

Protect code execution

Once the operating system is configured to reduce the ability to execute malware or unauthorized access activity, it is necessary to review the characteristics and execution capabilities of the different applications and programs.

How do we know if a program we download from the Internet contains malware?

What tools are available in the operating system itself to prevent malware from running or minimize the impact if a malicious application is run?

Publishing a Hash associated with a file or program available for download makes it more difficult to modify the program with malware.

Windows PowerShell uses `get-filehash` to verify the signature of a file.

Cryptographic software signature

One of the best guarantees for running legitimate software is through the cryptographic signature of the program manufacturer. Digital certificate legitimizes the authorship of a product, and makes it very difficult to modify software to add malware.

There are some tools that allow you to verify the digital certificate associated with a certain manufacturer. From the properties of the executable image itself you can see the digital certificate. In addition, sysinternals tools offers us to verify that digital certificate.

Sigcheck

Sysinternals Suite tools are available for free download on the page <https://learn.microsoft.com/en-us/sysinternals/> there is a specific one to perform file signature checks: Sigcheck

usage: sigcheck [-a][-h][-i][-e][-l][-n][[-s][[-c]-ct]][-m][-q] [-r][-u][[-vt][[-v[r][s]]][-f catalog file] <file or directory>

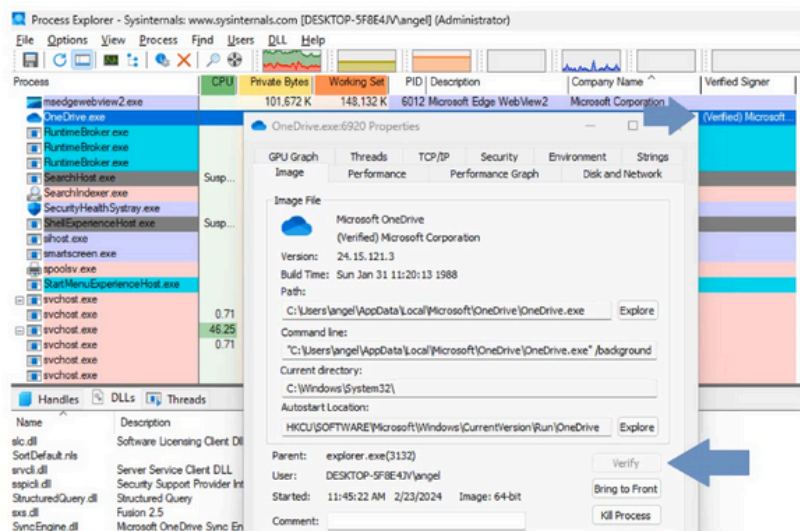
usage: sigcheck -d [-c]-ct <file or directory>

usage: sigcheck -o [-vt][[-v[r]]] <sigcheck csv file>

usage: sigcheck -t[u][v] [-i] [-c]-ct <certificate store name|*>

Sysinternals Suite: Process Explorer

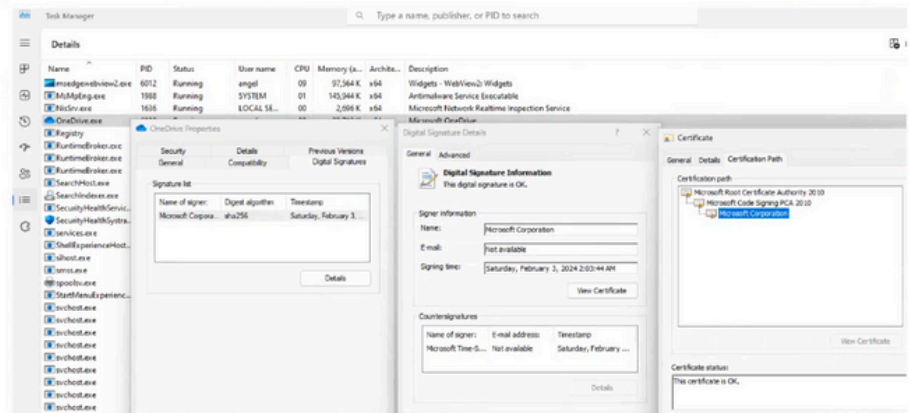
Process Explorer also allows you to verify the signature of an executable, even from the running process itself. In addition to being able to send or verify that process with Virus Total.



