Report sull'Analisi del Malware "Malware_U3_W2_L5"

Data 09/02/24

Analisi delle Librerie Importate

Dopo un'analisi preliminare del file eseguibile del malware "Malware_U3_W2_L5", sono state identificate le seguenti librerie importate:

kernel32.dll: Questa libreria contiene numerose funzioni di sistema essenziali per la gestione dei processi, dei file e della memoria. Alcune delle funzioni comuni importate da questa libreria potrebbero includere CreateProcess, CreateFile, ReadFile e WriteFile.

wininet.dll: Questa libreria contiene funzioni per la comunicazione di rete su Internet. Alcune funzioni comuni importate potrebbero includere InternetOpen, InternetConnect, HttpOpenRequest e InternetReadFile.

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Nam
szAnsi	(nFunctions)	Dword	Dword	Dword	Dwo
KERNEL32.dll	44	00006518	00000000	00000000	0000
WININET.dll	5	000065CC	00000000	00000000	0000

Analisi delle Sezioni del File Eseguibile:

Il file eseguibile del malware "Malware_U3_W2_L5" è composto dalle seguenti sezioni:

.text: Questa sezione contiene il codice eseguibile del programma. Qui si trovano le istruzioni che vengono eseguite dalla CPU quando il programma viene avviato.

.data: Questa sezione contiene dati statici utilizzati dal programma durante l'esecuzione. Questi dati potrebbero includere variabili globali, costanti o tabelle di lookup.

.rdata: Questa sezione contiene dati di sola lettura utilizzati dal programma durante l'esecuzione. Questi dati potrebbero includere stringhe costanti, tabelle di lookup o altri dati di sola lettura.

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address
Byte[8]	Dword	Dword	Dword	Dword	Dword
.text	00004A78	00001000	00005000	00001000	00000000
.rdata	0000095E	00006000	00001000	00006000	00000000
.data	00003F08	00007000	00003000	00007000	00000000

Strumenti Utilizzati per l'Analisi

Durante l'analisi del malware "Malware_U3_W2_L5", abbiamo impiegato diversi strumenti per ottenere informazioni dettagliate sul comportamento del malware e sulle azioni che esso intraprende. Di seguito sono elencati gli strumenti utilizzati e le loro funzioni specifiche:

CFF Explorer: Abbiamo utilizzato CFF Explorer per esaminare il file eseguibile del malware al fine di identificare le librerie importate e le sezioni del file eseguibile. Questo ci ha permesso di comprendere meglio le dipendenze del malware e la sua struttura interna.

Regshot: Abbiamo eseguito uno screenshot del registro di sistema prima e dopo l'esecuzione del malware utilizzando Regshot. Questo ci ha consentito di rilevare eventuali modifiche apportate dal malware al registro di sistema, identificando eventuali attività dannose come l'aggiunta di chiavi di registro o la modifica delle impostazioni di sistema.

