (moderate Confidence)	Emsisoft	Gen:Variant.Doina.65814 (B)

Come fase successiva avvieremo il tool di string per vedere le stringhe presenti nell'eseguibile; e già potremmo notare delle chiamate interessanti ,riguardanti le modifiche di alcune chiavi e la creazione di un file.

```
C:\Windows\system32\cmd.exe
WlxDisplayStatusMessage
WlxGetConsoleSwitchCredentials
WlxGetStatusMessage
WlxInitialize
WlxIsLockOk
WlxIsLogoffOk
WlxLoggedOnSAS
WlxLogoff
WlxNegotiate
WlxNetworkProviderLoad
WlxReconnectNotify
WlxRemoveStatusMessage
WlxScreenSaverNotify
WlxShutdown
WlxStartApplication
WlxWkstaLockedSAS
GinaDLL
Software\Microsoft\Windows NT\CurrentVersion\Winlogon
MSGina.dll
UN %s DM %s PW %s OLD %s
WlxLoggedOutSAS
ErrorCode:%d ErrorMessage:%s.
%s %s - %s
msutil32.sys
080-080j0z0
3!313A3Q3a3q3
4#4*474B4Y4
4Z5c5
6!686b6h6n6t6z6
7"7<7J7\7

C:\Users\user\Desktop\Software Malware analysis\SysinternalsSuite>strings C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\Malware_Build_Week_U3.exe_
SetStdHandle
FlushFileBuffers
SetFilePointer
CreateFileA
GetCPIInfo
GetACP
GetOEMCP
GetProcAddress
LoadLibraryA
SetEndOfFile
ReadFile
MultiByteToWideChar
LCMapStringA
LCMapStringW
GetStringTypeA
GetStringTypeW
dTE
TGAD
BINARY
GinaDLL
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
msgina32.dll
\msgina32.dll
Xqe
Hqe
xse
lse
```

```

user32.dll
9d0
=d0
CloseHandle
FreeResource
VirtualAlloc
SizeofResource
LockResource
LoadResource
FindResourceA
GetModuleFileNameA
GetModuleHandleA
kernel32.dll
RegSetValueExA
RegCreateKeyExA
advapi32.dll
GetCommandLineA
GetVersion
ExitProcess
HeapFree
GetLastError
WriteFile
TerminateProcess
GetCurrentProcess

```

Come fase successiva ,utilizzo CFF Explorer per analizzare le sezioni presenti nel Headers; notiamo che ne sono presenti 4:

- .rsrc : contiene le risorse del programma
- .rdata : contiene dati che sono solo in lettura durante l'esecuzione del programma (read-only data)
- .data : contiene i dati globali e statici che possono essere modificati durante l'esecuzione del programma
- .text : contiene il codice eseguibile ,ovvero le istruzioni che vengono eseguite dal processore

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	00005646	00001000	00006000	00001000	00000000	00000000	0000	0000	60000020
.rdata	000009AE	00007000	00001000	00007000	00000000	00000000	0000	0000	40000040
.data	00003EAB	00008000	00003000	00008000	00000000	00000000	0000	0000	C0000040
.rsrc	00001A70	0000C000	00002000	0000B000	00000000	00000000	0000	0000	40000040

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ.....yy..
00000010	B8	00	00	00	00	00	00	40	00	00	00	00	00	00	00	00@.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	E0	00	00	00à.....
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	...esp..iI..I..
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is:program.canno

Abbiamo lo stesso riscontro con ExeInfo

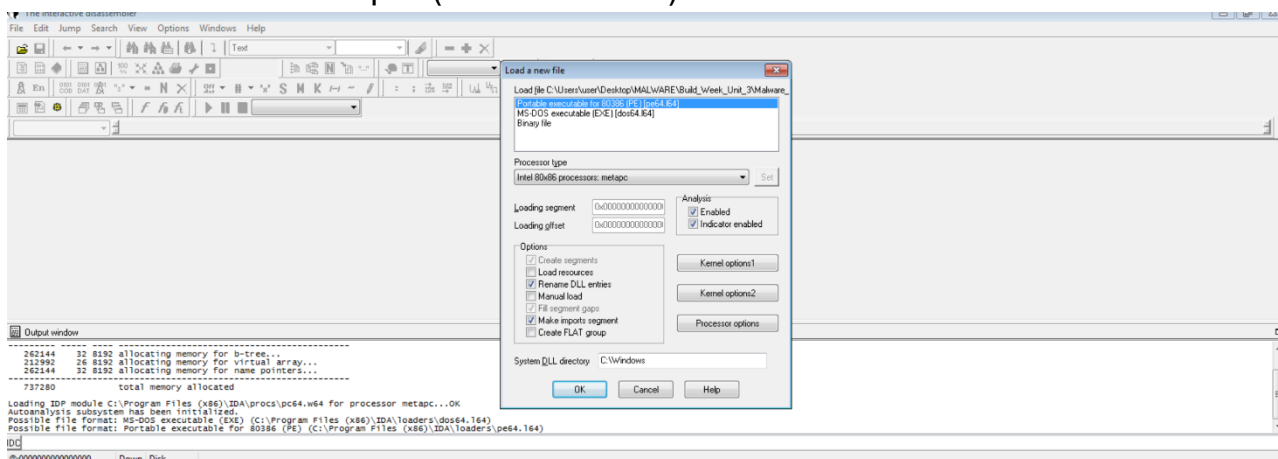
[illegible]

