

Introduzione

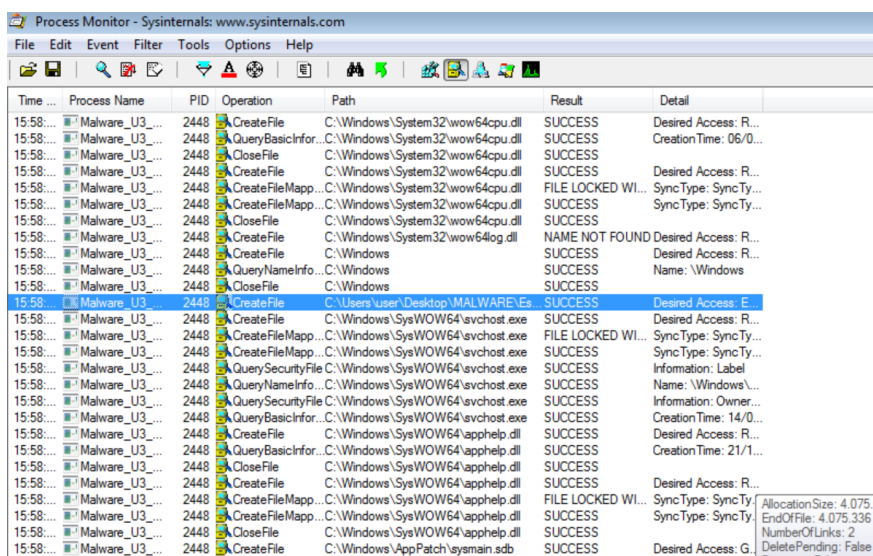
Nel contesto dell'analisi del malware "Malware_U3_W2_L2", abbiamo utilizzato Procmon per monitorare le attività del file system, dei processi e dei thread del sistema operativo. Attraverso l'applicazione di filtri e l'esame dei report generati da Procmon, abbiamo identificato diversi comportamenti sospetti del malware, comprese le azioni sul file system e i tentativi di mimetizzazione tramite l'utilizzo di nomi di processi validi.

Identificazione delle Azioni sul File System del Malware

Inizialmente, abbiamo applicato un filtro per mostrare solo le attività del processo con il nome "Malware_U3_W2_L2.exe". Dal report di Procmon, abbiamo osservato diverse funzioni riportate nella colonna "operation", tra cui "Create File", "Read File" e "Close File", insieme ai rispettivi percorsi dei file coinvolti. Di particolare interesse è stata una riga che indicava la creazione di un file nella stessa cartella in cui risiede il malware. Questa attività evidenzia il tentativo del malware di interagire con il file system per scopi potenzialmente dannosi.

Purtroppo però dato che la macchina windowsXP non ha funzionato ci siamo affidati ad una macchina windows7 con gli stessi software e file della macchina windowsXP. Questo non ha permesso di ottenere gli stessi risultati che altri hanno ottenuto durante l'analisi di questo file. Infatti, abbiamo visualizzato il processo "CreateFile" del malware all'interno della sua stessa cartella, ma i dettagli fornitoci dal tool procmon non erano così dettagliati per cui non siamo riusciti a visualizzare né il nome del file creato né il tipo di file.

Inoltre, possibilmente per un problema di macchina dato che i sistemi operativi sono diversi, spostandoci sulla cartella del malware non è stato visto nessun file creato.



