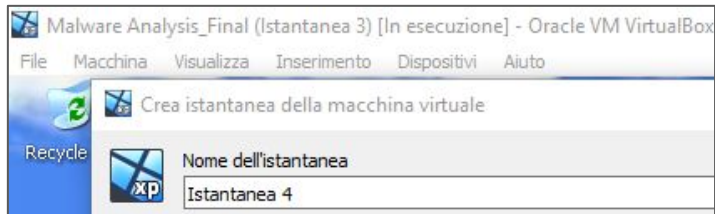


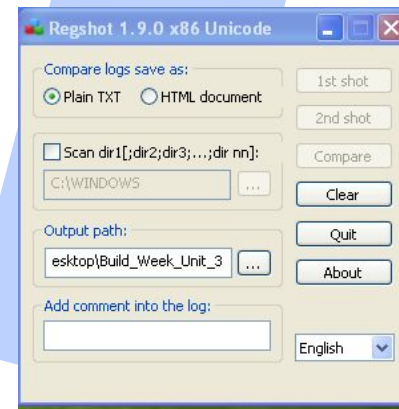
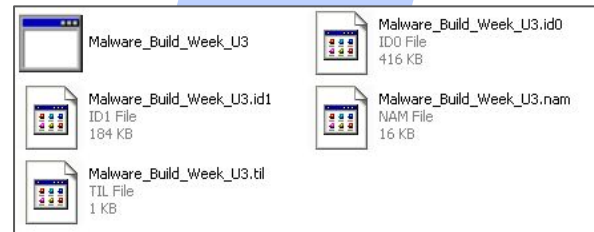
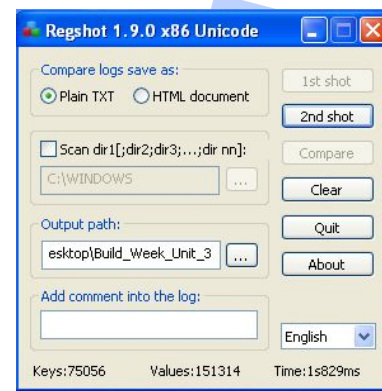


### Giorno 3:

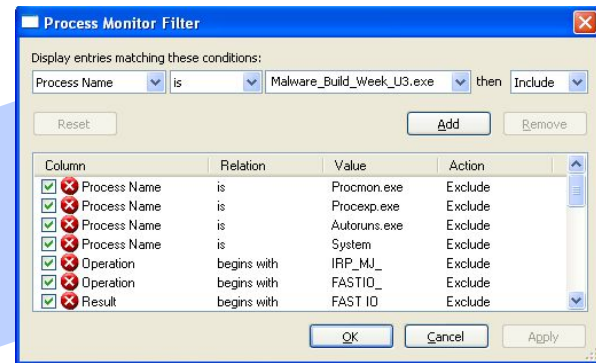
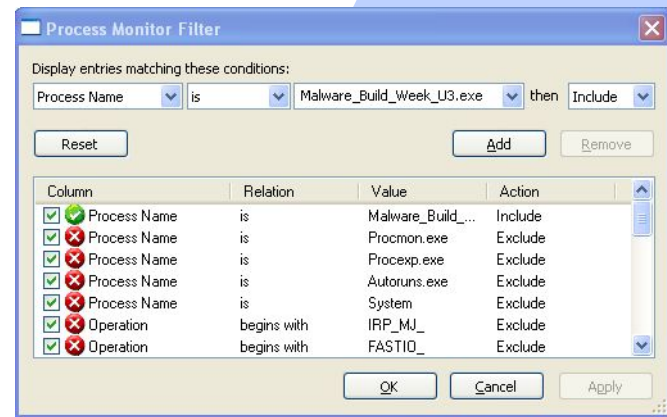
Preparate l'ambiente ed i tool per l'esecuzione del Malware (suggerimento: avviate principalmente Process Monitor ed assicurate di eliminare ogni filtro cliccando sul tasto «reset» quando richiesto in fase di avvio). Eseguite il Malware, facendo doppio click sull'icona dell'eseguibile



Per condurre l'analisi del malware del giorno 3, è essenziale preparare **un ambiente isolato dedicato all'analisi dinamica**. Creiamo un'istantanea della macchina virtuale. Successivamente, utilizziamo il software "Regshot" per acquisire **uno snapshot delle chiavi di registro**. Una volta completata questa fase preliminare, procediamo **all'esecuzione del malware**. Dopo aver eseguito il malware, acquisiamo un altro snapshot per identificare e visualizzare i cambiamenti effettuati nel registro di sistema dopo l'avvio del malware.


