

# PROGETTO S10

FUNDAMENTALS OF MALWARE  
ANALYSIS AND REVERSE  
ENGINEERING

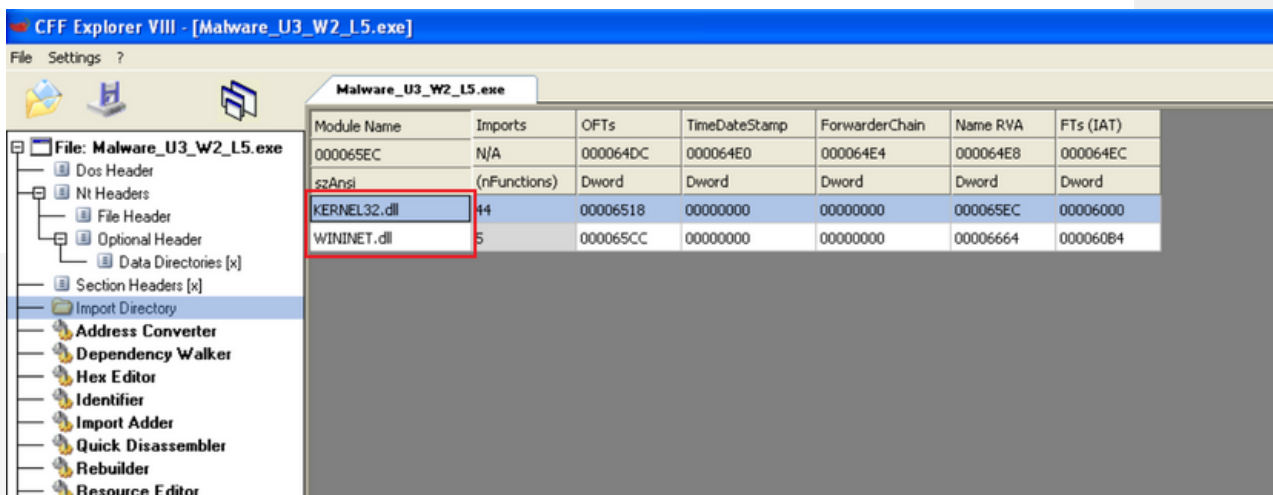
ANALISI STATICA E  
DINAMICA: UN APPROCCIO  
PRATICO

FERNANDO CATRAMBONE

# TRACCIA

CON RIFERIMENTO AL FILE  
MALWARE\_U3\_W2\_L5 PRESENTE  
ALL'INTERNO DELLA CARTELLA  
«**ESERCIZIO\_PRATICO\_U3\_W2\_L5**» SUL  
DESKTOP DELLA MACCHINA VIRTUALE  
DEDICATA PER L'ANALISI DEI MALWARE,  
RISPONDERE AI SEGUENTI QUESITI:

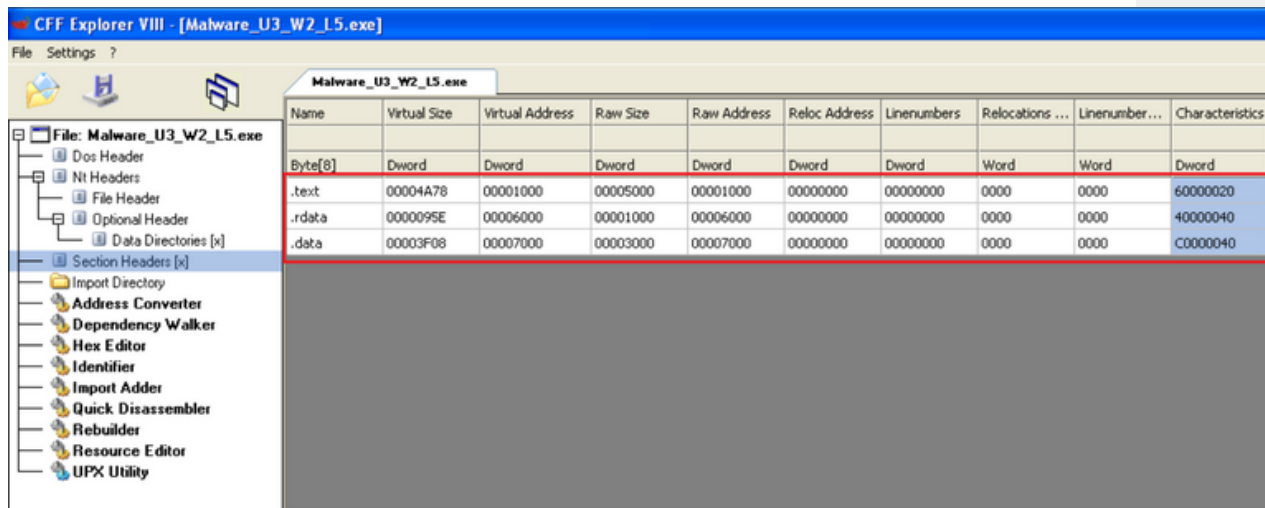
**QUALI LIBRERIE VENGONO IMPORTATE DAL  
FILE ESEGUIBILE?**



LE LIBRERIE IMPORTATE SONO:

- **KERNEL32.DLL**, CHE INCLUDE LE FUNZIONI CORE DEL SISTEMA OPERATIVO.
- **WININET.DLL**, INCLUDE LE FUNZIONE PER IMPLEMENTARE I SERVIZI DI RETE COME FTP, NTP, HTTP

QUALI SONO LE SEZIONI DI CUI SI  
COMPONE IL FILE ESEGUIBILE DEL  
MALWARE?

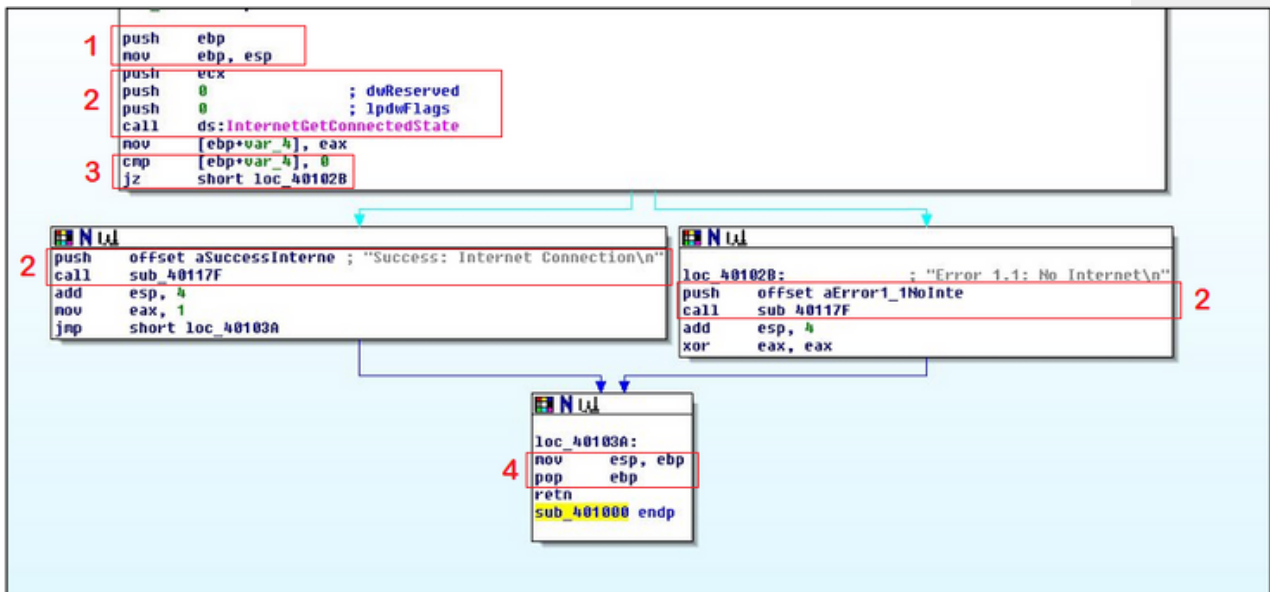


Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber ...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	00004A78	00001000	00005000	00001000	00000000	00000000	0000	0000	60000020
.rdata	0000095E	00006000	00001000	00006000	00000000	00000000	0000	0000	40000040
.data	00003F08	00007000	00003000	00007000	00000000	00000000	0000	0000	C0000040

LE SEZIONI SONO:

- **.TEXT**, CONTIENE LE ISTRUZIONI CHE LA CPU ESEGUIRÀ QUANDO IL FILE ESEGUIBILE VERRÀ AVVIATO.
- **.RDATA**, INCLUDE INFORMAZIONI SULLE LIBRERIE E LE FUNZIONI IMPORTATE ED ESPORTATE DALL'ESEGUIBILE.
- **.DATA**, CONTIENE I DATI E LE VARIBIALI GLOBALI CHE DEVONO ESSERE DISPONIBILI PER OGNI PARTE DEL SOFTWARE.