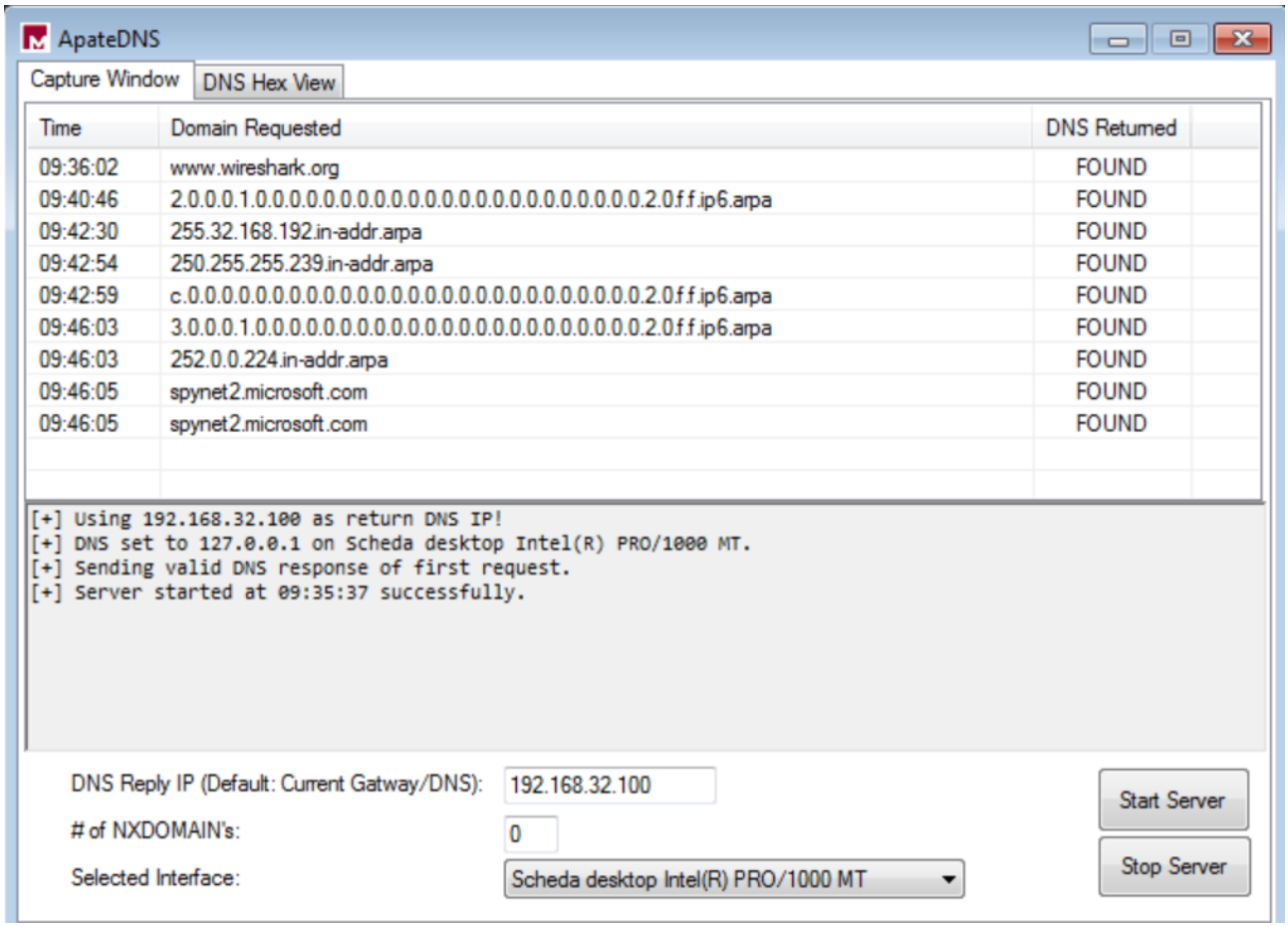
Analisi con Regshot

Abbiamo utilizzato Regshot per eseguire uno screenshot del registro di sistema prima e dopo l'esecuzione del malware "Malware_U3_W2_L5". Questo strumento ci ha consentito di rilevare le modifiche apportate al registro di sistema durante l'esecuzione del malware, consentendoci di identificare potenziali attività dannose o sospette.

Dopo aver confrontato i due screenshot generati da Regshot, abbiamo individuato un totale di 7 chiavi di registro modificate e alcune chiavi di registro eliminate. Queste modifiche indicano che il malware potrebbe aver apportato modifiche al registro di sistema al fine di compromettere il funzionamento del sistema o di nascondere le sue attività dannose. La natura esatta di queste modifiche richiede ulteriori analisi per determinare l'impatto completo del malware sul sistema infetto.

```
Regshot 1.9.0 x86 Unicode
Comments:
Datetime: 2024/2/9 08:37:05  ,  2024/2/9 08:50:09
Computer: USER-PC , USER-PC
Username: user , user

---------------------------------
Keys deleted: 2
---------------------------------
HKLM\SYSTEM\ControlSet001\services\PROCMON23\Enum
HKLM\SYSTEM\CurrentControlSet\services\PROCMON23\Enum

---------------------------------
Keys added: 7
---------------------------------
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_PROCMON23\0000\Control
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROCMON23\0000\Control
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\82\Shell\{5C4F28B5-F869-4E
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\89\Shell\{5C4F28B5-F869-4E
HKU\S-1-5-21-3771313050-58705377-3452663501-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\82\Shell\{5C4F28B5-F869-4E84-8E60-F
HKU\S-1-5-21-3771313050-58705377-3452663501-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\89\Shell\{5C4F28B5-F869-4E84-8E60-F

---------------------------------
Values deleted: 6
---------------------------------
HKLM\SYSTEM\ControlSet001\services\PROCMON23\Enum\0: "Root\LEGACY_PROCMON23\0000"
HKLM\SYSTEM\ControlSet001\services\PROCMON23\Enum\Count: 0x00000001
HKLM\SYSTEM\ControlSet001\services\PROCMON23\Enum\NextInstance: 0x00000001
HKLM\SYSTEM\CurrentControlSet\services\PROCMON23\Enum\0: "Root\LEGACY_PROCMON23\0000"
HKLM\SYSTEM\CurrentControlSet\services\PROCMON23\Enum\Count: 0x00000001
HKLM\SYSTEM\CurrentControlSet\services\PROCMON23\Enum\NextInstance: 0x00000001

---------------------------------
Values added: 76
---------------------------------
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_PROCMON23\0000\Control\ActiveService: "PROCMON23"
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROCMON23\0000\Control\ActiveService: "PROCMON23"
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Applets\Wordpad\Recent File List\File2: "C:\Users\user
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU\*\11:  92 00 32 00 0
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU\hivu\3:  92 00 32 00
```