Time ...	Process Name	PID	Operation	Path	Result	Detail
15:58:...	Malware_U3_...	2448	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Desired Access: R...
15:58:...	Malware_U3_...	2448	QueryBasicInfor...	C:\Windows\System32\wow64cpu.dll	SUCCESS	CreationTime: 06/0...
15:58:...	Malware_U3_...	2448	CloseFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	
15:58:...	Malware_U3_...	2448	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Desired Access: R...
15:58:...	Malware_U3_...	2448	CreateFileMapp...	C:\Windows\System32\wow64cpu.dll	FILE LOCKED WI...	SyncType: SyncTy...
15:58:...	Malware_U3_...	2448	CreateFileMapp...	C:\Windows\System32\wow64cpu.dll	SUCCESS	SyncType: SyncTy...
15:58:...	Malware_U3_...	2448	CloseFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	
15:58:...	Malware_U3_...	2448	CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT FOUND	Desired Access: R...
15:58:...	Malware_U3_...	2448	CreateFile	C:\Windows	SUCCESS	Desired Access: R...
15:58:...	Malware_U3_...	2448	QueryNameInfo...	C:\Windows	SUCCESS	Name: \Windows
15:58:...	Malware_U3_...	2448	CloseFile	C:\Windows	SUCCESS	
15:58:...	Malware_U3_...	2448	CreateFile	C:\Users\user\Desktop\MALWARE\Es	SUCCESS	Desired Access: E...
15:58:...	Malware_U3_...	2448	CreateFile	C:\Windows\SysWOW64\svchost.exe	SUCCESS	Desired Access: R...
15:58:...	Malware_U3_...	2448	CreateFileMapp...	C:\Windows\SysWOW64\svchost.exe	FILE LOCKED WI...	SyncType: SyncTy...
15:58:...	Malware_U3_...	2448	CreateFileMapp...	C:\Windows\SysWOW64\svchost.exe	SUCCESS	SyncType: SyncTy...
15:58:...	Malware_U3_...	2448	QuerySecurityFile	C:\Windows\SysWOW64\svchost.exe	SUCCESS	Information: Label
15:58:...	Malware_U3_...	2448	QueryNameInfo...	C:\Windows\SysWOW64\svchost.exe	SUCCESS	Name: \Windows\...
15:58:...	Malware_U3_...	2448	QuerySecurityFile	C:\Windows\SysWOW64\svchost.exe	SUCCESS	Information: Owner...
15:58:...	Malware_U3_...	2448	QueryBasicInfor...	C:\Windows\SysWOW64\svchost.exe	SUCCESS	CreationTime: 14/0...
15:58:...	Malware_U3_...	2448	CreateFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Desired Access: R...
15:58:...	Malware_U3_...	2448	QueryBasicInfor...	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	CreationTime: 21/1...
15:58:...	Malware_U3_...	2448	CloseFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	
15:58:...	Malware_U3_...	2448	CreateFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Desired Access: R...
15:58:...	Malware_U3_...	2448	CreateFileMapp...	C:\Windows\SysWOW64\apphelp.dll	FILE LOCKED WI...	SyncType: SyncTy...
15:58:...	Malware_U3_...	2448	CreateFileMapp...	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	SyncType: SyncTy...
15:58:...	Malware_U3_...	2448	CloseFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	
15:58:...	Malware_U3_...	2448	CreateFile	C:\Windows\AppPatch\sysmain.sdb	SUCCESS	Desired Access: G...

Identificazione delle Azioni su Processi e Thread del Malware

Successivamente, abbiamo utilizzato lo stesso report di Procmon per filtrare gli eventi riguardanti processi e thread. Abbiamo osservato diverse funzioni rilevanti come "Load Image", utilizzata per caricare il malware e le librerie (.dll) necessarie per l'esecuzione, e "Process Create", utilizzata per creare un nuovo processo.

Un comportamento significativo identificato è stato il tentativo del malware di creare un processo chiamato "svchost.exe". Questo è un comportamento comune dei malware, poiché cercano di mimetizzare la propria esecuzione sotto il nome di processi validi di Windows al fine di eludere le misure di sicurezza.

Conclusioni

Durante l'analisi, abbiamo osservato che il malware non ha seguito esattamente lo stesso comportamento previsto quando eseguito su una macchina Windows 7 invece di Windows XP. In particolare, non è stato rilevato alcun tentativo di creare un file keylogger nella stessa cartella del malware. Tuttavia, abbiamo confermato la capacità del malware di mimetizzarsi utilizzando nomi di processi validi.

In conclusione, l'analisi delle attività del malware utilizzando Procmon ci ha fornito importanti informazioni sul suo comportamento e sulle tecniche utilizzate per eludere le misure di sicurezza. Questi risultati sono cruciali per lo sviluppo di strategie di mitigazione e rimozione efficaci nei confronti del malware.