## IDENTIFICARE I COSTRUTTI NOTI (CREAZIONE DELLO STACK, EVENTUALI CICLI, COSTRUTTI)



NELLA FIGURA SOPRA SONO INDICATI I  
SEGUENTI COSTRUTTI:

- **1**, CREAZIONE DELLO **STACK**, LO **STACK** RAPPRESENTA UNA PARTE DI MEMORIA DESTINATA PER CONSERVARE LE VARIABILI LOCALI DI UNA FUNZIONE SPECIFICA. VIENE DEFINITO ATTRAVERSO I PUNTATORI ALLO **STACK**: **EBP**, CHE INDICA LA **BASE DELLO STACK**, ED **ESP**, CHE INDICA LA **CIMA DELLO STACK**.
- **2**, CHIAMATE A DIVERSE FUNZIONI, PRIMA DI CHIAMARE LA FUNZIONE CON IL COMANDO **CALL** VENGONO CARICATE SULLO **STACK** TUTTE LE VARIABILI NECESSARIE CON IL COMANDO **PUSH**.
- **3**, **CICLO IF ELSE**.
- **4**, **RIMOZIONE DELLO STACK**, LO **STACK** VIENE ELIMINATO UNA VOLTA CHE LA FUNZIONE HA TERMINATO IL SUO COMPITO.

## I POTIZZARE IL COMPORTAMENTO DELLA FUNZIONALITÀ IMPLEMENTATA

DA QUESTA PORZIONE DI CODICE ASSEMBLY POSSIAMO DIRE CHE IL MALWARE CHIAMA LA FUNZIONE **INTERNETGETCONNECTEDSTATE**, QUESTA FUNZIONE RESTITUISCE UN VALORE DI RITORNO CHE PUÒ ESSERE “0” O DIVERSO DA “0”. TRAMITE IL **CICLO IF** RESTITUISCE UN MESSAGGIO CHE INDICA SE È PRESENTE O NO UNA CONNESSIONE AD INTERNET. SE LA CONNESSIONE È PRESENTE COMPARIRÀ IL MESSAGGIO: **“SUCCESS, INTERNET CONNECTION”**. ALTRIMENTI IL MESSAGGIO SARÀ: **“ERROR 1.1: NO INTERNET”**

### PSEUDOCODICE :

```
4  int main()
5  {
6
7      state = internetGetConnectedState (par1,0,0);
8
9      if( state != 0)
10     {
11         printf ("success, internet connection\n");
12     }
13     else
14     {
15         printf ("error 1.1: no internet\n");
16     }
17
18     return 0;
19 }
```

## FARE LA TABELLA CON LE SINGOLE RIGHE DI CODICE ASSEMBLY

1. **PUSH EBP**: SALVA IL VALORE CORRENTE DEL REGISTRO BASE (EBP) NELLO STACK.
2. **MOV EBP, ESP**: IMPOSTA IL PUNTATORE ALLA BASE DELLO STACK (EBP) AL VALORE DEL PUNTATORE ALLA CIMA DELLO STACK (ESP) PER DESTINARE UNA PARTE DI MEMORIA ALLA FUNZIONE.
3. **PUSH ECX**: SALVA IL VALORE CORRENTE DEL REGISTRO ECX NELLO STACK.
4. **PUSH 0**: PONE 0 NELLO STACK COME ARGOMENTO PER LA FUNZIONE SUCCESSIVA.
5. **PUSH 0**: PONE UN ALTRO 0 NELLO STACK COME SECONDO ARGOMENTO PER LA FUNZIONE.
6. **CALL DS:INTERNETGETCONNECTEDSTATE**: CHIAMA LA FUNZIONE INTERNETGETCONNECTEDSTATE.
7. **MOV [EBP+VAR\_4], EAX**: COPIA IL RISULTATO DELLA CHIAMATA A INTERNETGETCONNECTEDSTATE NELLA VARIABILE LOCALE [EBP+VAR\_4].
8. **CMP [EBP+VAR\_4], 0**: COMPARA IL VALORE MEMORIZZATO CON 0.
9. **JZ SHORT LOC\_40102B**: SALTA A LOC\_40102B SE IL VALORE È ZERO

