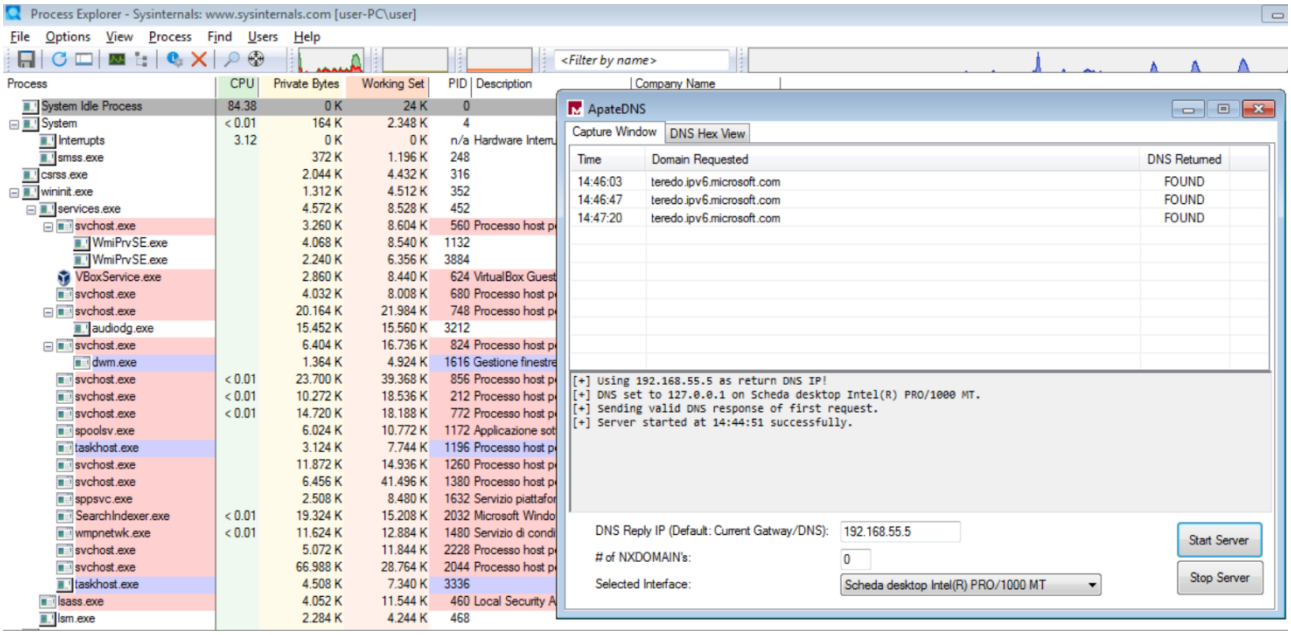
Analisi di base dinamica

Traccia:

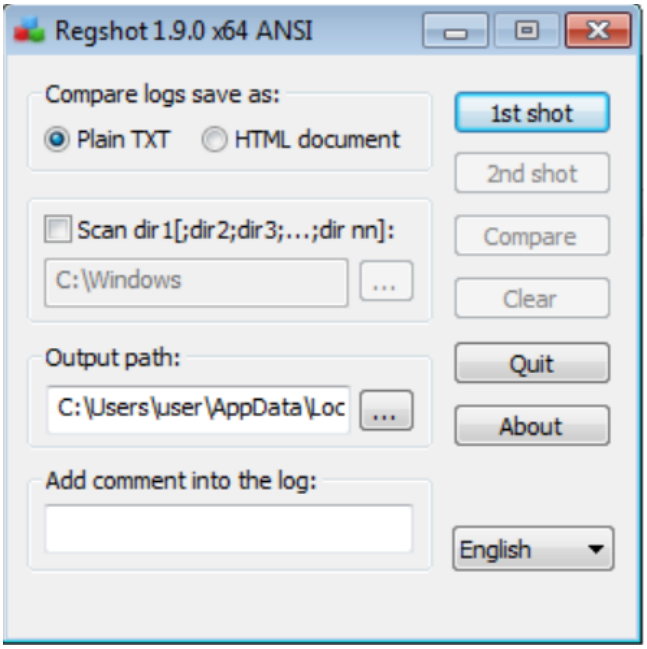
Esercizio Analisi dinamica Configurare la macchina virtuale per l'analisi dinamica (il malware sarà effettivamente eseguito) rispondere ai seguenti quesiti
• Identificare eventuali azioni del malware sul file system utilizzando Process Monitor (procmon)
• Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor
• Modifiche del registro dopo il malware (le differenze)
• Provare a profilare il malware in base alla correlazione tra «operation» e Path.

