

# **C.5 MATERIALE ȘI METODE ÎN INGINERIA ÎNVERSĂ (II)**

**PAUL A. GAGNIUC**



**Academia Tehnică Militară „Ferdinand I”**

# **PRINCIPALELE PĂRȚI ALE PREZENTĂRII**

---

**C.5 Materiale și metode în ingineria inversă:**

- **C.5.2 INSTRUMENTELE DE INGINERIE INVERSĂ (II)**
- **C.5.3 AUTOMATIZAREA MAȘINII VIRTUALE**
- **C.5.4 MOSTRE MALWARE & PROTOCOALE DE MANIPULARE**

# PACHETUL DE FIŞIERE PENTRU INSTRUMENTE

- kit\Gazda\VirtualBox.exe
- kit\Gazda\win7.iso
- kit\Gazda\IDA.zip
  
- kit\Gazda\PEstudioX86.zip
- kit\Gazda\Cutter.zip
- kit\Gazda\x64dbg.zip
- kit\Masina Virtuala\sysinternals.zip
- kit\Masina Virtuala\wireshark.zip
- kit\Masina Virtuala\procdot.zip
- kit\Masina Virtuala\pestudio.zip
- kit\Masina Virtuala\BCompare.exe

(Gazdă)

(Masina Virtuală)

C.5.2

# INSTRUMENTELE DE INGINERIE INVERSĂ



Metodologie:



## Analiza Statică

Măsoară potențialul



## Analiza Dinamică

Observați comportamentul



## Analiza Cloud

La distanță:  
potențial și comportament

# ANALIZA DINAMICĂ:



Observatie/Comportament

# COD MALIȚIOS: INSTRUMENTE DE ANALIZĂ

■ PEStudio

■ Bcompare

■ Cutter & IDA & x64dbg

■ **Sysinternals**

■ Wireshark

■ procDOT

■ Analiza malware in Cloud

Analiză Statică

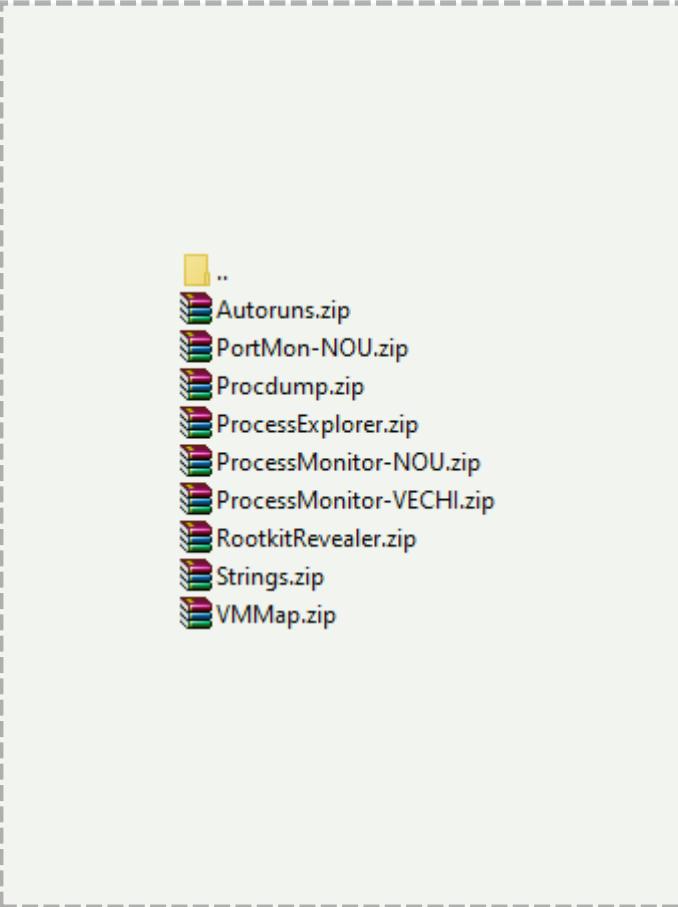
Analiză Dinamică

Analiză Cloud



# SYSTEM INTERNALS

## APLICATII CRITICE



- ..
- Autoruns.zip
- PortMon-NOU.zip
- Procdump.zip
- ProcessExplorer.zip
- ProcessMonitor-NOU.zip
- ProcessMonitor-VECHI.zip
- RootkitRevealer.zip
- Strings.zip
- VMMMap.zip

