Report di Analisi del Malware

Introduzione

Durante l'esercizio pratico, ho seguito i passaggi per recuperare informazioni su un malware tramite l'analisi dinamica basica utilizzando Multimon e Process Monitor. Questo report documenta i passaggi eseguiti e le osservazioni fatte durante l'analisi del file eseguibile Malware_U3_W2_L1.exe.

Preparazione dell'Ambiente

1. **Creazione di un'Istantanea della VM:**
    - Ho creato un'istantanea della macchina virtuale Windows 7 per garantire la possibilità di ripristinare lo stato iniziale in caso di problemi.
2. **Download e Installazione di Multimon:**
    - Ho scaricato e installato Multimon dal sito Resplendence Multimon.

Esecuzione del Monitoraggio con Multimon

1. **Configurazione di Multimon:**
    - Ho avviato Multimon e selezionato l'opzione per monitorare il File System.
    - Ho avviato il monitoraggio cliccando sul pulsante di avvio.
2. **Esecuzione del Malware:**
    - Ho eseguito il file eseguibile del malware Malware_U3_W2_L1.exe dalla cartella Esercizio_Pratico_U3_W2_L1 sul desktop.
3. **Raccolta dei Log:**
    - Multimon ha registrato varie operazioni di file system, incluse operazioni di lettura (IRP_MJ_READ), scrittura (IRP_MJ_WRITE) e creazione (IRP_MJ_CREATE).

Analisi dei Log di Multimon

1. **Operazioni Rilevate:**
    - Ho identificato le operazioni associate a svchost.exe, un processo di sistema legittimo che potrebbe essere utilizzato dal malware per camuffarsi.
2. **Percorsi Monitorati:**
    - Le operazioni sui seguenti percorsi sono state considerate sospette:
        - C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windows\INetCache
        - C:\Users\simone\AppData\Local\Temp\sample.tmp

Utilizzo di Process Monitor per Analisi Dettagliata

1. **Configurazione di Process Monitor:**
    - Ho scaricato e avviato Process Monitor da Sysinternals.
    - Ho configurato Process Monitor per registrare operazioni come CreateFile, RegOpenKey, Load Image, ecc.
2. **Esecuzione del Malware e Raccolta dei Log:**
    - Ho eseguito il malware e monitorato le sue attività con Process Monitor.
3. **Analisi dei Log di Process Monitor:**
    - Ho identificato operazioni di creazione file (CreateFile), caricamento di immagini (Load Image) e modifiche al registro di sistema (RegOpenKey).

Identificazione delle Attività del Malware

1. **Persistenza:**
    - Il malware ha eseguito operazioni su chiavi di registro critiche per il caricamento automatico all'avvio:

sql

Copia codice

RegOpenKey - HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\00001

2. **Modifica del Sistema:**
    - Ho identificato operazioni sospette su file di sistema:

mathematica

Copia codice

CreateFile - C:\Windows\System32\svchost.dll

3. **Esfiltrazione di Dati:**
    - Il malware ha creato file temporanei in directory sospette:

mathematica

Copia codice

CreateFile - C:\Users\simone\AppData\Local\Temp\sample.tmp

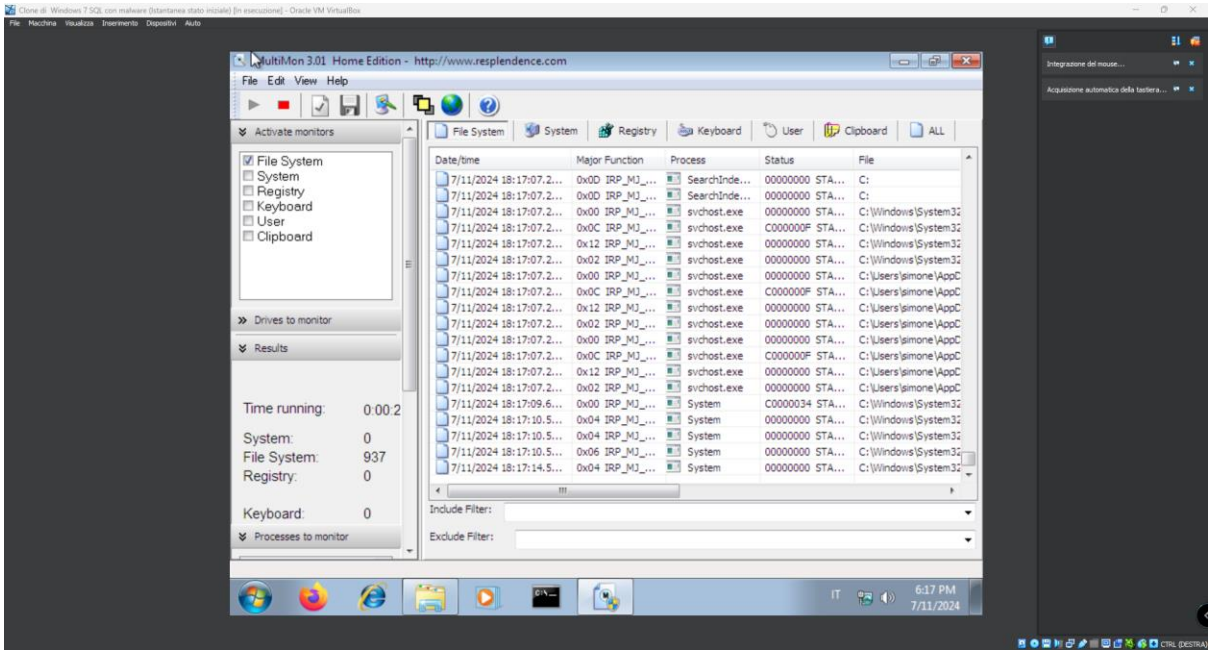
Conclusioni

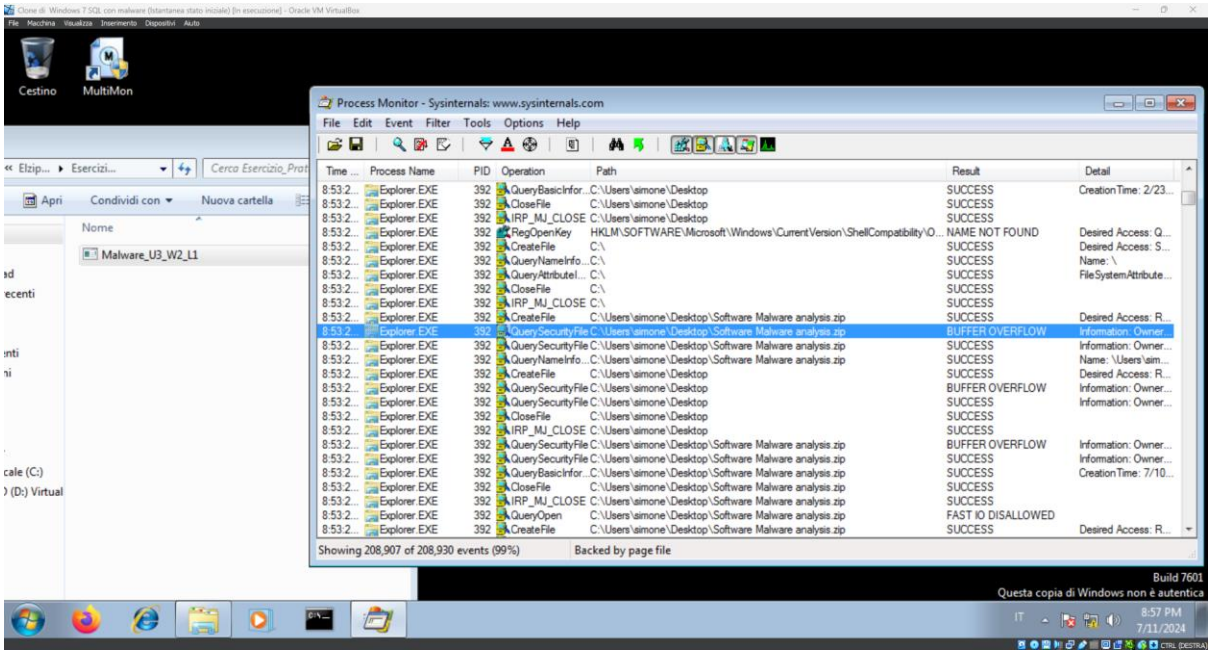
L'analisi dinamica del malware ha rivelato che il file Malware_U3_W2_L1.exe esegue operazioni sospette come modifiche al registro di sistema per ottenere persistenza, accesso a file di sistema critici e creazione di file temporanei per potenziali esfiltrazioni di dati. Basandomi su queste osservazioni, ho sviluppato un profilo comportamentale del malware che potrà essere utilizzato per ulteriori analisi e per la creazione di un piano di mitigazione.