ApateDNS: Abbiamo configurato un server DNS locale sulla stessa macchina in cui abbiamo eseguito il malware utilizzando ApateDNS. Questo ci ha permesso di controllare e manipolare il traffico DNS generato dal malware, consentendoci di rilevare una serie di comunicazioni di rete sospette ma nessuna che possa confermare la comunicazione verso un server remoto. L'ipotesi potrebbe essere che la macchina utilizzata non è connessa a internet.

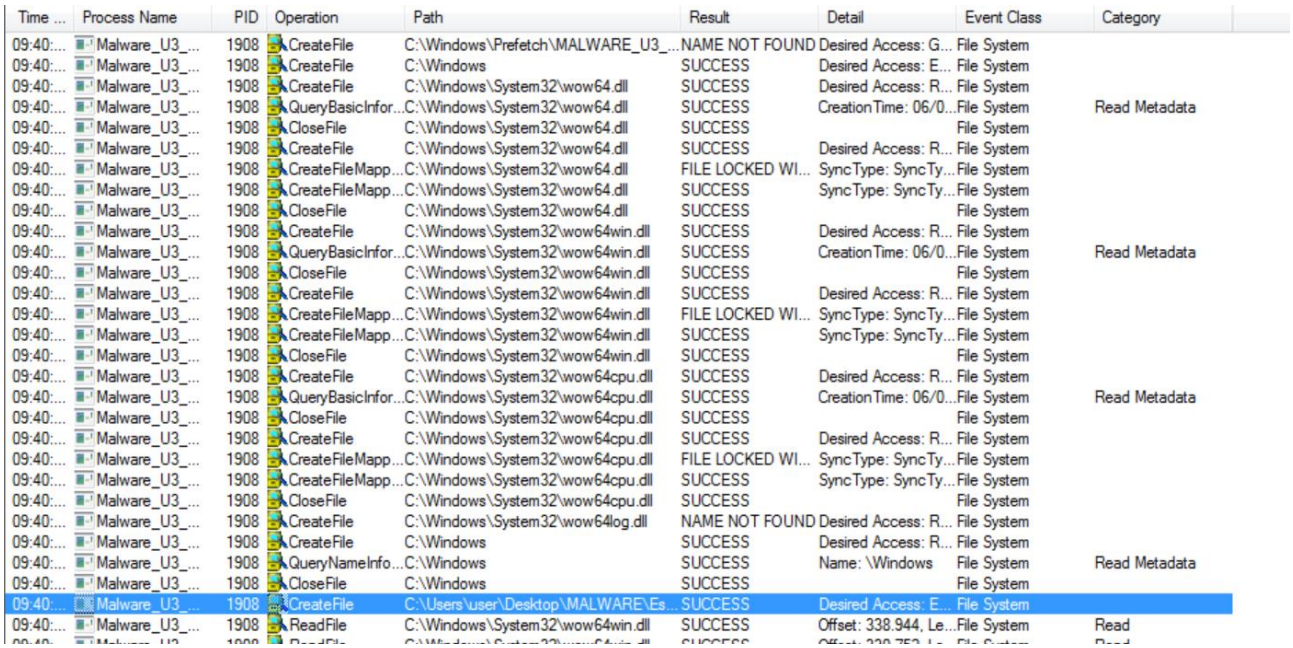


Wireshark: Abbiamo utilizzato Wireshark per catturare e analizzare il traffico di rete generato dal malware. Ciò ci ha fornito informazioni dettagliate sulle comunicazioni di rete del malware, inclusi gli indirizzi IP di destinazione e i protocolli utilizzati, aiutandoci a comprendere meglio il comportamento del malware.

