

## PROCEDIMENTO ANALISI STATICA Rogue Malware

1. Comincio con l'analisi del rogue malware Adwcleaner mediante Cff explorer da cui estraggo alcune informazioni cruciali.

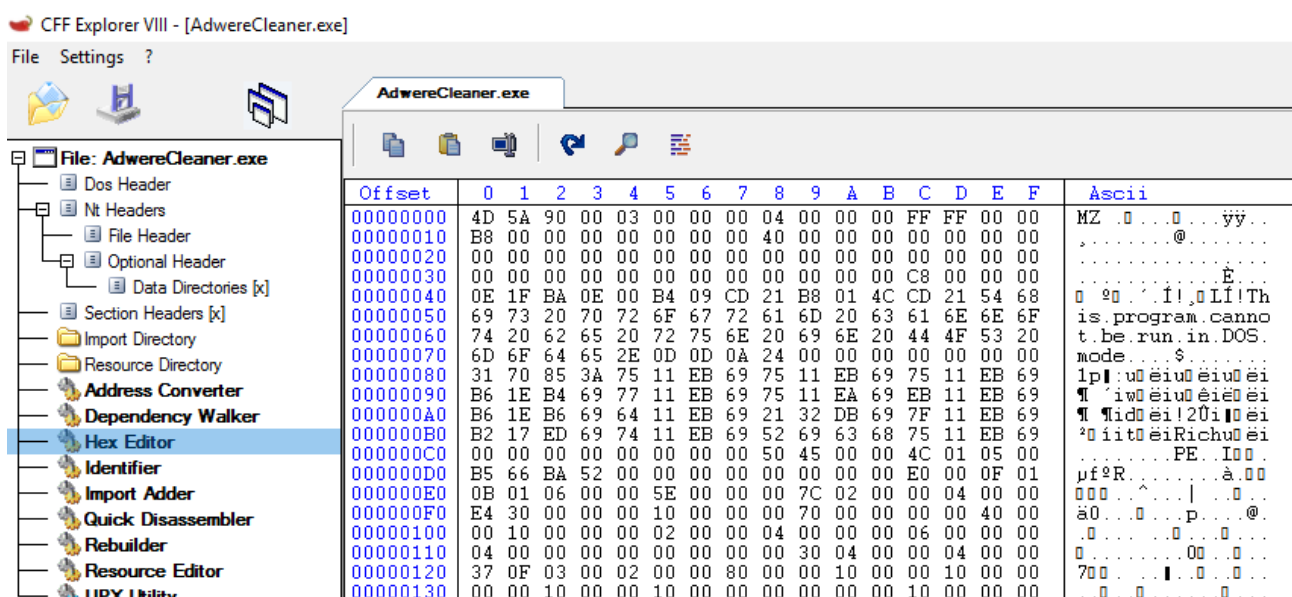
Property	Value
File Name	C:\Users\flare\Desktop\AdwareCleaner.exe
File Type	Portable Executable 32
File Info	Nullsoft PiMP Stub -> SFX
File Size	190.82 KB (195400 bytes)
PE Size	75.50 KB (77312 bytes)
Created	Monday 28 October 2024, 10.22.37
Modified	Monday 14 October 2024, 06.55.49
Accessed	Monday 28 October 2024, 10.22.37
MD5	248AADD395FFA7FFB1670392A9398454
SHA-1	C53C140BBDEB556FCA33BC7F9B2E44E9061EA3E5
Property	Value
Empty	No additional info available

Ricaviamo quindi gli hash Md5 e SHA1 del file e la sua dimensione.