Pictures own elaboration

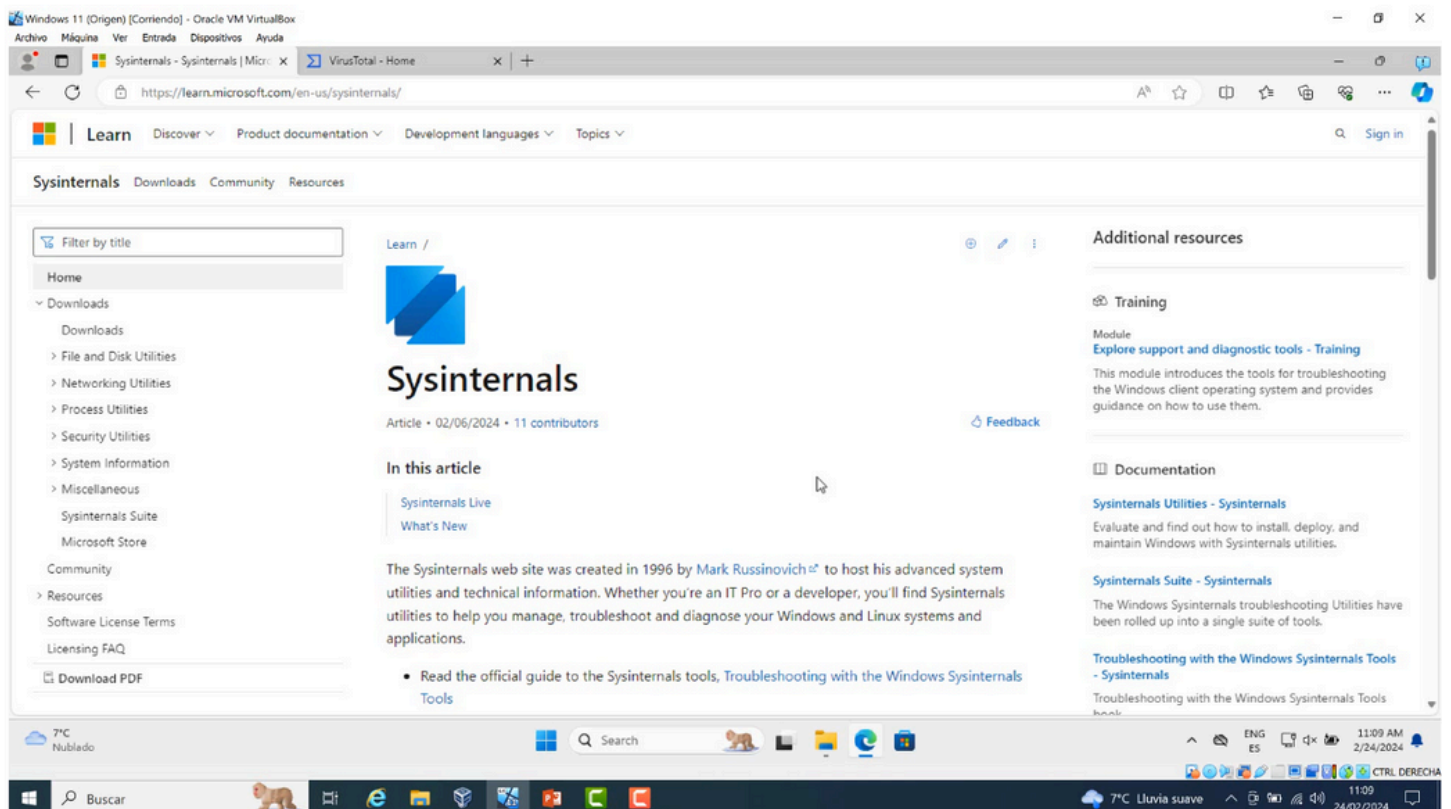
Demo

- Verify the digital certificate of a process from the Task manager.
- Verify that certificate from Process Explorer.