Dall'analisi abbiamo rilevato una serie di comunicazioni che la macchina effettua il locale ma niente che possa far pensare che il malware abbia comunicato.

Abbiamo ipotizzato che non ha potuto stabilire una connessione perché la macchina è stata postata su rete interna.

Process Monitor: Abbiamo monitorato le attività del sistema utilizzando Process Monitor. Questo ci ha consentito di tracciare tutte le operazioni di file e di registro eseguite dal malware, inclusa la creazione di file nella directory del malware e in altre posizioni del sistema, come la cartella dei cookie del browser. Ciò ha portato all'ipotesi che il malware potrebbe inviare informazioni sulla macchina infetta tramite Internet. Purtroppo utilizzando Windows7 come macchina virtuale il malware non ha un comportamento come è previsto per chi lo esegue in una macchina windowsXP.



Time ...	Process Name	PID	Operation	Path	Result	Detail	Event Class	Category
09:40:...	Malware_U3_...	1908	CreateFile	C:\Windows\Prefetch\MALWARE_U3_...	NAME NOT FOUND	Desired Access: G...	File System	
09:40:...	Malware_U3_...	1908	CreateFile	C:\Windows	SUCCESS	Desired Access: E...	File System	
09:40:...	Malware_U3_...	1908	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: R...	File System	
09:40:...	Malware_U3_...	1908	QueryBasicInfor...	C:\Windows\System32\wow64.dll	SUCCESS	CreationTime: 06/0...	File System	Read Metadata
09:40:...	Malware_U3_...	1908	CloseFile	C:\Windows\System32\wow64.dll	SUCCESS		File System	
09:40:...	Malware_U3_...	1908	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: R...	File System	
09:40:...	Malware_U3_...	1908	CreateFileMapp...	C:\Windows\System32\wow64.dll	FILE LOCKED WI...	SyncType: SyncTy...	File System	
09:40:...	Malware_U3_...	1908	CreateFileMapp...	C:\Windows\System32\wow64.dll	SUCCESS	SyncType: SyncTy...	File System	
09:40:...	Malware_U3_...	1908	CloseFile	C:\Windows\System32\wow64.dll	SUCCESS		File System	
09:40:...	Malware_U3_...	1908	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: R...	File System	
09:40:...	Malware_U3_...	1908	QueryBasicInfor...	C:\Windows\System32\wow64win.dll	SUCCESS	CreationTime: 06/0...	File System	Read Metadata
09:40:...	Malware_U3_...	1908	CloseFile	C:\Windows\System32\wow64win.dll	SUCCESS		File System	
09:40:...	Malware_U3_...	1908	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: R...	File System	
09:40:...	Malware_U3_...	1908	CreateFileMapp...	C:\Windows\System32\wow64win.dll	FILE LOCKED WI...	SyncType: SyncTy...	File System	
09:40:...	Malware_U3_...	1908	CreateFileMapp...	C:\Windows\System32\wow64win.dll	SUCCESS	SyncType: SyncTy...	File System	
09:40:...	Malware_U3_...	1908	CloseFile	C:\Windows\System32\wow64win.dll	SUCCESS		File System	
09:40:...	Malware_U3_...	1908	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Desired Access: R...	File System	
09:40:...	Malware_U3_...	1908	QueryBasicInfor...	C:\Windows\System32\wow64cpu.dll	SUCCESS	CreationTime: 06/0...	File System	Read Metadata
09:40:...	Malware_U3_...	1908	CloseFile	C:\Windows\System32\wow64cpu.dll	SUCCESS		File System	
09:40:...	Malware_U3_...	1908	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Desired Access: R...	File System	
09:40:...	Malware_U3_...	1908	CreateFileMapp...	C:\Windows\System32\wow64cpu.dll	FILE LOCKED WI...	SyncType: SyncTy...	File System	
09:40:...	Malware_U3_...	1908	CreateFileMapp...	C:\Windows\System32\wow64cpu.dll	SUCCESS	SyncType: SyncTy...	File System	
09:40:...	Malware_U3_...	1908	CloseFile	C:\Windows\System32\wow64cpu.dll	SUCCESS		File System	
09:40:...	Malware_U3_...	1908	CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT FOUND	Desired Access: R...	File System	
09:40:...	Malware_U3_...	1908	CreateFile	C:\Windows	SUCCESS	Desired Access: R...	File System	
09:40:...	Malware_U3_...	1908	QueryNameInfo...	C:\Windows	SUCCESS	Name: \Windows	File System	Read Metadata
09:40:...	Malware_U3_...	1908	CloseFile	C:\Windows	SUCCESS		File System	
09:40:...	Malware_U3_...	1908	CreateFile	C:\Users\user\Desktop\MALWARE\Es...	SUCCESS	Desired Access: E...	File System	
09:40:...	Malware_U3_...	1908	ReadFile	C:\Windows\System32\wow64win.dll	SUCCESS	Offset: 338.944, Le...	File System	Read