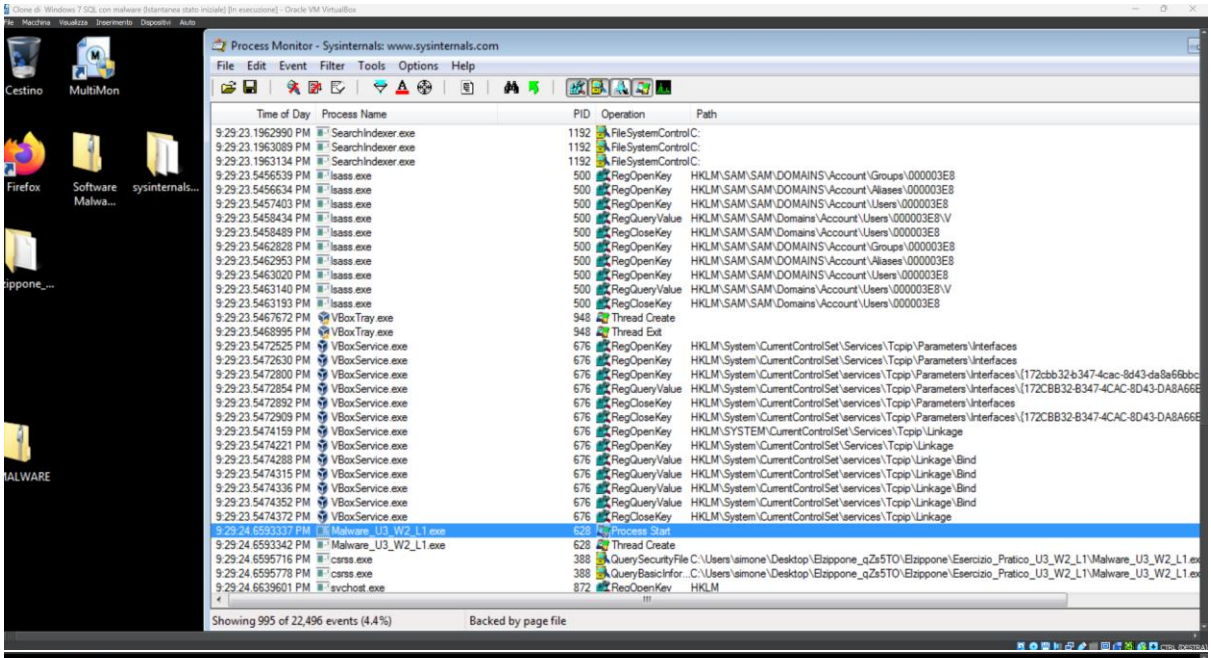
Passi Successivi

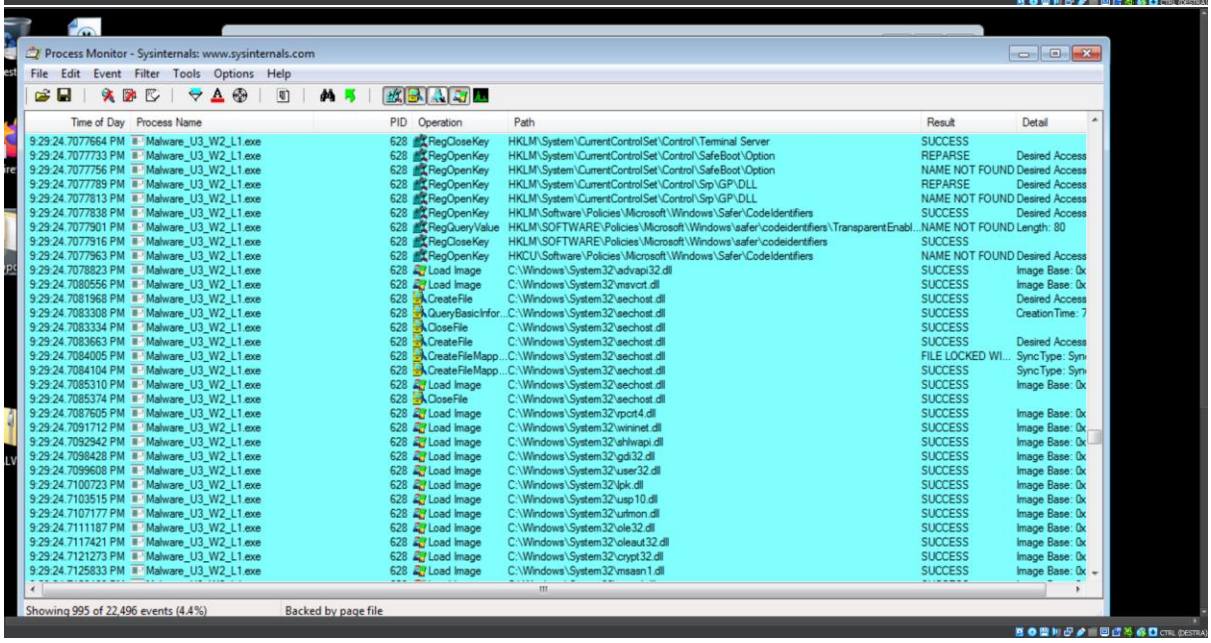
1. **Documentare le osservazioni**: Preparare un rapporto dettagliato con tutte le operazioni sospette identificate.
2. **Analisi più approfondita**: Utilizzare altri strumenti di analisi dinamica o statica per comprendere ulteriormente il comportamento del malware.
3. **Piano di mitigazione**: Sviluppare un piano per rimuovere il malware e ripristinare la sicurezza del sistema.

