Maurizio Marcantoni

Bonus

S10/L5

DATA SHIELDS

Introduzione

Per affrontare la preoccupazione sollevata dal nuovo dipendente riguardo alla presenza del file iexplore.exe, puoi seguire i seguenti passaggi per fornire un'analisi approfondita e dimostrare che il file non è maligno

Click For Index

DATA SHIELDS

Traccia Bonus

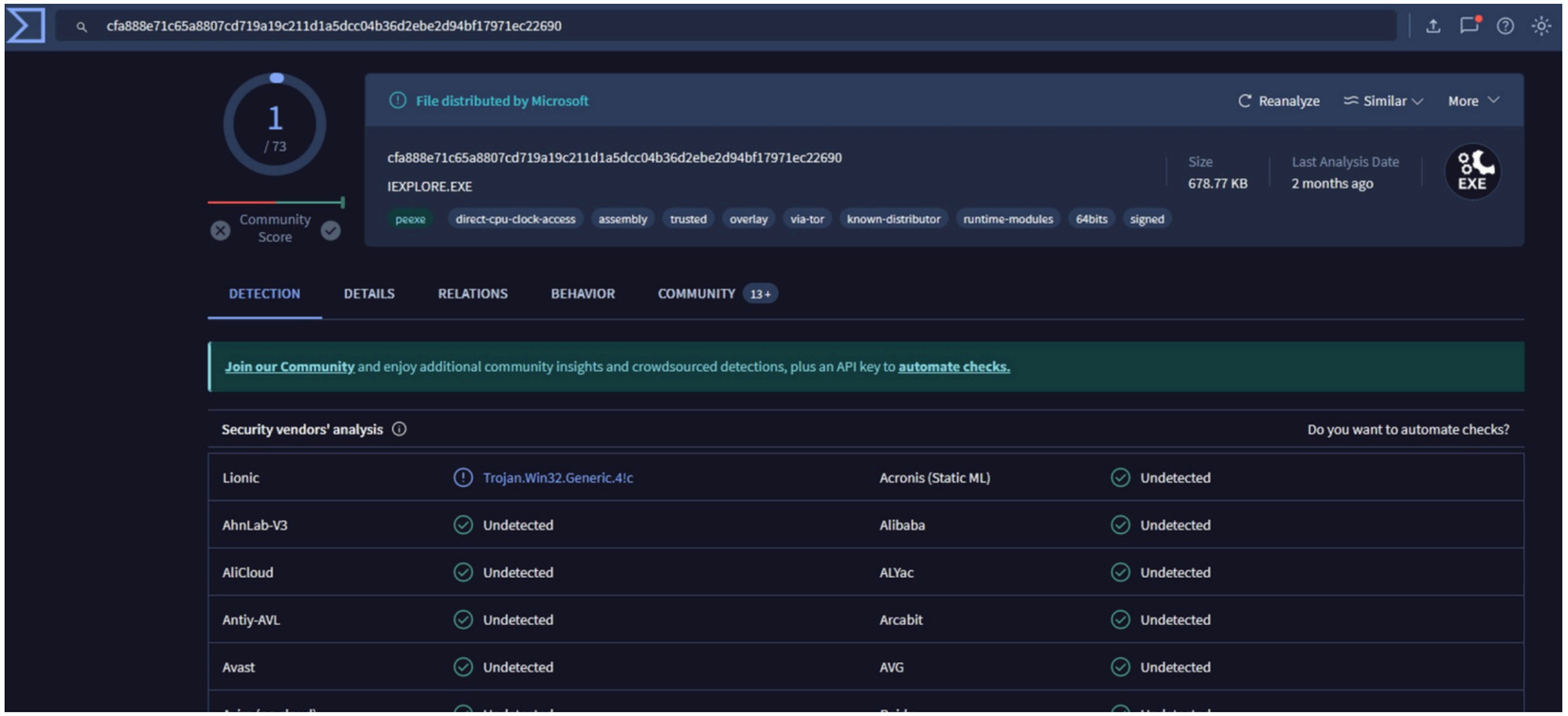
Un giovane dipendente neo assunto segnala al reparto tecnico la presenza di un programma sospetto. Il suo superiore gli dice di stare tranquillo ma lui non è soddisfatto e chiede supporto al SOC. Il file "sospetto" è **iexplore.exe** contenuto nella cartella **C:\Programmi\Internet Explorer** (no, non ridete ragazzi)