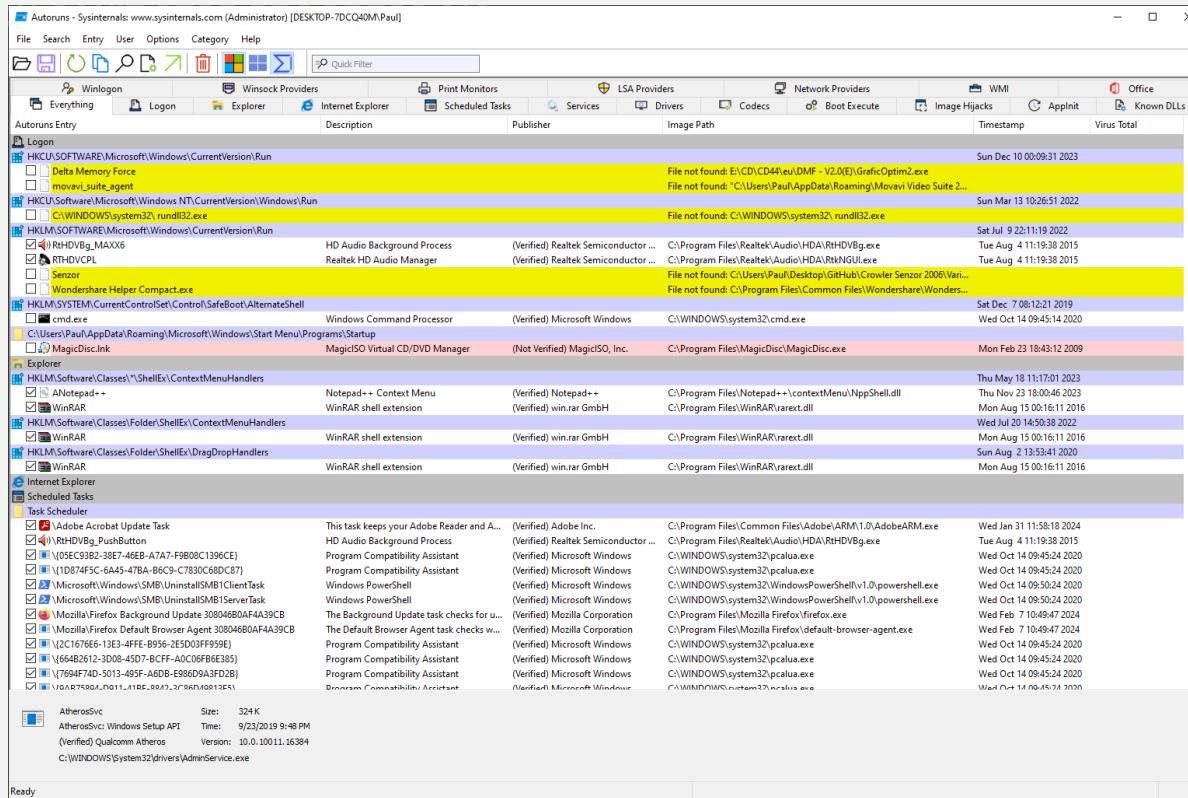
sysinternals

Process  
Monitor

Process  
Explorer

# AUTORUNS

## PRINCIPALELE CARACTERISTICI ALE AUTORUNS INCLUD:



**Detalierea Extinsă.** Autoruns identifică și afișează locațiile din care se lansează automat programe, inclusiv cheile de registry Run, Task Scheduler, serviciile Windows, driverele de dispozitiv, extensiile shell de browser, toolbar-uri, obiecte de ajutor pentru browser, programe de start din folderele de pornire și multe altele.

**Filtrarea și Căutarea.** Utilitarul permite utilizatorilor să filtreze intrările pe care nu doresc să le vadă sau să caute anumite programe care se execută la start-up, făcând mai ușoară identificarea și gestionarea elementelor nedorite sau suspecte.