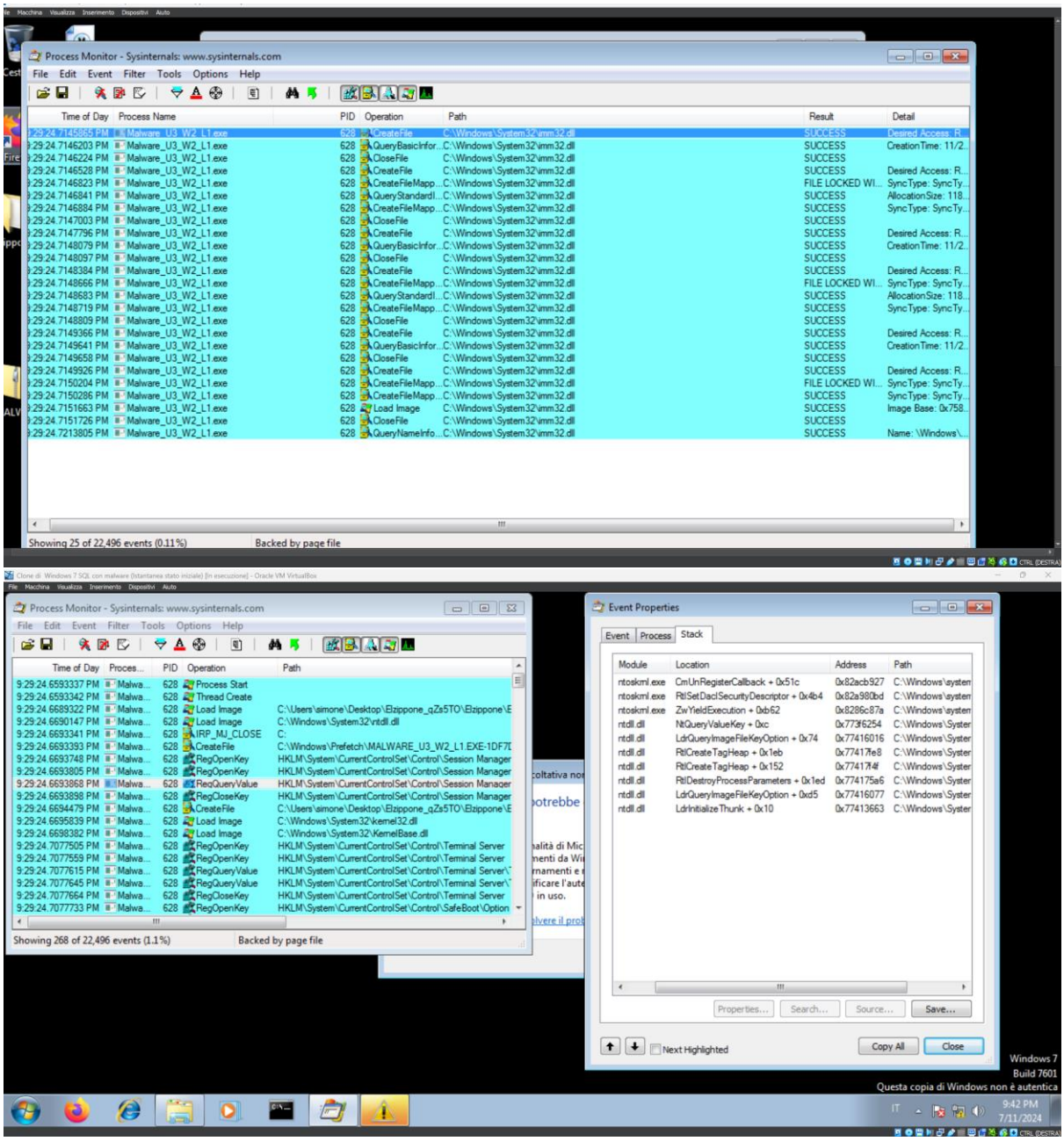
Screenshot






Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time of Day Process Name PID Operation Path
9:29:23.1962990 PM SearchIndexer.exe 1192 FileSystemControl C:
9:29:23.1963089 PM SearchIndexer.exe 1192 FileSystemControl C:
9:29:23.1963134 PM SearchIndexer.exe 1192 FileSystemControl C:
9:29:23.5456539 PM lsass.exe 500 RegOpenKey HKLM\SAM\SAM\DOMAINS\Account\Groups\000003E8
9:29:23.5456634 PM lsass.exe 500 RegOpenKey HKLM\SAM\SAM\DOMAINS\Account\Aliases\000003E8
9:29:23.5457403 PM lsass.exe 500 RegOpenKey HKLM\SAM\SAM\DOMAINS\Account\Users\000003E8
9:29:23.5458434 PM lsass.exe 500 RegQueryValue HKLM\SAM\SAM\Domains\Account\Users\000003E8\V
9:29:23.5458489 PM lsass.exe 500 RegCloseKey HKLM\SAM\SAM\Domains\Account\Users\000003E8
9:29:23.5462828 PM lsass.exe 500 RegOpenKey HKLM\SAM\SAM\DOMAINS\Account\Groups\000003E8
9:29:23.5462953 PM lsass.exe 500 RegOpenKey HKLM\SAM\SAM\DOMAINS\Account\Aliases\000003E8
9:29:23.5463020 PM lsass.exe 500 RegOpenKey HKLM\SAM\SAM\DOMAINS\Account\Users\000003E8
9:29:23.5463140 PM lsass.exe 500 RegQueryValue HKLM\SAM\SAM\Domains\Account\Users\000003E8\V
9:29:23.5463193 PM lsass.exe 500 RegCloseKey HKLM\SAM\SAM\Domains\Account\Users\000003E8
9:29:23.5467672 PM VBoxTray.exe 948 Thread Create
9:29:23.5468995 PM VBoxTray.exe 948 Thread Exit
9:29:23.5472525 PM VBoxService.exe 676 RegOpenKey HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces
9:29:23.5472630 PM VBoxService.exe 676 RegOpenKey HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces
9:29:23.5472800 PM VBoxService.exe 676 RegOpenKey HKLM\System\CurrentControlSet\services\Tcpip\Parameters\Interfaces\{172cbb32-b347-4cac-8d43-da8a66bbc