Come membro senior del SOC ti è richiesto di convincere il dipendente che il file non è maligno. Esercizio Traccia e requisiti Possono essere usati gli strumenti di analisi statica basica e/o analisi dinamica basica visti a lezione. No disassembly no debug o similari VirusTotal non basta, ovviamente Non basta dire iexplorer è Microsoft quindi è buono, punto.

DATA SHIELDS

Confronto con Software Antimalware

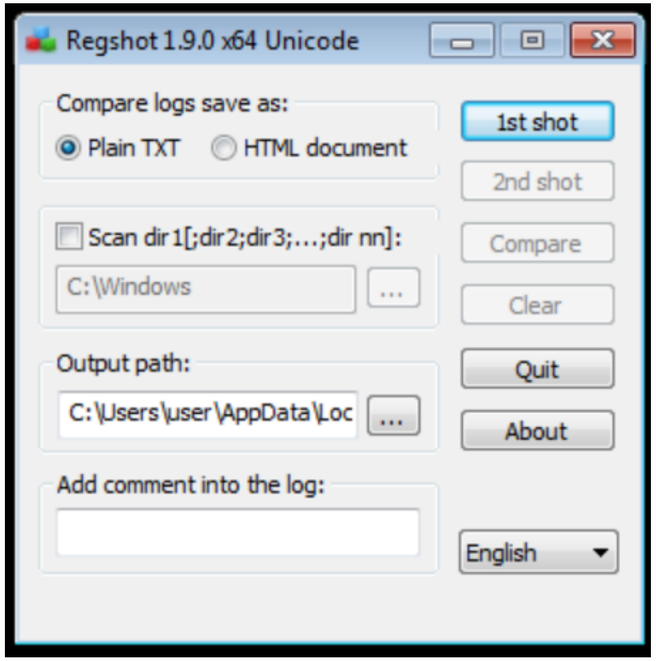
Per analizzare il file in questione(iexplore.exe) procediamo con un analisi statica di base tramite un confronto con un software antimalware. Procediamo utilizzando VirusTotal. Caricando il file su VirusTotal possiamo effettuare un'analisi approfondita tramite molteplici motori antivirus. Anche se VirusTotal non è sufficiente da solo , può fornire un primo riscontro sull'integrità del file.



DATA SHIELDS

Analisi Dinamica Base

Come possiamo notare la maggior parte dei vendor identifica IEXPLORE.EXE come un file di tipo NON malevolo. Procediamo ad effettuare un esame ancora più approfondito tramite l'analisi dinamica di base. Utilizziamo come primo tool **Regshot**.
Regshot è un'utility che cattura due istantanee diverse, una del registro di sistema e una del file system, consentendo quindi di confrontare le due immagini per individuare tutte le modifiche apportate tra i due momenti. Questa informazione può essere particolarmente utile per comprendere quali chiavi di registro o file vengono alterati durante l'installazione di un programma, la modifica delle impostazioni del sistema o altre azioni che potrebbero avere un impatto sul sistema.



