

TRACCIA FINALE W24D4

MALWARE ANALYSIS ANALISI DINAMICA

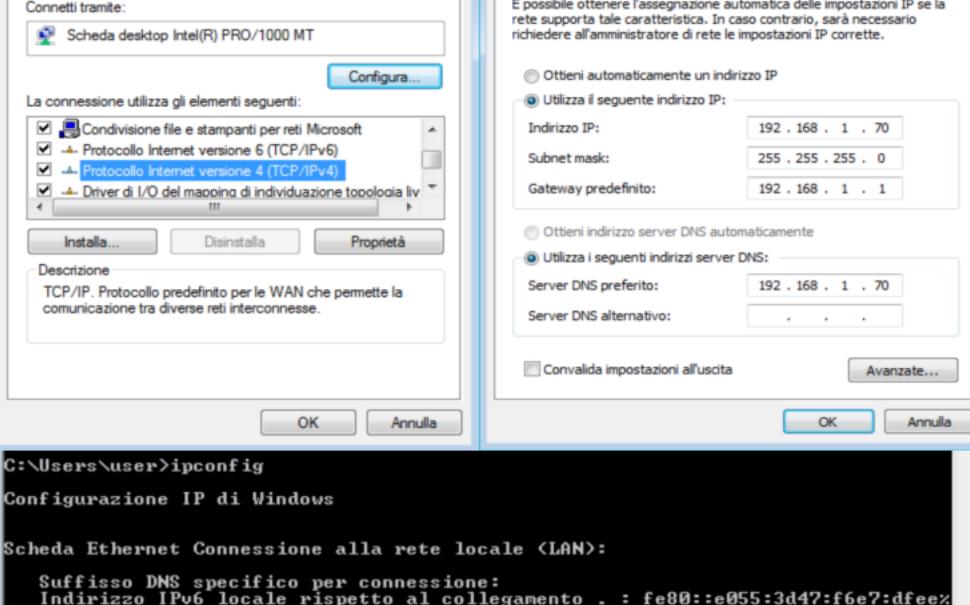
TRACCIA:

ANALISI DINAMICA

PREPARATE L'AMBIENTE ED I TOOL PER L'ESECUZIONE DEL MALWARE (SUGGERIMENTO: AVViate PRINCIPALMENTE **PROCESS MONITOR** ED ASSICURATE DI ELIMINARE OGNI FILTRO CLICCANDO SUL TASTO «**RESET**» QUANDO RICHIESTO IN FASE DI AVVIO). ESEGUITE IL MALWARE, FACENDO DOPPIO CLICK SULL'ICONA DELL'ESEGUIBILE

- COSA NOTATE ALL'INTERNO DELLA CARTELLA DOVE È SITUATO L'ESEGUIBILE DEL MALWARE? SPIEGATE COSA È AVVENUTO, UNENDO LE EVIDENZE CHE AVETE RACCOLTO FINORA PER RISPONDERE ALLA DOMANDA.

