UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

Software Security

Malware Analysis – Agent Tesla

Anno Accademico 2023/2024

Professore

Prof. Roberto Natella

Studente

Marco Cimmino M63001528

Indice

Introduzione 2

1) Basic Static Analysis 3

- **Prima considerazione:** 8
- **Seconda considerazione:** 13

2) Advanced Static Analysis 22

- **Terza considerazione:** 28

3) Basic Dynamic Analysis 29

4) Malware Detection 38

5) Mitre ATT&CK 39

6) Considerazioni finali 41

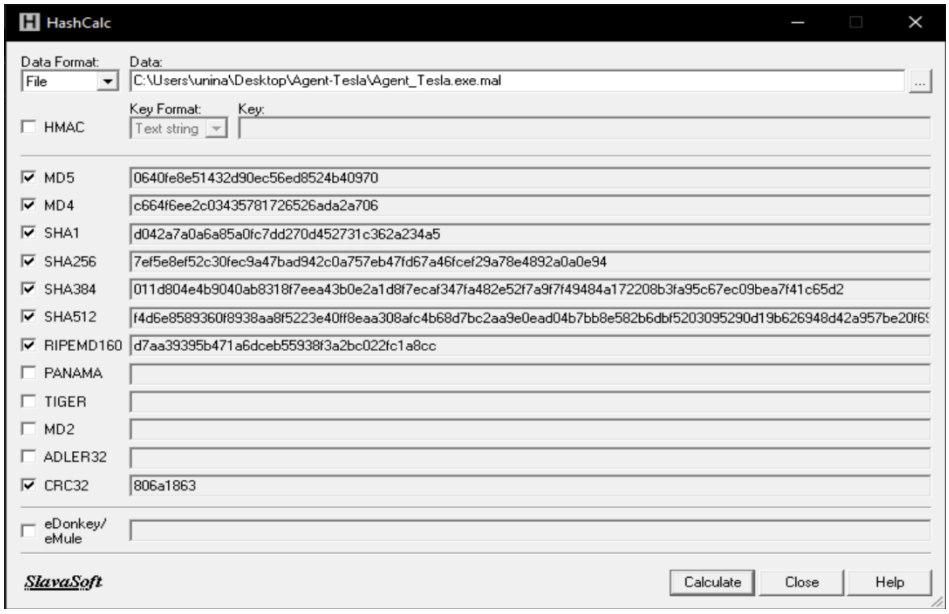
Introduzione

Nel progetto verranno esaminate le diverse fasi dell'analisi di base del malware per comprendere il comportamento, la struttura e l'impatto potenziale di un software malevolo. Inizieremo con l'ottenimento di un campione del malware, per poi procedere con l'analisi statica, che comprenderà l'esame delle proprietà del file, la generazione degli hash, l'analisi del formato PE per gli eseguibili Windows e la ricerca di stringhe nel codice. Analizzeremo poi il codice tramite tecniche di reverse engineering per comprendere le istruzioni e le funzioni principali. Successivamente, ci occuperemo dell'analisi dinamica, eseguendo il malware in un ambiente sicuro e monitorando le attività e le modifiche al sistema.

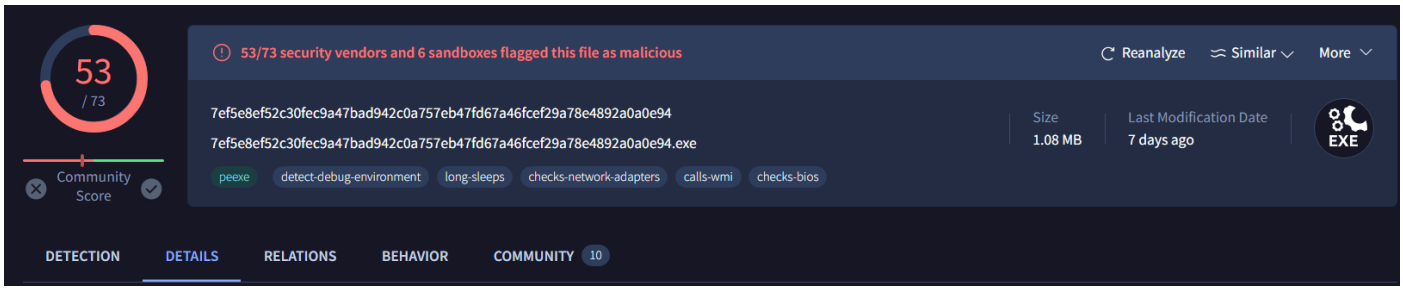
Il malware in questione è "Agent Tesla", che di recente ha intensificato le sue campagne di phishing contro il nostro Paese, arricchendo costantemente il suo arsenale di nuove funzionalità. Approfittando della pandemia di Covid-19 – che ha rappresentato un vero e proprio impulso per il cybercrime – Agent Tesla è riuscito a evolversi, sfruttando l'aumento dei potenziali obiettivi dovuto alla diffusione dello smart working. Lo scorso 10 settembre, l'Indipendent Malware Hunter JAMESWT ha condiviso su Twitter uno screenshot di un allegato (una fattura) proveniente dalla sede uruguayana di un’azienda reale, destinata a un’organizzazione nel nostro Paese. Il testo, in spagnolo, era una classica esca per trarre in inganno le organizzazioni: “ricevuta riguardo l’ultimo pagamento”. Il payload era nascosto nell’allegato compresso. Ovviamente, se cliccato ed estratto, questo documento avviava la catena d’infezione di Agent Tesla.

1) Basic Static Analysis

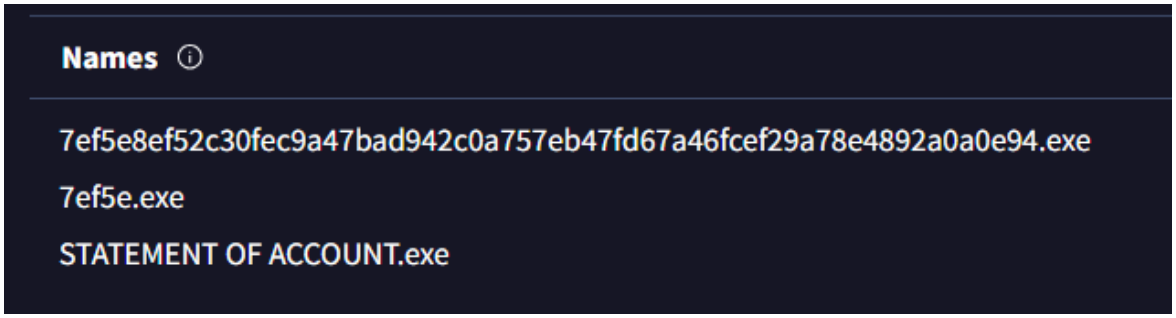
Il primo passo è stato estrarre i valori degli hash utilizzando il tool HashCalc, al fine di analizzarli sul sito VirusTotal.



Esso viene correttamente riconosciuto da VirusTotal il quale ne riporta uno score Flag di 53/73:



Andando ad analizzare ulteriori dettagli forniti da VirusTotal possiamo scoprire anche gli altri nomi con cui è conosciuto il malware:



Ci fornisce inoltre dettagli sulla storia passata del malware:

History

Creation Time	2024-05-02 22:40:19 UTC
First Seen In The Wild	2024-05-03 01:24:07 UTC
First Submission	2024-05-03 00:38:46 UTC
Last Submission	2024-06-25 09:12:02 UTC
Last Analysis	2024-05-14 12:28:28 UTC

La creazione risale al 02/05/2024. Ciò è confermata anche analizzando il .exe tramite PE View

pFile	Data	Description	Value
00000124	014C	Machine	IMAGE_FILE_MACHINE_I386
00000126	0005	Number of Sections	
00000128	66341653	Time Date Stamp	2024/05/02 Thu 22:40:19 UTC
0000012C	00000000	Pointer to Symbol Table	
00000130	00000000	Number of Symbols	
00000134	00E0	Size of Optional Header	
00000136	0122	Characteristics	
		0002	IMAGE_FILE_EXECUTABLE_IMAGE
		0020	IMAGE_FILE_LARGE_ADDRESS_AWARE
		0100	IMAGE_FILE_32BIT_MACHINE

Altre informazioni molto utili fornite da VirusTotal sono il valore di entropia che come previsto risulta elevato:

Sections

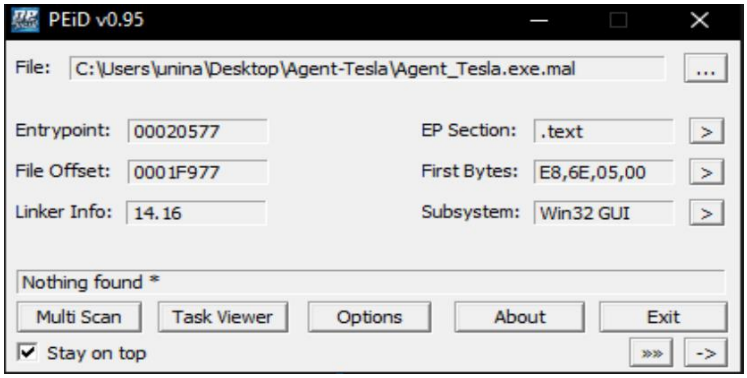
Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
.text	4096	633629	633856	6.67	0a1473f3064dcbc32ef93c5c8a90f3a6	3340767.5
.rdata	638976	195458	195584	5.69	c9cf2468b60bf4f80f136ed54b3989fb	5254473.5
.data	835584	28780	18432	0.58	53b9025d545d65e23295e30afdbd16d9	4245034.5
.rsrc	868352	257116	257536	7.83	3844fa967d8dd9c139696ac5def7bea6	207176.03
.reloc	1126400	30100	30208	6.8	c68ee8931a32d45eb82dc450ee40efc3	113360.77

Analizzando l’eseguibile possiamo ricavare anche il valore di Entropy generale del file, oltre a informazioni come il file-size ma soprattuto la signature con Microsoft Visual C++, che è un info utile che rivedremo in seguito:

file-size	1136640 bytes
entropy	6.998
imphash	n/a
signature	Microsoft Visual C++
tooling	Visual Studio 2017 - 15.5.0 preview 2

VirusTotal ci fornisce anche una rapida panoramica sulle librerie importante, che andremo ad analizzare più nel dettaglio in seguito grazie al tool Dependency Walker:

A questo punto, Tramite il tool PEId, è possibile ottenere degli indizi sul fatto se il malware è packed. Esso può rilevare packer, cryptor o compilatori utilizzati per creare il file eseguibile.



Tuttavia, questo non ci aiuta a capire se il file sia packed o meno, bisognerà quindi utilizzare nuovamente PE view per valutare una possibile discrepanza significativa tra la dimensione dei Raw Data e la Virtual Size.

pFile	Data	Description	Value
00000240	2E 72 64 61	Name	.rdata
00000244	74 61 00 00		
00000248	0002FB82	Virtual Size	
0000024C	0009C000	RVA	
00000250	0002FC00	Size of Raw Data	
00000254	0009B000	Pointer to Raw Data	
00000258	00000000	Pointer to Relocations	
0000025C	00000000	Pointer to Line Numbers	
00000260	0000	Number of Relocations	
00000262	0000	Number of Line Numbers	
00000264	40000040	Characteristics	
		00000040	IMAGE_SCN_CNT_INITIALIZED_DATA
		40000000	IMAGE_SCN_MEM_READ

.rdata

pFile	Data	Description	Value
000002B8	2E 72 65 6C	Name	.reloc
000002BC	6F 63 00 00		
000002C0	00007594	Virtual Size	
000002C4	00113000	RVA	
000002C8	00007600	Size of Raw Data	
000002CC	0010E200	Pointer to Raw Data	
000002D0	00000000	Pointer to Relocations	
000002D4	00000000	Pointer to Line Numbers	
000002D8	0000	Number of Relocations	
000002DA	0000	Number of Line Numbers	
000002DC	42000040	Characteristics	
		00000040	IMAGE_SCN_CNT_INITIALIZED_DATA
		02000000	IMAGE_SCN_MEM_DISCARDABLE
		40000000	IMAGE_SCN_MEM_READ

.reloc

pFile	Data	Description	Value
00000290	2E 72 73 72	Name	.rsrc
00000294	63 00 00 00		
00000298	0003EC5C	Virtual Size	
0000029C	000D4000	RVA	
000002A0	0003EE00	Size of Raw Data	
000002A4	000CF400	Pointer to Raw Data	
000002A8	00000000	Pointer to Relocations	
000002AC	00000000	Pointer to Line Numbers	
000002B0	0000	Number of Relocations	
000002B2	0000	Number of Line Numbers	
000002B4	40000040	Characteristics	
		00000040	IMAGE_SCN_CNT_INITIALIZED_DATA
		40000000	IMAGE_SCN_MEM_READ

.rsrc

pFile	Data	Description	Value
00000218	2E 74 65 78	Name	.text
0000021C	74 00 00 00		
00000220	0009AB1D	Virtual Size	
00000224	00001000	RVA	
00000228	0009AC00	Size of Raw Data	
0000022C	00000400	Pointer to Raw Data	
00000230	00000000	Pointer to Relocations	
00000234	00000000	Pointer to Line Numbers	
00000238	0000	Number of Relocations	
0000023A	0000	Number of Line Numbers	
0000023C	60000020	Characteristics	
		00000020	IMAGE_SCN_CNT_CODE
		20000000	IMAGE_SCN_MEM_EXECUTE
		40000000	IMAGE_SCN_MEM_READ

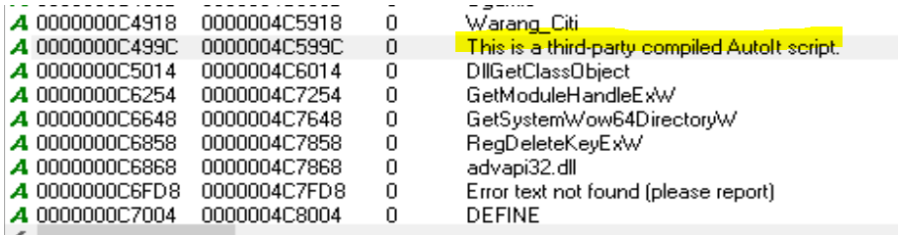
.text

pFile	Data	Description	Value
00000268	2E 64 61 74	Name	.data
0000026C	61 00 00 00		
00000270	0000706C	Virtual Size	
00000274	000CC000	RVA	
00000278	00004800	Size of Raw Data	
0000027C	000CAC00	Pointer to Raw Data	
00000280	00000000	Pointer to Relocations	
00000284	00000000	Pointer to Line Numbers	
00000288	0000	Number of Relocations	
0000028A	0000	Number of Line Numbers	
0000028C	C0000040	Characteristics	
		00000040	IMAGE_SCN_CNT_INITIALIZED_DATA
		40000000	IMAGE_SCN_MEM_READ
		80000000	IMAGE_SCN_MEM_WRITE