**IL CODICE HA DUE PERCORSI:**

**SE LA CONNESSIONE INTERNET È PRESENTE:**

1. **PUSH OFFSET ASUCCESSINTERNE:** METTE NELLO STACK LA STRINGA PER LA FUNZIONE SUCCESSIVA.
2. **CALL SUB\_40117F:** CHIAMA UNA FUNZIONE DENOMINATA SUB\_40117F CON L'INDIRIZZO DELLA STRINGA COME ARGOMENTO, PRESUMIBILMENTE SI TRATTA DI UNA PRINTF.
3. **ADD ESP, 4:** PULISCE LO STACK DOPO LA CHIAMATA DELLA FUNZIONE.
4. **MOV EAX, 1:** IMPOSTA EAX A 1.
5. **JMP SHORT LOC\_40103A:** SALTA A LOC\_40103A.

**SE LA CONNESSIONE INTERNET NON È PRESENTE:**

1. **LOC\_40102B:** ETICHETTA DI DESTINAZIONE.
2. **PUSH OFFSET AERROR1\_1NOINTE:** METTE NELLO STACK LA STRINGA PER LA FUNZIONE SUCCESSIVA.
3. **CALL SUB\_40117F:** CHIAMA UNA FUNZIONE DENOMINATA SUB\_40117F CON L'INDIRIZZO DELLA STRINGA COME ARGOMENTO, PRESUMIBILMENTE SI TRATTA DI UNA PRINTF.
4. **ADD ESP, 4:** PULISCE LO STACK DOPO LA CHIAMATA DELLA FUNZIONE.
5. **XOR EAX, EAX:** ESEGUE UN XOR DI EAX CON SE STESSO, IMPOSTANDO EAX A ZERO.

## L'ULTIMA PARTE GESTISCE LA CONCLUSIONE DELLA FUNZIONE:

1. **LOC\_40103A**: ETICHETTA DI DESTINAZIONE.
2. **MOV ESP, EBP**: RIPRISTINA ESP AL VALORE DI EBP, LIBERANDO LO SPAZIO PRECEDENTEMENTE ALLOCATO PER QUESTA FUNZIONE.
3. **POP EBP**: RIPRISTINA EBP AL SUO VALORE PRECEDENTE.
4. **RETN**: TERMINA LA FUNZIONE E TORNA AL CHIAMANTE.
5. **SUB\_401000 ENDP**: FINE DELLA FUNZIONE.



# EXTRA

## ANALISI DINAMICA.

DOPO L'ANALISI STATICA EFFETTUATA EFFETTUIAMO UNA ANALISI DINAMICA DEL MALWARE PER CAPIRNE IN MANIERA PIÙ APPROFONDATA IL FUNZIONAMENTO.

```
AVVIAMO PROCMON, REGSHOT, APATEDNS E
WIRESHARK PRIMA DI ESEGUIRE IL
MALWARE.
DOPO CIRCA UN MINUTO ANALIZZIAMO I
REPORT.
```

[illegible]

## IL FILTRO SUI PROCESSI E THREAD.

# EXTRA

IL FILTRO SULLE ATTIVITÀ SUL FILE  
SYSTEM EVIDENZIA COME IL MALWARE  
EFFETTUI UN CERTO NUMERO DI ATTIVITÀ  
DI CREAZIONE E COPIA DI FILE IN  
DIVERSE DIRECTORY DEL COMPUTER.