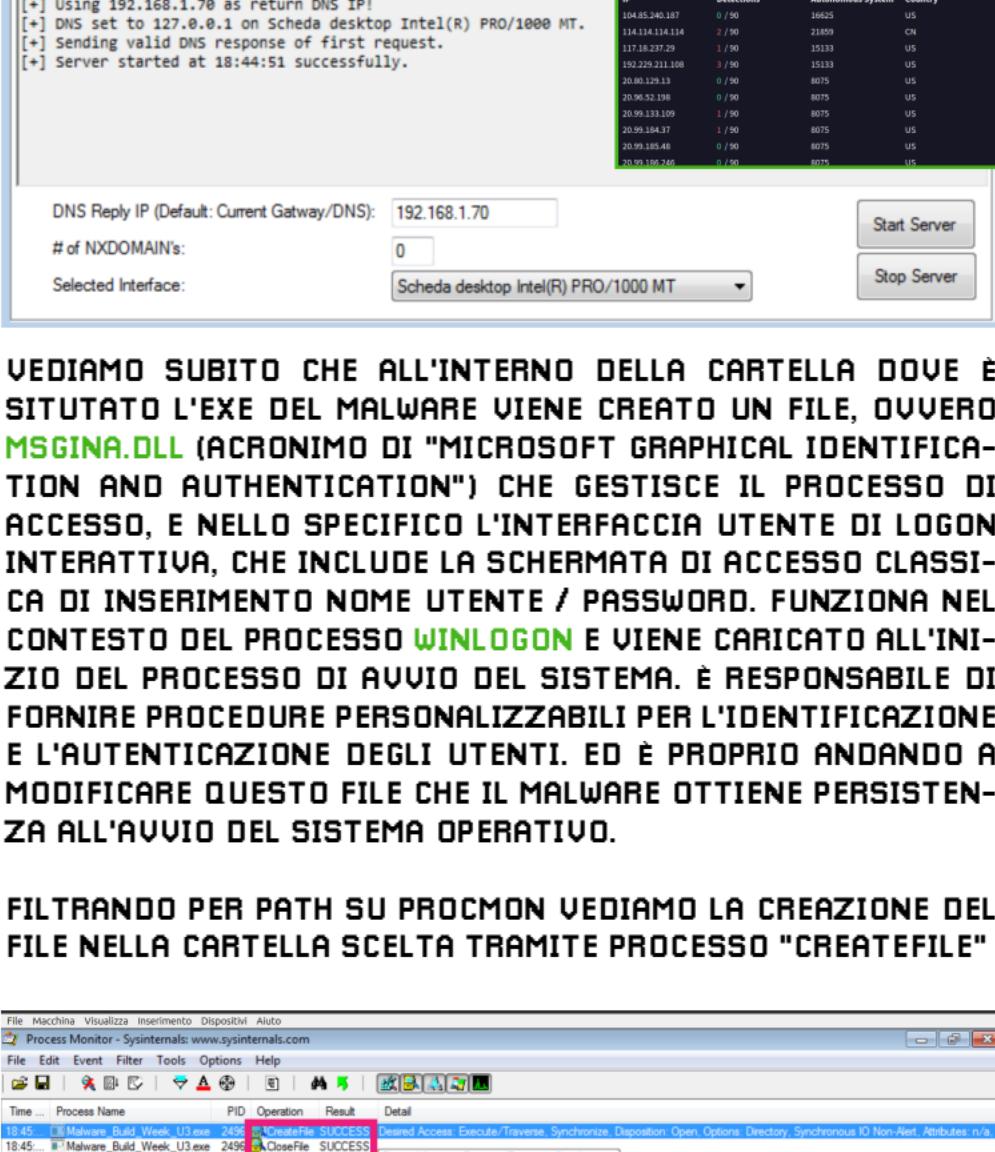
ANALIZZATE ORA I RISULTATI DI PROCESS MONITOR (CONSIGLIO: UTILIZZATE IL FILTRO COME IN FIGURA SOTTO PER ESTRARRE SOLO LE MODIFICHE APPORTATE AL SISTEMA DA PARTE DEL MALWARE). FATE CLICK SU «**ADD**» POI SU «**APPLY**» COME ABBIAMO VISTO NELLA LEZIONE TEORICA.