Come librerie invece vedremo importate la kernel32 e la ADVAPI32, all'interno della quale ritroveremo le chiamate alle modifiche delle chiavi di registro.

ADVAPI32.dll	2	00007528	00000000	00000000	000076D0	00007000
--------------	---	----------	----------	----------	----------	----------

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
000076AC	000076AC	0186	RegSetValueExA
000076BE	000076BE	015F	RegCreateKeyExA

Fatti questi primi test preliminari di analisi statica basica , vado ad analizzare il codice mediante Ida pro (disassambler).



Analizzando il codice potremmo notare che vengono passati 3 parametri alla funzione Main

```
; int __cdecl main(int argc, const char **argv, const char **envp)
_main proc near

hModule= dword ptr -11Ch
Data= byte ptr -118h
var_117= byte ptr -117h
var_8= dword ptr -8
var_4= dword ptr -4
argc= dword ptr 8
argv= dword ptr 0Ch
envp= dword ptr 10h

push    ebp
mov     ebp, esp
sub     esp, 11Ch
push    ebx
push    esi
```

E vengono dichiarate 5 variabili

```
hModule= dword ptr -11Ch
Data= byte ptr -118h
var_117= byte ptr -117h
var_8= dword ptr -8
var_4= dword ptr -4
```

Nella sezione import potremmo vedere nuovamente l'utilizzo delle due librerie:

-KERNEL32 : Utilizzata per la creazione di un file per avere la persistenza

-ADVAPI32 : Utilizzata per modificare dei valori ed aggiungere una chiave per essere eseguito all'avvio del SO

Da una prima analisi, posso supporre ,che il malware è un dropper/trojan perché una volta eseguito va ad importare/creare un file; potremmo escludere una backdoor, in quanto non utilizza la libreria winsock per le funzioni networking, ed escludere Keylogger in quanto non utilizza API per la gestione di periferiche.

Continuando ad analizzare le locazioni di memoria all'interno del codice ,noto che alla locazione **00401021** viene chiamata la funzione RegCreateKeyExA (una funzione dell'API di windows utilizzata per creare o aprire una chiave del registro di sistema) , alla quale vengono passati 9 parametri:

```
.text:00401000      push    ebp
.text:00401000      mov     ebp, esp
.text:00401001      push    ecx
.text:00401004      push    0                ; lpdwDisposition
.text:00401006      lea     eax, [ebp+hObject]
.text:00401009      push    eax              ; phkResult
.text:0040100A      push    0                ; lpSecurityAttributes
.text:0040100C      push    0F003Fh          ; samDesired
.text:00401011      push    0                ; dwOptions
.text:00401013      push    0                ; lpClass
.text:00401015      push    0                ; Reserved
.text:00401017      push    offset SubKey     ; "SOFTWARE\\Microsoft\\Windows NT\\CurrentVe...
.text:0040101C      push    8000002h          ; hKey
.text:00401021      call    ds:RegCreateKeyExA
.text:00401027      test    eax, eax
```

```

.text:00401000
.text:00401000      push    ebp
.text:00401001      mov     ebp, esp
.text:00401003      push    ecx
.text:00401004      push    0 ; lpdwDisposition
.text:00401006      lea     eax, [ebp+hObject]
.text:00401009      push    eax ; phkResult
.text:0040100A      push    0 ; lpSecurityAttributes
.text:0040100C      push    0F003Fh ; samDesired
.text:00401011      push    0 ; dwOptions
.text:00401013      push    0 ; lpClass
.text:00401015      push    0 ; Reserved
.text:00401017      push    offset SubKey ; "SOFTWARE\\Microsoft\\Windows NT\\CurrentVe..."
.text:0040101C      push    80000002h ; hKey
.text:00401021      call    ds:RegCreateKeyExA
.text:00401027      test    eax, eax

```

-hKey: chiave registro padre sotto la quale verrà creata o aperta la nuova chiave