10.10.53.80508	Malware_U3_W2_L5.exe	3312	QueryNameInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L5\Malware_U3_W2_	SUCCESS	Name: 'Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_
10.10.53.80154	Malware_U3_W2_L5.exe	3312	QueryNameInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L5\Malware_U3_W2_	SUCCESS	Name: 'Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_
10.10.53.801645 PM	Malware_U3_W2_L5.exe	3312	CreateFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L5.EXE-3C8D103.pf	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous I/O NonVolatile
10.10.53.80183	Malware_U3_W2_L5.exe	3312	QueryStandardInformationFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L5.EXE-3C8D103.pf	SUCCESS	AllocationSize: 16384, EndOfFile: 16392, NumberLinks: 1, DeletePending: False, Offset: 0, Length: 16392
10.10.53.80174	Malware_U3_W2_L5.exe	3312	ReadFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L5.EXE-3C8D103.pf	SUCCESS	
10.10.53.80271	Malware_U3_W2_L5.exe	3312	CloseFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L5.EXE-3C8D103.pf	SUCCESS	
10.10.53.80273	Malware_U3_W2_L5.exe	3312	CreateFile	C:\	SUCCESS	
10.10.53.80275	Malware_U3_W2_L5.exe	3312	QueryInformationVolume	C:\	SUCCESS	Desired Access: Read Attributes, Write Attributes, Synchronize, Disposition: Open, 0
10.10.53.80278	Malware_U3_W2_L5.exe	3312	FileSystemControl	C:\	SUCCESS	Volume Control File: 3/20/2017 9 34 16 PM, VolumeSerialNumber: 0DBA-8021, Sd
10.10.53.80319	Malware_U3_W2_L5.exe	3312	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L5\	SUCCESS	Control FSCTL_FILE_PREFETCH
10.10.53.80320	Malware_U3_W2_L5.exe	3312	QueryDirectory	C:\	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: 0
10.10.53.80325	Malware_U3_W2_L5.exe	3312	QueryDirectory	C:\	NO MORE FILES	0, 6565d5ca391440239550a6e7eb, 1, AUTOEXEC.BAT, FileInformationClass: File
10.10.53.80356	Malware_U3_W2_L5.exe	3312	CloseFile	C:\	SUCCESS	
10.10.53.80360	Malware_U3_W2_L5.exe	3312	CreateFile	C:\DOCUMENTS AND SETTINGS	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: 0
10.10.53.80362	Malware_U3_W2_L5.exe	3312	QueryDirectory	C:\Documents and Settings	SUCCESS	0, ..., FileInformationClass: FileNamesInformation, 3, All Users, 4, Default User, 5,
10.10.53.80390	Malware_U3_W2_L5.exe	3312	QueryDirectory	C:\Documents and Settings	NO MORE FILES	
10.10.53.80394	Malware_U3_W2_L5.exe	3312	CloseFile	C:\Documents and Settings	SUCCESS	
10.10.53.80420	Malware_U3_W2_L5.exe	3312	CreateFile	C:\Documents and Settings\ADMINISTRATOR	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: 0
10.10.53.80421	Malware_U3_W2_L5.exe	3312	QueryDirectory	C:\Documents and Settings\Administrator	SUCCESS	0, ..., FileInformationClass: FileNamesInformation, 3, Cookies, 4, Desktop, 5, Fav
10.10.53.80425	Malware_U3_W2_L5.exe	3312	QueryDirectory	C:\Documents and Settings\Administrator	NO MORE FILES	
10.10.53.80450	Malware_U3_W2_L5.exe	3312	CloseFile	C:\Documents and Settings\Administrator	SUCCESS	
10.10.53.80456	Malware_U3_W2_L5.exe	3312	CreateFile	C:\Documents and Settings\Administrator\Cookies	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: 0
10.10.53.80460	Malware_U3_W2_L5.exe	3312	QueryDirectory	C:\Documents and Settings\Administrator\Cookies	SUCCESS	0, ..., FileInformationClass: FileNamesInformation
10.10.53.80506	Malware_U3_W2_L5.exe	3312	QueryDirectory	C:\Documents and Settings\Administrator\Cookies	NO MORE FILES	
10.10.53.80510	Malware_U3_W2_L5.exe	3312	CloseFile	C:\Documents and Settings\Administrator\Cookies	SUCCESS	
10.10.53.80557	Malware_U3_W2_L5.exe	3312	CreateFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: 0
10.10.53.80561	Malware_U3_W2_L5.exe	3312	QueryDirectory	C:\Documents and Settings\Administrator\Desktop	SUCCESS	0, ..., FileInformationClass: FileNamesInformation, 3, cultura.registri.bst, 4, CFF
10.10.53.80567	Malware_U3_W2_L5.exe	3312	QueryDirectory	C:\Documents and Settings\Administrator\Desktop	NO MORE FILES	
10.10.53.80572	Malware_U3_W2_L5.exe	3312	CloseFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS	
10.10.53.80579	Malware_U3_W2_L5.exe	3312	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L5	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: 0
10.10.53.80595	Malware_U3_W2_L5.exe	3312	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L5	SUCCESS	0, ..., FileInformationClass: FileNamesInformation
10.10.53.80598	Malware_U3_W2_L5.exe	3312	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L5	NO MORE FILES	
10.10.53.80600	Malware_U3_W2_L5.exe	3312	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L5	SUCCESS	
10.10.53.80607	Malware_U3_W2_L5.exe	3312	CreateFile	C:\Documents and Settings\Administrator\LOCAL SETTINGS	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: 0
10.10.53.80609	Malware_U3_W2_L5.exe	3312	QueryDirectory	C:\Documents and Settings\Administrator\Local Settings	SUCCESS	0, ..., FileInformationClass: FileNamesInformation, 3, Apps, 4, desktop.ini, 5, Histo
10.10.53.80613	Malware_U3_W2_L5.exe	3312	QueryDirectory	C:\Documents and Settings\Administrator\Local Settings	NO MORE FILES	
10.10.53.80616	Malware_U3_W2_L5.exe	3312	CloseFile	C:\Documents and Settings\Administrator\Local Settings	SUCCESS	
10.10.53.80622	Malware_U3_W2_L5.exe	3312	QueryDirectory	C:\Documents and Settings\Administrator\Local Settings\History	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: 0
10.10.53.80626	Malware_U3_W2_L5.exe	3312	QueryDirectory	C:\Documents and Settings\Administrator\Local Settings\History	SUCCESS	0, ..., FileInformationClass: FileNamesInformation, 3, History, IE5
10.10.53.80632	Malware_U3_W2_L5.exe	3312	QueryDirectory	C:\Documents and Settings\Administrator\Local Settings\History	NO MORE FILES	