.data

Solo nel .data vi è una differenza sostanziale, mentre nel resto del file vi è solo una leggera discrepanza tra le due Size. Ciò ci lascia pensare che il File potrebbe essere packed, ma non nella sua interezza. La conferma la otteniamo grazie al tool BinText, che ci presenta una sezione totalmente illeggibile:

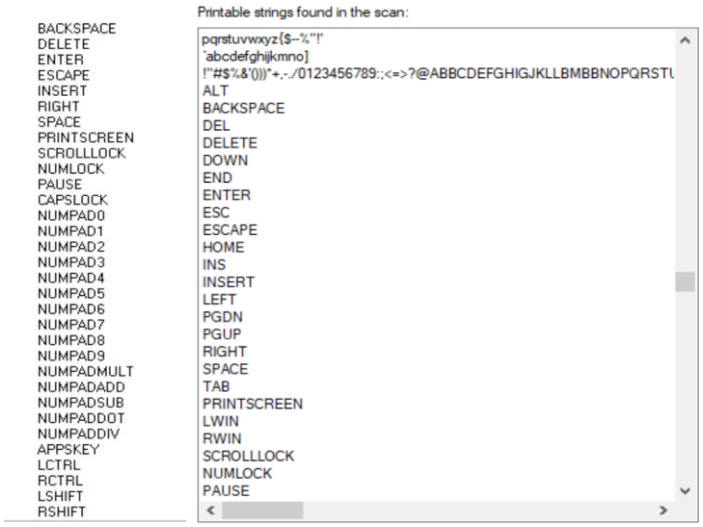
Mentre un’altra sezione con informazioni utili, Come la presenza di uno script AutoIt:



0000000C4918	0000004C5918	0	Warang_Citi
0000000C499C	0000004C599C	0	This is a third-party compiled AutoIt script.
0000000C5014	0000004C6014	0	DllGetClassObject
0000000C6254	0000004C7254	0	GetModuleHandleExW
0000000C6648	0000004C7648	0	GetSystemWow64DirectoryW
0000000C6858	0000004C7858	0	RegDeleteKeyExW
0000000C6868	0000004C7868	0	advapi32.dll
0000000C6FD8	0000004C7FD8	0	Error text not found (please report)
0000000C7004	0000004C8004	0	DEFINE

AutoIt è un linguaggio di scripting gratuito progettato per automatizzare l'interfaccia grafica di Windows e le attività di scripting in generale. Originariamente è stato sviluppato per automatizzare la configurazione di grandi numeri di PC, ma ad oggi AutoIt è utilizzato per automatizzare qualsiasi attività di amministrazione di Windows.

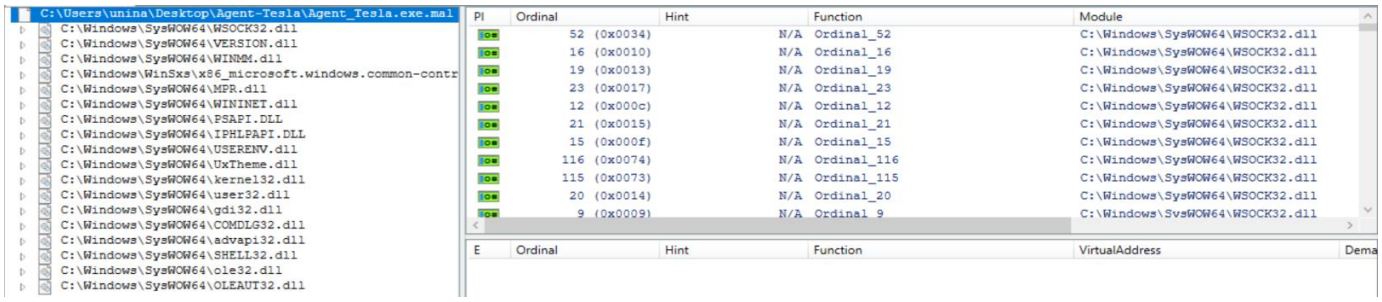
Inoltre, è presente un chiaro identificativo di un keylogger, ovvero la possibilità di essere navigato con i tasti per poter verificare tutti i caratteri registrati, che si trovano nelle stringhe del programma:



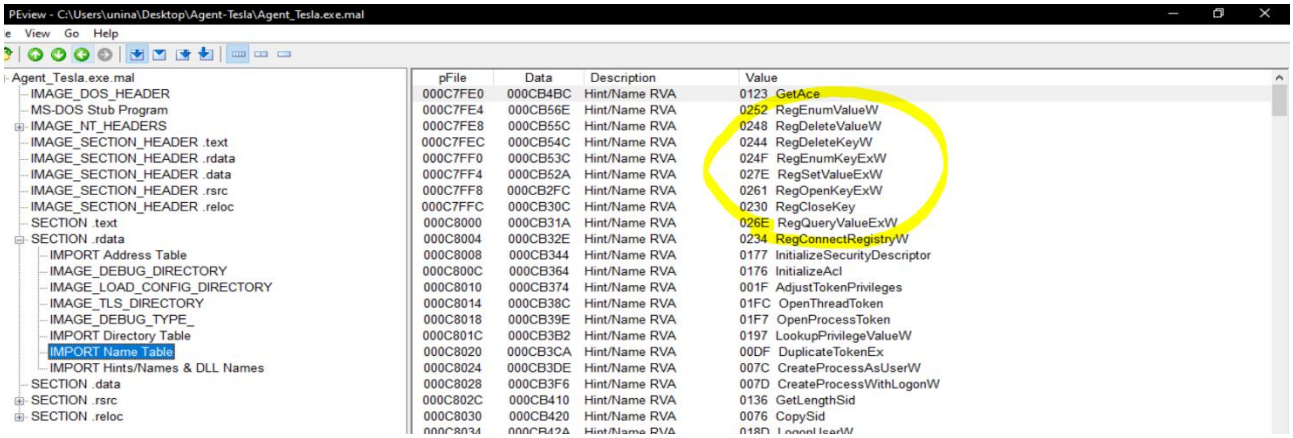
• Prima considerazione:

Una prima analisi del funzionamento del malware potrebbe derivare dall'integrazione dello script AutoIt con l'uso del compilatore Microsoft Visual C++. Possiamo dedurre che questo eseguibile agisca come un loader o uno stealer che prepara la memoria e carica lo script AutoIt per l'esecuzione.

Passiamo ora all'analisi delle librerie, grazie al tool Dependecy Walker. È presente una mole non indifferente di librerie importate:



Altri elementi sospetti nell'import name table

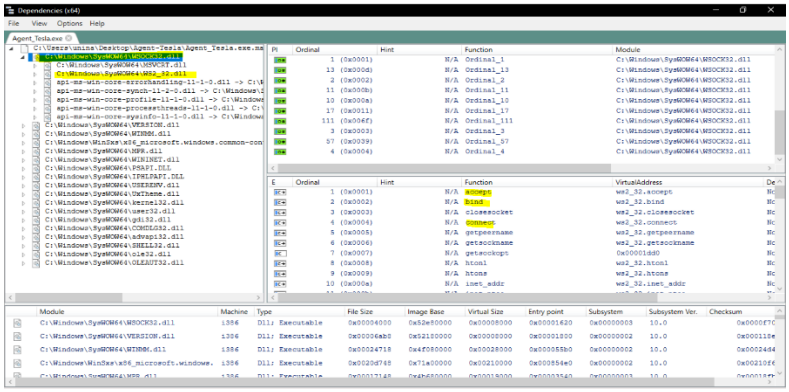


Le funzioni come RegSetValueExA, RegOpenKeyA, RegCloseKey, RegDeleteValue e simili sono funzioni dell'API di Windows utilizzate per manipolare il Registro di Sistema.

Queste funzioni non sono di per sé sospette, in quanto sono parte integrante delle operazioni legittime di gestione del Registro di Sistema in Windows. Tuttavia, nel nostro contesto, l'uso eccessivo o anomalo di queste funzioni può indicare attività dannose. Ad esempio, il malware potrebbe utilizzare queste funzioni per:

Modificare impostazioni critiche nel Registro di Sistema per avviarsi all'avvio del sistema, garantendosi persistenza o modificare il comportamento del sistema. Inoltre, potrebbe nascondere le sue tracce cancellando o modificando valori nel Registro.

Ritroviamo anche WS2_32.dll e WININET, librerie di Windows che forniscono le API per la comunicazione di rete.



Queste librerie contengono funzioni e strumenti per la creazione, la gestione e la comunicazione con le connessioni di rete. In particolare, l’utilizzo delle funzioni accept, bind e connect potrebbe essere un campanello di allarme. Queste funzioni sono tipicamente utilizzate nella programmazione delle socket per stabilire e gestire connessioni di rete, e potrebbero indicare che il malware ha funzionalità di comunicazione in rete.

• **accept:** Questa funzione viene utilizzata per accettare una nuova connessione in arrivo su una socket. Se il malware utilizzasse questa funzione, potrebbe significare che il malware stesso agisce come un server, consentendo a client esterni di connettersi ad esso.

• **bind:** Questo è un passo necessario prima di chiamare listen o connect. Se il malware utilizza bind, potrebbe significare che sta cercando di legarsi a un'interfaccia di rete specifica per ascoltare o inviare dati.

• **connect**: Questa funzione viene utilizzata per iniziare una connessione a un altro endpoint (come un server) su una socket. Se il malware utilizza connect, potrebbe significare che sta cercando di stabilire una connessione con un server remoto o con un altro dispositivo sulla rete. Tra le funzioni più note, ritroviamo la presenza di:

• FindNextFileA e FindFirstFileA

Utilizzate da malware per cercare e individuare determinati tipi di file nel sistema, come file di configurazione sensibili, file di password o file di sistema critici. Queste informazioni possono quindi essere utilizzate per scopi dannosi, come il furto di dati o la compromissione del sistema.

• CopyFileA

Può essere utilizzata da malware per creare copie di file dannosi o per distribuire sé stesso attraverso una rete. Ad esempio, un malware potrebbe copiare sé stesso in una posizione diversa del sistema per eludere la rilevazione dell'antivirus o potrebbe copiare file dannosi nei percorsi di avvio per garantire l'esecuzione automatica al riavvio del sistema.

Di seguito riportiamo una lista di funzioni sospette importate:

Funzioni di Manipolazione dei File:

DeleteFileW - Elimina un file.

MoveFileW - Sposta un file.

FindFirstFileW - Cerca il primo file che corrisponde a un certo modello di nome.

Funzioni di Manipolazione dei Processi:

CreateProcessW – OpenProcess: Apre processi o ne crea di nuovi.

Funzioni di Manipolazione del Registro di Sistema:

RegSetValueExW - Imposta il valore di un'entrata nel Registro di Sistema.

RegCreateKeyExW - Crea o apre una chiave del Registro di Sistema.

Funzioni di Esecuzione di Programmi (Process Injection) e Funzioni di Manipolazione della Memoria:

ShellExecuteW - Esegue un programma specificato da un file, gestisce i collegamenti e le applicazioni.

LoadLibraryW - Carica dinamicamente una libreria (DLL).

VirtualAllocEx - Alloca memoria nello spazio di indirizzamento di un processo.

WriteProcessMemory - Scrive dati nella memoria di un processo.

ReadProcessMemory - Legge dati dalla memoria di un processo.

VirtualAlloc - Alloca memoria nel proprio spazio di indirizzamento.

Funzioni di Sicurezza e Accesso Token:

InitializeSecurityDescriptor - Inizializza un descrittore di sicurezza.

InitializeAcl - Inizializza una lista di controllo di accesso (ACL).

AdjustTokenPrivileges - Modifica i privilegi associati a un token di accesso.

OpenThreadToken - Ottiene un token di accesso associato a un thread.

Funzioni di Riconoscimento del Sistema:

GetSystemDirectoryW - Ottiene il percorso del directory system di Windows.

GetWindowsDirectoryW - Ottiene il percorso del directory di Windows.

Funzioni di Rilevamento e Analisi del Sistema:

IsDebuggerPresent - Verifica se il processo è in esecuzione in un debugger.

Tramite la Kernel32.dll e la User32.dll l'eseguibile è in grado di utilizzare funzioni di manipolazione di file e processi, e grazie a WS2_32.dll e WININET.dll è in grado di generare connessioni. Infine, utilizza AVDVAPI32.dll per una presunta Privilage Escalation e Process Injection.

• **Seconda considerazione:**

Possiamo dunque ipotizzare che questo programma prepari il file incorporato per l'esecuzione, utilizzando tecniche di Privilage Escalation per avviarlo. In questo modo il programma potrebbe effettuare una Process Injection, modificando un processo in esecuzione in modo da ospitare lo script dannoso AutoIt trovato precedentemente, permettendo così all'attaccante di eseguire operazioni come la creazione di una Backdoor, lo Stealing dei dati o il Loading di altri eseguibili.

Questa, tuttavia, è solo una considerazione sulla base delle informazioni ricavate. Per avere un'idea più precisa del suo funzionamento è necessario eseguire un'analisi statica avanzata, analizzando più nel dettaglio il codice disassemblato dell'eseguibile.