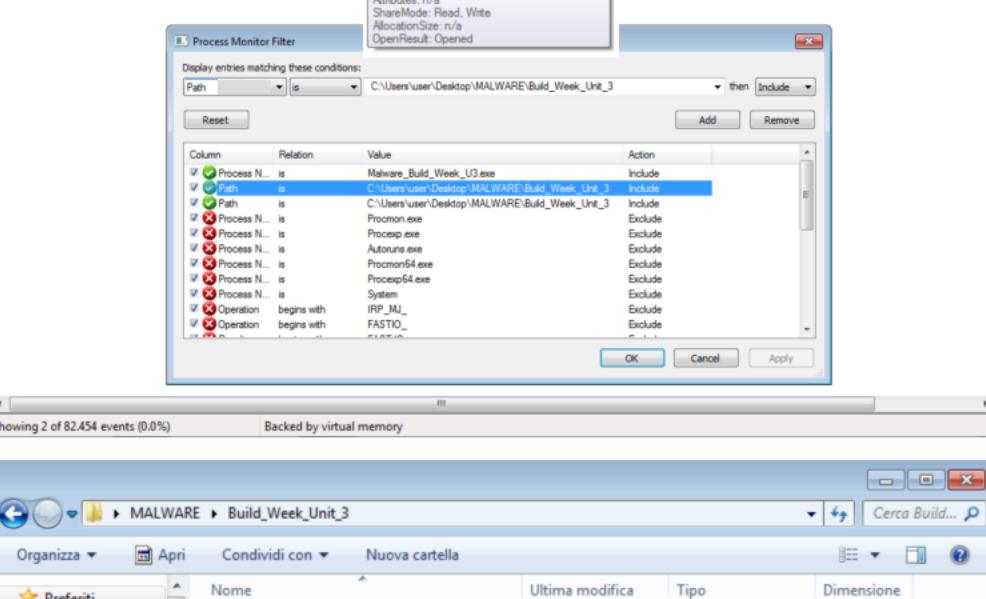
RICREO UN'INSTANTANEA DA VIRTUALBOX DELLA MACCHINA WINDOWS PRIMA DI INIZIARE, PER POTER RIPRISTINARE IN CASO DI PROBLEMI, E VISTO CHE ANDRÒ AD ESEGUIRE IL MALWARE MI ASSICURO DI RISPETTARE I SEGUENTI ACCORGIMENTI:

- DISATTIVARE CONTROLLER USB**
- DISATTIVARE COMUNICAZIONE CON LA RETE (SOLO INT)**
- DISABILITARE LA CODIVISIONE DELLE CARTELLE**
- DISABILITARE APPUNTI CONDIVISI (COPIA / INCOLLA)**

PRIMA DI APRIRE IL MALWARE, MI ASSICURO DI ANDARE A CATTURARE TUTTI GLI EVENTI APRENDO **PROCMON**, AL FINE DI IDENTIFICARE EVENTUALI AZIONI DEL MALWARE SU PROCESSI E THREAD, E MODIFICHE REGISTRO; AVVIO **REGSHOT** PER CONFRONTARE TRAMITE SCREENSHOT (PRIMA / DOPO) LE MODIFICHE CHE AVVERRANNO A LIVELLO DI SISTEMA, ED IMPOSTO UN IP STATICO PER VEDERE TRAMITE **APATEDNS** LE CHIAMATE CHE IL MALWARE ANDRA A FARE NEL WEB (QUALI SITI). AVENDOLO ISOLATO DALLA RETE OVVIAMENTE NON POTRA ESEGUIRE TUTTE LE SUE FUNZIONI.



DI SEGUITO ALCUNE DELLE CHIAMATE INTERCETTATE:



ApatedNS

Capture Window DNS Hex View

Time Domain Requested DNS Returned

18:44:53 teredo.ipv6.microsoft.com FOUND

18:45:35 teredo.ipv6.microsoft.com FOUND

18:45:51 ocsp.digicert.com FOUND

18:46:03 ocsp.digicert.com FOUND

18:46:15 www.download.windowsupdate.com FOUND

18:46:16 teredo.ipv6.microsoft.com FOUND

18:46:28 ocsp.digicert.com FOUND

18:47:18 ocsp.usertrust.com FOUND

18:47:26 teredo.ipv6.microsoft.com FOUND

18:47:31 ocsp.sectigo.com FOUND

18:47:31 ocsp.comodoca.com FOUND

18:47:43 ocsp.comodoca.com FOUND

18:47:58 teredo.ipv6.microsoft.com FOUND

18:48:14 spynet2.microsoft.com FOUND

18:48:14 spynet2.microsoft.com FOUND

18:48:33 teredo.ipv6.microsoft.com FOUND

[+] Using 192.168.1.70 as return DNS IP!
[+] DNS set to 127.0.0.1 on Scheda desktop Intel(R) PRO/1000 MT.
[+] Sending valid DNS response of first request.
[+] Server started at 18:44:51 successfully.