IL FILTRO SU LE ATTIVITÀ SUL  
REGISTRO MOSTRA COME IL MALWARE STIA  
OSSERVANDO MOLTE INFORMAZIONI  
RIGUARDO LA MACCHINA VITTIMA.

1:10.53.9082034	PM\Malware_U3_W2_L5.exe	3312	RegOpenKey	HKLM\Software\Microsoft\Windows NT\Current...	NAME NOT FOUND	Desired Access: Read
1:10.53.90869...	Malware_U3_W2_L5.exe	3312	RegOpenKey	HKLM\System\CurrentControlSet\Control\Termi...	SUCCESS	Desired Access: Read
1:10.53.90870...	Malware_U3_W2_L5.exe	3312	RegQueryValue	HKLM\System\CurrentControlSet\Control\Termi...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
1:10.53.90872...	Malware_U3_W2_L5.exe	3312	RegCloseKey	HKLM\System\CurrentControlSet\Control\Termi...	SUCCESS	
1:10.53.91455...	Malware_U3_W2_L5.exe	3312	RegOpenKey	HKLM\System\CurrentControlSet\Control\Termi...	SUCCESS	Desired Access: Read
1:10.53.91456...	Malware_U3_W2_L5.exe	3312	RegQueryValue	HKLM\System\CurrentControlSet\Control\Termi...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
1:10.53.91458...	Malware_U3_W2_L5.exe	3312	RegCloseKey	HKLM\System\CurrentControlSet\Control\Termi...	SUCCESS	
1:10.53.91466...	Malware_U3_W2_L5.exe	3312	RegOpenKey	HKLM\Software\Microsoft\Windows NT\Current...	NAME NOT FOUND	Desired Access: Read
1:10.53.91468...	Malware_U3_W2_L5.exe	3312	RegOpenKey	HKLM\Software\Microsoft\Windows NT\Current...	NAME NOT FOUND	Desired Access: Read
1:10.53.91469...	Malware_U3_W2_L5.exe	3312	RegOpenKey	HKLM\Software\Microsoft\Windows NT\Current...	NAME NOT FOUND	Desired Access: Read
1:10.53.91471...	Malware_U3_W2_L5.exe	3312	RegOpenKey	HKLM\System\CurrentControlSet\Control\Termi...	SUCCESS	Desired Access: Read
1:10.53.91472...	Malware_U3_W2_L5.exe	3312	RegQueryValue	HKLM\System\CurrentControlSet\Control\Termi...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
1:10.53.91473...	Malware_U3_W2_L5.exe	3312	RegQueryValue	HKLM\System\CurrentControlSet\Control\Termi...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
1:10.53.91474...	Malware_U3_W2_L5.exe	3312	RegCloseKey	HKLM\System\CurrentControlSet\Control\Termi...	SUCCESS	
1:10.53.91474...	Malware_U3_W2_L5.exe	3312	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\Cur...	SUCCESS	Desired Access: Read
1:10.53.91476...	Malware_U3_W2_L5.exe	3312	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\Cur...	NAME NOT FOUND	Length: 144
1:10.53.91477...	Malware_U3_W2_L5.exe	3312	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\Cur...	SUCCESS	
1:10.53.91477...	Malware_U3_W2_L5.exe	3312	RegOpenKey	HKLM	SUCCESS	Desired Access: Maximum Allowed
1:10.53.91478...	Malware_U3_W2_L5.exe	3312	RegOpenKey	HKLM\Software\Microsoft\Windows NT\Current...	NAME NOT FOUND	Desired Access: Read
1:10.53.91480...	Malware_U3_W2_L5.exe	3312	RegOpenKey	HKLM\Software\Microsoft\Windows NT\Current...	NAME NOT FOUND	Desired Access: Read