Cominciamo l'analisi usando gli strumenti a nostra disposizione. Per prima cosa avviamo Process Explorer, Apate DNS e poi, usando Reg Shot, fare un'istantanea delle chiavi di registro prima dell'esecuzione del malware.

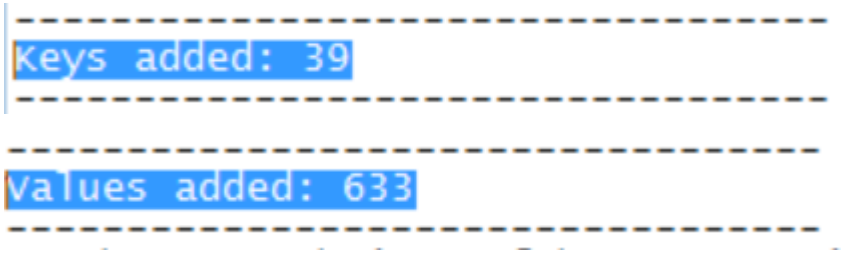


A questo punto eseguiamo ProcMoc e Wireshak ed, infine, facciamo partire il malware.

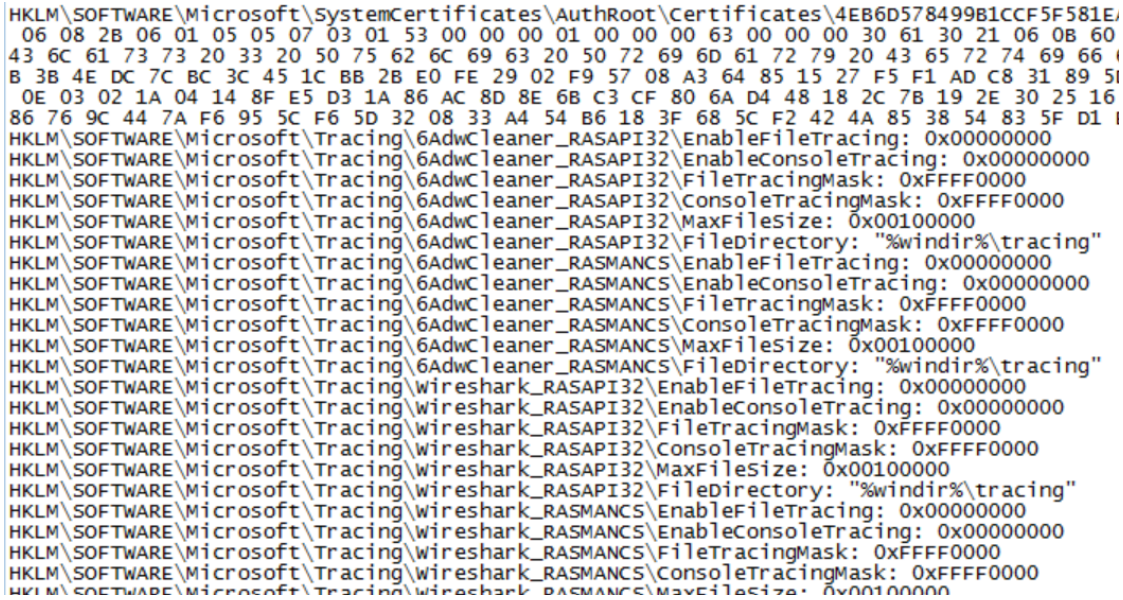
Lo lasciamo eseguire per un minuto.