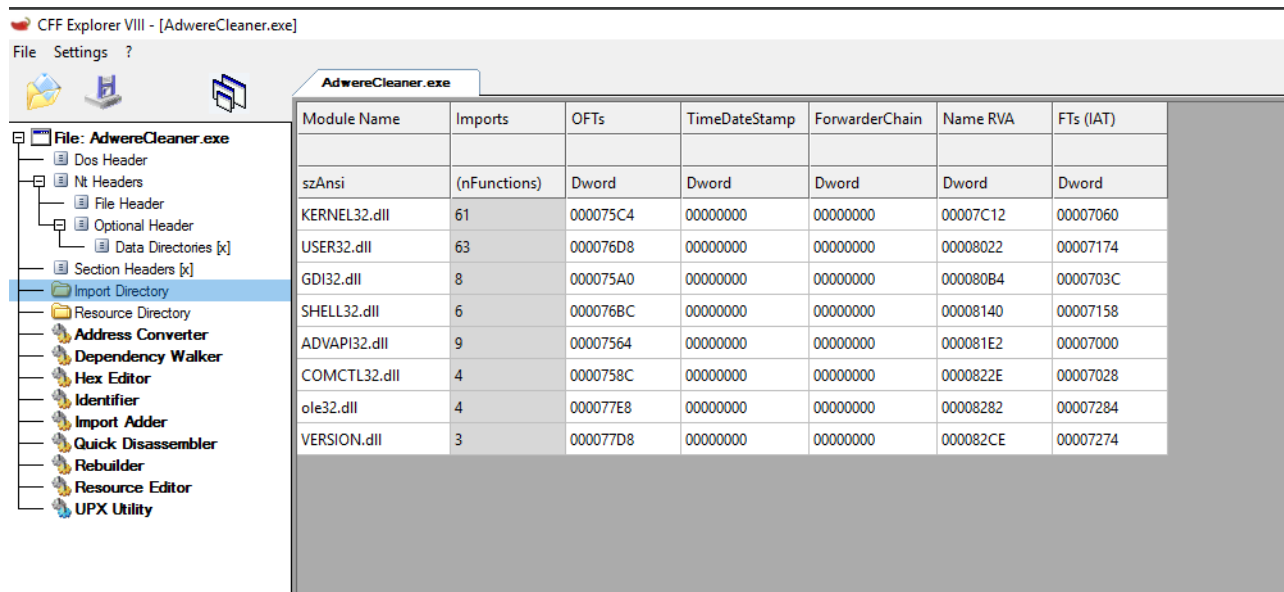
2. Mediante l'Hex editor visualizzo il contenuto del file in formato esadecimale e noto la stringa esadecimale '4D 5A'.

Su un sistema Windows, la presenza della stringa ASCII 'MZ' (in esadecimale: '4D 5A') all'inizio di un file (conosciuta come "numero magico") indica che si tratta di un file eseguibile.

3. Controllo le librerie importate dall'eseguibile.



### 3. Controllo le librerie importate dall'eseguibile.



Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	61	000075C4	00000000	00000000	00007C12	00007060
USER32.dll	63	000076D8	00000000	00000000	00008022	00007174
GDI32.dll	8	000075A0	00000000	00000000	000080B4	0000703C
SHELL32.dll	6	000076BC	00000000	00000000	00008140	00007158
ADVAPI32.dll	9	00007564	00000000	00000000	000081E2	00007000
COMCTL32.dll	4	0000758C	00000000	00000000	0000822E	00007028
ole32.dll	4	000077E8	00000000	00000000	00008282	00007284
VERSION.dll	3	000077D8	00000000	00000000	000082CE	00007274

Queste librerie forniscono funzionalità essenziali per interagire con il sistema operativo, il file system, il registro di sistema e l'interfaccia utente. Importando queste librerie, un malware può:

- **Eseguire operazioni malevole** come la lettura e la scrittura di file, la creazione di processi, e la manipolazione della memoria.
- **Manipolare il sistema operativo** per ottenere permessi, nascondersi o persistere nei riavvii.
- **Interagire con l'utente o ingannarlo**, tramite interfacce false o la cattura di input.

### 4. Controllo le stringhe del file per comprendere le funzionalità del programma.

La sequenza delle API suggerisce varie capacità e intenti del malware, tra cui:

#### 1. File e Directory Management:

- **CreateFileA, DeleteFileA, CopyFileA** e altre funzioni simili per manipolare i file (cancellare, spostare, creare directory, ecc.).
- **SHFileOperationA** e altre funzioni di Shell, suggeriscono un possibile tentativo di copiare, rinominare o cancellare file in modo più avanzato.

#### 2. Accesso e Manipolazione del Registro di Sistema:

- **RegCreateKeyExA, RegOpenKeyExA, RegSetValueExA** per creare e modificare chiavi e valori del registro di sistema.
- **RegDeleteKeyA e RegDeleteValueA** per rimuovere chiavi e valori, indicando un possibile tentativo di alterare o nascondere le tracce nel sistema o modificare configurazioni critiche.