DNS Reply IP (Default: Current Gateway/DNS): 192.168.1.70 Start Server Stop Server

of NXDOMAIN's: 0

Selected Interface: Scheda desktop Intel(R) PRO/1000 MT

Process Monitor Filter

Display entries matching these conditions: Path is C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3 then Include

Column Relation Value Action

Process N... is Malware_Build_Week_U3.exe Include

Path is C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3 Exclude

Process N... is Procmn.exe Exclude

Process N... is Autorun.exe Exclude

Process N... is Procmn64.exe Exclude

Process N... is System Exclude

Operation begins with IRP_MJ_FASTIO_ Exclude

Operation begins with IRP_MJ_ Exclude

OK Cancel Apply

VEDIAMO SUBITO CHE ALL'INTERNO DELLA CARTELLA DOVE È SITUTATO L'EXE DEL MALWARE VIENE CREATO UN FILE, OVVERO **MSGINA.DLL** (ACRONIMO DI "MICROSOFT GRAPHICAL IDENTIFICATION AND AUTHENTICATION") CHE GESTISCE IL PROCESSO DI ACCESSO, E NELLO SPECIFICO L'INTERFACCIA UTENTE DI LOGON INTERATTIVA, CHE INCLUDE LA SCHERMATA DI ACCESSO CLASSICA DI INSERIMENTO NOME UTENTE / PASSWORD. FUNZIONA NEL CONTESTO DEL PROCESSO **WINLOGON** E VIENE CARICATO ALL'INIZIO DEL PROCESSO DI AVVIO DEL SISTEMA. È RESPONSABILE DI FORNIRE PROCEDURE PERSONALIZZABILI PER L'IDENTIFICAZIONE E L'AUTENTICAZIONE DEGLI UTENTI. ED È PROPRIO ANDANDO A MODIFICARE QUESTO FILE CHE IL MALWARE OTTIENE PERSISTENZA ALL'AVVIO DEL SISTEMA OPERATIVO.

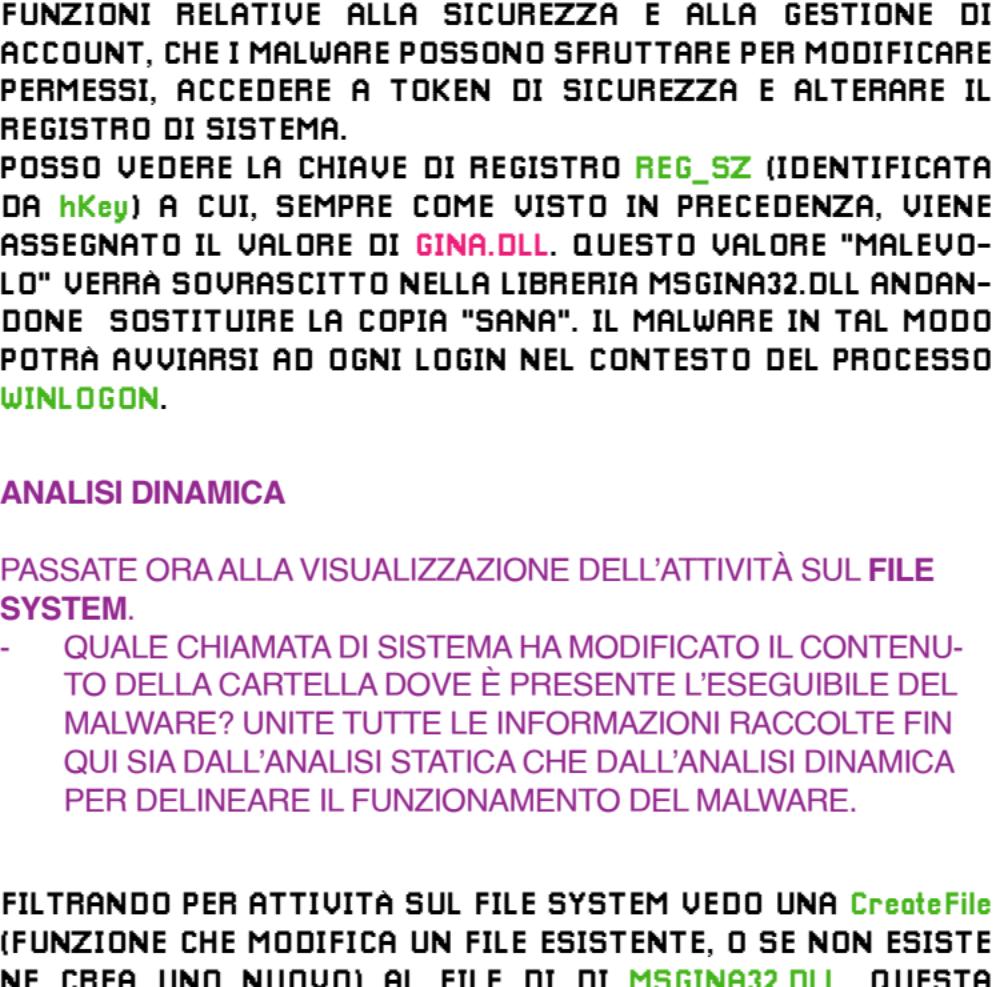
FILTRANDO PER PATH SU PROCMON VEDIAMO LA CREAZIONE DEL FILE NELLA CARTELLA SCELTA TRAMITE PROCESSO "CREATEFILE"