Come fase preparatoria analizziamo il file tramite capa.exe:

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

C:\Users\unina\Desktop\Tools>capa.exe C:\Users\unina\Desktop\Agent-Tesla\Agent_Tesla.exe.mal
loading : 100%|▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰▰| 661/661 [00:00<00:00, 2014.85 rules/s]
WARNING:capa:-------------------------------------------------------------------------------
WARNING:capa: This sample appears to be compiled with AutoIt.
WARNING:capa:
WARNING:capa: AutoIt is a freeware BASIC-like scripting language designed for automating the Windows GUI.
WARNING:capa: capa cannot handle AutoIt scripts. This means that the results will be misleading or incomplete.
WARNING:capa: You may have to analyze the file manually, using a tool like the AutoIt decompiler MyAut2Exe.
WARNING:capa:
WARNING:capa: Identified via rule: (internal) autoit file limitation
WARNING:capa:
WARNING:capa: Use -v or -vv if you really want to see the capabilities identified by capa.
WARNING:capa:-------------------------------------------------------------------------------
```

Essendo compilato in AutoIt dovremo accontentarci di un'analisi più limitata. Tuttavia, riusciamo comunque ad estrapolare delle informazioni utili in vista dell'analisi del codice tramite IDAPro

L’output di capa è il seguente:

```
check for time delay via QueryPerformanceCounter (4 matches)
namespace  anti-analysis/anti-debugging/debugger-detection
scope      function
matches    0x469C49
           0x469C60
           0x46B0A8
           0x46E97B

check for unmoving mouse cursor (2 matches)
namespace  anti-analysis/anti-vm/vm-detection
scope      function
matches    0x498FC9
           0x499576

receive and write data from server to client
namespace  c2/file-transfer
scope      function
matches    0x47CE44

log keystrokes (9 matches)
namespace  collection/keylog
scope      function
matches    0x401BC3
           0x41F98E
           0x4625A2
           0x462DA7
           0x463A3D
           0x46A9ED
           0x46B12F
           0x46B27A
           0x46B2DF

log keystrokes via polling (11 matches)
namespace  collection/keylog
scope      function
matches    0x41912D
           0x41E187
           0x469C79
           0x469F91
           0x46A9ED
           0x46AA57
```

```
capture screenshot
namespace  collection/screenshot
scope      function
matches    0x48255C

query remote server for available data
namespace  communication
scope      basic block
matches    0x47CF1A

receive data (3 matches)
namespace    communication
description  all known techniques for receiving data from a potential C2 server
scope        function
matches      0x47CE44
             0x47CF1A
             0x481433

send data (2 matches)
namespace    communication
description  all known techniques for sending data to a potential C2 server
scope        function
matches      0x47C476
             0x4815CA

connect network resource
namespace    communication/http
description  connect to disk or print resource
scope        function
matches      0x4606DE

parse URL
namespace  communication/http
scope      basic block
matches    0x47D0F4

check HTTP status code
namespace  communication/http/client
scope      function
matches    0x494873
```

```
connect to HTTP server (2 matches)
namespace  communication/http/client
scope      function
matches    0x47C143
           0x47C476

connect to URL
namespace  communication/http/client
scope      function
matches    0x47C253

create HTTP request
namespace  communication/http/client
scope      function
matches    0x47CD1E

read data from Internet (2 matches)
namespace  communication/http/client
scope      function
matches    0x47CE44
           0x47CF1A
```

```
send HTTP request
namespace  communication/http/client
scope      function
matches    0x47C476

send ICMP echo request
namespace  communication/icmp
scope      function
matches    0x48055B

create pipe (2 matches)
namespace  communication/named-pipe/create
scope      function
matches    0x4704D2
           0x4705A7

receive data on socket
namespace  communication/socket/receive
scope      function
matches    0x481433
```

```
send data on socket
namespace  communication/socket/send
scope      function
matches    0x4815CA

connect TCP socket
namespace  communication/socket/tcp
scope      function
matches    0x4810B8

create TCP socket (2 matches)
namespace  communication/socket/tcp
scope      basic block
matches    0x48110C
           0x481270

create UDP socket (2 matches)
namespace  communication/socket/udp/send
scope      basic block
matches    0x481857
           0x481AD6

act as TCP client
namespace  communication/tcp/client
scope      function
matches    0x4810B8

compiled with AutoIt
namespace  compiler/autoit
scope      file

encode data using Base64
namespace  data-manipulation/encoding/base64
scope      function
matches    0x41B731

encode data using XOR (7 matches)
namespace  data-manipulation/encoding/xor
scope      basic block
matches    0x4696D0
           0x472012
           0x47207E
```

```
encrypt data using RC4 PRGA
namespace  data-manipulation/encryption/rc4
scope      function
matches    0x41CB89

authenticate HMAC
namespace  data-manipulation/hmac
scope      function
matches    0x41B731

generate random numbers using a Mersenne Twister (4 matches)
namespace  data-manipulation/prng/mersenne
scope      function
matches    0x471F5C
           0x471FA2
           0x472006
           0x472046

contain a resource (.rsrc) section
namespace  executable/pe/section/rsrc
scope      file

extract resource via kernel32 functions (7 matches)
namespace  executable/resource
scope      function
matches    0x403923
           0x4042A2
           0x4696E2
           0x46989B
           0x46DA5A
           0x473388
           0x47359C

list drag and drop files
namespace  host-interaction/clipboard
scope      function
matches    0x47EAFF

open clipboard (2 matches)
namespace  host-interaction/clipboard
scope      function
matches    0x47EAFF
           0x47ED6A
```

```
read clipboard data
namespace  host-interaction/clipboard
scope      function
matches    0x47EAFF

replace clipboard data
namespace  host-interaction/clipboard
scope      function
matches    0x47ED6A

write clipboard data
namespace  host-interaction/clipboard
scope      function
matches    0x47ED6A

interact with driver via control codes (4 matches)
namespace  host-interaction/driver
scope      function
matches    0x46D5EB
           0x46D66A
           0x46D6E6
           0x473D1E

get COMSPEC environment variable
namespace  host-interaction/environment-variable
scope      function
matches    0x41CF92

query environment variable (3 matches)
namespace  host-interaction/environment-variable
scope      function
matches    0x41CF92
           0x47EEED
           0x487632

set environment variable (2 matches)
namespace  host-interaction/environment-variable
scope      function
matches    0x43D1D0
           0x47EF5D

get common file path (9 matches)
namespace  host-interaction/file-system
scope      function
```

```
copy file (2 matches)
namespace  host-interaction/file-system/copy
scope      function
matches    0x46D29C
           0x472947

create directory (2 matches)
namespace  host-interaction/file-system/create
scope      function
matches    0x46D2C1
           0x473D1E

delete directory (2 matches)
namespace  host-interaction/file-system/delete
scope      function
matches    0x46E85D
           0x473D1E

delete file (4 matches)
namespace  host-interaction/file-system/delete
scope      function
matches    0x46D076
           0x46D3A9
           0x472947
           0x4756D9

check if file exists (3 matches)
namespace  host-interaction/file-system/exists
scope      function
matches    0x46D2C1
           0x46DBBE
           0x46E199

enumerate files recursively (3 matches)
namespace  host-interaction/file-system/files/list
scope      function
matches    0x479642
           0x47979D
           0x479B2B

enumerate files via kernel32 functions (6 matches)
namespace  host-interaction/file-system/files/list
scope      function
matches    0x46D076
```

```
get file attributes (5 matches)
namespace  host-interaction/file-system/meta
scope      basic block
matches    0x46D2C1
           0x46DBDC
           0x46E199
           0x477FE6
           0x47969A

get file size (2 matches)
namespace  host-interaction/file-system/meta
scope      function
matches    0x482ADE
           0x49856F

get file version info
namespace  host-interaction/file-system/meta
scope      function
matches    0x46DC0E

set file attributes (2 matches)
namespace  host-interaction/file-system/meta
scope      basic block
matches    0x477FE6
           0x47969A

move file (3 matches)
namespace  host-interaction/file-system/move
scope      function
matches    0x46CF00
           0x46D076
           0x46E3FB

read .ini file (4 matches)
namespace  host-interaction/file-system/read
scope      function
matches    0x4784DF
           0x4785A1
           0x4788DE
           0x478AFB
```

```
read file on Windows (5 matches)
namespace  host-interaction/file-system/read
scope      function
matches    0x4098C0
           0x409A40
           0x4707EF
           0x482ADE
           0x49856F

create shortcut via IShellLink (2 matches)
namespace  host-interaction/file-system/write
scope      function
matches    0x47581E
           0x47648E

write file on Windows (7 matches)
namespace  host-interaction/file-system/write
scope      function
matches    0x41F4D4
           0x46CCFF
           0x470715
           0x4726D7
           0x472724
           0x472947
           0x47CE44

enumerate gui resources
namespace  host-interaction/gui
scope      function
matches    0x4641FC

find taskbar (3 matches)
namespace  host-interaction/gui/taskbar/find
scope      function
matches    0x41F98E
           0x492322
           0x492356

find graphical window (4 matches)
namespace  host-interaction/gui/window/find
scope      function
matches    0x41F98E
           0x46E6B0
```

```
get graphical window text (11 matches)
namespace  host-interaction/gui/window/get-text
scope      function
matches    0x461B2C
           0x46365B
           0x463BC4
           0x464954
           0x464C7D
           0x465C44
           0x47E9D0
           0x491EDA
           0x494873
           0x4970D5
           0x4973E8

hide graphical window (8 matches)
namespace  host-interaction/gui/window/hide
scope      basic block
matches    0x45F3DC
           0x48289B
           0x49022A
           0x4951BD
           0x496C93
           0x498248
           0x4982CD
           0x49A27E

get keyboard layout
namespace  host-interaction/hardware/keyboard
scope      function
matches    0x41CF92

get memory capacity
namespace  host-interaction/hardware/memory
scope      function
matches    0x41F291

get disk information (6 matches)
namespace  host-interaction/hardware/storage
scope      function
matches    0x473E79
           0x4744C0
```

```
get disk size (3 matches)
namespace  host-interaction/hardware/storage
scope      function
matches    0x4751CD
           0x4752B0
           0x475393

get storage device properties (2 matches)
namespace  host-interaction/hardware/storage
scope      function
matches    0x46D5EB
           0x46D66A

print debug messages
namespace  host-interaction/log/debug/write-event
scope      function
matches    0x41F4D4

resolve DNS (3 matches)
namespace  host-interaction/network/dns/resolve
scope      function
matches    0x46DE27
           0x48055B
           0x481361

shutdown system
namespace  host-interaction/os
scope      function
matches    0x46E8F6

get hostname (2 matches)
namespace  host-interaction/os/hostname
scope      function
matches    0x41CF92
           0x46DE27

get system information on Windows
namespace  host-interaction/os/info
scope      function
matches    0x4042DE

check OS version
namespace  host-interaction/os/version
```

```
read process memory
namespace  host-interaction/process
scope      function
matches    0x46B3CE

create process on Windows (6 matches)
namespace  host-interaction/process/create
scope      basic block
matches    0x442BFE
           0x461406
           0x46152E
           0x48AE53
           0x48B39A
           0x498172

allocate RWX memory
namespace  host-interaction/process/inject
scope      basic block
matches    0x48995A

enumerate processes (2 matches)
namespace  host-interaction/process/list
scope      function
matches    0x46D4DC
           0x48A67C

acquire debug privileges
namespace  host-interaction/process/modify
scope      basic block
matches    0x48A18F

modify access privileges (2 matches)
namespace  host-interaction/process/modify
scope      function
matches    0x4610BF
           0x4616C3

terminate process (3 matches)
namespace  host-interaction/process/terminate
scope      function
matches    0x46EB20
           0x487F59
```

```
empty recycle bin quietly
namespace  host-interaction/recycle-bin
scope      basic block
matches    0x477A54

empty the recycle bin
namespace  host-interaction/recycle-bin
scope      function
matches    0x477A35

create or open registry key (9 matches)
namespace  host-interaction/registry
scope      basic block
matches    0x40344D
           0x403B30
           0x4607CA
           0x48B75C
           0x48BAEA
           0x48BD0F
           0x48BF92
           0x48C521
           0x48CC7F

query or enumerate registry key (2 matches)
namespace  host-interaction/registry
scope      function
matches    0x48B9C9
           0x48CC34

query or enumerate registry value (5 matches)
namespace  host-interaction/registry
scope      function
matches    0x40344D
           0x403B1C
           0x4606DE
           0x48BBDB
           0x48BE44

set registry value
namespace  host-interaction/registry/create
scope      function
matches    0x48C3B7
```

```
get registry value
namespace  host-interaction/registry/create
scope      function
matches    0x48C3B7

delete registry key (2 matches)
namespace  host-interaction/registry/delete
scope      function
matches    0x48B60E
           0x48CC34

delete registry value
namespace  host-interaction/registry/delete
scope      function
matches    0x48B60E

get session user name
namespace  host-interaction/session
scope      function
matches    0x41CF92

get token membership
namespace  host-interaction/session
scope      function
matches    0x461663

get token privileges
namespace  host-interaction/session
scope      function
matches    0x461014

create thread (2 matches)
namespace  host-interaction/thread/create
scope      basic block
matches    0x461803
           0x470952

terminate thread
namespace  host-interaction/thread/terminate
scope      basic block
matches    0x470988

impersonate user
namespace  host-interaction/user
```

```
impersonate user
namespace  host-interaction/user
scope      function
matches    0x461201

(internal) autoit file limitation
namespace    internal/limitation/file
description  This sample appears to be compiled with AutoIt.