### 3. Manipolazione del Contesto di Esecuzione:

- **LoadLibraryA** e **GetProcAddress** per caricare librerie e risolvere le funzioni, consentendo di utilizzare funzioni di API dinamicamente.
- **GetModuleHandleA** e **FreeLibrary** per gestire le librerie, suggerendo la capacità di modulare e adattare il codice a seconda dell'ambiente.

### 4. Gestione delle Privilegi e Accesso al Processore:

- **AdjustTokenPrivileges** e **LookupPrivilegeValueA** per ottenere privilegi elevati, necessari per eseguire determinate operazioni sensibili.
- **OpenProcessToken** per ottenere token di sicurezza di altri processi, potenzialmente per impersonare o eseguire codice con i privilegi di altri utenti.

### 5. Interazione con l'Interfaccia Utente:

- **FindWindowExA**, **SendMessageA** e **SetForegroundWindow** per individuare e interagire con le finestre dell'interfaccia utente, il che può suggerire capacità di manipolare o monitorare finestre aperte.
- 

### 6. Routine di Installazione e Persistenza:

- Alcuni messaggi di errore e riferimenti, come "Installer integrity check has failed" e "NSIS Error," indicano che il malware può presentarsi come un installer.
- **CreateProcessA** e **CreateThread** permettono di eseguire e creare nuovi processi e thread, suggerendo tecniche di evasione o un approccio modulare.

Questo malware sembra essere progettato per manipolare il file system, interagire con il registro di sistema per garantire persistenza, e potrebbe eseguire modifiche all'ambiente utente per evitare rilevamenti o interagire con il sistema in modo più profondo, accedendo anche a privilegi avanzati per eseguire azioni non autorizzate.

5. Continuo l'analisi delle stringhe.

Ecco alcuni dettagli e osservazioni rilevanti:

#### 1. Certificati e Autorità di Certificazione (CA):

- Sono presenti riferimenti a diverse autorità di certificazione (CA), tra cui:
  - **USERTRUST Network**: con dettagli come UTN-USERFirst-Object e vari URL per controlli CRL (Certificate Revocation List), come <http://crl.usertrust.com/UTN-USERFirst-Object.crl>.
  - **COMODO CA Limited**: il cui certificato è associato alla firma del codice, con URL per i servizi di CRL e OCSP (Online Certificate Status Protocol), come <http://crl.comodoca.com/COMODOCodeSigningCA2.crl>.

- **DigiCert Inc:** con riferimenti a certificati e servizi di verifica, come <http://ocsp.digicert.com> e il nome DigiCert Assured ID CA-1.

## 2. Date di validità:

- Alcuni certificati elencano date di inizio e fine validità, che tipicamente indicano i periodi in cui i certificati sono validi. Ad esempio:
  - 110824000000Z a 200530104838Z (per il certificato UTN-USERFirst).
  - 141022000000Z a 241022000000Z (per il certificato DigiCert Assured ID).

## 3. Controlli e verifica certificati:

- Il malware sembra contenere URL verso le liste di revoca (CRL) e i servizi OCSP per le CA coinvolte, come <http://crl3.digicert.com/DigiCertAssuredIDCA-1.crl> o <http://ocsp.usertrust.com>. Questi collegamenti sono utilizzati per verificare se un certificato è stato revocato, segno che il malware potrebbe utilizzare questi certificati per verificare la firma digitale di alcune componenti o addirittura installare certificati falsi.

## 4. Possibile Evasione o Autenticazione Mascherata:

- L'uso di certificati validi potrebbe servire a mascherare attività dannose o convincere l'utente (o un software di sicurezza) dell'autenticità del codice eseguibile. Inoltre, la presenza di certificati di **Code Signing (firma del codice)** suggerisce che il malware potrebbe tentare di apparire legittimo sfruttando certificati emessi da CA rinomate.

## 5. Indirizzi e-mail e nomi delle aziende:

- Appare un indirizzo email ([robert@jlflor.com](mailto:robert@jlflor.com)) che potrebbe essere collegato al creatore o ad uno dei componenti del malware. È anche menzionata un'entità chiamata **WAT Software Rotterdam**, che potrebbe rappresentare un'azienda fasulla o un'identità usata dal malware per creare certificati apparentemente legittimi.

Questa struttura di certificati digitali indica che il malware potrebbe essere progettato per apparire legittimo, sfruttando certificati di CA note o falsificando la firma digitale del proprio codice per eludere i controlli di sicurezza.