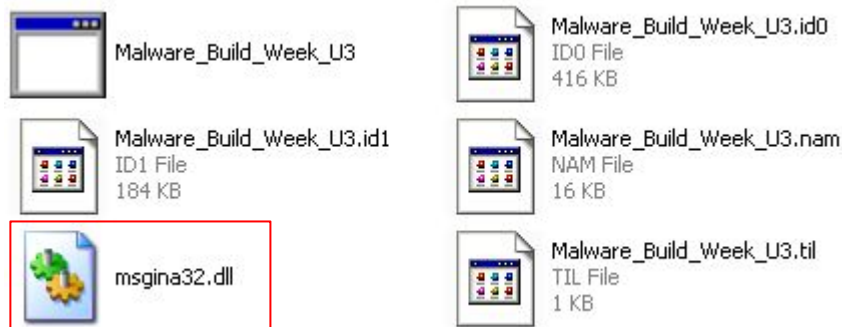


Eseguite il Malware, facendo doppio click sull'icona dell'eseguibile



In seguito analizziamo i risultati di Process Monitor **filtrando** il risultato con il nome del malware in questione

- 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



Process Monitor			
1020	CreateFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS
1020	CreateFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3	SUCCESS
1020	CloseFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3	SUCCESS
1020	WriteFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS
1020	WriteFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS

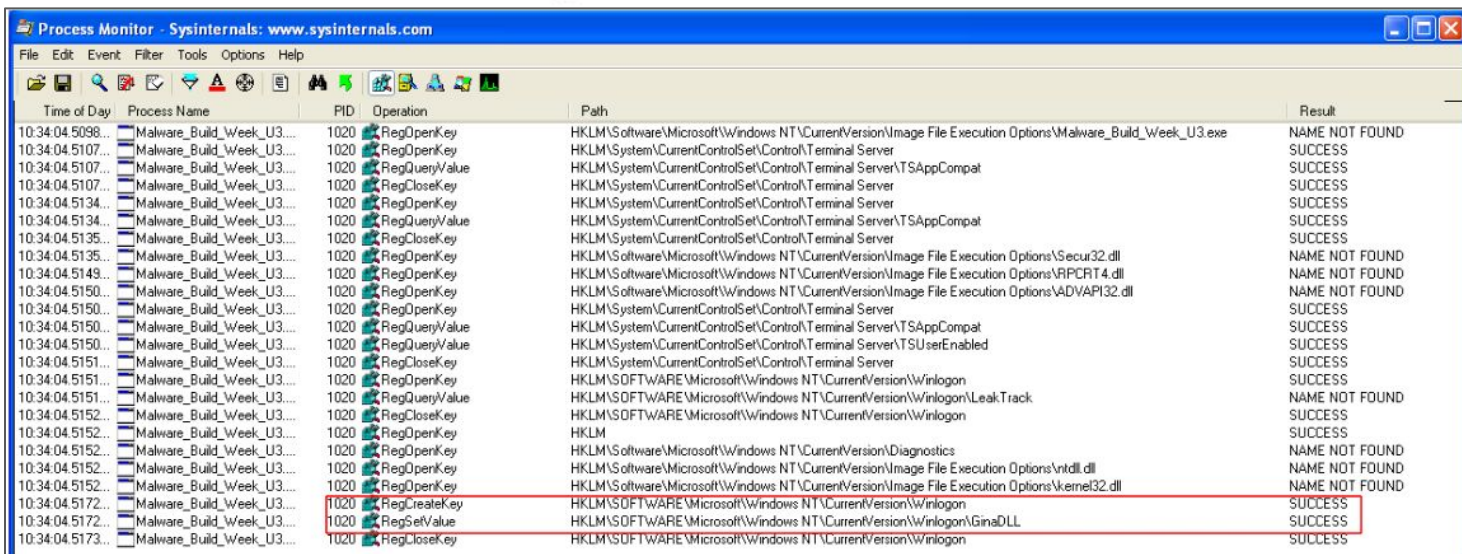
Tramite **Procmon** verifichiamo che l'eseguibile ha creato all'interno della cartella vari file tra cui **msgina32.dll**.