**Dezactivarea sau Ștergerea Elementelor.** Autoruns nu doar că afișează programele și serviciile care se execută automat, dar oferă și posibilitatea de a dezactiva sau elimina intrările, ajutând în optimizarea start-up-ului și îmbunătățirea performanței generale a sistemului.

**Identificarea Malware-ului.** Este frecvent utilizat în depanarea sistemelor și identificarea software-ului rău intenționat sau a programelor nedorite care se execută automat, adesea fără știrea utilizatorului.

**Verificarea Semnăturilor Digitale.** Autoruns poate verifica semnăturile digitale ale fișierelor executabile, ajutând la distingerea între software-ul legitim și cel potențial nesigur sau neautorizat.

# PROCESS MONITOR

## ANALIZA UNUI MALWARE ÎNTR-O MAȘINĂ VIRTUALĂ (VM)

### I. Activitatea Proceselor

- Crearea și terminarea proceselor.** Observați procesele create de malware. Anumite malware-uri pot lansa noi procese, fie pentru a executa sarcini specifice, fie pentru a se masca.
- Relațiile între procese.** Identificați dacă malware-ul creează procese copil sau dacă interacționează cu alte procese existente.

### 2. Modificări în Sistemul de Fișiere

- Crearea, modificarea și ștergerea fișierelor.** Fiți atenți la fișierele create sau modificate de malware, deoarece acestea pot indica activități precum extracția de date, instalarea de componente suplimentare sau încercări de persistență.
- Accesări suspecte de fișiere.** Monitorizați accesul la fișiere de configurare sau sistem, care ar putea sugera încercări de modificare a setărilor sistemului.

### 3. Modificări în Registri

- Crearea, modificarea și ștergerea cheilor de registru.** Malware-ul adesea modifică registrii pentru a asigura persistența, a modifica setările sistemului sau a dezactiva funcții de securitate.
- Acces la registri specifici.** Observați accesul la chei de registru ce controlează autorun, servicii, sau setări de rețea.

### 4. Activitatea de Rețea

- Conexiuni de rețea.** Monitorizați orice încercare de conexiune la adrese IP sau domenii externe, ceea ce poate indica comunicații cu un server de comandă și control (C&C) sau încercări de exfiltrare a datelor.
- Modificări ale setărilor de rețea.** Verificați dacă malware-ul modifică setările de rețea, cum ar fi proxy-uri sau DNS.

### 5. Hook-uri și DLL-uri Injectate

- Injectarea de cod.** Multe tipuri de malware injectează cod în alte procese pentru a executa operațiuni în mod ascuns sau pentru a obține drepturi de acces mai mari.
- Modificări ale DLL-urilor.** Atunci când un malware adaugă sau modifică DLL-uri, poate afecta funcționalitatea sistemului sau poate obține funcționalități suplimentare.

