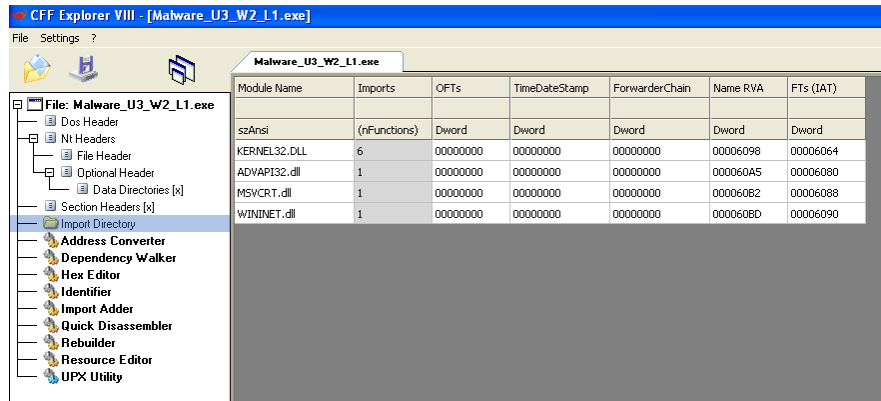


Dopo aver importato il malware in CFF Explorer procediamo con l'analisi, in questo caso ci concentreremo sulle directory esterne da cui dipende il programma per funzionare.

Come possiamo vedere nel programma sono richiamate 4 librerie esterne, rispettivamente ognuna attinge ad una sola funzione in essa tranne la prima che ne accede a 6. Ma dopo aver eseguito l'unpack se ne rivelano molte di più.

| Module Name | Imports | OFTs | TimeDateStamp | ForwarderChain | Name RVA | FTs (IAT) |
|--------------|--------------|----------|---------------|----------------|----------|-----------|
| szAnsi | (nFunctions) | Dword | Dword | Dword | Dword | Dword |
| KERNEL32.DLL | 9 | 00000000 | 00000000 | 00000000 | 0000216C | 00002010 |
| ADVAPI32.dll | 3 | 00000000 | 00000000 | 00000000 | 00002179 | 00002000 |
| MSVCRT.dll | 13 | 00000000 | 00000000 | 00002186 | 00002038 | |
| WININET.dll | 2 | 00000000 | 00000000 | 00002191 | 00002070 | |



| Module Name | Imports | OFTs | TimeDateStamp | ForwarderChain | Name RVA | FTs (IAT) |
|--------------|--------------|----------|---------------|----------------|----------|-----------|
| 0000216C | N/A | 0000208C | 00002090 | 00002094 | 00002098 | 0000209C |
| szAnsi | (nFunctions) | Dword | Dword | Dword | Dword | Dword |
| KERNEL32.DLL | 9 | 00000000 | 00000000 | 00000000 | 0000216C | 00002010 |
| ADVAPI32.dll | 3 | 00000000 | 00000000 | 00000000 | 00002179 | 00002000 |
| MSVCRT.dll | 13 | 00000000 | 00000000 | 00000000 | 00002186 | 00002038 |
| WININET.dll | 2 | 00000000 | 00000000 | 00000000 | 00002191 | 00002070 |

La prima libreria è molto comune e contiene funzioni per interagire con il sistema, in questo caso sono chiamate varie funzioni per creare ed uscire da processi, ottenere nomi di file e cartelle e l'impostazione di un timer. Il modulo si avvia con il sistema, e windows non permetta la corruzione o modifica di questa zona di memoria, oltre alle funzioni implementate dal virus permette anche varie opzioni di input-output, accesso a locazioni di memoria e la comunicazione interna tra processi.