Il file "**msgina32.dll**" è un componente del sistema operativo Microsoft Windows. Esso è **responsabile dell'interfaccia di accesso di Windows** (GINA, Graphical Identification and Authentication) per le versioni precedenti di Windows come Windows XP e Windows Server 2003.

La libreria gestisce le funzioni di **autenticazione** e l'**interfaccia utente per il processo di accesso al sistema operativo**. Quando si avvia un computer con Windows XP o Windows Server 2003, l'interfaccia di accesso di Windows viene visualizzata, consentendo agli utenti di inserire le loro credenziali (come nome utente e password) per accedere al sistema.

Filtrate includendo solamente l'attività sul registro di Windows.

- Quale chiave di registro viene creata?
- Quale valore viene associato alla chiave di registro creata?



Time of Day	Process Name	PID	Operation	Path	Result
10:34:04.5098...	Malware_Build_Week_U3...	1020	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Malware_Build_Week_U3.exe	NAME NOT FOUND
10:34:04.5107...	Malware_Build_Week_U3...	1020	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS
10:34:04.5107...	Malware_Build_Week_U3...	1020	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	SUCCESS
10:34:04.5107...	Malware_Build_Week_U3...	1020	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS
10:34:04.5134...	Malware_Build_Week_U3...	1020	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS
10:34:04.5134...	Malware_Build_Week_U3...	1020	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	SUCCESS
10:34:04.5135...	Malware_Build_Week_U3...	1020	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS
10:34:04.5135...	Malware_Build_Week_U3...	1020	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Secur32.dll	NAME NOT FOUND
10:34:04.5143...	Malware_Build_Week_U3...	1020	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\RPCRT4.dll	NAME NOT FOUND
10:34:04.5150...	Malware_Build_Week_U3...	1020	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ADVAPI32.dll	NAME NOT FOUND
10:34:04.5150...	Malware_Build_Week_U3...	1020	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS
10:34:04.5150...	Malware_Build_Week_U3...	1020	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	SUCCESS
10:34:04.5150...	Malware_Build_Week_U3...	1020	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSUserEnabled	SUCCESS
10:34:04.5151...	Malware_Build_Week_U3...	1020	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS
10:34:04.5151...	Malware_Build_Week_U3...	1020	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS
10:34:04.5151...	Malware_Build_Week_U3...	1020	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\LeakTrack	NAME NOT FOUND
10:34:04.5152...	Malware_Build_Week_U3...	1020	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS
10:34:04.5152...	Malware_Build_Week_U3...	1020	RegOpenKey	HKLM	SUCCESS
10:34:04.5152...	Malware_Build_Week_U3...	1020	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Diagnostics	NAME NOT FOUND
10:34:04.5152...	Malware_Build_Week_U3...	1020	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ntdll.dll	NAME NOT FOUND
10:34:04.5152...	Malware_Build_Week_U3...	1020	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\kernel32.dll	NAME NOT FOUND
10:34:04.5172...	Malware_Build_Week_U3...	1020	RegCreateKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS
10:34:04.5172...	Malware_Build_Week_U3...	1020	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL	SUCCESS
10:34:04.5173...	Malware_Build_Week_U3...	1020	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS

Su ProcMon possiamo vedere la chiave di registro "HKLM(Local Machine)\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" creata dal comando "RegCreateKey" dal malware.