Pictures own elaboration

Sysinternals, presentación:



Windows 11 (Origen) [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Sysinternals Utilities - Sysinternals x VirusTotal - Home

https://learn.microsoft.com/en-us/sysinternals/downloads/

Learn Discover Product documentation Development languages Topics

Sysinternals Downloads Community Resources

Filter by title

Home

Downloads

File and Disk Utilities

Networking Utilities

Process Utilities

Security Utilities

System Information

Miscellaneous

Sysinternals Suite

Microsoft Store

Community

Resources

Software License Terms

Licensing FAQ

Download PDF

Sysinternals Utilities Index

Article • 02/13/2024 • 6 contributors

[Feedback](#)

Sysinternals Suite

The entire set of Sysinternals Utilities rolled up into a single download.

Sysinternals Suite for Nano Server

Sysinternals Utilities for Nano Server in a single download.

Sysinternals Suite for ARM64

Sysinternals Utilities for ARM64 in a single download.

Sysinternals Suite from the Microsoft Store

Sysinternals Utilities installation and updates via Microsoft Store.

AccessChk

v6.15 (May 11, 2022)

AccessChk is a command-line tool for viewing the effective permissions on files, registry keys, services, processes, kernel objects, and more.

Additional resources

Training

Module

[Explore support and diagnostic tools - Training](#)

This module introduces the tools for troubleshooting the Windows client operating system and provides guidance on how to use them.

Documentation

[Sysinternals - Sysinternals](#)

Library, learning resources, downloads, support, and community. Evaluate and find out how to install, deploy, and maintain Windows with Sysinternals utilities.

[Sysinternals Suite - Sysinternals](#)

The Windows Sysinternals troubleshooting Utilities have been rolled up into a single suite of tools.

[Troubleshooting with the Windows Sysinternals Tools - Sysinternals](#)

7°C Nublado

Search

ENG ES

11:10 AM 2/24/2024

7°C Lluvia suave

11:10 24/02/2024

Con Task manager, verificar la firma digital y el copyright:

Windows 11 (Origen) [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Task Manager

Type a name, publisher, or PID to search

Run new task End task

Name	PID	Status	User name	CPU	Memory (x...)	Archite...	Description
AggregatorHost.exe	2936	Running	SYSTEM	00	852 K	x64	Microsoft (R) Aggregator Host
ApplicationFrameHost.exe	1216	Running	angel	00	1,596 K	x64	Application Frame Host
audiohost.exe	7648	Running	LOCAL SE...	00	3,804 K	x64	Windows Audio Device Graph Isolation
backgroundTaskHost.exe	5332	Suspended	angel	00	0 K	x64	Background Task Host
backgroundTaskHost.exe	2292	Running	angel	00	1,408 K	x64	Background Task Host
backgroundTaskHost.exe	2252	Running	angel	00	1,320 K	x64	Background Task Host
backgroundTaskHost.exe	6900	Running	angel	00	1,476 K	x64	Background Task Host
conhost.exe	6684	Running	SYSTEM	00	5,244 K	x64	Console Window Host
csrss.exe	592	Running	SYSTEM	00	592 K	x64	Client Server Runtime Process
csrss.exe	668	Running	SYSTEM	02	668 K	x64	Client Server Runtime Process
ctfmon.exe	3,756	Running	angel	00	3,756 K	x64	CTF Loader
dihost.exe	1,412	Running	angel	00	1,412 K	x64	COM Surrogate
dihost.exe	944	Running	angel	00	944 K	x64	COM Surrogate
dwm.exe	57,988	Running	angel	03	57,988 K	x64	Desktop Window Manager
explorer.exe	67,596	Running	angel	01	67,596 K	x64	Windows Explorer
FileCoAuth.exe	2,616	Running	angel	00	2,616 K	x64	Microsoft OneDriveFile Co-Authenticating Executable
fontdrvhost.exe	152	Running	angel	00	152 K	x64	Usermode Font Driver Host
fontdrvhost.exe	1,960	Running	angel	00	1,960 K	x64	Usermode Font Driver Host
LockApp.exe	0	Running	angel	00	0 K	x64	LockApp.exe
lsass.exe	3,596	Running	angel	00	3,596 K	x64	Local Security Authority Process
MoUserCoreWork.exe	27,060	Running	angel	00	27,060 K	x64	MoIUSO Core Worker Process
MpDefenderCore.exe	1,700	Running	angel	00	1,700 K	x64	Antimalware Core Service
mscorsvw.exe	28,028	Running	angel	14	28,028 K	x64	.NET Runtime Optimization Service
msedge.exe	36,360	Running	angel	00	36,360 K	x64	Microsoft Edge
msedge.exe	548	Running	angel	00	548 K	x64	Microsoft Edge
msedge.exe	9,900	Running	angel	00	9,900 K	x64	Microsoft Edge
msedge.exe	8,816	Running	angel	00	8,816 K	x64	Microsoft Edge
msedge.exe	1,412	Running	angel	00	1,412 K	x64	Microsoft Edge
msedge.exe	1,600	Running	angel	00	1,600 K	x64	Microsoft Edge
msedge.exe	992	Running	angel	00	992 K	x64	Microsoft Edge
msedge.exe	35,980	Running	angel	00	35,980 K	x64	Microsoft Edge
msedge.exe	33,200	Running	angel	00	33,200 K	x64	Microsoft Edge