               AutoIt is a freeware BASIC-like scripting language designed for automating the Windows GUI.
               capa cannot handle AutoIt scripts. This means that the results will be misleading or incomplete.
               You may have to analyze the file manually, using a tool like the AutoIt decompiler MyAut2Exe.
scope        file

link function at runtime on Windows (8 matches)
namespace  linking/runtime-linking
scope      function
matches    0x4042DE
           0x404E59
           0x404E90
           0x41CF92
           0x483FE9
           0x488EE4
           0x48B60E
           0x48CC34

parse PE header
namespace  load-code/pe
scope      function
matches    0x409E90
```

Sintetizzando questo output abbiamo:

Manipolazione del file system

- Get Common File Path
- Copy File
- Create Directory
- Delete Directory
- Delete File
- Check If File Exists
- Enumerate Files Recursively
- Enumerate Files Via Kernel32 Functions
- Get File Attributes
- Get File Size
- Get File Version Info
- Set File Attributes
- Move File
- Read .ini File
- Read File on Windows
- Create Shortcut via IShellLink
- Write File on Windows

Interazione con l'interfaccia grafica

- Enumerate GUI Resources
- Find Taskbar
- Find Graphical Window
- Get Graphical Window Text
- Hide Graphical Window

Interazione con hardware e memoria

- Get Keyboard Layout
- Get Memory Capacity
- Get Disk Information
- Get Disk Size
- Get Storage Device Properties

Comunicazione di rete

- Resolve DNS

Interazione con il sistema operativo

- Shutdown System
- Get System Information on Windows
- Check OS Version

Gestione di processi

- Read Process Memory
- Create Process on Windows
- Allocate RWX Memory
- Enumerate Processes
- Acquire Debug Privileges
- Modify Access Privileges
- Terminate Process

Comunicazione di rete (HTTP/ICMP)

- Check HTTP Status Code
- Connect to HTTP Server
- Connect to URL
- Create HTTP Request
- Read Data from Internet
- Send HTTP Request
- Send ICMP Echo Request

Gestione della registry

- Create or Open Registry Key
- Query or Enumerate Registry Key
- Query or Enumerate Registry Value
- Set Registry Value
- Delete Registry Key
- Delete Registry Value

Interazione con l'ambiente di sistema

- Get COMSPEC Environment Variable
- Query Environment Variable
- Set Environment Variable
- Get Hostname

Host-interaction: Clipboard

- List Drag and Drop Files
- Open Clipboard
- Read Clipboard Data
- Replace Clipboard Data
- Write Clipboard Data

Host-interaction: Driver

- Interact with Driver via Control Codes

Host-interaction: Log/Debug

- Print Debug Messages

Host-interaction: Session/User

- Get Session User Name
- Get Token Membership
- Get Token Privileges

Host-interaction: Thread

- Create Thread
- Terminate Thread

Manipolazione dati ed encoding

- Encode Data using Base64
- Encode Data using XOR
- Encrypt Data using RC4 PRGA
- Authenticate HMAC
- Generate Random Numbers using a Mersenne Twister

Host-interaction: Recycle Bin

- Empty Recycle Bin
- Empty Recycle Bin Quietly

Linking/Runtime Linking

- Link Function at Runtime on Windows

Load-code: PE

- Parse PE Header

Internal/AutoIt

- (Internal) AutoIt File Limitation (Sample compiled with AutoIt)

Questi gruppi forniscono un quadro completo delle operazioni che il malware potrebbe eseguire sul sistema compromesso. Ogni gruppo riflette un insieme di funzionalità correlate che il malware può sfruttare per raggiungere i suoi obiettivi.

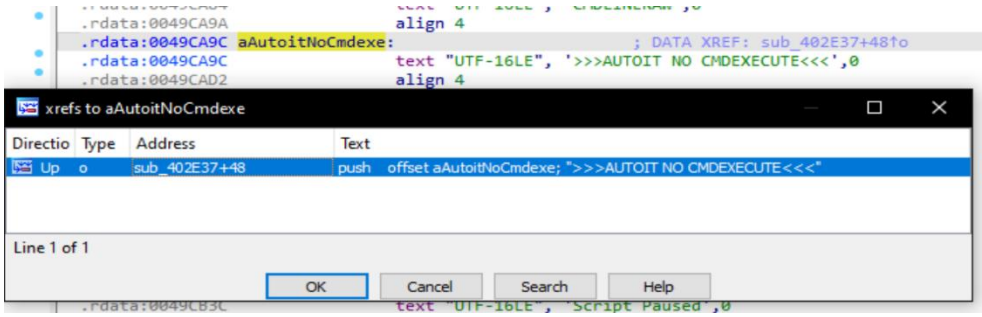
Inoltre, ci forniscono anche la posizione in memoria nel campo: “matches”, molto utili per effettuare un “Jump address” su IDAPro al relativo indirizzo.

2) Advanced Static Analysis

Il primo step effettuato per orientarsi all'interno di IDAPro è stato cercare nel "search" possibili stringhe di testo legate all'esecuzione dello script malevolo oppure eventuali indirizzi grazie a capa nel campo "Jump". In particolare, iniziamo ricercando la stringa "AutoIt" ritroviamo questo:

```
.rdata:0049C9C8 ; const WCHAR WindowName
.rdata:0049C9C8 WindowName:                             ; DATA XREF: sub_402B83+AC↑o
.rdata:0049C9C8                                         ; sub_402C63+26↑o ...
.rdata:0049C9C8                 text "UTF-16LE", 'AutoIt v3',0
.rdata:0049C9DC aAutoit3execute_0:                      ; DATA XREF: sub_402E37+157↑o
.rdata:0049C9DC                 text "UTF-16LE", '/AutoIt3ExecuteScript',0
.rdata:0049CA08 aAutoit3execute:                        ; DATA XREF: sub_402E37+142↑o
.rdata:0049CA08                 text "UTF-16LE", '/AutoIt3ExecuteLine',0
.rdata:0049CA30 aAutoit3outputd:                        ; DATA XREF: sub_402E37+12D↑o
.rdata:0049CA30                 text "UTF-16LE", '/AutoIt3OutputDebug',0
.rdata:0049CA58 aErrorstdout:                           ; DATA XREF: sub_402E37+118↑o
.rdata:0049CA58                 text "UTF-16LE", '/ErrorStdOut',0
.rdata:0049CA72                 align 4
.rdata:0049CA74 aCmdline:                               ; DATA XREF: sub_402E37+BD↑o
.rdata:0049CA74                 text "UTF-16LE", 'CMDLINE',0
.rdata:0049CA84 aCmdlineraw:                            ; DATA XREF: sub_402E37+98↑o
.rdata:0049CA84                 text "UTF-16LE", 'CMDLINERAW',0
.rdata:0049CA9A                 align 4
.rdata:0049CA9C aAutoitNoCmdexe:                        ; DATA XREF: sub_402E37+48↑o
.rdata:0049CA9C                 text "UTF-16LE", '>>>AUTOIT NO CMDEXECUTE<<<',0
.rdata:0049CAD2                 align 4
```

Possiamo grazie a "Ctrl – x" risalire alle chiamate di queste ultime, risalendo all'origine. In particolare, la Sub-routine 402E37:



Che viene a sua volta richiamata in questo punto:

```
.text:00402A62                 call    ds:GetCurrentDirectoryW
.text:00402A68                 lea     eax, [esp+20038h+var_20025]
.text:00402A6C                 push    eax
.text:00402A6D                 push    [ebp+arg_0]
.text:00402A70                 call    sub_402E37
.text:00402A75                 call    ds:IsDebuggerPresent
```

E rappresenta la funzione che prepara l'esecuzione dello script.

```
.text:00402F63
.text:00402F63 loc_402F63:                              ; CODE XREF: sub_402E37+3FECE↓j
.text:00402F63                 push    edi
.text:00402F64                 push    offset aAutoit3outputd ; "/AutoIt3OutputDebug"
.text:00402F69                 call    sub_424A28
.text:00402F6E                 pop     ecx
.text:00402F6F                 pop     ecx
.text:00402F70                 test    eax, eax
.text:00402F72                 jz      loc_442D0A
.text:00402F78
.text:00402F78 loc_402F78:                              ; CODE XREF: sub_402E37+3FEEA↓j
.text:00402F78                 push    edi
.text:00402F79                 push    offset aAutoit3execute ; "/AutoIt3ExecuteLine"
.text:00402F7E                 call    sub_424A28
.text:00402F83                 pop     ecx
.text:00402F84                 pop     ecx
.text:00402F85                 test    eax, eax
.text:00402F87                 jz      loc_442D26
.text:00402F8D
.text:00402F8D loc_402F8D:                              ; CODE XREF: sub_402E37+3FF39↓j
.text:00402F8D                 push    edi
.text:00402F8E                 push    offset aAutoit3execute_0 ; "/AutoIt3ExecuteScript"
.text:00402F93                 call    sub_424A28
.text:00402F98                 pop     ecx
.text:00402F99                 pop     ecx
.text:00402F9A                 test    eax, eax
.text:00402F9C                 jnz     short loc_402FDC
.text:00402F9E                 mov     dword_4D1400, ebx
.text:00402FA4                 cmp     byte ptr [ebp+lpMem+3], bl
.text:00402FA7                 jnz     short loc_402FB3
.text:00402FA9                 mov     dword_4D1400, 3
```

Ritroviamo per l'appunto "AutoIt3ExecuteScript" e "AutoIt3ExecuteLine". La preparazione dello script è effettuata subito dopo la chiamata a "GetCurrentDirectoryW" e subito prima del "IsDebbugerPresent" per controllare se il malware sta venendo eseguito sotto De-bugger.

L'esecuzione prosegue con la chiamata a sub_402DE3 che, se rispetta una cmp effettua un jmp alla locazione loc_442C2B:

```
.text:00442C2B loc_442C2B:                              ; CODE XREF: sub_402DE3+20↑j
.text:00442C2B                 xor     eax, eax
.text:00442C2D                 mov     [ebp+var_10058], ax
.text:00442C34                 mov     eax, [ebp+arg_C]
.text:00442C37                 push    58h ; 'X'
.text:00442C39                 push    0
.text:00442C3B                 mov     byte ptr [eax], 1
.text:00442C3E                 lea     eax, [ebp+var_58]
.text:00442C41                 push    eax
.text:00442C42                 call    sub_422340
.text:00442C47                 and     [ebp+var_58.hwndOwner], 0
.text:00442C4B                 lea     eax, [ebp+var_10058]
.text:00442C51                 add     esp, 0Ch
.text:00442C54                 mov     [ebp+var_58.lpstrFile], eax
.text:00442C57                 lea     eax, [ebp+var_58]
.text:00442C5A                 mov     [ebp+var_58.lStructSize], 58h ; 'X'
.text:00442C61                 mov     [ebp+var_58.lpstrTitle], offset aRunScript ; "Run Script:"
.text:00442C68                 mov     [ebp+var_58.nMaxFile], 7FFFh
.text:00442C6F                 push    eax             ; LPOPENFILENAMEW
.text:00442C70                 mov     [ebp+var_58.lpstrFilter], offset aAutoitScriptFi ; "AutoIt script files (*.au3, *.a3x)"
.text:00442C77                 mov     [ebp+var_58.nFilterIndex], 1
.text:00442C7E                 mov     [ebp+var_58.Flags], 1804h
.text:00442C85                 mov     [ebp+var_58.lpstrDefExt], offset aAu3_0 ; "au3"
.text:00442C8C                 call    ds:GetOpenFileNameW
.text:00442C92                 test    eax, eax
.text:00442C94                 jnz     short loc_442C9D
.text:00442C96                 xor     al, al
.text:00442C98                 jmp     loc_402E31
```

Che effettua il vero e prorio "Run" dello script.

Qualora la cmp non fosse rispettata vengono effettuare una serie di chiamate a sub-routine:

```
.text:00402DFF                 cmp     dword ptr [esi+4], 0
.text:00402E03                 jz      loc_442C2B
.text:00402E09
.text:00402E09 loc_402E09:                             ; CODE XREF: sub_402DE3+3FEC8↓j
.text:00402E09                 mov     edx, esi
.text:00402E0B                 mov     ecx, esi
.text:00402E0D                 call    sub_403AA2
.text:00402E12                 mov     edx, esi
.text:00402E14                 mov     ecx, esi
.text:00402E16                 call    sub_402DA5
.text:00402E1B                 push    [ebp+arg_4]
.text:00402E1E                 push    ecx
.text:00402E1F                 push    esi
.text:00402E20                 mov     ecx, edi
.text:00402E22                 call    sub_403598
.text:00402E27                 pop     ecx
.text:00402E28                 push    eax
.text:00402E29                 push    esi
.text:00402E2A                 mov     ecx, edi
.text:00402E2C                 call    sub_4044A8
```

In ognuna delle sub-routine vengono richiamate funzioni come “GetFullPathNameW”, “GetLongPathNameW” e altre informazioni probabilmente necessarie al fine di eseguire lo script.

Di conseguenza possiamo dire che le funzioni sub_402E37 e sub_402DE3 siano di grande importanza, e rappresentino un turning-point nell’esecuzione del malware.

Tuttavia, ricordiamo come all’inizio si sospettava di una possibile Privilage Escalation, che effettivamente avviene all’interno del malware. Possiamo identificare il processo dalla seguente stringa:

“pIdentifierAuthority= _SID_IDENTIFIER_AUTHORITY”

Che richiama le seguenti funzioni, effettuando il Check dei privilegi:

- AllocateAndInitializeSid
- CheckTokenMemberShip
- FreeSid

E viene riportato di seguito una parte del flusso per l’identificazione dei permessi del processo:

```
pIdentifierAuthority= _SID_IDENTIFIER_AUTHORITY ptr -10h
pSid= dword ptr -8
IsMember= dword ptr -4

push    ebp
mov     ebp, esp
sub     esp, 10h
push    ebx
xor     ebx, ebx
mov     word ptr [ebp+pIdentifierAuthority.Value+4], 500h
lea     eax, [ebp+pSid]
mov     dword ptr [ebp+pIdentifierAuthority.Value], ebx
push    eax             ; pSid
push    ebx             ; nSubAuthority7
push    ebx             ; nSubAuthority6
push    ebx             ; nSubAuthority5
push    ebx             ; nSubAuthority4
push    ebx             ; nSubAuthority3
push    ebx             ; nSubAuthority2
push    220h            ; nSubAuthority1
push    20h ; ' '       ; nSubAuthority0
push    2               ; nSubAuthorityCount
lea     eax, [ebp+pIdentifierAuthority]
push    eax             ; pIdentifierAuthority
call    ds:AllocateAndInitializeSid
mov     [ebp+IsMember], eax
test    eax, eax
jz      short loc_4616BA
```

```
lea     eax, [ebp+IsMember]
push    eax             ; IsMember
push    [ebp+pSid]      ; SidToCheck
push    ebx             ; TokenHandle
call    ds:CheckTokenMembership
push    [ebp+pSid]      ; pSid
neg     eax
sbb     eax, eax
and     [ebp+IsMember], eax
call    ds:FreeSid
mov     eax, [ebp+IsMember]
```