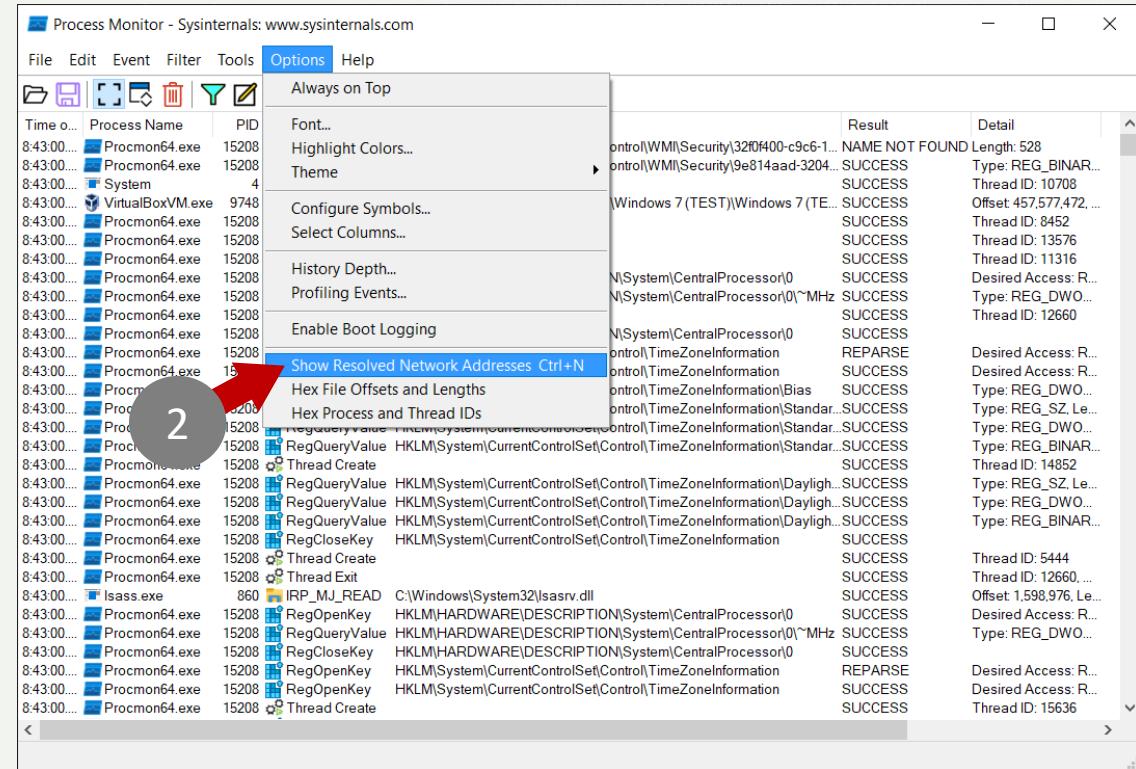
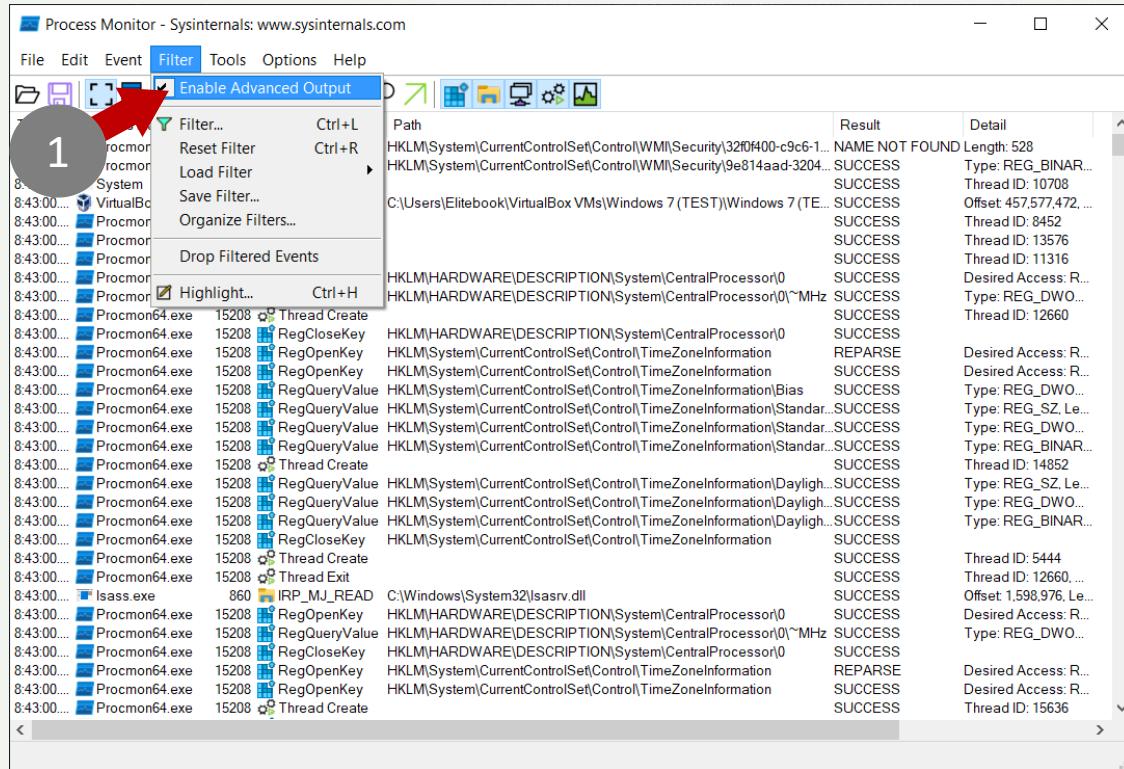
## SFATURI GENERALE