9:29:23.5472854 PM VBoxService.exe 676 RegQueryValue HKLM\System\CurrentControlSet\services\Tcpip\Parameters\Interfaces\{172CBB32-B347-4CAC-8D43-DA8A66E
9:29:23.5472892 PM VBoxService.exe 676 RegCloseKey HKLM\System\CurrentControlSet\services\Tcpip\Parameters\Interfaces
9:29:23.5472909 PM VBoxService.exe 676 RegCloseKey HKLM\System\CurrentControlSet\services\Tcpip\Parameters\Interfaces\{172CBB32-B347-4CAC-8D43-DA8A66E
9:29:23.5474159 PM VBoxService.exe 676 RegOpenKey HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Linkage
9:29:23.5474221 PM VBoxService.exe 676 RegOpenKey HKLM\System\CurrentControlSet\Services\Tcpip\Linkage
9:29:23.5474288 PM VBoxService.exe 676 RegQueryValue HKLM\System\CurrentControlSet\services\Tcpip\Linkage\Bind
9:29:23.5474315 PM VBoxService.exe 676 RegQueryValue HKLM\System\CurrentControlSet\services\Tcpip\Linkage\Bind
9:29:23.5474336 PM VBoxService.exe 676 RegQueryValue HKLM\System\CurrentControlSet\services\Tcpip\Linkage\Bind
9:29:23.5474352 PM VBoxService.exe 676 RegQueryValue HKLM\System\CurrentControlSet\services\Tcpip\Linkage\Bind
9:29:23.5474372 PM VBoxService.exe 676 RegCloseKey HKLM\System\CurrentControlSet\services\Tcpip\Linkage
9:29:24.6593337 PM Malware_U3_W2_L1.exe 628 Process Start
9:29:24.6593342 PM Malware_U3_W2_L1.exe 628 Thread Create
9:29:24.6595716 PM csrss.exe 388 QuerySecurityFile C:\Users\simone\Desktop\Elzippone_qZs5TO\Elzippone\Esercizio_Pratico_U3_W2_L1\Malware_U3_W2_L1.ex
9:29:24.6595778 PM csrss.exe 388 QueryBasicInfor... C:\Users\simone\Desktop\Elzippone_qZs5TO\Elzippone\Esercizio_Pratico_U3_W2_L1\Malware_U3_W2_L1.ex
9:29:24.6639601 PM svchost.exe 872 RegOpenKey HKLM
Showing 995 of 22,496 events (4.4%)
Backed by page file