Con il comando "RegSetValue" viene associato il valore "GinaDLL".



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?

Process Monitor				
Malware_Build_Week_U3...	1020	CreateFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3	SUCCESS
Malware_Build_Week_U3...	1020	FileSystemControl	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3	SUCCESS
Malware_Build_Week_U3...	1020	QueryOpen	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\Malware_Build_Week_U3.exe.Local	NAME NOT FOUND
Malware_Build_Week_U3...	1020	CreateFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS
Malware_Build_Week_U3...	1020	CreateFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3	SUCCESS
Malware_Build_Week_U3...	1020	CloseFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3	SUCCESS
Malware_Build_Week_U3...	1020	WriteFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS
Malware_Build_Week_U3...	1020	WriteFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS
Malware_Build_Week_U3...	1020	CloseFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS
Malware_Build_Week_U3...	1020	CloseFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3	SUCCESS

La chiamata di sistema **CreateFile** con il PID 1020 sta creando il file **msgina32.dll** nel percorso **C:\Documents and Settings\Administrator\Desktop\Build\_Week\_Unit\_3\**.

La chiamata di sistema **“WriteFile”** è stata utilizzata dal malware per apportare modifiche al contenuto della cartella in cui si trova l'eseguibile dannoso. Il malware ha eseguito questa chiamata **due volte**: nella prima occasione, ha scritto il proprio contenuto all'interno del file “msgina32.dll”, sovrascrivendo il suo contenuto precedente. Successivamente, nella seconda chiamata **“WriteFile”**, il malware ha sovrascritto nuovamente il contenuto di **“msgina32.dll”**, presumibilmente per mascherare la propria presenza o per nascondere le sue attività dannose.

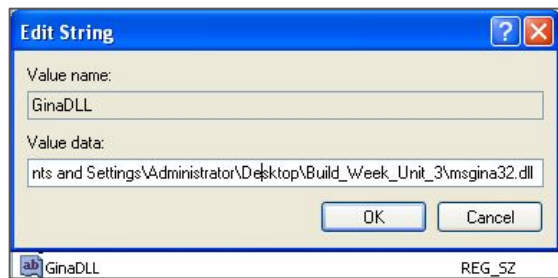
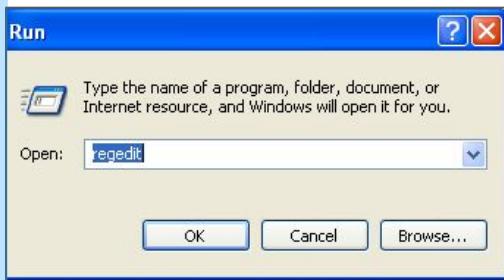
La chiamata di sistema **“WriteFile”** ha esito positivo in entrambi i casi. Ciò significa che i dati sono stati scritti correttamente nei file.

**Il malware è ora presente nel file “C:\Documents and Settings Administrator\Desktop\Build\_Week\_Unit\_3\msgina32.dll”**. Questo file può essere eseguito per infettare il sistema con il malware.

Unite tutte le informazioni raccolte fin qui sia dall'analisi statica che dall'analisi dinamica per delineare il funzionamento del Malware.

1020	CreateFile	C:\WINDOWS\system32\dwwin.exe
1020	CreateFileMapping	C:\WINDOWS\system32\dwwin.exe
1020	QueryStandardInformationFile	C:\WINDOWS\system32\dwwin.exe
1020	CreateFileMapping	C:\WINDOWS\system32\dwwin.exe

1020	CreateFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS
1020	CreateFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3	SUCCESS
1020	CloseFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3	SUCCESS
1020	WriteFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS
1020	WriteFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS



Con le **informazioni raccolte al momento** possiamo affermare la nostra teoria, il malware è un **Dropper** in quanto al suo interno contiene un file, **msgina32.dll**, che viene estratto al momento dell'esecuzione del file.

**Questo malware ottiene la persistenza creando una nuova chiave di registro con la chiamata di funzione RegCreateKeyExA e la modifica con un'altra chiamata di funzione RegSetValueExA.**