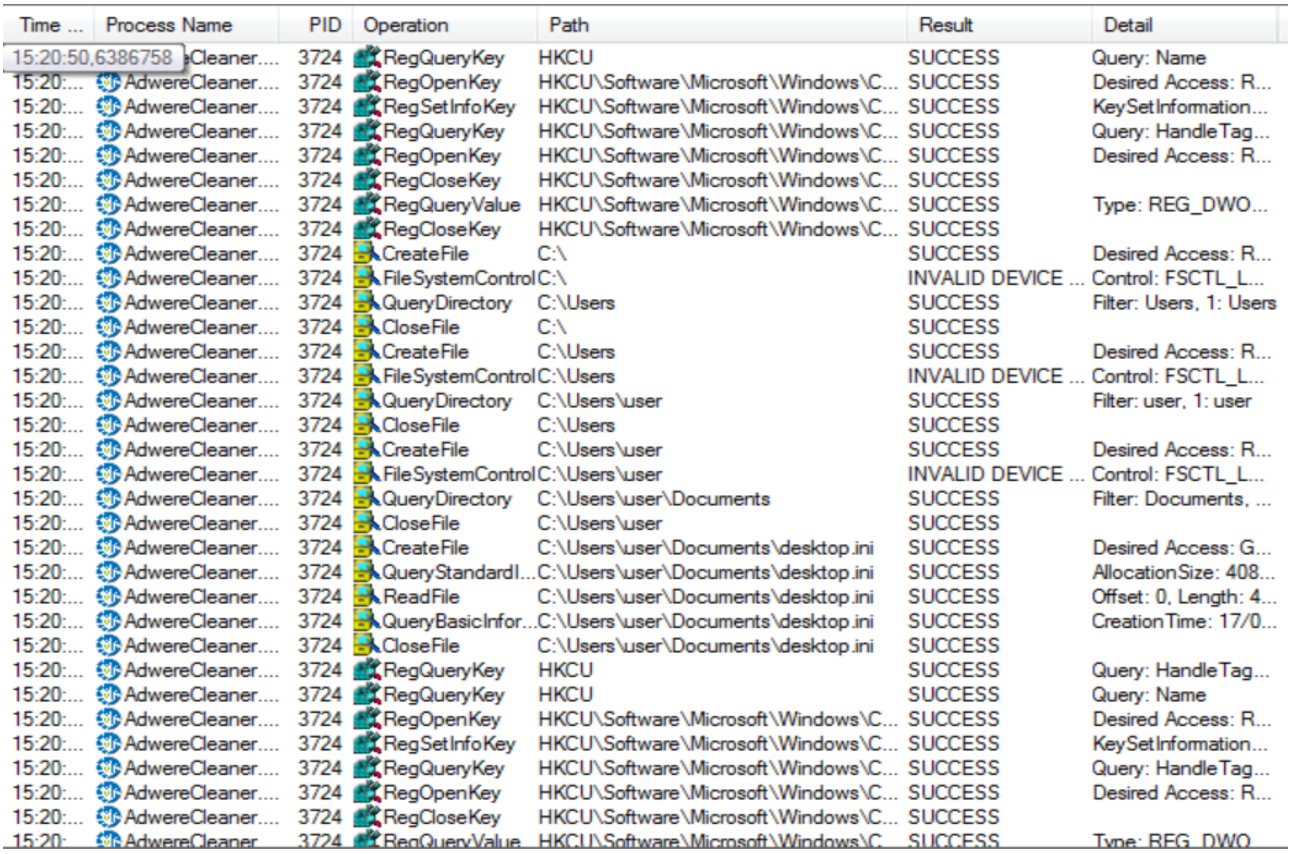
Dopodiché fermiamo Apate DNS e Process Explorer e faccio la seconda istantanea con Reg Shot



Questo malware sembra che si finga un programma di pulizia. Così facendo ha tolto una chiave che riguarda una scansione di Windows Defender e ha tolto una protezione. Io oltre ha aggiunto chiave nuove per tracciare le sue attività. Praticamente va a cambiare le nostre misure di sicurezza con quelle che aggradano a lui.