7°C Para la lluvia

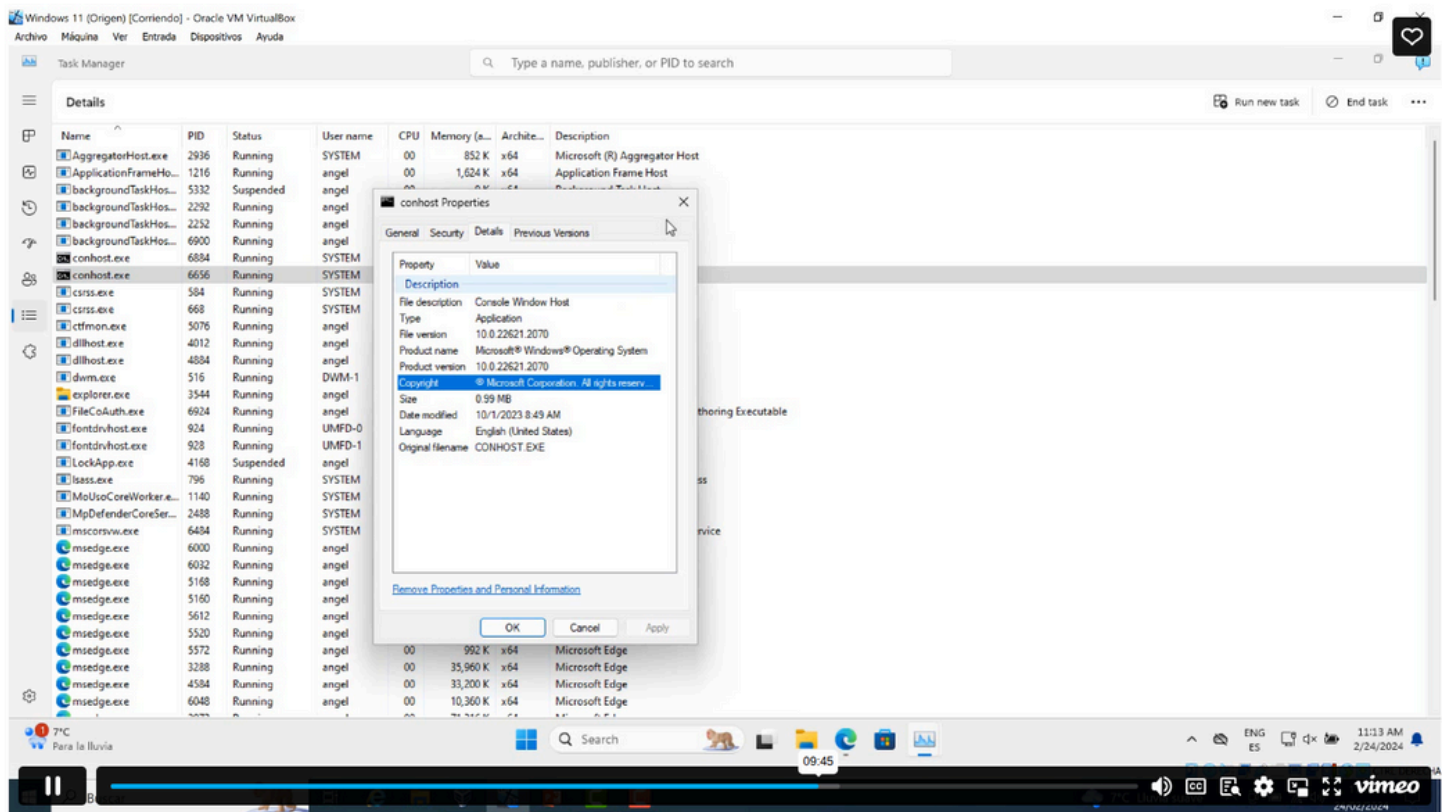
Search

ENG ES

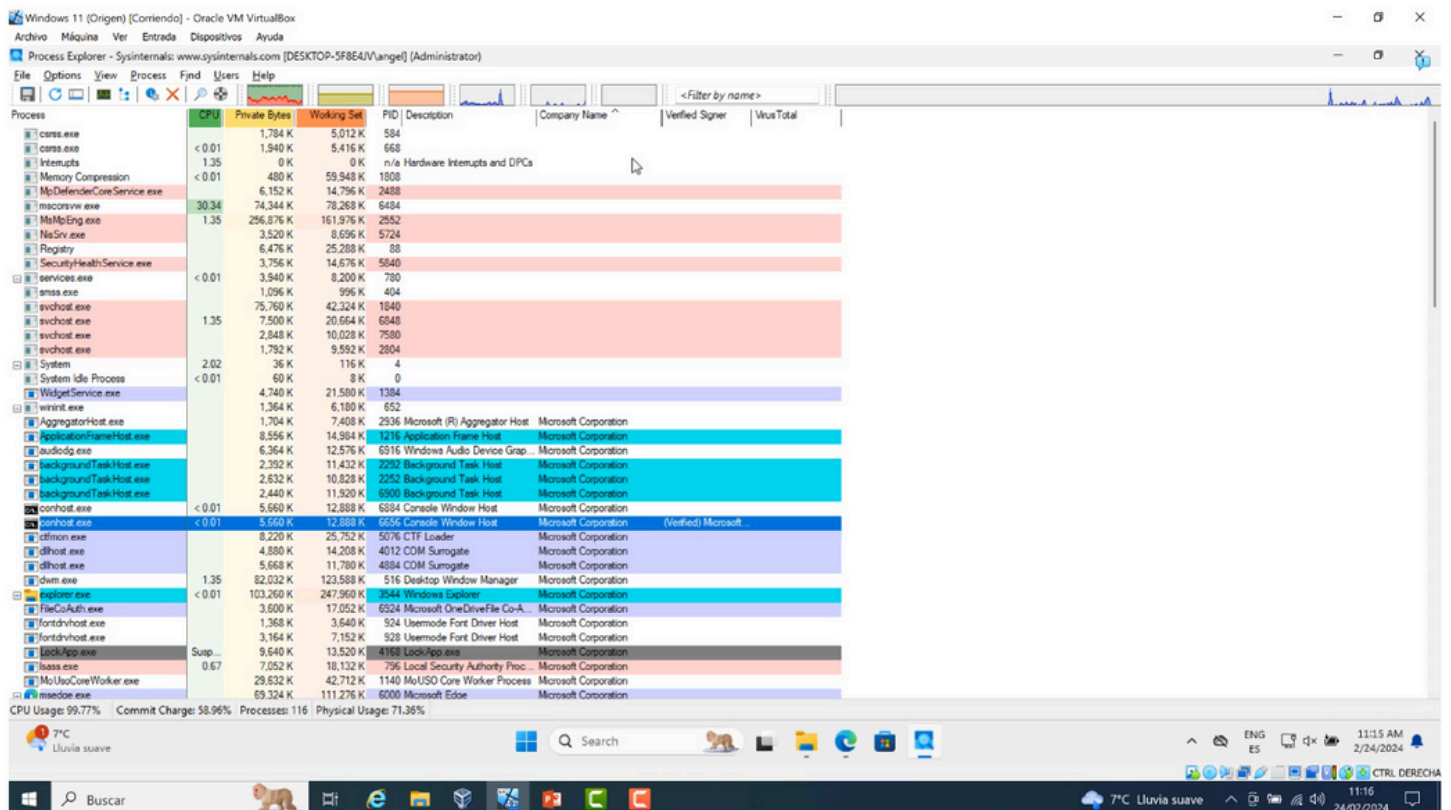
11:13 AM 2/24/2024

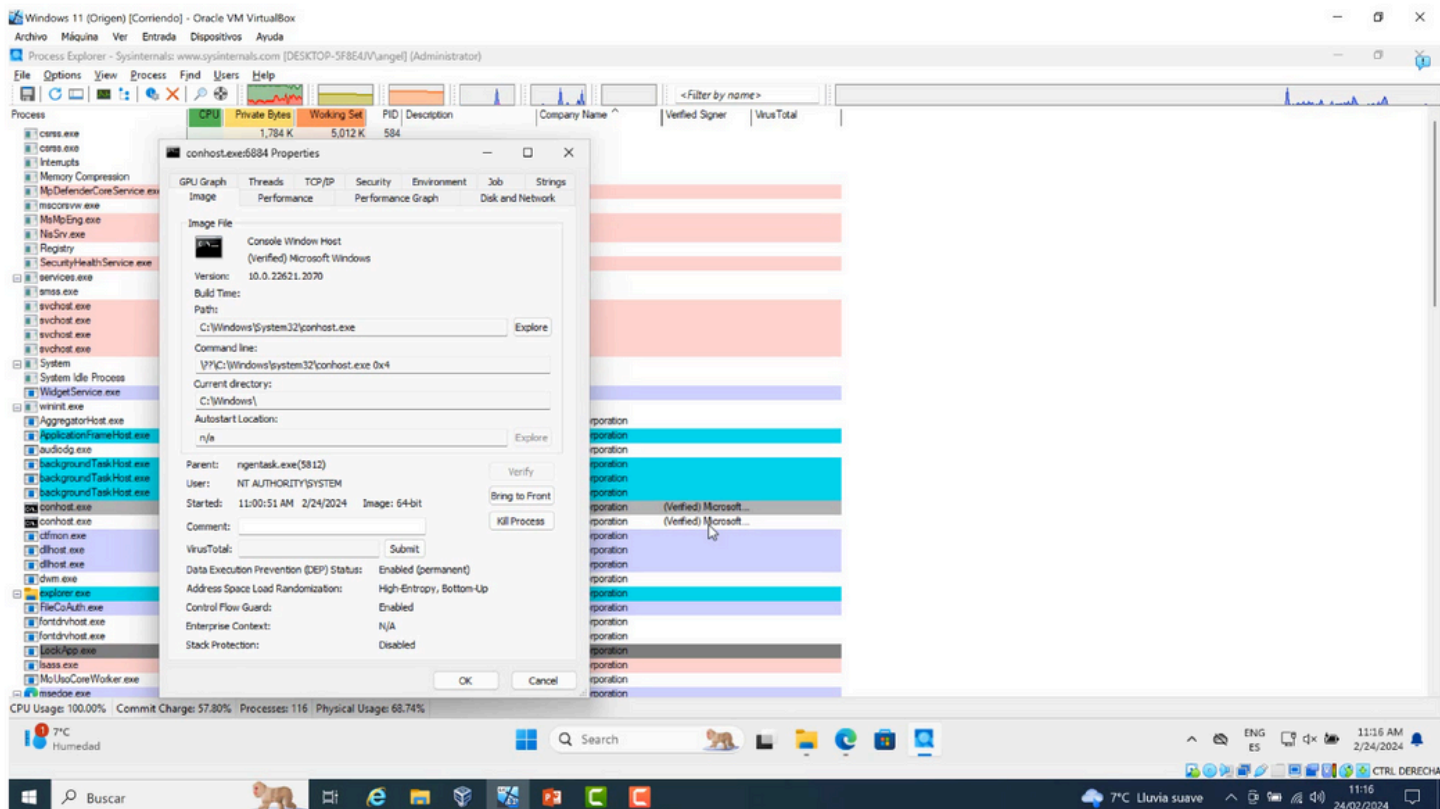
7°C Lluvia suave

11:13 24/02/2024

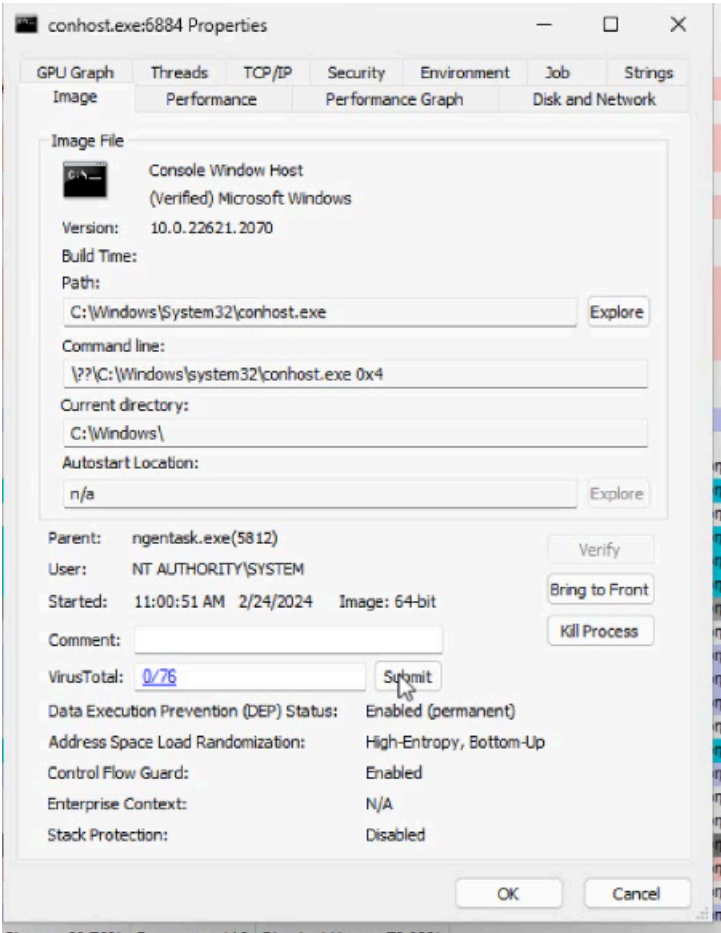


Vamos a verificar la firma digital usando Sysinternals ahora, mas preciso con process explorer:





Podemos enviarlo a Virus Total para mayor inspección, análisis con ese determinado hash del archivo en la base de datos de Virus Total:



Windows 11 (Origen) [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-SF864J\Angel] (Administrator)

File Options View Process Find Users Help

Run At Login

Verify Image Signatures

Process Name Private Bytes Working Set PID Description Company Name Verified Signer VirusTotal

Process Name Private Bytes Working Set PID Description Company Name Verified Signer VirusTotal

CPU Usage: 100.00% Commit Charge: 58.08% Processes: 116 Physical Usage: 69.02%

7°C Lluvia suave

Search

ENG ES

11:19 AM 2/24/2024

11:19 24/02/2024

Conclusions

- There are several tools that allow you to verify the origin of the software, in this way the execution of malicious software is prevented, or at least made more difficult.
- The sysinternals suite of tools offers us a wide number of utilities for different security purposes, such as the possibility of verifying digital certificates associated with the signing of programs and applications.



Singularity Hackers

0xWORD



My Public
Inbox