-SubKey : nome nuova chiave

-Reserved : impostato su NULL

-lpClass: NULL non specifica una classe

-dwOption : opzioni aggiuntive per la creazione della chiave

-samDesired: specifica le autorizzazioni richieste per la chiave di registro che si sta creando o aprendo

-lpSecurityAttributes: impostato su NULL per non specificare attributi di sicurezza custom

-phkResult: punta ad una variabile in cui verrà restituito un handle per la chiave

-lpdwDisposition: puntatore a variabile DWORD utilizzato per restituire informazioni sull'esito dell'operazione di creazione o apertura della chiave

Successivamente alla locazione 00401027 e 00401029 troviamo un jump (come un ciclo IF in C) con la chiamata alla funzione RegSetValueExA (loc 00401047), con il valore del parametro "ValueName" → GinaDLL.

```

.text:00401021      call    ds:RegCreateKeyExA
.text:00401027      test    eax, eax
.text:00401029      jz      short loc_401032
.text:0040102B      mov     eax, 1
.text:00401030      jmp     short loc_40107B
; -----
.text:00401032      loc_401032:
.text:00401032      mov     ecx, [ebp+cbData] ; CODE XREF: sub_401000+29fj
.text:00401035      push    ecx ; cbData
.text:00401036      mov     edx, [ebp+lpData]
.text:00401039      push    edx ; lpData
.text:0040103A      push    1 ; dwType
.text:0040103C      push    0 ; Reserved
.text:0040103E      push    offset ValueName ; "GinaDLL"
.text:00401043      mov     eax, [ebp+hObject]
.text:00401046      push    eax ; hKey
.text:00401047      call    ds:RegSetValueExA

```


Con riferimento alla locazione 00401027 e 00401029 potremmo tradurre quel ciclo in C →

```
If(eax == 0){
```

```
Esegui l'operazione
```

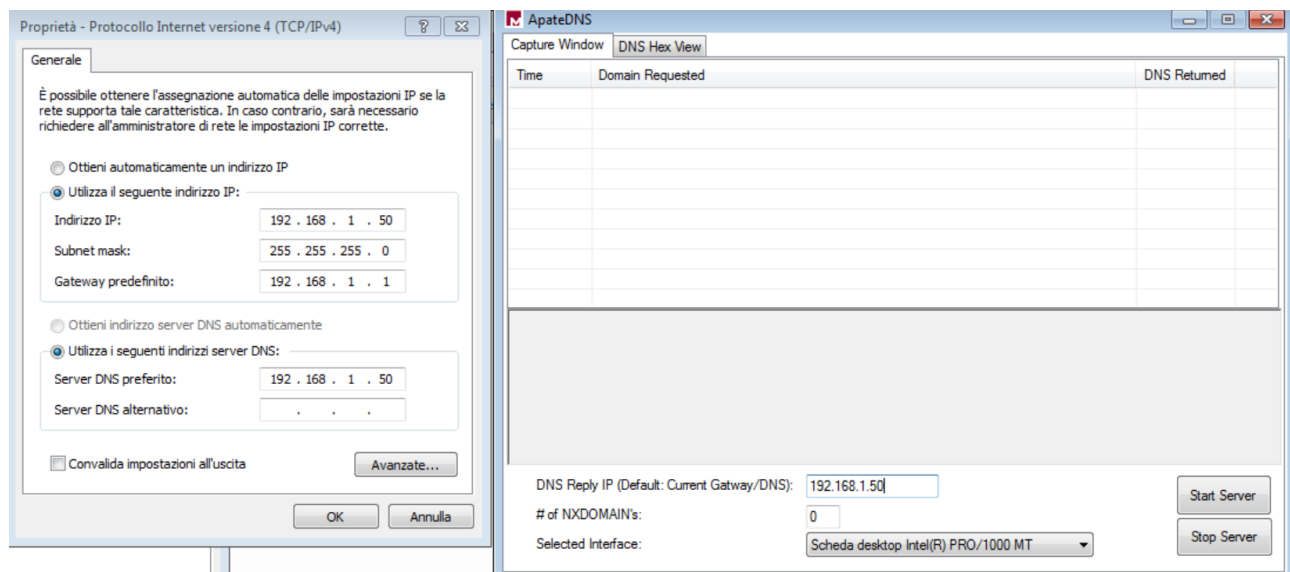
```
}else {
```

```
Fai altro
```

```
}
```

Successivamente passeremo all'analisi dinamica del malware mediante l'utilizzo di:

- ApateDNS per monitorare le richieste verso siti
- ProcessExplorer e Procmon per monitorare il comportamento del malware una volta avviato
- RegShot per comparare dei screenshot del sistema, prima e dopo l'avvio del malware.