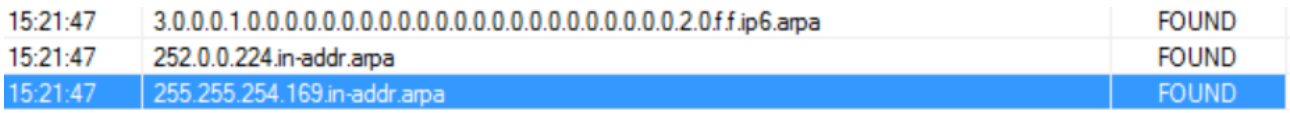


Torniamo su Proc Mon e fermiamo la carruta. Applichiamo un filtro per vedere solo le arrività del malware così da vedere tutto quello che il malware ha fatto



Time ...	Process Name	PID	Operation	Path	Result	Detail
15:20:50,6386758	Cleaner....	3724	RegQueryKey	HKCU	SUCCESS	Query: Name
15:20:...	AdwereCleaner....	3724	RegOpenKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Desired Access: R...
15:20:...	AdwereCleaner....	3724	RegSetInfoKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	KeySetInformation...
15:20:...	AdwereCleaner....	3724	RegQueryKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Query: HandleTag...
15:20:...	AdwereCleaner....	3724	RegOpenKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Desired Access: R...
15:20:...	AdwereCleaner....	3724	RegCloseKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	
15:20:...	AdwereCleaner....	3724	RegQueryValue	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Type: REG_DWO...
15:20:...	AdwereCleaner....	3724	RegCloseKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	
15:20:...	AdwereCleaner....	3724	CreateFile	C:\	SUCCESS	Desired Access: R...
15:20:...	AdwereCleaner....	3724	FileSystemControl	C:\	INVALID DEVICE ...	Control: FSCTL_L...
15:20:...	AdwereCleaner....	3724	QueryDirectory	C:\Users	SUCCESS	Filter: Users, 1: Users
15:20:...	AdwereCleaner....	3724	CloseFile	C:\	SUCCESS	
15:20:...	AdwereCleaner....	3724	CreateFile	C:\Users	SUCCESS	Desired Access: R...
15:20:...	AdwereCleaner....	3724	FileSystemControl	C:\Users	INVALID DEVICE ...	Control: FSCTL_L...
15:20:...	AdwereCleaner....	3724	QueryDirectory	C:\Users\user	SUCCESS	Filter: user, 1: user
15:20:...	AdwereCleaner....	3724	CloseFile	C:\Users	SUCCESS	
15:20:...	AdwereCleaner....	3724	CreateFile	C:\Users\user	SUCCESS	Desired Access: R...
15:20:...	AdwereCleaner....	3724	FileSystemControl	C:\Users\user	INVALID DEVICE ...	Control: FSCTL_L...
15:20:...	AdwereCleaner....	3724	QueryDirectory	C:\Users\user\Documents	SUCCESS	Filter: Documents, ...
15:20:...	AdwereCleaner....	3724	CloseFile	C:\Users\user	SUCCESS	
15:20:...	AdwereCleaner....	3724	CreateFile	C:\Users\user\Documents\desktop.ini	SUCCESS	Desired Access: G...
15:20:...	AdwereCleaner....	3724	QueryStandardI...	C:\Users\user\Documents\desktop.ini	SUCCESS	AllocationSize: 408...
15:20:...	AdwereCleaner....	3724	ReadFile	C:\Users\user\Documents\desktop.ini	SUCCESS	Offset: 0, Length: 4...
15:20:...	AdwereCleaner....	3724	QueryBasicInfor...	C:\Users\user\Documents\desktop.ini	SUCCESS	CreationTime: 17/0...
15:20:...	AdwereCleaner....	3724	CloseFile	C:\Users\user\Documents\desktop.ini	SUCCESS	
15:20:...	AdwereCleaner....	3724	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
15:20:...	AdwereCleaner....	3724	RegQueryKey	HKCU	SUCCESS	Query: Name
15:20:...	AdwereCleaner....	3724	RegOpenKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Desired Access: R...
15:20:...	AdwereCleaner....	3724	RegSetInfoKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	KeySetInformation...
15:20:...	AdwereCleaner....	3724	RegQueryKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Query: HandleTag...
15:20:...	AdwereCleaner....	3724	RegOpenKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Desired Access: R...
15:20:...	AdwereCleaner....	3724	RegCloseKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	
15:20:...	AdwereCleaner....	3724	RegQueryValue	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Type: REG_DWO...

Andando su Apate DNS possiamo vedere anche delle richieste DNS piuttosto strane e che potrebbero essere siti di phishing o siti con altri malware



15:21:47	3.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.ip6.arpa	FOUND
15:21:47	252.0.0.224.in-addr.arpa	FOUND
15:21:47	255.255.254.169.in-addr.arpa	FOUND