TRACCIA:

ANALISI DINAMICA

FILTRARE INCLUDENDO SOLAMENTE L'ATTIVITÀ SUL REGISTRO DI WINDOWS.

- QUALE CHIAVE DI REGISTRO VIENE CREATA?
- QUALE VALORE VIENE ASSOCIAUTO ALLA CHIAVE DI REGISTRO CREATTA?



FILTRANDO PER CHIAVI DI REGISTRO SI PUÒ NOTARE CHE AD UN CERTO PUNTO VIENE PASSATA LA FUNZIONE `RegSetValue` CHE È UNA FUNZIONE TIPICA DELLA LIBRERIA IMPORTATA DAL MALWARE **ADVAPI32.DLL CHE, COME DETTO IN PRECEDENZA, FORNISCE FUNZIONI RELATIVE ALLA SICUREZZA E ALLA GESTIONE DI ACCOUNT, CHE I MALWARE POSSONO SFRUTTARE PER MODIFICARE PERMESSI, ACCEDERE A TOKEN DI SICUREZZA E ALTERARE IL REGISTRO DI SISTEMA.**

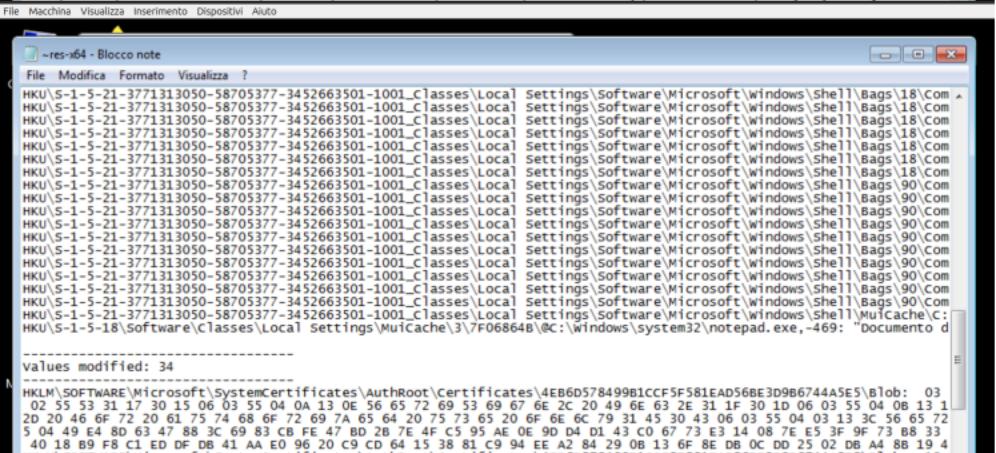
POSSO VEDERE LA CHIAVE DI REGISTRO **REG_SZ** (IDENTIFICATA DA **hKey**) A CUI, SEMPRE COME VISTO IN PRECEDENZA, VIENE ASSEGNAUTO IL VALORE DI **GINA.DLL**. QUESTO VALORE "MALEVOLO" VERRÀ SOVRASCITTTO NELLA LIBRERIA MSGINA32.DLL ANDANDONE SOSTITUIRE LA COPIA "SANA". IL MALWARE IN TAL MODO POTRÀ AVVIARSI AD OGNI LOGIN NEL CONTESTO DEL PROCESSO **WINLOGON**.