Time ...	Process Name	PID	Operation	Path	Result	Detail
17:20:...	SearchIndexer...	1924	ReadFile	C:\Windows\System32\mssrch.dll	SUCCESS	Offset: 2.088.960, ...
17:20:...	SearchIndexer...	1924	ReadFile	C:\Windows\System32\mssrch.dll	SUCCESS	Offset: 2.056.192, ...
17:20:...	SearchIndexer...	1924	ReadFile	C:\Windows\System32\mssrch.dll	SUCCESS	Offset: 2.035.712, ...
17:20:...	SearchIndexer...	1924	ReadFile	C:\Windows\System32\mssrch.dll	SUCCESS	Offset: 2.027.520, ...
17:20:...	SearchIndexer...	1924	ReadFile	C:\Windows\System32\mssrch.dll	SUCCESS	Offset: 1.757.184, ...
17:20:...	SearchIndexer...	1924	FileSystemControlC:		SUCCESS	Control: FSCTL_R...
17:20:...	SearchIndexer...	1924	FileSystemControlC:		SUCCESS	Control: FSCTL_R...
17:20:...	svchost.exe	1504	ReadFile	C:\Program Files\Windows Defender\M...	SUCCESS	Offset: 551.424, Le...
17:20:...	svchost.exe	1504	ReadFile	C:\Program Files\Windows Defender\M...	SUCCESS	Offset: 539.136, Le...
17:20:...	svchost.exe	1504	ReadFile	C:\Program Files\Windows Defender\M...	SUCCESS	Offset: 484.352, Le...
17:20:...	svchost.exe	1504	RegOpenKey	HKLM	SUCCESS	Desired Access: M...
17:20:...	svchost.exe	1504	RegQueryValue	HKLM	SUCCESS	Query: HandleTag...
17:20:...	svchost.exe	1504	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\...	NAME NOT FOUND	Desired Access: R...
17:20:...	svchost.exe	1504	RegCloseKey	HKLM	SUCCESS	
17:20:...	svchost.exe	1504	RegOpenKey	HKLM	SUCCESS	Desired Access: M...
17:20:...	svchost.exe	1504	RegQueryValue	HKLM	SUCCESS	Query: HandleTag...
17:20:...	svchost.exe	1504	RegOpenKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Desired Access: R...
17:20:...	svchost.exe	1504	RegCloseKey	HKLM	SUCCESS	
17:20:...	svchost.exe	1504	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Type: REG_DW...
17:20:...	svchost.exe	1504	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	
17:20:...	svchost.exe	1504	ReadFile	C:\Program Files\Windows Defender\M...	SUCCESS	Offset: 954.880, Le...
17:20:...	svchost.exe	1504	ReadFile	C:\Program Files\Windows Defender\M...	SUCCESS	Offset: 865.280, Le...
17:20:...	svchost.exe	1504	ReadFile	C:\Program Files\Windows Defender\M...	SUCCESS	Offset: 836.608, Le...
17:20:...	svchost.exe	1504	RegOpenKey	HKLM	SUCCESS	Desired Access: M...
17:20:...	svchost.exe	1504	RegQueryValue	HKLM	SUCCESS	Query: HandleTag...
17:20:...	svchost.exe	1504	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\...	NAME NOT FOUND	Desired Access: R...
17:20:...	svchost.exe	1504	RegCloseKey	HKLM	SUCCESS	
17:20:...	svchost.exe	1504	RegOpenKey	HKLM	SUCCESS	Desired Access: M...
17:20:...	svchost.exe	1504	RegQueryValue	HKLM	SUCCESS	Query: HandleTag...
17:20:...	svchost.exe	1504	RegOpenKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Desired Access: R...
17:20:...	svchost.exe	1504	RegCloseKey	HKLM	SUCCESS	
17:20:...	svchost.exe	1504	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Type: REG_DW...
17:20:...	svchost.exe	1504	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	

Regshot 1.9.0 x64 ANSI

Compare logs save as:

☒ Plain TXT ☐ HTML document

☐ Scan dir 1[;dir 2;dir 3;...;dir nn]:

C:\Windows ...

Output path:

C:\Users\user\AppData\Loc ...