1:10.53.91505...	Malware_U3_W2_L5.exe	3312	RegOpenKey	HKLM\Software\Microsoft\Windows NT\Current...	NAME NOT FOUND	Desired Access: Read
1:10.53.91506...	Malware_U3_W2_L5.exe	3312	RegOpenKey	HKLM\Software\Microsoft\Windows NT\Current...	NAME NOT FOUND	Desired Access: Read
1:10.53.91509...	Malware_U3_W2_L5.exe	3312	RegOpenKey	HKLM\System\CurrentControlSet\Control\Error...	NAME NOT FOUND	Desired Access: Read
1:10.53.91511...	Malware_U3_W2_L5.exe	3312	RegOpenKey	HKLM\Software\Microsoft\Windows NT\Current...	SUCCESS	Desired Access: Read
1:10.53.91512...	Malware_U3_W2_L5.exe	3312	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\Cur...	NAME NOT FOUND	Length: 20
1:10.53.91513...	Malware_U3_W2_L5.exe	3312	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\Cur...	SUCCESS	
1:10.53.91525...	Malware_U3_W2_L5.exe	3312	RegOpenKey	HKLM\Software\Microsoft\Windows NT\Current...	SUCCESS	Desired Access: Read
1:10.53.91527...	Malware_U3_W2_L5.exe	3312	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\Cur...	NAME NOT FOUND	Length: 172
1:10.53.91527...	Malware_U3_W2_L5.exe	3312	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\Cur...	SUCCESS	
1:10.53.91528...	Malware_U3_W2_L5.exe	3312	RegOpenKey	HKLM\Software\Microsoft\Windows NT\Current...	SUCCESS	Desired Access: Read
1:10.53.91529...	Malware_U3_W2_L5.exe	3312	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\Cur...	NAME NOT FOUND	Length: 172
1:10.53.91530...	Malware_U3_W2_L5.exe	3312	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\Cur...	SUCCESS	
1:10.53.91533...	Malware_U3_W2_L5.exe	3312	RegOpenKey	HKLM\Software\Microsoft\Windows NT\Current...	SUCCESS	Desired Access: Read
1:10.53.91534...	Malware_U3_W2_L5.exe	3312	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\Cur...	SUCCESS	Type: REG_SZ, Length: 2, Data:
1:10.53.91535...	Malware_U3_W2_L5.exe	3312	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\Cur...	SUCCESS	
1:10.53.91539...	Malware_U3_W2_L5.exe	3312	RegOpenKey	HKLM\Software\Microsoft\Windows NT\Current...	NAME NOT FOUND	Desired Access: Read
1:10.53.91541...	Malware_U3_W2_L5.exe	3312	RegOpenKey	HKLM\Software\Microsoft\Windows NT\Current...	NAME NOT FOUND	Desired Access: Read
1:10.53.91543...	Malware_U3_W2_L5.exe	3312	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Services\cy...	NAME NOT FOUND	Desired Access: Read
1:10.53.91551...	Malware_U3_W2_L5.exe	3312	RegOpenKey	HKLM\System\CurrentControlSet\Control\Sessio...	SUCCESS	Desired Access: Query Value
1:10.53.91552...	Malware_U3_W2_L5.exe	3312	RegQueryValue	HKLM\System\CurrentControlSet\Control\Sessio...	NAME NOT FOUND	Length: 16
1:10.53.91637...	Malware_U3_W2_L5.exe	3312	RegCloseKey	HKLM\System\CurrentControlSet\Control\Sessio...	SUCCESS	