Ipotesi sul Comportamento:

Basandoci sull'analisi condotta con gli strumenti sopra menzionati, ipotizziamo che il malware "Malware_U3_W2_L5" potrebbe essere progettato per raccogliere informazioni dalla macchina infetta e inviarle a un server remoto attraverso la rete. Le attività osservate, come la verifica della connessione Internet, la creazione di file nella directory del malware e nelle cartelle di sistema pertinenti ai cookie dei browser, supportano questa ipotesi. Tuttavia, è necessario ulteriore analisi per confermare questa ipotesi e per comprendere appieno l'impatto del malware sul sistema infetto.

Analisi del codice fornitoci nella seconda parte parte

Dall'analisi del codice del malware, sono stati identificati i seguenti costrutti noti:

Creazione dello Stack: Il malware sembra utilizzare la funzione CreateThread per creare uno o più thread di esecuzione, che potrebbero essere utilizzati per eseguire operazioni in background senza bloccare l'esecuzione principale del programma.

Cicli: Sono presenti cicli all'interno del codice del malware, indicando che potrebbe essere coinvolto in iterazioni ripetute di codice per eseguire determinate azioni o per eseguire il codice in modo iterativo. Il ciclo in questione che abbiamo identificato è un ciclo If.

Ipotizzazione del Comportamento

Basandoci sull'analisi del codice, è possibile ipotizzare il seguente comportamento del malware:

Verifica Connessione Internet: Il malware utilizza la funzione InternetGetConnectedState per verificare se è disponibile una connessione a Internet. Il risultato della chiamata a questa funzione viene memorizzato in una variabile locale.

Elaborazione del Risultato: Il malware confronta il risultato della verifica della connessione Internet. Se la connessione è attiva (risultato diverso da zero), il malware continua l'esecuzione. Altrimenti, potrebbe eseguire azioni alternative o sospendere l'esecuzione.

Output di un Messaggio di Successo: Se la connessione a Internet è attiva, il malware potrebbe visualizzare un messaggio di successo attraverso una chiamata a una funzione sub_40105F.

Continuazione dell'Esecuzione: Dopo l'elaborazione del risultato, il malware continua l'esecuzione del suo codice, eseguendo eventualmente ulteriori azioni dannose o comunicazioni di rete.

Conclusioni

Dall'analisi delle librerie importate nel file eseguibile del malware "Malware_U3_W2_L5", è emerso un quadro significativo delle funzionalità e delle dipendenze del malware. Le due principali librerie identificate sono kernel32.dll e wininet.dll.

La presenza di kernel32.dll suggerisce che il malware fa ampio uso di funzioni di sistema essenziali per la gestione dei processi, dei file e della memoria. Queste funzioni possono essere utilizzate per eseguire operazioni di base come la creazione e la gestione dei processi, la lettura e la scrittura dei file, e altre operazioni di basso livello.

D'altra parte, l'importazione della libreria wininet.dll indica che il malware potrebbe essere coinvolto in attività di comunicazione di rete su Internet. Funzioni come InternetGetConnectedState possono essere utilizzate per verificare lo stato della connessione Internet, mentre altre funzioni come InternetOpen, InternetConnect, HttpOpenRequest e InternetReadFile possono essere utilizzate per effettuare richieste HTTP e leggere dati dalla rete.

Insieme, queste librerie forniscono al malware la capacità di interagire con il sistema e la rete, consentendogli di eseguire azioni dannose come la comunicazione con server remoti, il download di file dannosi e altre attività di rete potenzialmente dannose.

Quest'analisi preliminare delle librerie importate fornisce una solida base per ulteriori investigazioni sull'obiettivo e il comportamento del malware, che possono essere ulteriormente approfondite mediante l'analisi delle altre sezioni del file eseguibile e l'osservazione delle attività del malware sul sistema infetto.

Nota: Si consiglia di continuare l'analisi del malware utilizzando gli altri strumenti e approcci menzionati nel report, al fine di ottenere una comprensione completa del suo comportamento e delle sue potenziali minacce per il sistema.