Add comment into the log:

1st shot

2nd shot



Compare

Clear

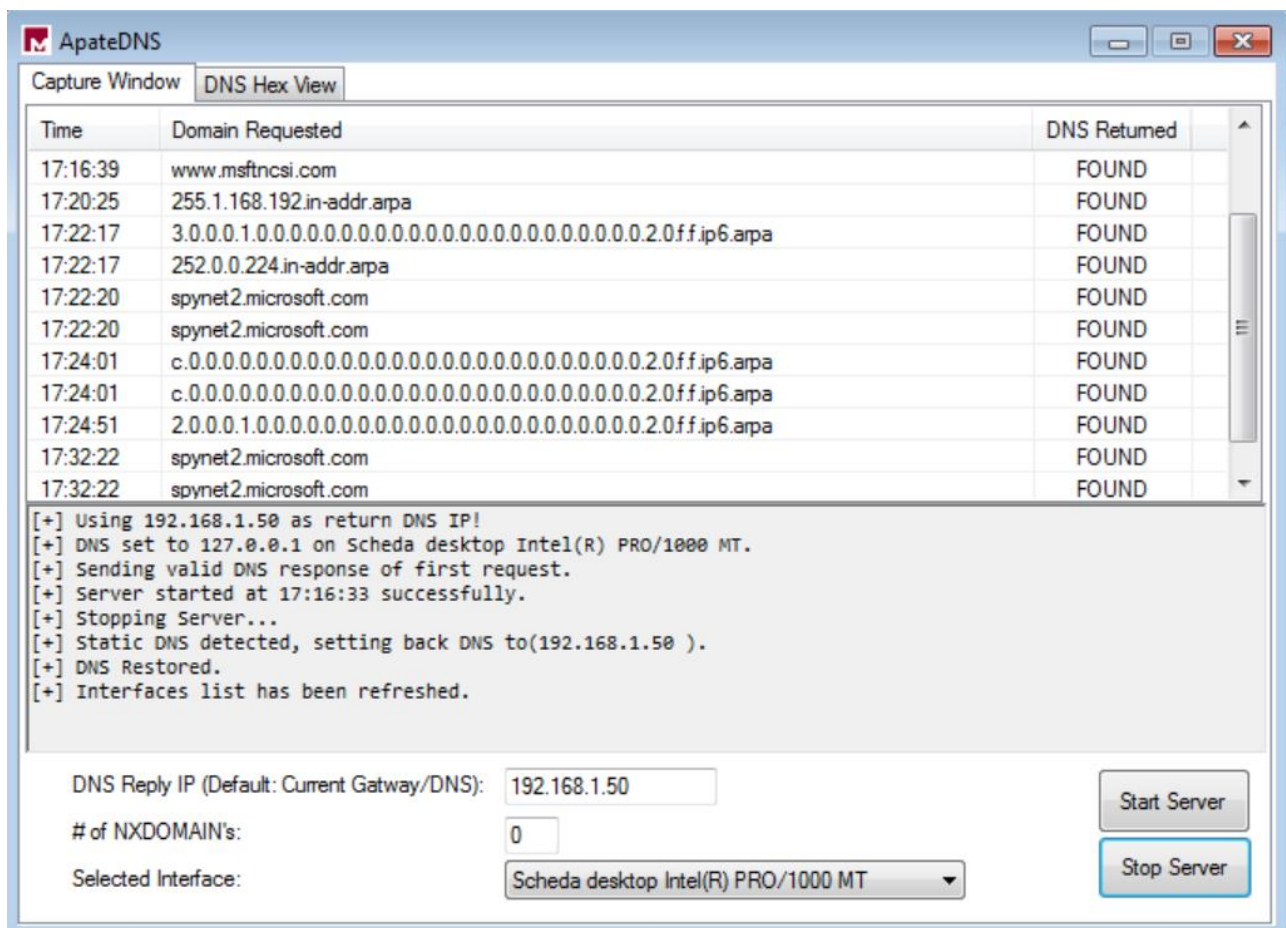
Quit

About

English ▼

Includi nella raccolta ▼	Condividi con ▼	Nuova cartella			
	Nome	Ultima modifica	Tipo	Dimensione	
	 Malware_Build_Week_U3	17/01/2024 17:48	Applicazione	52 KB	
	 msgina32.dll	20/04/2024 17:26	Estensione dell'ap...	7 KB	

[illegible]



Andiamo su procmon , mettiamo il filtro “process name” con il nome dell’eseguibile e potremmo vedere quella che è l’effettiva esecuzione del malware.

