

Pratica S10-L2 Analisi dinamica basica

L'esercizio di oggi consiste nell'analizzare un malware attraverso un'analisi dinamica.

Come tool ho utilizzato Process Monitor e Regshot, una volta avviati i programmi ho lanciato il malware e possiamo vedere i risultati trovati:

1. File system

[illegible]

Qui possiamo notare come il malware si è inserito nel nostro pc e ha creato un nuovo processo chiamandosi svchost.exe mascherandosi in mezzo a tanti altri.

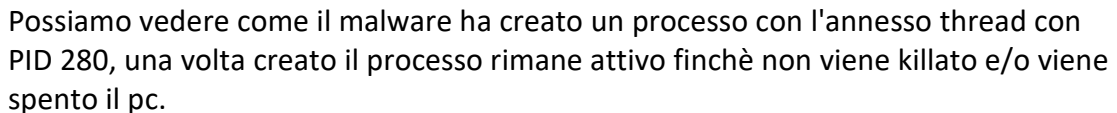
Qui sotto un dimostrazione:

The screenshot displays a Windows XP desktop environment. In the foreground, the 'Process Monitor - Sysinternals: www.sysinternals.com' window is open, showing a log of system events. The log includes columns for 'Time of Day', 'Process Name', 'PID', 'Operation', 'Path', 'Result', and 'Detail'. The events listed are related to the execution of 'Esercizio_Pratico_18.exe' and its associated processes, such as 'Process Start', 'Thread Create', 'Load Image', and 'Process Exit'.

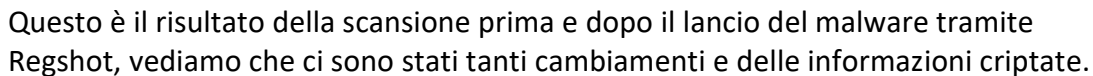
In the background, the 'Process Explorer - Sysinternals: www.sysinternals.com [MMLWARE_TEST\Administrator]' window is open, showing a list of running processes. The processes listed include 'apach2ng.exe', 'Process.exe', 'notepad.exe', and 'Esercizio_Pratico_18.exe'. The 'Esercizio_Pratico_18.exe' process is highlighted, showing its CPU usage, private bytes, working set, PID, description, and company name.

The desktop also features several icons: 'start', 'Esercizio_Pratico_18...', 'Shut', 'Apache2NG', and 'Process Monitor - Sys...'. The taskbar at the bottom shows the 'start' button and several open applications, including 'Esercizio_Pratico_18...', 'Shut', 'Apache2NG', 'Process Monitor - Sys...', 'Esercizio_Pratico_18...', and 'Process Explorer - Sys...'. The system clock in the bottom right corner indicates the time as 2:26 PM on 11/11/2011.

2.Processi e thread



3. Le modifiche di registro



Questo malware è un keylogger e possiamo notarlo perchè dentro la cartella del malware si è creato un file notepad dove teneva registrato tutto ciò che veniva

inserito con la tastiera e le applicazioni aperte.