```
loc_4616BA:
cmp     eax, 1
pop     ebx
setz    al
leave
retn
sub_461663 endp
```

Proseguendo era possibile vedere anche la chiamata a funzione come “LookupPrivilegeValueW” e “AdjustTokenPrivileges”, che dimostrano la presenza di una Privilage Escalation.

Dopo aver fatto un “Privilage Check” seguito da una “Privilage Escalation”, riportiamo la parte di codice finalizzata alla creazione del processo. È stato possibile individuare tale sezione ricercando la stringa “Create”. Inizialmente viene effettuata la “LoadUserProfileW” seguita da una “CreateEnvironmentBlock”, utilizzate per configurare l'ambiente di esecuzione di un processo esistente o futuro:

```
.text:004613D6 loc_4613D6:                          ; CODE XREF: sub_461201+1A7↑j
.text:004613D6                 cmp     byte ptr [ebp+lpszUsername], 0
.text:004613DA                 jz      short loc_4613ED
.text:004613DC                 lea     eax, [ebp+ProfileInfo]
.text:004613DF                 push    eax             ; lpProfileInfo
.text:004613E0                 push    [ebp+phToken]   ; hToken
.text:004613E3                 call    ds:LoadUserProfileW
.text:004613E9                 test    eax, eax
.text:004613EB                 jz      short loc_46144F
.text:004613ED
.text:004613ED loc_4613ED:                          ; CODE XREF: sub_461201+1D9↑j
.text:004613ED                 test    byte ptr [ebp+arg_C], 4
.text:004613F1                 jnz     short loc_461406
.text:004613F3                 push    0               ; bInherit
.text:004613F5                 push    [ebp+phToken]   ; hToken
.text:004613F8                 lea     eax, [ebp+Environment]
.text:004613FB                 push    eax             ; lpEnvironment
.text:004613FC                 call    ds:CreateEnvironmentBlock
.text:00461402                 test    eax, eax
.text:00461404                 jz      short loc_46144F
```

Seguita dalla creazione del nuovo processo:

```
.text:00461429                 call    ds:CreateProcessAsUserW
.text:0046142F                 test    eax, eax
.text:00461431                 jz      short loc_46144F
.text:00461433                 cmp     byte ptr [ebp+lpszUsername], 0
.text:00461437                 jz      short loc_461449
.text:00461439                 lea     eax, [ebp+phToken]
.text:0046143C                 push    eax
.text:0046143D                 lea     eax, [ebp+ProfileInfo.hProfile]
.text:00461440                 push    eax
.text:00461441                 push    [ebp+lpProcessInformation]
.text:00461444                 call    sub_461803
```

Quest’ultima seguita da una chiamata alla sub_461803:

```
.text:0046180A                 push    8               ; dwFlags
.text:0046180C                 call    ds:GetProcessHeap
.text:00461812                 push    eax             ; hHeap
.text:00461813                 call    ds:HeapAlloc
.text:00461819                 mov     edi, ds:GetCurrentProcess
.text:0046181F                 mov     ebx, eax
.text:00461821                 push    2               ; dwOptions
.text:00461823                 push    0               ; bInheritHandle
.text:00461825                 push    0               ; dwDesiredAccess
.text:00461827                 push    ebx             ; lpTargetHandle
.text:00461828                 call    edi ; GetCurrentProcess
.text:0046182A                 push    eax             ; hTargetProcessHandle
.text:0046182B                 mov     eax, [ebp+arg_0]
.text:0046182E                 push    dword ptr [eax] ; hSourceHandle
.text:00461830                 call    edi ; GetCurrentProcess
.text:00461832                 push    eax             ; hSourceProcessHandle
.text:00461833                 call    ds:DuplicateHandle
.text:00461839                 push    2               ; dwOptions
.text:0046183B                 push    0               ; bInheritHandle
.text:0046183D                 push    0               ; dwDesiredAccess
.text:0046183F                 lea     eax, [ebx+8]
.text:00461842                 push    eax             ; lpTargetHandle
.text:00461843                 call    edi ; GetCurrentProcess
.text:00461845                 push    eax             ; hTargetProcessHandle
.text:00461846                 mov     eax, [ebp+arg_8]
.text:00461849                 push    dword ptr [eax] ; hSourceHandle
.text:0046184B                 call    edi ; GetCurrentProcess
.text:0046184D                 push    eax             ; hSourceProcessHandle
.text:0046184E                 call    ds:DuplicateHandle
.text:00461854                 mov     eax, [ebp+arg_4]
```

Ed infine la creazione del Thread:

```
.text:0046185E                 push    eax             ; lpThreadId
.text:0046185F                 push    eax             ; dwCreationFlags
.text:00461860                 push    ebx             ; lpParameter
.text:00461861                 push    offset sub_461874 ; lpStartAddress
.text:00461866                 push    eax             ; dwStackSize
.text:00461867                 push    eax             ; lpThreadAttributes
.text:00461868                 call    ds:CreateThread
.text:0046186E                 pop     edi
.text:0046186F                 pop     ebx
.text:00461870                 pop     ebp
.text:00461871                 retn    0Ch
.text:00461871 sub_461803      endp
```

Lo step seguente rappresenta una Process Injection, individuata dalle chiamate alle seguenti funzioni:

```
.text:0046B34E loc_46B34E:                             ; CODE XREF: sub_46B32A+1E↑j
.text:0046B34E                 lea     eax, [ebp+dwProcessId]
.text:0046B351                 push    eax             ; lpdwProcessId
.text:0046B352                 push    [ebp+hWnd]      ; hWnd
.text:0046B355                 call    ds:GetWindowThreadProcessId
.text:0046B35B                 push    [ebp+dwProcessId] ; dwProcessId
.text:0046B35E                 push    0               ; bInheritHandle
.text:0046B360                 push    438h            ; dwDesiredAccess
.text:0046B365                 call    ds:OpenProcess
.text:0046B36B                 push    4               ; flProtect
.text:0046B36D                 push    1000h           ; flAllocationType
.text:0046B372                 push    [ebp+dwSize]    ; dwSize
.text:0046B375                 mov     [edi+esi*8], eax
.text:0046B378                 push    0               ; lpAddress
.text:0046B37A                 push    eax             ; hProcess
.text:0046B37B                 call    ds:VirtualAllocEx
.text:0046B381                 mov     [edi+esi*8+4], eax
```

- Il malware ottiene l'ID del thread e l'ID del processo associato a una finestra specifica identificata da hWnd.
- In seguito, apre il processo identificato dall'ID di processo ottenuto in precedenza, con il livello di accesso specificato da dwDesiredAccess (0x438). Questo accesso include probabilmente i permessi necessari per manipolare il processo target, ottenuti in precedenza.
- Le ultime istruzioni allocano memoria nel processo target. VirtualAllocEx viene usato per riservare memoria nello spazio degli indirizzi di un altro processo.

Infine, abbiamo l’esecuzione del processo tramite ShellExecuteW, che di fatto conclude l’analisi statica avanzata:

```
.text:00442BFE                 lea     eax, [esp+2003Ch+Buffer]
.text:00442C02                 push    eax             ; lpDirectory
.text:00442C03                 push    [esp+20040h+lpParameters] ; lpParameters
.text:00442C07                 push    [esp+20044h+lpFile] ; lpFile
.text:00442C0B                 push    offset Operation ; "runas"
.text:00442C10                 call    ds:GetForegroundWindow
.text:00442C16                 push    eax             ; hwnd
.text:00442C17                 call    ds:ShellExecuteW
.text:00442C1D                 lea     ecx, [esp+20038h+lpParameters]
.text:00442C21                 call    sub_40988F
.text:00442C26                 jmp     loc_402B5F
.text:00442C26 ; END OF FUNCTION CHUNK FOR sub_402A32
```

• Terza considerazione:

Sintetizziamo gli step individuati e le tecniche utilizzate:

Preparation: Il malware prepara lo script e l'ambiente per l’esecuzione.

Privilege Check: Il codice verifica se il processo corrente dispone dei privilegi necessari per eseguire operazioni critiche

Privilege Escalation / Process Replacement: Se i privilegi necessari non sono presenti, vengono eseguite tecniche di escalation dei privilegi. Funzioni come OpenProcessToken, e AdjustTokenPrivileges vengono utilizzate per ottenere e manipolare token di accesso con privilegi elevati.

Process Creation: Una volta acquisiti i privilegi necessari, il malware crea un nuovo processo. Vengono utilizzate funzioni per lanciare il processo con il token di accesso manipolato e le variabili di ambiente appropriate.

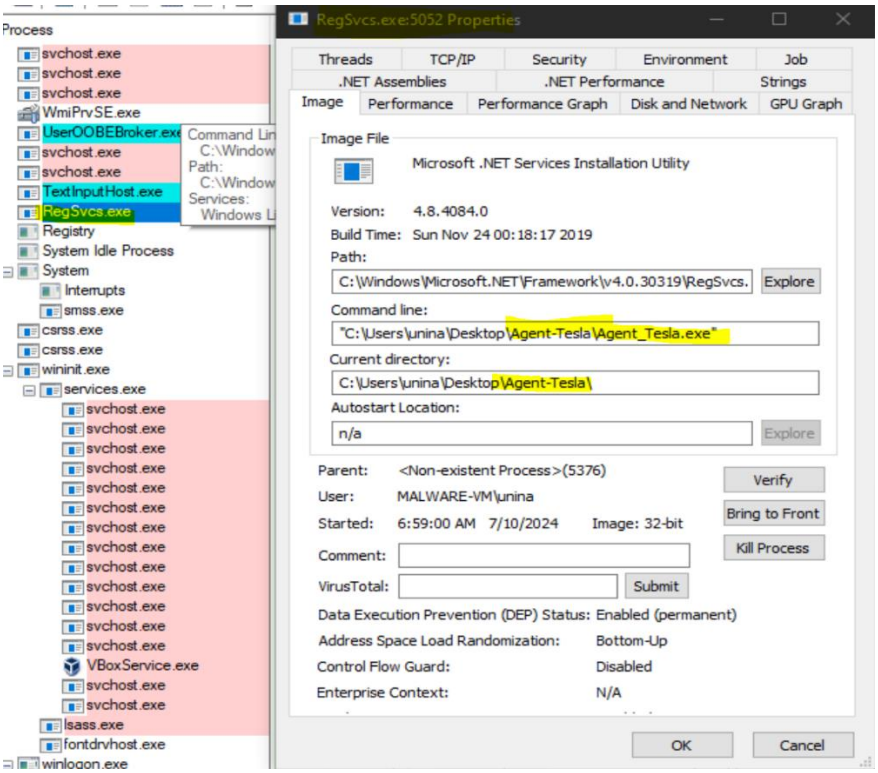
Process Injection: Il malware inietta codice maligno nel processo appena creato.

Execution: Il codice iniettato viene eseguito, permettendo al malware di operare con privilegi elevati

3) Basic Dynamic Analysis

Eseguendo il malware come amministratore, il primo passo è stato cercare l'eseguibile tra i processi attivi utilizzando Process Explorer. Tuttavia, non è stato trovato alcun processo denominato "Agent_Tesla.exe", il che suggerisce che potrebbe essere stato camuffato con un nome diverso.

Per identificare il nome effettivo, invece di cercare esplicitamente "Agent_Tesla.exe", ho monitorato l'avvio di qualsiasi nuovo processo, individuando "Regsvcs.exe" come file sospetto, e verificandone le proprietà, ho confermato la teoria iniziale.



Questa rappresenta un’ulteriore conferma che l’eseguibile “Agent_Tesla” crea un nuovo processo chiamato “Regsvcs.exe” nel quale esegue la Process Injection (quindi non all’interno di un processo legittimo, bensì quello appena creato).

Il malware sembra principalmente occuparsi della verifica delle informazioni di sistema affinché il codice maligno possa operare. Effettua controlli, ad esempio, sulle impostazioni di internet tramite chiavi di registro, interroga le informazioni di sistema e le passa al vero processo dannoso "RegSvcs.exe tentando nel mentre di nascondersi camuffandosi come uno strumento di installazione dei servizi .NET; la motivazione presumibilmente è che tenti di eludere la rilevazione e confondendosi con gli altri processi al fine di interrogare meglio le informazioni sui file e apportare modifiche al sistema senza essere individuato.

Utilizzando Procmon, possiamo visualizzare il funzionamento di entrambi i programmi durante l'esecuzione, analizzandone tutti gli step.

Nella seguente immagine vediamo l'inizio del Processo "Agent_Tesla":

6:59:0...	taskhostw.exe	4080	RegQueryValue	HKCU\(Default)	NAME NOT FOUND	Length:
6:59:0...	taskhostw.exe	4080	RegCloseKey	HKCU	SUCCESS	
6:59:0...	dwm.exe	60	RegQueryValue	HKCU\SOFTWARE\Microsoft\Window...	SUCCESS	Type: R
6:59:0...	dwm.exe	60	RegQueryValue	HKCU\SOFTWARE\Microsoft\Window...	SUCCESS	Type: R
6:59:0...	dwm.exe	60	RegQueryValue	HKCU\SOFTWARE\Microsoft\Window...	SUCCESS	Type: R
6:59:0...	dwm.exe	60	RegQueryValue	HKCU\SOFTWARE\Microsoft\Window...	SUCCESS	Type: R
6:59:0...	dwm.exe	60	RegQueryValue	HKCU\SOFTWARE\Microsoft\Window...	SUCCESS	Type: R
6:59:0...	dwm.exe	60	RegQueryValue	HKCU\SOFTWARE\Microsoft\Window...	SUCCESS	Type: R
6:59:0...	Agent_Tesla.exe	5376	Process Start		SUCCESS	Parent P
6:59:0...	Agent_Tesla.exe	5376	Thread Create		SUCCESS	Thread
6:59:0...	csrss.exe	528	QuerySecurityFile	C:\Users\unina\Desktop\Agent-Tesla\...	SUCCESS	Informati
6:59:0...	csrss.exe	528	CreateFile	C:\Windows\apppatch\sysmain.sdb	SUCCESS	Desired
6:59:0...	csrss.exe	528	QueryBasicInfor...	C:\Windows\apppatch\sysmain.sdb	SUCCESS	Creation
6:59:0...	csrss.exe	528	CloseFile	C:\Windows\apppatch\sysmain.sdb	SUCCESS	
6:59:0...	csrss.exe	528	QueryBasicInfor...	C:\Users\unina\Desktop\Agent-Tesla\...	SUCCESS	Creation
6:59:0...	csrss.exe	528	QuerySecurityFile	C:\Users\unina\Desktop\Agent-Tesla\...	SUCCESS	Informati
6:59:0...	csrss.exe	528	QueryBasicInfor...	C:\Users\unina\Desktop\Agent-Tesla\...	SUCCESS	Creation
6:59:0...	csrss.exe	528	CreateFile	C:\Users\unina\Desktop\Agent-Tesla\...	NAME NOT FOUND	Desired
6:59:0...	csrss.exe	528	QueryBasicInfor...	C:\Users\unina\Desktop\Agent-Tesla\...	SUCCESS	Creation
6:59:0...	csrss.exe	528	QueryIdInformat...	C:\Users\unina\Desktop\Agent-Tesla\...	SUCCESS	

Dopo che l'eseguibile di Agent Tesla ha completato la raccolta delle informazioni di sistema avvia il processo Regsvcs per eseguire effettivamente il codice maligno.

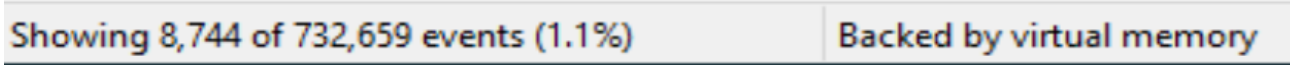
6:59:0...	Agent_Tesla.exe	5376	CreateFile	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Desired Access: G...
6:59:0...	Agent_Tesla.exe	5376	QueryStandardI...	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	AllocationSize: 1,7...
6:59:0...	Agent_Tesla.exe	5376	ReadFile	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Offset: 0, Length: 1...
6:59:0...	Agent_Tesla.exe	5376	CloseFile	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	
6:59:0...	Agent_Tesla.exe	5376	CreateFile	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Desired Access: G...
6:59:0...	Agent_Tesla.exe	5376	QueryStandardI...	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	AllocationSize: 1,7...
6:59:0...	Agent_Tesla.exe	5376	ReadFile	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Offset: 0, Length: 1...
6:59:0...	Agent_Tesla.exe	5376	CloseFile	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	
6:59:0...	Agent_Tesla.exe	5376	CreateFile	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Desired Access: G...
6:59:0...	Agent_Tesla.exe	5376	QueryStandardI...	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	AllocationSize: 1,7...
6:59:0...	Agent_Tesla.exe	5376	ReadFile	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Offset: 0, Length: 1...
6:59:0...	Agent_Tesla.exe	5376	CloseFile	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	
6:59:0...	Agent_Tesla.exe	5376	CreateFile	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Desired Access: G...
6:59:0...	Agent_Tesla.exe	5376	QueryStandardI...	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	AllocationSize: 1,7...
6:59:0...	Agent_Tesla.exe	5376	ReadFile	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Offset: 0, Length: 1...
6:59:0...	Agent_Tesla.exe	5376	CloseFile	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	
6:59:0...	RegSvcs.exe	5052	Load Image	C:\Windows\Microsoft.NET\Framework...	SUCCESS	Image Base: 0x290...
6:59:0...	RegSvcs.exe	5052	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7ffc...
6:59:0...	RegSvcs.exe	5052	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x76f...
6:59:0...	RegSvcs.exe	5052	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
6:59:0...	RegSvcs.exe	5052	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
6:59:0...	RegSvcs.exe	5052	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 80
6:59:0...	RegSvcs.exe	5052	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
6:59:0...	RegSvcs.exe	5052	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
6:59:0...	RegSvcs.exe	5052	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
6:59:0...	RegSvcs.exe	5052	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
6:59:0...	RegSvcs.exe	5052	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
6:59:0...	RegSvcs.exe	5052	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 24

Finita la sua utilità in seguito il processo Agent_Tesla termina, lasciando spazio a RegSvcs.exe.

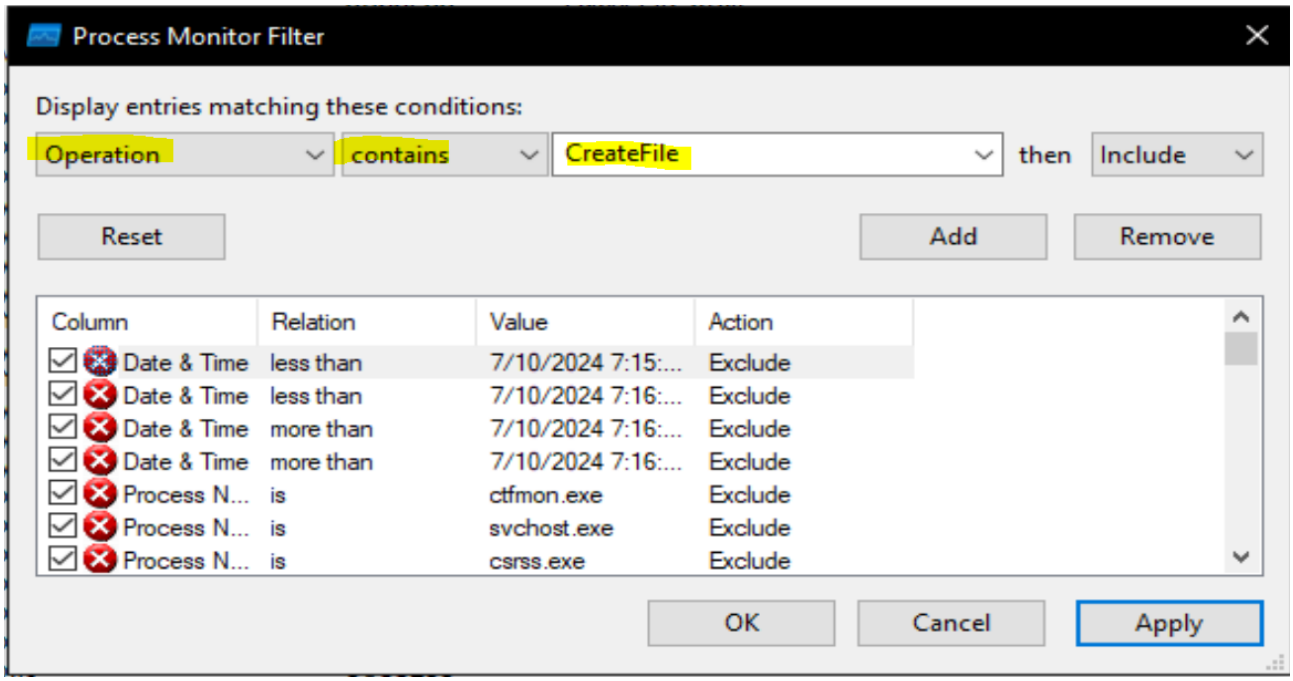
6:59:0...	RegSvcs.exe	5052	RegCloseKey	HKLM\SOFTWARE\WOW6432Node\...	SUCCESS	
6:59:0...	RegSvcs.exe	5052	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
6:59:0...	RegSvcs.exe	5052	RegQueryKey	HKLM	SUCCESS	Query: Name
6:59:0...	RegSvcs.exe	5052	RegOpenKey	HKLM\Software\WOW6432Node\Micr...	SUCCESS	Desired Access: R...
6:59:0...	RegSvcs.exe	5052	RegSetInfoKey	HKLM\SOFTWARE\WOW6432Node\...	SUCCESS	KeySetInformation...
6:59:0...	RegSvcs.exe	5052	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\...	BUFFER OVERFL...	Length: 12
6:59:0...	RegSvcs.exe	5052	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\...	SUCCESS	Type: REG_SZ, Le...
6:59:0...	RegSvcs.exe	5052	RegCloseKey	HKLM\SOFTWARE\WOW6432Node\...	SUCCESS	
6:59:0...	RegSvcs.exe	5052	CreateFile	C:\Windows\Microsoft.NET\Framework...	SUCCESS	Desired Access: R...
6:59:0...	RegSvcs.exe	5052	QueryDirectory	C:\Windows\Microsoft.NET\Framework...	SUCCESS	FileInformationClas...
6:59:0...	RegSvcs.exe	5052	CloseFile	C:\Windows\Microsoft.NET\Framework...	SUCCESS	
6:59:0...	RegSvcs.exe	5052	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
6:59:0...	RegSvcs.exe	5052	RegQueryKey	HKLM	SUCCESS	Query: Name
6:59:0...	RegSvcs.exe	5052	RegOpenKey	HKLM\Software\WOW6432Node\Micr...	SUCCESS	Desired Access: R...
6:59:0...	RegSvcs.exe	5052	RegSetInfoKey	HKLM\SOFTWARE\WOW6432Node\...	SUCCESS	KeySetInformation...
6:59:0...	RegSvcs.exe	5052	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\...	BUFFER OVERFL...	Length: 12
6:59:0...	RegSvcs.exe	5052	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\...	SUCCESS	Type: REG_SZ, Le...
6:59:0...	Agent_Tesla.exe	5376	CloseFile	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	
6:59:0...	Agent_Tesla.exe	5376	ReadFile	C:\Windows\SysWOW64\msctf.dll	SUCCESS	Offset: 87,040, L
6:59:0...	RegSvcs.exe	5052	RegCloseKey	HKLM\SOFTWARE\WOW6432Node\...	SUCCESS	
6:59:0...	RegSvcs.exe	5052	QueryOpen	C:\Windows\Microsoft.NET\Framework...	SUCCESS	CreationTime: 3
6:59:0...	Agent_Tesla.exe	5376	Thread Exit		SUCCESS	Thread ID: 1248, ...
6:59:0...	Agent_Tesla.exe	5376	Thread Exit		SUCCESS	Thread ID: 6604, ...
6:59:0...	Agent_Tesla.exe	5376	Thread Exit		SUCCESS	Thread ID: 5380, ...
6:59:0...	RegSvcs.exe	5052	ReadFile	C:\Windows\Microsoft.NET\Framework...	SUCCESS	Offset: 496,640, Le...
6:59:0...	RegSvcs.exe	5052	ReadFile	C:\Windows\Microsoft.NET\Framework...	SUCCESS	Offset: 74,752, Len...
6:59:0...	taskhostw.exe	4080	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
6:59:0...	Agent_Tesla.exe	5376	Process Exit		SUCCESS	Exit Status: 0, User...

Per analizzare approfonditamente le fasi di RegSvcs, abbiamo deciso di filtrare le operazioni più comuni eseguite da questo tipo di malware e i percorsi più frequentemente bersagliati.

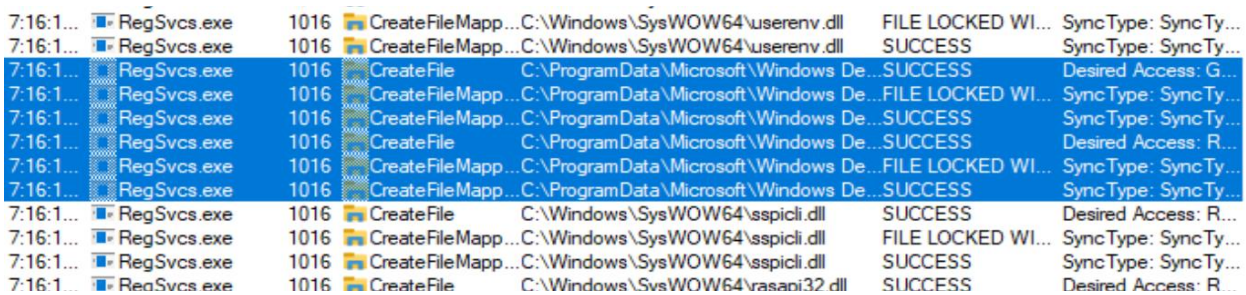
È stato particolarmente utile escludere tutti i processi estranei e le voci di registro avvenute prima e dopo l'esecuzione, anche per avere un'idea sulla mole di step eseguiti dal malware, circa 8750 eventi:



Questo ci permette, ad esempio, di valutare tutti i file creati dal malware.:



Nel CreateFile notiamo come un path particolarmente bersagliato è quello di Microsoft\WindowsDefender:



Infatti, senza nemmeno bisogno di filtrare tramite nome cartella, possiamo notare come il malware cerchi di disabilitare WindowsDefendenr andando ad intervenire sulla libreria MpOAV.dll. Tutti gli eventi nella foto qui sotto avvengono uno di seguito all'altro.

7:16:16.7808284 AM	exe	1016	CreateFile	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	SUCCESS	Desired Access: G...
7:16:1...	RegSvcs.exe	1016	QueryEAFile	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	SUCCESS	
7:16:1...	RegSvcs.exe	1016	QueryStandardI...	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	SUCCESS	AllocationSize: 462...
7:16:1...	RegSvcs.exe	1016	CreateFileMapp...	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	FILE LOCKED WI...	SyncType: SyncTy...
7:16:1...	RegSvcs.exe	1016	QueryStandardI...	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	SUCCESS	AllocationSize: 462...
7:16:1...	RegSvcs.exe	1016	CreateFileMapp...	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	SUCCESS	SyncType: SyncTy...
7:16:1...	RegSvcs.exe	1016	ReadFile	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	SUCCESS	Offset: 0, Length: 3...
7:16:1...	RegSvcs.exe	1016	ReadFile	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	SUCCESS	Offset: 430,080, Le...
7:16:1...	RegSvcs.exe	1016	ReadFile	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	SUCCESS	Offset: 32,768, Len...
7:16:1...	RegSvcs.exe	1016	ReadFile	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	SUCCESS	Offset: 65,536, Len...
7:16:1...	RegSvcs.exe	1016	ReadFile	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	SUCCESS	Offset: 98,304, Len...
7:16:1...	RegSvcs.exe	1016	ReadFile	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	SUCCESS	Offset: 131,072, Le...
7:16:1...	RegSvcs.exe	1016	ReadFile	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	SUCCESS	Offset: 163,840, Le...
7:16:1...	RegSvcs.exe	1016	ReadFile	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	SUCCESS	Offset: 196,608, Le...
7:16:1...	RegSvcs.exe	1016	ReadFile	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	SUCCESS	Offset: 229,376, Le...
7:16:1...	RegSvcs.exe	1016	ReadFile	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	SUCCESS	Offset: 262,144, Le...
7:16:1...	RegSvcs.exe	1016	ReadFile	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	SUCCESS	Offset: 294,912, Le...
7:16:1...	RegSvcs.exe	1016	ReadFile	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	SUCCESS	Offset: 327,680, Le...
7:16:1...	RegSvcs.exe	1016	ReadFile	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	SUCCESS	Offset: 360,448, Le...
7:16:1...	RegSvcs.exe	1016	ReadFile	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	SUCCESS	Offset: 393,216, Le...
7:16:1...	RegSvcs.exe	1016	ReadFile	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	SUCCESS	Offset: 425,984, Le...
7:16:1...	RegSvcs.exe	1016	FileSystemControl	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	SUCCESS	Control: FSCTL_W...
7:16:1...	RegSvcs.exe	1016	FileSystemControl	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	INVALID DEVICE ...	Control: FSCTL_G...
7:16:1...	RegSvcs.exe	1016	FileSystemControl	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	SUCCESS	Control: FSCTL_Q...
7:16:1...	RegSvcs.exe	1016	SetEAFile	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	SUCCESS	
7:16:1...	RegSvcs.exe	1016	QueryEAFile	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	SUCCESS	
7:16:1...	RegSvcs.exe	1016	FileSystemControl	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	INVALID DEVICE ...	Control: FSCTL_G...
7:16:1...	RegSvcs.exe	1016	FileSystemControl	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	SUCCESS	Control: FSCTL_Q...
7:16:1...	RegSvcs.exe	1016	CloseFile	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	SUCCESS	
7:16:1...	RegSvcs.exe	1016	QueryOpen	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	SUCCESS	CreationTime: 6/27...
7:16:1...	RegSvcs.exe	1016	CreateFile	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	SUCCESS	Desired Access: R...
7:16:1...	RegSvcs.exe	1016	CreateFileMapp...	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	FILE LOCKED WI...	SyncType: SyncTy...
7:16:1...	RegSvcs.exe	1016	QueryStandardI...	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	SUCCESS	AllocationSize: 462...
7:16:1...	RegSvcs.exe	1016	CreateFileMapp...	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	SUCCESS	SyncType: SyncTy...
7:16:1...	RegSvcs.exe	1016	Load Image	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	SUCCESS	Image Base: 0x747...
7:16:1...	RegSvcs.exe	1016	CloseFile	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24050.7-0\X86\MpOAV.dll	SUCCESS	

MpOAV.dll è parte dei componenti di protezione di Microsoft e svolge un ruolo nelle funzionalità antivirus e antimalware del sistema operativo Windows.

È una delle librerie utilizzate da Windows Defender per identificare, bloccare e rimuovere software dannoso. Partecipando alla scansione e al monitoraggio del sistema, contribuisce alla protezione in tempo reale contro le minacce. Contiene anche codice che permette a Windows Defender di eseguire scansioni su file e processi in esecuzione, rilevando firme di virus conosciuti e comportamenti sospetti.

Quindi è comprensibile che sia un obiettivo del malware, poiché disabilitandola può prendere pieno controllo del sistema senza ostacoli.

Altri eventi degni di nota sono quelli associati a wsock32.dll e wininet.dll:

7:16:1...	C:\Users\unina\Desktop\Agent-Tesla\Agent_Tesla.exe		dows\SysWOW64\wsock32.dll	SUCCESS	Desired Access: R...
7:16:1...	Agent_Tesla.exe	1560	CreateFileMapp...	C:\Windows\SysWOW64\wsock32.dll	FILE LOCKED WI...	SyncType: SyncTy...