The screenshot shows the Process Monitor application window. The main pane displays a list of system events with columns for Time, Process Name, PID, Operation, Path, Result, and Detail. The events are filtered to show only those related to the process 'Malware_Build_Week_U3.exe'. The filter dialog box is open, showing the filter conditions: 'Process Name is Malware_Build_Week_U3.exe then Include'. The filter table shows the following entries:

Column	Relation	Value	Action
Process Name	is	Malware_Build_Week_U3.exe	Include
Process Name	is	Procmon.exe	Exclude
Process Name	is	Procexp.exe	Exclude
Process Name	is	Autonuma.exe	Exclude
Process Name	is	Procmon64.exe	Exclude
Process Name	is	Process64.exe	Exclude
Process Name	is	System	Exclude

The main pane shows the following events for 'Malware_Build_Week_U3.exe':

Time	Process Name	PID	Operation	Path	Result	Detail
17:25...	SearchIndexer.exe	1524	FileSystemControl	C:\...	SUCCESS	Control: FSCTL_Q...
17:25...	SearchIndexer.exe	1524	FileSystemControl	C:\...	SUCCESS	Control: FSCTL_R...
17:25...	VBoxService.exe	656	Thread Create		SUCCESS	Thread ID: 2352
17:25...	svchost.exe	280	RegOpenKey	HKLM	SUCCESS	Desired Access: M...
17:25...	svchost.exe	280	RegQueryValue	HKLM	SUCCESS	Query: HandleTag...
17:25...	svchost.exe	280	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Ser...	REPARSE	Desired Access: R...
17:25...	svchost.exe	280	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Ser...	NAME NOT FOUND	Desired Access: R...
17:25...	svchost.exe	280	RegCloseKey	HKLM	SUCCESS	
17:25...	svchost.exe	832	RegOpenKey	HKLM	SUCCESS	Desired Access: M...
17:25...	svchost.exe	832	RegQueryValue	HKLM	SUCCESS	Query: HandleTag...
17:25...	svchost.exe	832	RegOpenKey	HKLM\SOFTWARE\Microsoft\WBEM\...	NAME NOT FOUND	Desired Access: R...
17:25...	svchost.exe	832	RegCloseKey	HKLM	SUCCESS	
17:25...	svchost.exe	452	RegOpenKey	HKLM\SAM\SAM\DOMAINS\Account\...	NAME NOT FOUND	Desired Access: R...
17:25...	svchost.exe	452	RegOpenKey	HKLM\SAM\SAM\DOMAINS\Account\...	NAME NOT FOUND	Desired Access: R...
17:25...	svchost.exe	452	RegOpenKey	HKLM\SAM\SAM\DOMAINS\Account\...	SUCCESS	Desired Access: R...
17:25...	svchost.exe	452	RegQueryValue	HKLM\SAM\SAM\DOMAINS\Account\...	SUCCESS	Type: REG_BINARY...
17:25...	svchost.exe	452	RegCloseKey	HKLM\SAM\SAM\DOMAINS\Account\...	SUCCESS	
17:25...	svchost.exe	452	RegOpenKey	HKLM\SAM\SAM\DOMAINS\Account\...	NAME NOT FOUND	Desired Access: R...
17:25...	svchost.exe	452	RegOpenKey	HKLM\SAM\SAM\DOMAINS\Account\...	NAME NOT FOUND	Desired Access: R...
17:25...	svchost.exe	452	RegQueryValue	HKLM\SAM\SAM\DOMAINS\Account\...	SUCCESS	Desired Access: R...
17:25...	svchost.exe	452	RegCloseKey	HKLM\SAM\SAM\DOMAINS\Account\...	SUCCESS	Type: REG_BINARY...
17:25...	svchost.exe	452	RegOpenKey	HKLM\SAM\SAM\DOMAINS\Account\...	SUCCESS	Desired Access: R...
17:25...	svchost.exe	452	RegQueryValue	HKLM\SAM\SAM\DOMAINS\Account\...	SUCCESS	Type: REG_BINARY...
17:25...	svchost.exe	452	RegCloseKey	HKLM\SAM\SAM\DOMAINS\Account\...	SUCCESS	
17:25...	VBoxTray.exe	1040	Thread Create		SUCCESS	Thread ID: 2808
17:25...	VBoxTray.exe	1040	Thread Exit		SUCCESS	Thread ID: 2808...
17:25...	VBoxService.exe	656	RegQueryValue	HKLM	SUCCESS	Query: HandleTag...
17:25...	VBoxService.exe	656	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Ser...	REPARSE	Desired Access: R...
17:25...	VBoxService.exe	656	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Ser...	SUCCESS	Desired Access: R...
17:25...	VBoxService.exe	656	RegQueryValue	HKLM\SYSTEM\CurrentControlSet\ser...	SUCCESS	Query: HandleTag...
17:25...	VBoxService.exe	656	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\ser...	SUCCESS	Desired Access: Q...
17:25...	VBoxService.exe	656	RegQueryValue	HKLM\SYSTEM\CurrentControlSet\ser...	SUCCESS	Type: REG_DWORD...
17:25...	VBoxService.exe	656	RegCloseKey	HKLM\SYSTEM\CurrentControlSet\ser...	SUCCESS	
17:25...	VBoxService.exe	656	RegCloseKey	HKLM\SYSTEM\CurrentControlSet\ser...	SUCCESS	
2604	RegQueryKey		HKLM			
2604	RegOpenKey		HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Diagnostics			
2604	CreateFile		C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\msgina32.dll			
2604	WriteFile		C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\msgina32.dll			
2604	WriteFile		C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\msgina32.dll			
2604	CloseFile		C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\msgina32.dll			
2604	RegQueryKey		HKLM			
2604	RegCreateKey		HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon			
2604	RegSetInfoKey		HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon			
2604	RegQueryKey		HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon			
2604	RegSetValue		HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL			
2604	RegCloseKey		HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon			
2604	Thread Exit					