DATA SHIELDS

Analisi Dinamica Base

Effettuato il compare delle chiavi in due momenti diversi , possiamo notare come vengano aggiunte un totale di 7 chiavi di registro e 30 valori . Nella prossima slide una lista delle chiavi aggiunte e del loro funzionamento .

```
Regshot 1.9.0 x64 Unicode
Comments:
Datetime: 2024/8/2 13:09:33   ,   2024/8/2 13:10:25
Computer: USER-PC , USER-PC
Username: user , user

----------------------------------
Keys added: 7
----------------------------------
HKLM\SOFTWARE\Microsoft\Tracing\iexplore_RASAPI32
HKLM\SOFTWARE\Microsoft\Tracing\iexplore_RASMANCS
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Internet Explorer\Security\AntiPhishing
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Internet Explorer\Security\AntiPhishing\2CEDBFBC-DBA8-43AA-B1FD-CC8E6316E3E2
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012024080220240803
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\PrivacIE:
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\AntiPhishing

----------------------------------
Values added: 30
----------------------------------
HKLM\SOFTWARE\Microsoft\Tracing\iexplore_RASAPI32\EnableFileTracing: 0x00000000
HKLM\SOFTWARE\Microsoft\Tracing\iexplore_RASAPI32\EnableConsoleTracing: 0x00000000
HKLM\SOFTWARE\Microsoft\Tracing\iexplore_RASAPI32\FileTracingMask: 0xFFFF0000
HKLM\SOFTWARE\Microsoft\Tracing\iexplore_RASAPI32\ConsoleTracingMask: 0xFFFF0000
HKLM\SOFTWARE\Microsoft\Tracing\iexplore_RASAPI32\MaxFileSize: 0x00100000
HKLM\SOFTWARE\Microsoft\Tracing\iexplore_RASAPI32\FileDirectory: "%windir%\tracing"
HKLM\SOFTWARE\Microsoft\Tracing\iexplore_RASMANCS\EnableFileTracing: 0x00000000
HKLM\SOFTWARE\Microsoft\Tracing\iexplore_RASMANCS\EnableConsoleTracing: 0x00000000
HKLM\SOFTWARE\Microsoft\Tracing\iexplore_RASMANCS\FileTracingMask: 0xFFFF0000
HKLM\SOFTWARE\Microsoft\Tracing\iexplore_RASMANCS\ConsoleTracingMask: 0xFFFF0000
HKLM\SOFTWARE\Microsoft\Tracing\iexplore_RASMANCS\MaxFileSize: 0x00100000
HKLM\SOFTWARE\Microsoft\Tracing\iexplore_RASMANCS\FileDirectory: "%windir%\tracing"
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Internet Explorer\Recovery\Active\{90CE0B22-50D0-11EF-A5ED-080027EE8503}: 0x00000000
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU\*\6:  50 00 32 00 00 00 00 00 00 00 00 00 80 00 31 2E 68 69 76 75 00 00 3A 00 08 00 04
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU\hivu\1:  50 00 32 00 00 00 00 00 00 00 00 00 80 00 31 2E 68 69 76 75 00 00 3A 00 08 00
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\21:  31 00 2E 00 68 00 69 00 76 00 75 00 00 00 5C 00 32 00 00 00 00 00 00 00 00 00 00 00 31 2E 68 69
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.hivu\1:  31 00 2E 00 68 00 69 00 76 00 75 00 00 00 5C 00 32 00 00 00 00 00 00 00 00 00 00 00 31 2E
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\{6Q809377-6NS0-444O-8957-N3773S02200R}\Vagrearg Rkcyber
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\Zvpebfbsg.VagreargRkcybere.64Ovg:  00 00 00 00 00 00 00
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012024080220240803\CachePath: "%USERPROFILE%\AppData\Local\Microsoft\
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012024080220240803\CachePrefix: ":2024080220240803: "
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012024080220240803\CacheLimit: 0x00002000
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012024080220240803\CacheOptions: 0x0000000B
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012024080220240803\CacheRepair: 0x00000000
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\PrivacIE:\CachePath: "%APPDATA%\Microsoft\Windows\PrivacIE"
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\PrivacIE:\CachePrefix: "PrivacIE:"
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\PrivacIE:\CacheLimit: 0x00000400
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\PrivacIE:\CacheOptions: 0x00000009
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\PrivacIE:\CacheRepair: 0x00000000
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\AntiPhishing\i:  41 00 36 00 41 00 33 00 32 00 41 00 39 00 37 00 2D 00 32 00 45 00 32 00 42 00 2D 00 34 00 39 00 41 00 32 00 2D 00 39 00 43 00

----------------------------------
```

DATA SHIELDS

Chiavi di registro aggiunte

- **HKLM\SOFTWARE\Microsoft\Tracing\iexplore_RASAPI32**

Questa chiave è utilizzata per il tracciamento e il debug delle sessioni RAS (Remote Access Service) che coinvolgono Internet Explorer. RASAPI32 è una libreria di Windows che gestisce le connessioni di accesso remoto. Il tracciamento è spesso utilizzato per diagnosticare problemi di rete e connessione.