### PROCESS MONITOR

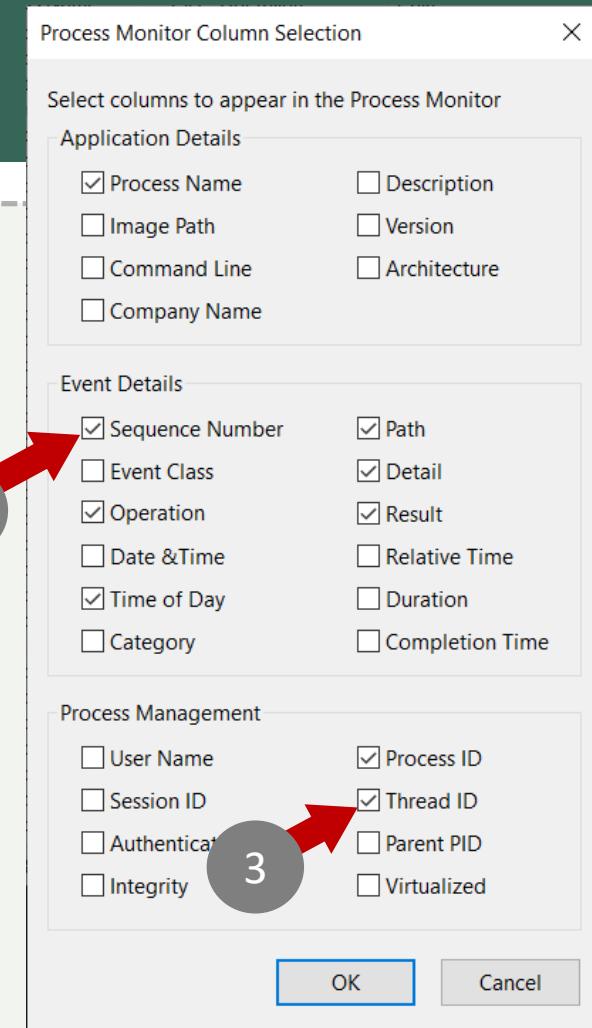
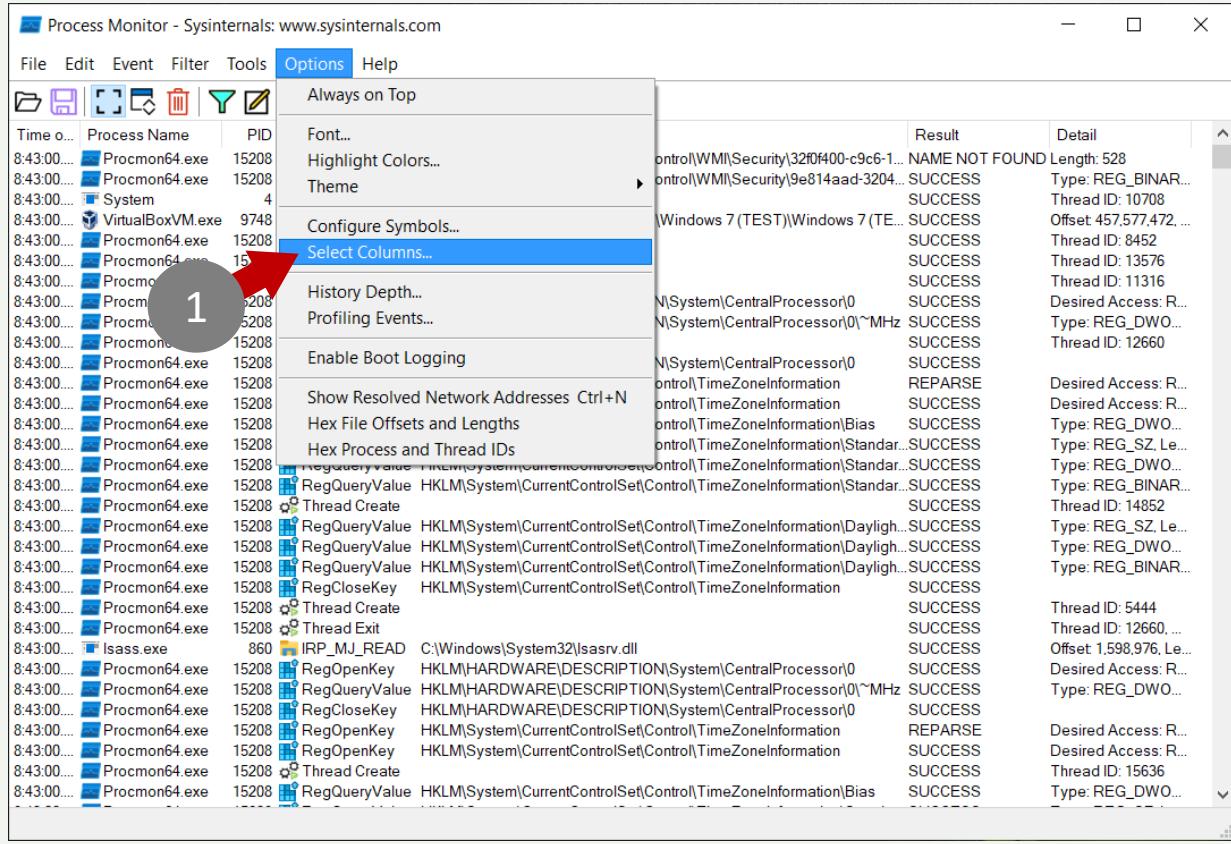
- **Filtrați și sortați datele.** Utilizați filtrele Process Monitor pentru a izola activitățile suspecte și a reduce zgomotul de fundal al activităților sistemului normal.
- **Exportați și salvați logurile.** Salvați logurile de monitorizare pentru analiză ulterioară și pentru a avea un punct de referință.
- **Utilizați snapshot-uri ale VM-ului.** Faceți snapshot-uri înainte și după detonarea malware-ului pentru a putea reveni rapid la o stare cunoscută și curată.
- **Folosiți alte unelte de analiză.** Complementați analiza cu alte unelte de securitate, cum ar fi antivirus, analizor de trafic de rețea, și unelte de analiză de malware pentru o imagine de ansamblu completă.