ANALISI DINAMICA

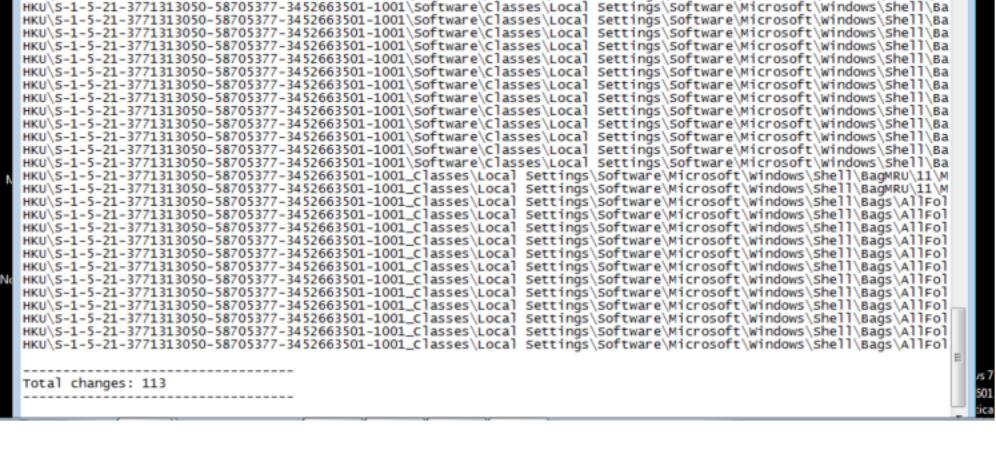
PASSATE ORA ALLA VISUALIZZAZIONE DELL'ATTIVITÀ SUL FILE SYSTEM.

- QUALE CHIAMATA DI SISTEMA HA MODIFICATO IL CONTENUTO DELLA CARTELLA DOVE È PRESENTE L'ESEGUIBILE DEL MALWARE? UNITE TUTTE LE INFORMAZIONI RACCOLTE FIN QUI SIA DALL'ANALISI STATICHE CHE DALL'ANALISI DINAMICA PER DELINEARE IL FUNZIONAMENTO DEL MALWARE.

FILTRANDO PER ATTIVITÀ SUL FILE SYSTEM VEDO UNA `CreateFile` (FUNZIONE CHE MODIFICA UN FILE ESISTENTE, O SE NON ESISTE NE CREA UNO NUOVO) AL FILE DI MSGINA32.DLL. QUESTA FUNZIONE è TIPICA DELLA LIBRERIA KERNEL32.DLL, CHE APPUNTO VIENE EVOCATA DAL MALWARE.



Dopo un confronto ottenuto tramite **REGSHTOOL** posso vedere che sono stati modificati 113 elementi tra cui 10 chiavi aggiunte, 1 cancellata; valori aggiunti 63, cancellati 5, modificati 34.



IN CONCLUSIONE SOMMANDO I DATI OTTENUTI DALL'ANALISI STATICHE + QUELLA DINAMICA POSSO EVINCERE CHE:

- IL MALWARE è UN TROJAN/DROPPER
- ALL'AVVIO GENERA UN FILE "SPORCO" NELLA CARTELLA DEL SUO ESEGUIBILE
- CERCA DI FARE UN PRIVILEGE ESCALATION ED OTTENERE "POTERI" AMMINISTRATIVI
- OTTIENE PERSISTENZA (ESECUSIONE AD OGNI AVVIO DEL SISTEMA OPERATIVO WINDOWS) MODIFICANDO UNA CHIAVE DI MSGINA32.DLL RESPONSABILE DEL LOGIN NEL CONTESTO DEL PROCESSO WINLOGON
- EVADE LA DIFESA INFILTRANDOSI IN UN PROCESSO COMUNE
- PUÒ OTTENERE L'ACCESSO ALLE CREDENZIALI DEGLI UTENTI
- PUÒ RACCOGLIERE DATI (CHE SALVA IN UN FILE CHIAMATO MSUTIL32.SYS -> SI PUÒ VEDERNE LA PRESENZA CON L'UTILITY STRINGS) E MONITORARE LE UTENZE