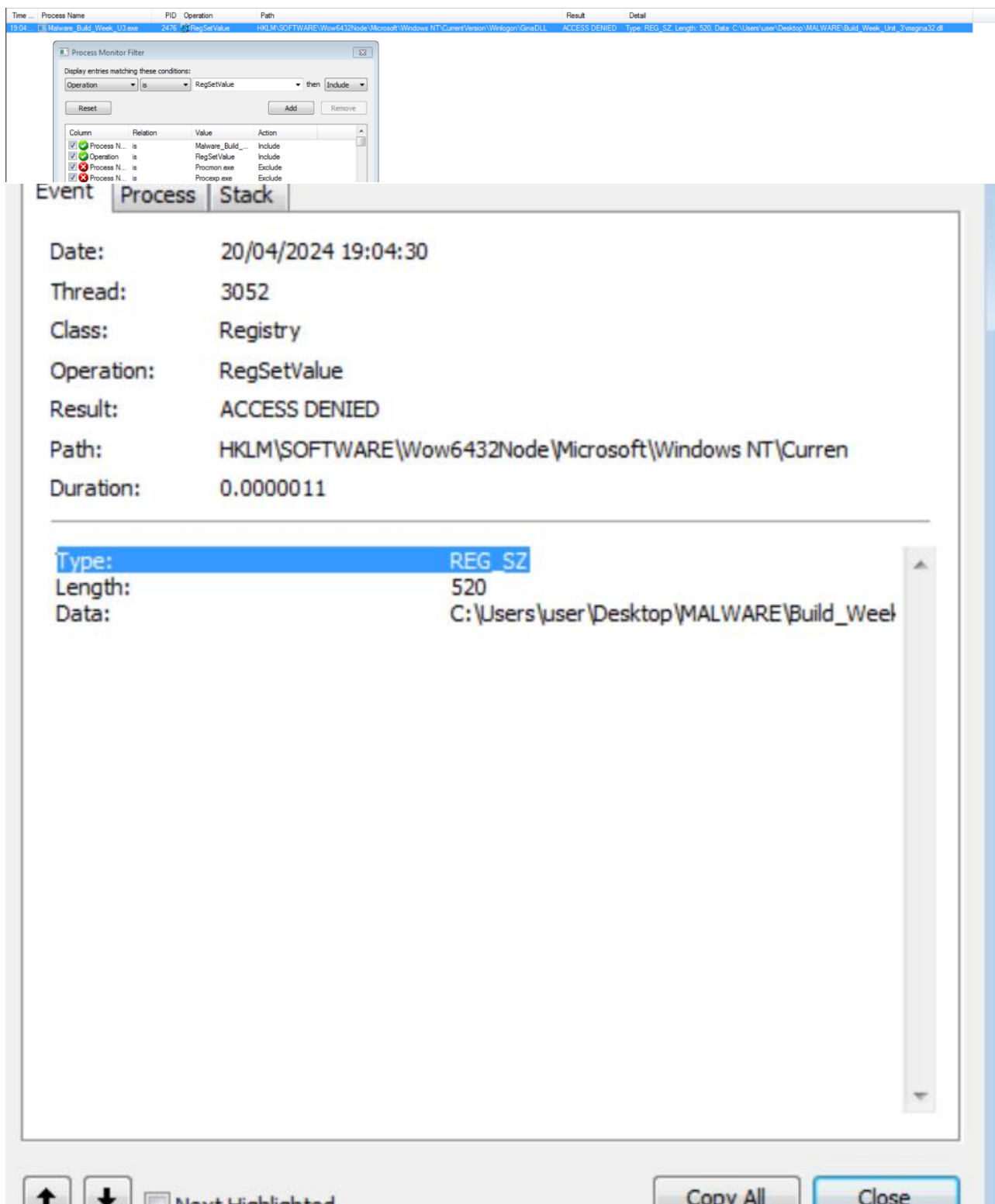
Analizzando le informazioni possiamo vedere qualche chiave verrà creata con il valore che le verrà associato e quale chiamata di sistema ha modificato il contenuto della cartella dov'è presente l'eseguibile.