| OFTs | FTs (IAT) | Hint | Name |
|-------|-----------|------|----------------------|
| Dword | Dword | Word | szAnsi |
| N/A | 0000219E | 0000 | SystemTimeToFileTime |
| N/A | 000021B4 | 0000 | GetModuleFileNameA |
| N/A | 000021C8 | 0000 | CreateWaitableTimerA |
| N/A | 000021DE | 0000 | ExitProcess |
| N/A | 000021EC | 0000 | OpenMutexA |
| N/A | 000021F8 | 0000 | SetWaitableTimer |
| N/A | 0000220A | 0000 | WaitForSingleObject |
| N/A | 00002220 | 0000 | CreateMutexA |
| N/A | 0000222E | 0000 | CreateThread |

| Module Name | Imports | OFTs | TimeDateStamp | ForwarderChain | Name RVA | FTs (IAT) |
|--------------|--------------|----------|---------------|----------------|----------|-----------|
| 00002179 | N/A | 000020A0 | 000020A4 | 000020A8 | 000020AC | 000020B0 |
| szAnsi | (nFunctions) | Dword | Dword | Dword | Dword | Dword |
| KERNEL32.DLL | 9 | 00000000 | 00000000 | 00000000 | 0000216C | 00002010 |
| ADVAPI32.dll | 3 | 00000000 | 00000000 | 00000000 | 00002179 | 00002000 |
| MSVCRT.dll | 13 | 00000000 | 00000000 | 00000000 | 00002186 | 00002038 |
| WININET.dll | 2 | 00000000 | 00000000 | 00000000 | 00002191 | 00002070 |

| OFTs | FTs (IAT) | Hint | Name |
|-------|-----------|------|-----------------------------|
| Dword | Dword | Word | szAnsi |
| N/A | 0000223C | 0000 | CreateServiceA |
| N/A | 0000224C | 0000 | StartServiceCtrlDispatcherA |
| N/A | 0000226A | 0000 | OpenSCManagerA |

La seconda libreria fa parte del sistema operativo di windows, è un'API avanzata per interagire con il sistema permettendo di accedere ai registri del sistema, avvio di servizi e il controllo dello stato della macchina permettendoti di spegnerla, accenderla e riavviarla.

| Module Name | Imports | OFTs | TimeDateStamp | ForwarderChain | Name RVA | FTs (IAT) |
|--------------|--------------|----------|---------------|----------------|----------|-----------|
| 00002186 | N/A | 000020B4 | 000020B8 | 000020BC | 000020C0 | 000020C4 |
| szAnsi | (nFunctions) | Dword | Dword | Dword | Dword | Dword |
| KERNEL32.DLL | 9 | 00000000 | 00000000 | 00000000 | 0000216C | 00002010 |
| ADVAPI32.dll | 3 | 00000000 | 00000000 | 00000000 | 00002179 | 00002000 |
| MSVCRT.dll | 13 | 00000000 | 00000000 | 00000000 | 00002186 | 00002038 |
| WININET.dll | 2 | 00000000 | 00000000 | 00000000 | 00002191 | 00002070 |

Il terzo modulo contiene varie funzioni in C, questa fa parte di una libreria a runtime e come possiamo vedere è quella che è stata più utilizzata dal programmatore del malware, e contiene varie funzione per la manipolazione di zone di memoria e la gestione di input-output.

| OFTs | FTs (IAT) | Hint | Name |
|-------|-----------|------|------------------|
| Dword | Dword | Word | szAnsi |
| N/A | 0000227A | 0000 | _exit |
| N/A | 00002282 | 0000 | _xcpkFilter |
| N/A | 00002290 | 0000 | exit |
| N/A | 00002296 | 0000 | __p__initenv |
| N/A | 000022A6 | 0000 | __getmainargs |
| N/A | 000022B6 | 0000 | _initterm |
| N/A | 000022C2 | 0000 | _setusermatherr |
| N/A | 000022D4 | 0000 | _adjust_fdiv |
| N/A | 000022E2 | 0000 | __p__commode |
| N/A | 000022F0 | 0000 | __p__fmode |
| N/A | 000022FC | 0000 | __set_app_type |
| N/A | 0000230C | 0000 | _except_handler3 |
| N/A | 0000231E | 0000 | _controlfp |