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time of Day Process Name PID Operation Path Result Detail
9:29:24.7077664 PM Malware_U3_W2_L1.exe 628 RegCloseKey HKLM\System\CurrentControlSet\Control\Terminal Server SUCCESS
9:29:24.7077733 PM Malware_U3_W2_L1.exe 628 RegOpenKey HKLM\System\CurrentControlSet\Control\SafeBoot\Option REPARSE Desired Access
9:29:24.7077756 PM Malware_U3_W2_L1.exe 628 RegOpenKey HKLM\System\CurrentControlSet\Control\SafeBoot\Option NAME NOT FOUND Desired Access
9:29:24.7077789 PM Malware_U3_W2_L1.exe 628 RegOpenKey HKLM\System\CurrentControlSet\Control\Srp\GP\DLL REPARSE Desired Access
9:29:24.7077813 PM Malware_U3_W2_L1.exe 628 RegOpenKey HKLM\System\CurrentControlSet\Control\Srp\GP\DLL NAME NOT FOUND Desired Access
9:29:24.7077838 PM Malware_U3_W2_L1.exe 628 RegOpenKey HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers SUCCESS Desired Access
9:29:24.7077901 PM Malware_U3_W2_L1.exe 628 RegQueryValue HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\TransparentEnabl... NAME NOT FOUND Length: 80
9:29:24.7077916 PM Malware_U3_W2_L1.exe 628 RegCloseKey HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers SUCCESS
9:29:24.7077963 PM Malware_U3_W2_L1.exe 628 RegOpenKey HKCU\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers NAME NOT FOUND Desired Access
9:29:24.7078823 PM Malware_U3_W2_L1.exe 628 Load Image C:\Windows\System32\advapi32.dll SUCCESS Image Base: 0x
9:29:24.7080556 PM Malware_U3_W2_L1.exe 628 Load Image C:\Windows\System32\msvcrt.dll SUCCESS Image Base: 0x
9:29:24.7081968 PM Malware_U3_W2_L1.exe 628 CreateFile C:\Windows\System32\sechost.dll SUCCESS Desired Access
9:29:24.7083308 PM Malware_U3_W2_L1.exe 628 QueryBasicInfor... C:\Windows\System32\sechost.dll SUCCESS CreationTime: 7
9:29:24.7083334 PM Malware_U3_W2_L1.exe 628 CloseFile C:\Windows\System32\sechost.dll SUCCESS
9:29:24.7083663 PM Malware_U3_W2_L1.exe 628 CreateFile C:\Windows\System32\sechost.dll SUCCESS Desired Access
9:29:24.7084005 PM Malware_U3_W2_L1.exe 628 CreateFileMapp... C:\Windows\System32\sechost.dll FILE LOCKED WI... SyncType: Syn
9:29:24.7084104 PM Malware_U3_W2_L1.exe 628 CreateFileMapp... C:\Windows\System32\sechost.dll SUCCESS SyncType: Syn
9:29:24.7085310 PM Malware_U3_W2_L1.exe 628 Load Image C:\Windows\System32\sechost.dll SUCCESS Image Base: 0x
9:29:24.7085374 PM Malware_U3_W2_L1.exe 628 CloseFile C:\Windows\System32\sechost.dll SUCCESS
9:29:24.7087605 PM Malware_U3_W2_L1.exe 628 Load Image C:\Windows\System32\rpcrt4.dll SUCCESS Image Base: 0x
9:29:24.7091712 PM Malware_U3_W2_L1.exe 628 Load Image C:\Windows\System32\wininet.dll SUCCESS Image Base: 0x
9:29:24.7092942 PM Malware_U3_W2_L1.exe 628 Load Image C:\Windows\System32\shlwapi.dll SUCCESS Image Base: 0x
9:29:24.7098428 PM Malware_U3_W2_L1.exe 628 Load Image C:\Windows\System32\gdi32.dll SUCCESS Image Base: 0x
9:29:24.7099608 PM Malware_U3_W2_L1.exe 628 Load Image C:\Windows\System32\user32.dll SUCCESS Image Base: 0x
9:29:24.7100723 PM Malware_U3_W2_L1.exe 628 Load Image C:\Windows\System32\lpk.dll SUCCESS Image Base: 0x
9:29:24.7103515 PM Malware_U3_W2_L1.exe 628 Load Image C:\Windows\System32\usp10.dll SUCCESS Image Base: 0x
9:29:24.7107177 PM Malware_U3_W2_L1.exe 628 Load Image C:\Windows\System32\urlmon.dll SUCCESS Image Base: 0x
9:29:24.7111187 PM Malware_U3_W2_L1.exe 628 Load Image C:\Windows\System32\ole32.dll SUCCESS Image Base: 0x
9:29:24.7117421 PM Malware_U3_W2_L1.exe 628 Load Image C:\Windows\System32\oleaut32.dll SUCCESS Image Base: 0x
9:29:24.7121273 PM Malware_U3_W2_L1.exe 628 Load Image C:\Windows\System32\crypt32.dll SUCCESS Image Base: 0x
9:29:24.7125833 PM Malware_U3_W2_L1.exe 628 Load Image C:\Windows\System32\msasn1.dll SUCCESS Image Base: 0x
Showing 995 of 22,496 events (4.4%)
Backed by page file


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time of Day Process Name PID Operation Path Result Detail
Showing 25 of 22,496 events (0.11%)
Backed by page file

Process Monitor - Sysinternals: www.sysinternals.com
Showing 268 of 22,496 events (1.1%)
Backed by page file
Event Properties
Event Process Stack
Module Location Address Path
Properties... Search... Source... Save...
Next Highlighted
Copy All Close
Windows 7
Build 7601
Questa copia di Windows non è autentica
9:42 PM
7/11/2024