The screenshot shows the Process Monitor application window. The main pane displays a list of system events with columns for Time, Process Name, PID, Operation, Path, Result, and Detail. The events are filtered to show only those related to the process 'Malware_Build_Week_U3.exe'. The filter dialog box is open, showing the filter conditions: 'Path is C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3 then Include'. The filter table shows the following entries:

Column	Relation	Value	Action
Process Name	is	Malware_Build_Week_U3.exe	Include
Operation	is	RegSetValue	Include
Process Name	is	Procmon.exe	Exclude

The main pane shows the following events for 'Malware_Build_Week_U3.exe':

Time	Process Name	PID	Operation	Path	Result	Detail
19:04...	Malware_Build_Week_U3.exe	2476	CreateFile	C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, ...
19:04...	Malware_Build_Week_U3.exe	2476	CloseFile	C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3	SUCCESS	



Con le informazioni raccolte posso quindi constatare che il malware una volta avviato, creerà una chiave all'interno del sistema con un file nella cartella di "partenza"; che otterrà persistenza e sarà avviato ad ogni start del SO.

Prendo inoltre in esame l'hash del file GinaDLL per confrontarlo nuovamente su virustotal e notare che effettivamente si tratti di un trojan, probabilmente utilizzato per fare una copia delle credenziali e salvarle tutte in un file system

chiamato msutil32.sys con il seguente path:
%SystemRoot%\System32\msutil32.sys

Nome	Ultima modifica	Tipo
Malware_Build_Week_U3	17/01/2024 17:48	Applicazione
msgina32.dll	20/04/2024 19:40	Estensione dell'

File: msgina32.dll

- Dos Header
- NT Headers
- File Header
- Optional Header
- Data Directories [x]
- Section Headers [x]
- Export Directory
- Import Directory
- Relocation Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Addr
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

Property	Value
File Name	C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\msgina32.dll
File Type	Portable Executable 32
File Info	Microsoft Visual C++ 6.0 DLL
File Size	6.50 KB (6656 bytes)
PE Size	6.50 KB (6656 bytes)
Created	Saturday 20 April 2024, 19:40:55
Modified	Saturday 20 April 2024, 19:40:55
Accessed	Saturday 20 April 2024, 19:40:55
MD5	7CE4F799946F0FA44E5B2B5E6A702F27
SHA-1	951FB580702D02E5C327B56CC709EE3AD5523D2

Property	Value
Empty	No additional info available

virustotal.com/gui/file/f8a4f61bccd5bab1cad0ab9e57f6f3092a8bd4dd0adfc4853e89ba96afc93f9/detection

51 / 71

93/71 security vendors and no sandboxes flagged this file as malicious

Size: 6.50 KB | Last Modification Date: 19 days ago

Popular threat label: trojan:fragtor/tiggre | Threat categories: trojan | Family labels: fragtor, tiggre

Security vendors' analysis	Do you want to automate checks?
Alibaba: Trojan.Win32/Tiggre-387d5a16	AICloud: Trojan.Win.Generic.F3be1728
ALYac: Gen:Variant.Fragtor.510142	AnSly-AVL: Trojan.Win32.FakeGina
Arcabit: Trojan.Fragtor.D7C88E	Avast: Win32:Trojan-gen
AVG: Win32:Trojan-gen	Avira (no cloud): HEUR/AGEN.1306250
BitDefender: Gen:Variant.Fragtor.510142	BitDefenderTheta: Gen.NN.Zedaf.36802.aq4@docOb
Bkav Pro: W32.Common.1467C8BC	ClamAV: Win.Trojan.Agent-595082
CrowdStrike Falcon: Win/malicious_confidence_100% (W)	Cylance: Unsafe
Cymet: Malicious (score: 100)	DeepInstinct: MALICIOUS
DrWeb: BackDoor.Siggen2.1609	Emisoft: Gen:Variant.Fragtor.510142 (B)

Capabilities

- Host-Interaction
 - Create or open registry key
 - Terminate process
 - Get common file path
 - Set registry value
 - Terminate process
 - Get common file path
 - Set registry value
- Persistence
 - Persist via GinaDLL registry key
- Linking
 - Link function at runtime on Windows

This malware is a credential stealer and he use msgina32.dll to take your credentials and save it all in a file system named msutil32.sys in the following path:
%SystemRoot%\System32\msutil32.sys

Capabilities ⓘ

— Host-Interaction

- Create or open registry key
- Terminate process
- Get common file path
- Set registry value
- Terminate process
- Get common file path
- Set registry value

— Persistence

- Persist via GinaDLL registry key

— Linking

- Link function at runtime on Windows