- **HKLM\SOFTWARE\Microsoft\Tracing\iexplore_RASMANCS**

Simile alla chiave precedente, questa è utilizzata per il tracciamento delle sessioni RAS specificamente attraverso il servizio RASMANCS. Questo aiuta a monitorare e diagnosticare le connessioni di accesso remoto gestite da Internet Explorer.

- **HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Internet Explorer\Security\AntiPhishing**

Questa chiave riguarda le impostazioni di sicurezza di Internet Explorer relative alla protezione anti-phishing. L'anti-phishing è una funzionalità che aiuta a proteggere gli utenti dai siti web dannosi che tentano di rubare informazioni personali.

- **HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Internet Explorer\Security\AntiPhishing\2CEDBFBC-DBA8-43AA-B1FD-CC8E6316E3E2**

Questa chiave specifica potrebbe rappresentare una particolare configurazione o stato del sistema anti-phishing, identificato da un GUID (Globally Unique Identifier). Potrebbe essere utilizzata per tracciare particolari impostazioni o istanze del sistema di protezione anti-phishing.

- **HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012024080220240803**

Questa chiave riguarda la cache di Internet Explorer. La cache è utilizzata per memorizzare temporaneamente i contenuti web per migliorare le prestazioni di navigazione. MSHist012024080220240803 potrebbe essere un identificatore per una particolare istanza di cache storica, probabilmente indicando una data e ora specifica.

- **HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\PrivacIE**

Questa chiave è legata alle impostazioni di privacy di Internet Explorer. PrivacIE potrebbe rappresentare un sottoinsieme di configurazioni relative alla gestione della privacy e dei dati memorizzati nella cache.

Conclusione Regshot

Le chiavi di registro visualizzate sono tutte legate a Internet Explorer e alla gestione delle sue impostazioni di tracciamento, sicurezza (anti-phishing) e cache. Sono utilizzate per configurare, monitorare e gestire diverse funzionalità di Internet Explorer, garantendo una navigazione sicura e ottimizzata per l'utente.
Sembra che non ci siano

CFF Explorer

Procediamo all'analisi statica del file IEXPLORER.exe cercando di capire se il file sia sicuro o no. Le librerie elencate nella tabella sono Dynamic Link Libraries (DLL) di Windows:

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
ADVAPI32.dll	13	0000F6B8	FFFFFFFF	FFFFFFFF	0000F6A8	00009000
KERNEL32.dll	56	0000F728	FFFFFFFF	FFFFFFFF	0000F698	00009070
USER32.dll	9	0000F8F0	FFFFFFFF	FFFFFFFF	0000F68C	00009238
msvcrt.dll	29	0000F940	FFFFFFFF	FFFFFFFF	0000F680	00009288
ntdll.dll	3	0000FA30	FFFFFFFF	FFFFFFFF	0000F674	00009378
SHLWAPI.dll	23	0000FA50	FFFFFFFF	FFFFFFFF	0000F668	00009398
SHELL32.dll	7	0000FB10	FFFFFFFF	FFFFFFFF	0000F65C	00009458
ole32.dll	5	0000FB50	FFFFFFFF	FFFFFFFF	0000F650	00009498
iertutil.dll	14	0000FB80	FFFFFFFF	FFFFFFFF	0000F640	000094C8
urlmon.dll	3	0000FBF8	FFFFFFFF	FFFFFFFF	0000F634	00009540