7:16:1...	Agent_Tesla.exe	1560	CreateFileMapp...	C:\Windows\SysWOW64\wsock32.dll	SUCCESS	SyncType: SyncTy...
7:16:1...	Agent_Tesla.exe	1560	CreateFile	C:\Windows\SysWOW64\winmm.dll	SUCCESS	Desired Access: R...
7:16:1...	Agent_Tesla.exe	1560	CreateFileMapp...	C:\Windows\SysWOW64\winmm.dll	FILE LOCKED WI...	SyncType: SyncTy...
7:16:1...	Agent_Tesla.exe	1560	CreateFile	C:\Windows\SysWOW64\version.dll	SUCCESS	Desired Access: R...
7:16:1...	Agent_Tesla.exe	1560	CreateFileMapp...	C:\Windows\SysWOW64\version.dll	FILE LOCKED WI...	SyncType: SyncTy...
7:16:1...	Agent_Tesla.exe	1560	CreateFileMapp...	C:\Windows\SysWOW64\version.dll	SUCCESS	SyncType: SyncTy...
7:16:1...	Agent_Tesla.exe	1560	CreateFileMapp...	C:\Windows\SysWOW64\winmm.dll	SUCCESS	SyncType: SyncTy...
7:16:1...	Agent_Tesla.exe	1560	CreateFile	C:\Windows\SysWOW64\mpr.dll	SUCCESS	Desired Access: R...
7:16:1...	Agent_Tesla.exe	1560	CreateFile	C:\Windows\WinSxS\x86_microsoft.win...	SUCCESS	Desired Access: R...
7:16:1...	Agent_Tesla.exe	1560	CreateFileMapp...	C:\Windows\SysWOW64\mpr.dll	FILE LOCKED WI...	SyncType: SyncTy...
7:16:1...	Agent_Tesla.exe	1560	CreateFileMapp...	C:\Windows\WinSxS\x86_microsoft.win...	FILE LOCKED WI...	SyncType: SyncTy...
7:16:1...	Agent_Tesla.exe	1560	CreateFileMapp...	C:\Windows\SysWOW64\mpr.dll	SUCCESS	SyncType: SyncTy...
7:16:1...	Agent_Tesla.exe	1560	CreateFile	C:\Windows\SysWOW64\IPHLPAPI.DLL	SUCCESS	Desired Access: R...
7:16:1...	Agent_Tesla.exe	1560	CreateFileMapp...	C:\Windows\SysWOW64\IPHLPAPI.DLL	FILE LOCKED WI...	SyncType: SyncTy...
7:16:1...	Agent_Tesla.exe	1560	CreateFileMapp...	C:\Windows\SysWOW64\IPHLPAPI.DLL	SUCCESS	SyncType: SyncTy...
7:16:1...	Agent_Tesla.exe	1560	CreateFile	C:\Windows\SysWOW64\userenv.dll	SUCCESS	Desired Access: R...
7:16:1...	Agent_Tesla.exe	1560	CreateFileMapp...	C:\Windows\SysWOW64\userenv.dll	FILE LOCKED WI...	SyncType: SyncTy...
7:16:1...	Agent_Tesla.exe	1560	CreateFileMapp...	C:\Windows\SysWOW64\userenv.dll	SUCCESS	SyncType: SyncTy...
7:16:1...	Agent_Tesla.exe	1560	CreateFile	C:\Windows\SysWOW64\uxtheme.dll	SUCCESS	Desired Access: R...
7:16:1...	Agent_Tesla.exe	1560	CreateFileMapp...	C:\Windows\SysWOW64\uxtheme.dll	FILE LOCKED WI...	SyncType: SyncTy...
7:16:1...	Agent_Tesla.exe	1560	CreateFile	C:\Windows\WinSxS\x86_microsoft.win...	SUCCESS	Desired Access: R...
7:16:1...	Agent_Tesla.exe	1560	CreateFileMapp...	C:\Windows\WinSxS\x86_microsoft.win...	FILE LOCKED WI...	SyncType: SyncTy...
7:16:1...	Agent_Tesla.exe	1560	CreateFileMapp...	C:\Windows\SysWOW64\uxtheme.dll	SUCCESS	SyncType: SyncTy...
7:16:1...	Agent_Tesla.exe	1560	CreateFileMapp...	C:\Windows\WinSxS\x86_microsoft.win...	FILE LOCKED WI...	SyncType: SyncTy...
7:16:1...	Agent_Tesla.exe	1560	CreateFileMapp...	C:\Windows\WinSxS\x86_microsoft.win...	SUCCESS	SyncType: SyncTy...
7:16:1...	Agent_Tesla.exe	1560	CreateFile	C:\Windows\SysWOW64\wininet.dll	SUCCESS	Desired Access: R...
7:16:1...	Agent_Tesla.exe	1560	CreateFileMapp...	C:\Windows\SysWOW64\wininet.dll	FILE LOCKED WI...	SyncType: SyncTy...
7:16:1...	Agent_Tesla.exe	1560	CreateFileMapp...	C:\Windows\WinSxS\x86_microsoft.win...	SUCCESS	SyncType: SyncTy...
7:16:1...	Agent_Tesla.exe	1560	CreateFileMapp...	C:\Windows\SysWOW64\wininet.dll	SUCCESS	SyncType: SyncTy...
7:16:1...	Agent_Tesla.exe	1560	CreateFile	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Desired Access: R...
7:16:1...	Agent_Tesla.exe	1560	CreateFileMapp...	C:\Windows\SysWOW64\imm32.dll	FILE LOCKED WI...	SyncType: SyncTy...

La wsock32.dll è una libreria di sistema di Windows associata a Windows Sockets API (Winsock), che fornisce un'interfaccia per la comunicazione di rete tramite TCP/IP. Consente alle applicazioni di comunicare su una rete utilizzando i protocolli TCP/IP. È responsabile delle operazioni di rete di basso livello, come l'apertura di connessioni socket, l'invio e la ricezione di dati.

Per quanto riguarda wininet.dll è sempre una libreria di sistema di Windows abbastanza simile a wsock32. Essa fornisce funzionalità per la connettività di rete e le operazioni Internet.

Possiamo sicuramente assumere che questo eseguibile stia cercando di inserire una backdoor nel sistema per ottenere accesso remoto e presumibilmente rubare informazioni di rete anche di altri computer nella rete infetta per continuare a diffondersi.

A riprova di ciò andiamo a valutare tutti gli eventi associati alle operazioni sui registri, come ad esempio: creazione, modifica, query o anche la semplice Open.

RegQueryKey: sono stati rilevati 1800 eventi

7:16:1...	RegSvcs.exe	1016	RegQueryKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces
7:16:1...	RegSvcs.exe	1016	RegQueryKey	HKLM\System\CurrentControlSet\Services\Tcpip6\Parameters\Interfaces
7:16:1...	RegSvcs.exe	1016	RegQueryKey	HKLM
7:16:19.0840085 AM	exe	1016	RegQueryKey	HKLM
7:16:1...	RegSvcs.exe	1016	RegQueryKey	HKLM\System\CurrentControlSet\Services\Tcpip6\Parameters\Interfaces
7:16:1...	RegSvcs.exe	1016	RegQueryKey	HKLM
7:16:1...	RegSvcs.exe	1016	RegQueryKey	HKLM
7:16:1...	RegSvcs.exe	1016	RegQueryKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces
7:16:1...	RegSvcs.exe	1016	RegQueryKey	HKLM
7:16:1...	RegSvcs.exe	1016	RegQueryKey	HKLM
7:16:1...	RegSvcs.exe	1016	RegQueryKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces
7:16:1...	RegSvcs.exe	1016	RegQueryKey	HKLM

Showing 1,866 of 2,094,233 events (0.089%) | Backed by virtual memory

RegSetInfoKey: rilevati 400 eventi

7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKCR\WOW6432Node\CLSID\{CF4CC405-E2C5-4DDD-B3CE-5E7582D8C9FA}\InprocServer32	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKCR\WOW6432Node\CLSID\{CF4CC405-E2C5-4DDD-B3CE-5E7582D8C9FA}\InprocServer32	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKCR\WOW6432Node\CLSID\{CF4CC405-E2C5-4DDD-B3CE-5E7582D8C9FA}\InprocServer32	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKCR\WOW6432Node\CLSID\{CF4CC405-E2C5-4DDD-B3CE-5E7582D8C9FA}\InprocServer32	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKCR\WOW6432Node\CLSID\{CF4CC405-E2C5-4DDD-B3CE-5E7582D8C9FA}\InprocServer32	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKCR\WOW6432Node\CLSID\{CF4CC405-E2C5-4DDD-B3CE-5E7582D8C9FA}\InprocServer32	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKCR\WOW6432Node\CLSID\{CF4CC405-E2C5-4DDD-B3CE-5E7582D8C9FA}\InprocServer32	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKCR\WOW6432Node\CLSID\{CF4CC405-E2C5-4DDD-B3CE-5E7582D8C9FA}\InprocServer32	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKCR\WOW6432Node\CLSID\{CF4CC405-E2C5-4DDD-B3CE-5E7582D8C9FA}\InprocServer32	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKCR\WOW6432Node\CLSID\{CF4CC405-E2C5-4DDD-B3CE-5E7582D8C9FA}\InprocServer32	SUCCESS	KeySetInformation...
7:16:18.8929468 AM	exe	1016	RegSetInfoKey	HKCR\WOW6432Node\CLSID\{CF4CC405-E2C5-4DDD-B3CE-5E7582D8C9FA}\InprocServer32	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\Hvsi	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Tracing	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Tracing	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Tracing\RegSvcs_RASAPI32	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Tracing	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Tracing	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Tracing\RegSvcs_RASMANCS	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Tracing	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKLM\System\CurrentControlSet\Services\RasMan\Parameters	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKLM\System\CurrentControlSet\Services\RasMan\Parameters	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKLM\System\CurrentControlSet\Services\Winsock\Parameters	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKLM\System\CurrentControlSet\Services\Winsock\Setup Migration\Providers	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKLM\System\CurrentControlSet\Services\Winsock\Parameters	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKLM\System\CurrentControlSet\Services\Tcpip6\Parameters\Winsock	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKLM\System\CurrentControlSet\Services\Winsock\Setup Migration\Providers	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKLM\System\CurrentControlSet\Services\Tcpip6\Parameters\Winsock	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKLM\System\CurrentControlSet\Services\RasMan\Parameters	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\Conn...	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\.NETFramework	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Internet Settings	SUCCESS	KeySetInformation...
7:16:1...	RegSvcs.exe	1016	RegSetInfoKey	HKLM\SOFTWARE\Policies\Microsoft\Internet Explorer\Main	SUCCESS	KeySetInformation...

Showing 404 of 1,939,634 events (0.020%) | Backed by virtual memory

RegCreateKey: 39 eventi

7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\Software\WOW6432Node\Microsoft\WBEM\CIMOM	SUCCESS	Desired Access: Q...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\Software\WOW6432Node\Microsoft\WBEM\CIMOM	SUCCESS	Desired Access: R...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\Software\WOW6432Node\Microsoft\Tracing	SUCCESS	Desired Access: Q...
7:16:18.9695197 AM	exe	1016	RegCreateKey	HKLM\Software\WOW6432Node\Microsoft\Tracing	SUCCESS	Desired Access: R...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\Software\WOW6432Node\Microsoft\Tracing\RegSvcs_RASAPI32	SUCCESS	Desired Access: R...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\Software\WOW6432Node\Microsoft\Tracing	SUCCESS	Desired Access: R...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\Software\WOW6432Node\Microsoft\Tracing\RegSvcs_RASMANCS	SUCCESS	Desired Access: R...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\SOFTWARE\WOW6432Node\Policies\Microsoft\Windows\TenantRestrictions\Payload	REPARSE	Desired Access: Q...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\TenantRestrictions\Payload	SUCCESS	Desired Access: Q...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\TenantRestrictions\Payload	SUCCESS	Desired Access: N...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\SOFTWARE\WOW6432Node\Policies\Microsoft\Windows\TenantRestrictions\Payload	REPARSE	Desired Access: Q...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\TenantRestrictions\Payload	SUCCESS	Desired Access: Q...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	SUCCESS	Desired Access: Q...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	REPARSE	Desired Access: R...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	SUCCESS	Desired Access: R...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	REPARSE	Desired Access: R...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	SUCCESS	Desired Access: R...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	REPARSE	Desired Access: R...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	SUCCESS	Desired Access: R...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	REPARSE	Desired Access: R...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	SUCCESS	Desired Access: R...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	REPARSE	Desired Access: R...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	SUCCESS	Desired Access: R...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	REPARSE	Desired Access: R...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	SUCCESS	Desired Access: R...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	REPARSE	Desired Access: R...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	SUCCESS	Desired Access: R...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	REPARSE	Desired Access: R...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	SUCCESS	Desired Access: R...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	REPARSE	Desired Access: R...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	SUCCESS	Desired Access: R...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	REPARSE	Desired Access: R...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	SUCCESS	Desired Access: R...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	REPARSE	Desired Access: R...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	SUCCESS	Desired Access: R...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	REPARSE	Desired Access: R...
7:16:1...	RegSvcs.exe	1016	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	SUCCESS	Desired Access: R...

Showing 39 of 2,051,975 events (0.0019%) Backed by virtual memory

Si possono notare due nomi sospetti abbastanza frequenti: RASAPI32 e RASMANCS.

La loro presenza ricorrente nei filtri delle operazioni RegSetValue suggerisce che potrebbero agire come la backdoor precedentemente ipotizzata.

7:16:1...	RegSvcs.exe	1016	RegSetValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Tracing\EnableConsoleTracing	SUCCESS	Type: REG_DWO...
7:16:1...	RegSvcs.exe	1016	RegSetValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Tracing\RegSvcs_RASAPI32\EnableFileTracing	SUCCESS	Type: REG_DWO...
7:16:1...	RegSvcs.exe	1016	RegSetValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Tracing\RegSvcs_RASAPI32\EnableAutoFileTr...	SUCCESS	Type: REG_DWO...
7:16:1...	RegSvcs.exe	1016	RegSetValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Tracing\RegSvcs_RASAPI32\EnableConsoleTr...	SUCCESS	Type: REG_DWO...
7:16:1...	RegSvcs.exe	1016	RegSetValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Tracing\RegSvcs_RASAPI32\FileTracingMask	SUCCESS	Type: REG_DWO...
7:16:1...	RegSvcs.exe	1016	RegSetValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Tracing\RegSvcs_RASAPI32\ConsoleTracingM...	SUCCESS	Type: REG_DWO...
7:16:1...	RegSvcs.exe	1016	RegSetValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Tracing\RegSvcs_RASAPI32\MaxFileSize	SUCCESS	Type: REG_DWO...
7:16:1...	RegSvcs.exe	1016	RegSetValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Tracing\RegSvcs_RASAPI32\FileDirectory	SUCCESS	Type: REG_EXPA...
7:16:1...	RegSvcs.exe	1016	RegSetValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Tracing\RegSvcs_RASMANCS\EnableFileTracing	SUCCESS	Type: REG_DWO...
7:16:1...	RegSvcs.exe	1016	RegSetValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Tracing\RegSvcs_RASMANCS\EnableAutoFile...	SUCCESS	Type: REG_DWO...
7:16:1...	RegSvcs.exe	1016	RegSetValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Tracing\RegSvcs_RASMANCS\EnableConsole...	SUCCESS	Type: REG_DWO...
7:16:1...	RegSvcs.exe	1016	RegSetValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Tracing\RegSvcs_RASMANCS\FileTracingMask	SUCCESS	Type: REG_DWO...
7:16:1...	RegSvcs.exe	1016	RegSetValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Tracing\RegSvcs_RASMANCS\ConsoleTracing...	SUCCESS	Type: REG_DWO...
7:16:1...	RegSvcs.exe	1016	RegSetValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Tracing\RegSvcs_RASMANCS\MaxFileSize	SUCCESS	Type: REG_DWO...
7:16:1...	RegSvcs.exe	1016	RegSetValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Tracing\RegSvcs_RASMANCS\FileDirectory	SUCCESS	Type: REG_EXPA...

Valore dei registri settati da RASAPI32 e RASMANCS:

\RegSvcs_RASMANCS

Name	Type	Data
(Default)	REG_SZ	(value not set)
ConsoleTracing...	REG_DWORD	0xffff0000 (4294901760)
EnableAutoFileT...	REG_DWORD	0x00000000 (0)
EnableConsoleTr...	REG_DWORD	0x00000000 (0)
EnableFileTracing	REG_DWORD	0x00000000 (0)
FileDirectory	REG_EXPAND_SZ	%windir%\tracing
FileTracingMask	REG_DWORD	0xffff0000 (4294901760)
MaxFileSize	REG_DWORD	0x00100000 (1048576)

\RegSvcs_RASAPI32

Name	Type	Data
(Default)	REG_SZ	(value not set)
ConsoleTracing...	REG_DWORD	0xffff0000 (4294901760)
EnableAutoFileT...	REG_DWORD	0x00000000 (0)
EnableConsoleTr...	REG_DWORD	0x00000000 (0)
EnableFileTracing	REG_DWORD	0x00000000 (0)
FileDirectory	REG_EXPAND_SZ	%windir%\tracing
FileTracingMask	REG_DWORD	0xffff0000 (4294901760)
MaxFileSize	REG_DWORD	0x00100000 (1048576)

L’ultimo check è stato quello di controllare tramite gli Handles la presenza di mutex nel programma, questo perché la maggioranza dei malware utilizza dei mutex al fine di assicurarsi che una sola copia del malware sia in esecuzione al momento. In windows, i mutex vengono chiamati "mutants":

Key	HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces
Key	HKLM\SYSTEM\ControlSet001\Services\Tcpip6\Parameters\Interfaces
Key	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\Folder..
Mutant	\Sessions\1\BaseNamedObjects\SM0:6500:168:WilStaging_02
Mutant	\Sessions\1\BaseNamedObjects\SM0:6500:64:WilError_03
Mutant	\BaseNamedObjects\RasPbFile
Section	\BaseNamedObjects\Cor_Private_IPCBlock_v4_6500
Section	\...\Cor_SxSPublic_IPCBlock

Come ultimo passaggio, si è provato ad analizzare il traffico di rete generato dal malware. Tuttavia, per qualche motivo, Wireshark non ha rilevato nulla, probabilmente a causa del malware stesso che potrebbe aver modificato le chiavi di configurazione del driver per evitare il rilevamento.

4) Malware Detection

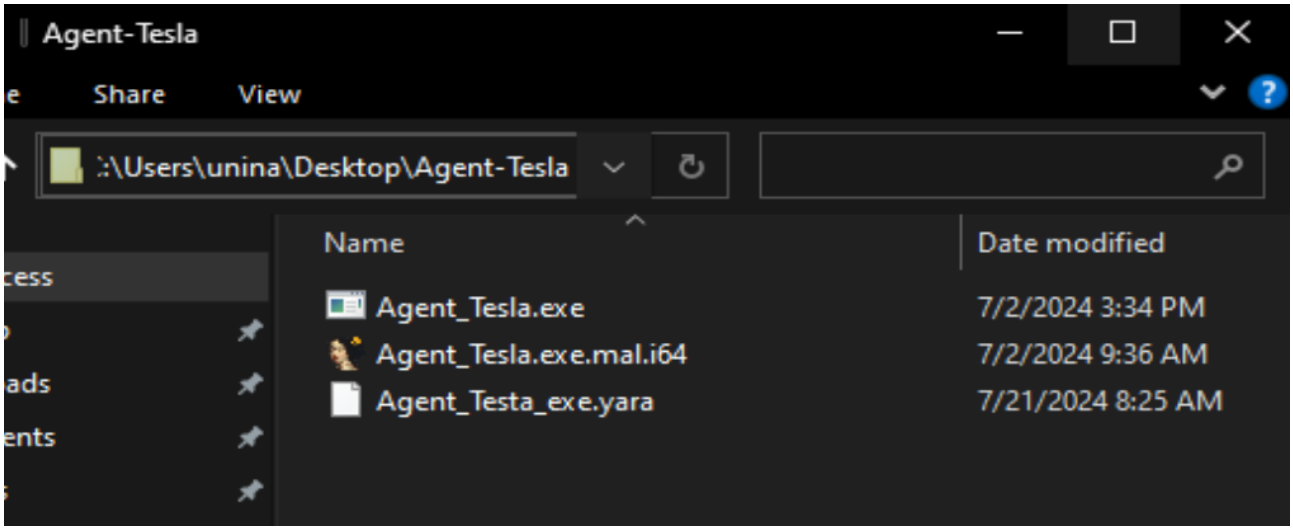
Utilizzando binText è stato possibile trovare ulteriori stringe più o meno specifiche tra cui:

```
rule Agent_Tesla_EXE {
    meta:
        description = "Agent_Tesla.exe"
        author = "MarcoC117"
        date = "2024-07-21"

    strings:
        $mz = {4d 5a}
        $x1 = ">>>AUTOIT SCRIPT<<<" wide ascii nocase
        $x2 = ">>>AUTOIT NO CMDEXECUTE<<<" wide ascii nocase
        $x3 = "Software\\AutoIt v3\\AutoIt" wide ascii nocase
        $x4 = "This is a third-party compiled AutoIt script." wide ascii nocase
        $x5 = "AutoIt Error" wide ascii nocase
        $s1 = "Sleep" ascii wide nocase

    condition:
        $mz at 0 and 1 of ($x*) and $s1
}
```

Trovate le stringhe è possibile scrivere la regola YARA: La cui esecuzione da riga di comando:

```
Administrator: C:\Windows\system32\cmd.exe - yara64.exe -r C:\Users\unina\Desktop\Agent-Tesla\Agent_Testa_exe.yara C:\Users\unina\Desktop

C:\Users\unina\Desktop\Tools>yara64.exe -r C:\Users\unina\Desktop\Agent-Tesla\Agent_Testa_exe.yara C:\Users\unina\Desktop
Agent_Tesla_EXE C:\Users\unina\Desktop\Agent-Tesla\Agent_Tesla.exe
```

La regola rileva correttamente l'eseguibile nella sua effettiva cartella:



5) Mitre ATT&CK

Tactic	Technique	Procedure
Initial Access	T1566: Phishing	Distributed via phishing email-attacks (Fake .pdf)
Execution	T1059.001: PowerShell	Used to execute scripts and commands
Execution	T1203: Exploitation for Client Execution	AutoIt-based script execution
Persistence	T1543.003: Windows Service: Service Creation	Creates a process named Regsvcs.exe for persistence
Privilege Escalation	T1055: Process Injection	Injects malicious code into Regsvcs.exe via Process Replacement
Defense Evasion	T1027: Obfuscated Files or Information	Uses obfuscation and evasion techniques to avoid detection
Credential Access	T1003.001: LSASS Memory	Likely interacts with LSASS memory to gather credentials
Collection	T1114: Email Collection	Uses RASAPI32 or RASMANCS for collecting and exfiltrating information

Command and Control	T1071.001: Application Layer Protocol: Web Protocols	Communicates with C2 servers to send collected data
Exfiltration	T1041: Exfiltration Over Command and Control Channel	Exfiltrates data over the internet via C2 channels
Impact	T1486: Data Encrypted for Impact	Potentially encrypts or otherwise modifies data to conceal activities
Execution	T1064: Sudo and Sudo Caching	May utilize elevated privileges for various operations
Defense Evasion	T1562.001: Disable or Modify Tools	Disables Windows Defender libraries to avoid detection
Process Injection	T1055.012: Process Injection: Process Hollowing/Replacement	Utilizes process hollowing for injecting code into legitimate processes
Discovery	T1012: Query Registry	Queries and manipulates Windows Registry settings
Discovery	T1082: System Information Discovery	Gathers system information, possibly to adjust attack strategies
Discovery	T1083: File and Directory Discovery	Enumerates files and directories
Defense Evasion	T1112: Modify Registry	Manipulates and modifyWindows Registry

6) Considerazioni finali

Agent Tesla è un malware sviluppato in AutoItv3, notevolmente compresso e diffuso principalmente tramite attacchi di phishing.

Durante l'esecuzione, con il nome di Agent Tesla, il malware prepara l'ambiente e lo script necessario per l’esecuzione. Verifica i privilegi del processo in corso per eseguire operazioni critiche e crea un nuovo processo chiamato Regsvcs.exe, nel quale inietta codice dannoso tramite Process Replacement. L'analisi rivela che Agent Tesla utilizza una backdoor nota come RASAPI32 o RASMANCS, molto probabilmente per inviare le informazioni raccolte agli autori dell'attacco.

Questo comportamento indica che Agent Tesla agisce principalmente come sofisticato Information Stealer. Utilizza anche tecniche avanzate di offuscamento ed elusione per evitare la rilevazione, inclusa l'attivazione contro le librerie utilizzate da Windows Defender, al fine di disabilitarlo. Questo schema di attacco mira a massimizzare l'accesso a informazioni riservate, compromettendo la sicurezza e la privacy degli utenti.