## **S10L2**

## Analisi dinamica

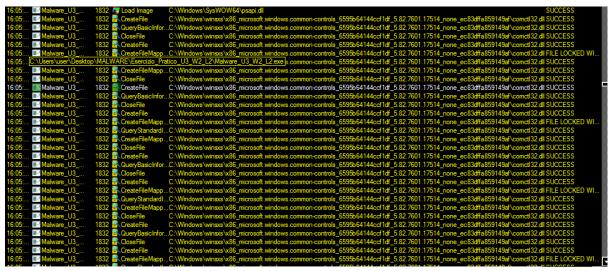
Identificare eventuali azioni del malware sul file system utilizzando ProcessMonitor (procmon), Identificare eventuali azioni del malware su processi e thread utilizzando ProcessMonitor.

## **SOLUZIONE**

Come prima cosa mettiamo la nostra macchina in sicurezza quindi, eliminiamo la connessione e eventuali cartelle condivise, una volta fatto ciò procediamo ad analizzare il malware in questione.

16:05:	Malware	U3	1832 🚜	Load Image	C:\Windows\SysWOW64	\psapi.dll	SUCCESS	Image Base: 0x77a
16:05:	■- Malware	U3	1832 📑	CreateFile	C:\Windows\winsxs\x86_	microsoft.wind	.SUCCESS	Desired Access: R
16:05:	■- Malware	U3	1832 📑	QueryBasicInfor	.C:\Windows\winsxs\x86	microsoft.wind	.SUCCESS	CreationTime: 21/1
16:05:	■- Malware	U3	1832 📑	CloseFile	C:\Windows\winsxs\x86	microsoft.wind	.SUCCESS	
16:05:	■- Malware	U3	1832 📑	CreateFile	C:\Windows\winsxs\x86	microsoft.wind	.SUCCESS	Desired Access: R
16:05:	■- Malware	U3	1832 📑	CreateFileMapp	C:\Windows\winsxs\x86	microsoft.wind	FILE LOCKED WI	SyncType: SyncTy
16:05:	■- Malware	U3	1832 📑	QueryStandardI	C:\Windows\winsxs\x86	microsoft.wind	.SUCCESS	AllocationSize: 532
16:05:	■- Malware	U3	1832 📑	CreateFileMapp	C:\Windows\winsxs\x86_	microsoft.wind	.SUCCESS	SyncType: SyncTy
16:05:	■- Malware	U3	1832 📑	CloseFile	C:\Windows\winsxs\x86_	microsoft.wind	.SUCCESS	
16:05:	■- Malware	U3	1832 📑	CreateFile	C:\Windows\winsxs\x86_	microsoft.wind	.SUCCESS	Desired Access: R
16:05:	■- Malware	U3	1832 📑	QueryBasicInfor	.C:\Windows\winsxs\x86_	microsoft.wind	.SUCCESS	CreationTime: 21/1
10.05	= 1 M-l	112	1022 🍑	Class Ela	C/\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	material and a second	CHCCECC	

Possiamo notare che il malware carica una libreria (psapi.dll) la quale fornisce funzioni per ottenere informazioni sui processi e sui moduli in esecuzione nel sistema, quindi sta cercando di raccogliere informazioni.



Dopodichè va a modificare la libreria 'comctl32.dll' per eseguire il proprio codice e inoltre invoca anche la libreria 'acgenral.dll' per eludere le misure di sicurezza.

Una volta che ha completato queste operazioni,il malware va a ottenere informazioni su varie librerie e si posiziona in una cartella di sistema in modo tale da avviarsi ogni volta che noi accendiamo il pc.

## Regshot

Attraverso un tool chiamato *regshot* andiamo a effettuare un'istantanea delle modifiche fatte dal malware una volta eseguito, e come possiamo notare ha effettuato 15 modifiche al sistema.