CFF Explorer Librerie

1. **ADVAPI32.dll**
   - **Descrizione:** contiene funzioni avanzate di API di Windows per la gestione della sicurezza e delle operazioni di registro.
   - **Funzioni Principali:** gestione dei servizi, gestione del registro di sistema, gestione delle autorizzazioni e dei token di sicurezza.
2. **KERNEL32.dll**
   - **Descrizione:** fornisce funzioni di base del sistema operativo Windows.
   - **Funzioni Principali:** gestione della memoria, gestione dei processi e dei thread, operazioni su file, gestione del tempo di sistema.
3. **USER32.dll**
   - **Descrizione:** contiene funzioni per la gestione delle interfacce utente e delle finestre.
   - **Funzioni Principali:** gestione delle finestre, input dell'utente (mouse e tastiera), messaggi di sistema, dialoghi.
4. **msvcrt.dll**
   - **Descrizione:** libreria di runtime del Microsoft Visual C++.
   - **Funzioni Principali:** funzioni standard del C come gestione della memoria, input/output di file, funzioni matematiche.
5. **ntdll.dll**
   - **Descrizione:** fornisce funzioni di basso livello del kernel di Windows.
   - **Funzioni Principali:** gestione delle eccezioni, gestione della memoria, chiamate di sistema a basso livello.
6. **SHLWAPI.dll**
   - **Descrizione:** contiene funzioni di utilità per le operazioni del file system e altre operazioni comuni.
   - **Funzioni Principali:** manipolazione di stringhe, operazioni su file e directory, gestione del registro di sistema.
7. **SHELL32.dll**
   - **Descrizione:** fornisce funzioni per l'interfaccia utente di Windows, specialmente per la shell di Windows.
   - **Funzioni Principali:** gestione del desktop, gestione delle icone, operazioni con file e cartelle (come copia, sposta, elimina).
8. **ole32.dll**
   - **Descrizione:** supporta la tecnologia Object Linking and Embedding (OLE) di Windows.
   - **Funzioni Principali:** gestione degli oggetti COM, gestione delle interfacce OLE per l'embedded di contenuti tra applicazioni.
9. **iertutil.dll**
   - **Descrizione:** contiene funzioni utilizzate da Internet Explorer.
   - **Funzioni Principali:** supporto per operazioni di rete, gestione delle connessioni HTTP, parsing di URL.
10. **urlmon.dll**
    - **Descrizione:** fornisce funzionalità per il download e la gestione di contenuti via URL.
    - **Funzioni Principali:** download di file da URL, gestione dei protocolli di rete, gestione dei cache.

Conclusioni

Chiavi Registro

1. Le chiavi di registro associate indicano che iexplorer.exe interagisce con diverse funzionalità di sicurezza e tracciamento di Internet Explorer. Questo include il tracciamento delle sessioni di rete tramite RASAPI32 e RASMANCS, nonché l'uso di impostazioni di sicurezza anti-phishing.
2. L'uso di chiavi relative alla cache di Internet Explorer (Extensible Cache) suggerisce che l'applicazione gestisce dati temporanei per migliorare la performance di navigazione.

Librerie .dll

1. Le librerie DLL importate da iexplorer.exe comprendono funzioni di base del sistema operativo (KERNEL32.dll, ntdll.dll), gestione dell'interfaccia utente (USER32.dll), e funzioni avanzate di sicurezza e registro (ADVAPI32.dll).
2. L'importazione di librerie specifiche di Internet Explorer (iertutil.dll, urlmon.dll) e della shell di Windows (SHLWAPI.dll, SHELL32.dll) indica che iexplorer.exe utilizza componenti cruciali per operazioni di rete e gestione del file system.
3. L'importazione di msvcrt.dll suggerisce l'uso di funzioni standard del C, comuni in molte applicazioni Windows.

Il file iexplorer.exe sembra essere una versione di Internet Explorer o un'applicazione strettamente legata a esso. La presenza di chiavi di registro e librerie DLL associate alle funzionalità di Internet Explorer supporta questa conclusione.

GRAZIE

Maurizio Marcantoni

www.datashields.tech

DATA SHIELDS