| Module Name | Imports | OFTs | TimeDateStamp | ForwarderChain | Name RVA | FTs (IAT) |
|--------------|--------------|----------|---------------|----------------|----------|-----------|
| 00002191 | N/A | 000020C8 | 000020CC | 000020D0 | 000020D4 | 000020D8 |
| szAnsi | (nFunctions) | Dword | Dword | Dword | Dword | Dword |
| KERNEL32.DLL | 9 | 00000000 | 00000000 | 00000000 | 0000216C | 00002010 |
| ADVAPI32.dll | 3 | 00000000 | 00000000 | 00000000 | 00002179 | 00002000 |
| MSVCRT.dll | 13 | 00000000 | 00000000 | 00000000 | 00002186 | 00002038 |
| WININET.dll | 2 | 00000000 | 00000000 | 00000000 | 00002191 | 00002070 |

| OFTs | FTs (IAT) | Hint | Name |
|-------|-----------|------|------------------|
| Dword | Dword | Word | szAnsi |
| N/A | 0000232A | 0000 | InternetOpenUrlA |
| N/A | 0000233C | 0000 | InternetOpenA |

Per quanto riguarda l'ultima libreria si tratta di un modulo base per varie funzioni connesse ad internet per fare richieste con vari protocolli di rete, potenzialmente per inviare comandi da remoto da parte dell'attaccante o saturare il buffer di richieste web.

Una volta spaccettato si ottiene la visione degli header PE in chiaro.

| Malware_U3_W2_L1.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 | 000002DC | 00001000 | 00001000 | 00001000 | 00000000 | 00000000 | 0000 | 0000 | 60000020 |
| .rdata | 00000372 | 00002000 | 00001000 | 00002000 | 00000000 | 00000000 | 0000 | 0000 | 40000040 |
| .data | 0000008C | 00003000 | 00001000 | 00003000 | 00000000 | 00000000 | 0000 | 0000 | C0000040 |

CONCLUSIONI FINALI

Il programma in questione è un trojan che una volta triggerato esegue un attacco DoS sulla macchina infettata.

| | | |
|------------|---|---|
| Info | Matching compiler(s): | Microsoft Visual C++ Microsoft Visual C++ v6.0 Microsoft Visual C++ v5.0/v6.0 (NFC) |
| Info | Interesting strings found in the binary: | Contains domain names: <ul style="list-style-type: none">http://www.malwareanalysisbook.commalwareanalysisbook.comwww.malwareanalysisbook.com |
| Suspicious | The PE contains functions most legitimate programs don't use. | Has Internet access capabilities: <ul style="list-style-type: none">InternetOpenUrlAInternetOpenK Interacts with services: <ul style="list-style-type: none">CreateServiceAOpenSCManagerA |
| Malicious | VirusTotal score: 50/70 (Scanned on 2023-01-31 00:25:18) | Lionic: Trojan.Win32.Ulisse.41c Elastic: malicious (high confidence) Cynet: Malicious (score: 100) ALYac: Gen:Variant.Ser.Ulisse.216 Malwarebytes: Riskware.Agent.H6A VIRB: Gen:Variant.Ser.Ulisse.216 Sangfor: Suspicious.Win32.Save.Ins K7AntiVirus: Spyware (00486daee1) Alibaba: TrojanClicker.Win32/Tnega.F504d3af K7Win: Spyware (00486daee1) Cybereason: malicious.6978f5 VirusIT: Trojan.Win32.Generic.CHEY Cyren: W32/Agent.D3C.gen/Eldorado Symantec: Trojan.Gen.2 ESET-NOD32: a variant of Win32/TrojanClicker.Agent.NPH APEX: Malicious BitDefender: Gen:Variant.Ser.Ulisse.216 NANO-Antivirus: Trojan.Win32.Click3.lvtltd MicroWorld-eScan: Gen:Variant.Ser.Ulisse.216 Avast: Win32:AdwareX-gen [Adw] Tencent: Win32:Trojan.Agen.00k1 Emsisoft: Gen:Variant.Ser.Ulisse.216 (B) DrWeb: Trojan.Click3.12740 Zillya: Trojan.Agent.Win32.557086 TrendMicro: TRD2_GEN.M04C0P222 McAfee-GW-Editon: GenericRKEE-VS1AE4CA70697DF Trapline: malicious.moderate.ml.score FireEye: Generic.ng.a64ca70697df5506 Jiangmin: Trojan.Generic.Fxjq Webroot: W32.Malware.Heur Avira: HEUR/AGEN.1223661 |