# EXTRA

ANALIZZANDO I REPORT DI REGSHOT E LE CATTURE DI WIRESHARK E APATEDNS POSSIAMO CAPIRE CHE: APPORTA DELLE MODIFICHE A CHIAVI DI REGISTRO. TENTA UNA CONNESSIONE AD INTERNET.

The image displays three overlapping windows from a Windows operating system, illustrating network-related activities.

**Notepad++ Window:** Shows a registry dump with values added and modified. The 'values added' section lists several registry paths under 'HKLM\SYSTEM\ControlSet002\Services\Tcpip\Parameters' and 'HKLM\SYSTEM\ControlSet002\Services\Tcpip\Parameters\Interfaces', including 'NameServer' and 'DefaultGateway'. The 'values modified' section shows changes to 'NameServer' and 'DefaultGateway' for the 'Intel(R) PRO/1000 MT Desktop Adapter' interface.

**ApatDNS Window:** Shows a table of DNS requests and responses. The 'Domain Requested' column lists domains like 'yulao318525.3322.org' and 'www.wireshark.org'. The 'DNS Return' column shows 'FOUND' for all requests. Below the table, there are fields for 'DNS Reply IP (Default: Current Gateway/DNS): 192.168.1.50' and '# of NODOMAIN's: 0'. There are also buttons for 'Start Server' and 'Stop Server'.

**Wireshark Window:** Shows a packet capture on interface '0'. The 'Filter' is set to 'Expression...'. The packet list shows several packets, including a '216 Get Backup List Request' (packet 1) and a '216 Get Backup List Request' (packet 2). The packet details show the '216 Get Backup List Request' packet structure, including '216 Get Backup List Request' and '216 Get Backup List Request'.

# EXTRA

ANDANDO A RIPRENDERE L'ANALISI  
STATICA PRECEDENTEMENTE FATTA E  
CONFRONTANDO I RISULTATI  
DELL'ANALISI DINAMICA CON LE  
INFORMAZIONI OTTENUTE TRAMITE UNA  
RICERCA PER L'HASH SU VIRUS TOTAL È  
POSSIBILE COMPRENDERE MEGLIO IL  
COMPORTAMENTO DEL MALWARE.

IL MALWARE EFFETTUA PRIMA UN PROCESS  
INJECTION OVVERO INIETTA CODICE NEI  
PROCESSI AL FINE DI ELUDERE LE  
DIFESE BASATE SUI PROCESSI E  
OTTENERE PRIVILEGI ELEVATI.

MODIFICA REGISTRI, FILE DI SISTEMA E  
CARTELLE PER CAMUFFARSI E NON FAR  
NOTARE LA SUA ATTIVITÀ.

OSSERVA I FILE DEGLI HOST, SE È  
PRESENTE UNA CONNESSIONE AD  
INTERNET, INFORMAZIONI SU I SOFTWARE  
INSTALLATI, SE SI TRATTA DI UNA VM E  
VERIFICA SE SONO PRESENTI EVVENTUALI  
SOFTWARE DI SICUREZZA.

TENTA UNA CONNESSIONE AD INTERNET.

## CONCLUSIONI

PROBABILMENTE SI TRATTA DI UN  
MALWARE CHE TRAMITE CAMUFFAMENTO E  
SCALATA AI PRIVILEGGI PERMETTE DI  
PRENDERE IL CONTROLLO DELLA MACCHINA  
VITTIMA ED ATTENDE COMANDI DA UN  
SERVER REMOTO VIA INTERNET.

The background features three overlapping light gray rectangles. One rectangle is positioned in the top right corner, another is on the left side extending towards the bottom, and a third is at the bottom center, partially overlapping the other two.

**GRAZIE**