# PROCESS MONITOR

## SETUP PENTRU SALVAREA JURNALULUI (ORDINEA COLOANELOR)



# PROCESS MONITOR SETUP



# PROCESS EXPLORER

## OFERĂ O VEDERE DETALIATĂ A PROCESELOR CARE RULEAZĂ PE UN SISTEM

- **Identificarea Proceselor Malware.** Urmăriți procesele noi sau necunoscute care apar după detonarea malware-ului. Malware-ul adesea lansează procese care pot avea nume similare cu procesele de sistem legitime, dar se execută din locații neobișnuite.
- **Verificarea Lanțurilor de Procese.** Process Explorer afișează procesele într-o structură ierarhică, care poate fi folosită pentru a identifica relațiile dintre procese. Verificați dacă procesele suspecte sunt lansate de alte aplicații sau servicii.
- **Analiza Detaliilor Procesului.** Faceți clic dreapta pe un proces pentru a accesa opțiuni precum "Properties" pentru a vedea detaliile, inclusiv locația fișierului executabil, firul de execuție, DLL-urile încărcate și cheile de registru asociate. Acest lucru poate ajuta la identificarea activității suspecte și a metodelor de persistență.
- **Monitorizarea Utilizării Resurselor.** Un malware poate consuma resurse semnificative, cum ar fi CPU, memorie sau accesul la rețea. Folosiți coloanele din Process Explorer pentru a urmări utilizarea resurselor și pentru a identifica procesele care se comportă anormal.
- **Verificarea Conexiunilor de Rețea.** Malware-ul poate încerca să comunice cu serverele de comandă și control (C&C) sau să transmită date sensibile. Verificați secțiunea "TCP/IP" în proprietățile procesului pentru a vedea activitatea rețelei.
- **Analiza DLL-urilor Încărcate.** Malware-ul poate injecta DLL-uri rele în procesele legitime pentru a ascunde activitatea sa. Verificați DLL-urile încărcate de procese pentru orice fișiere necunoscute sau suspecte.
- **Utilizarea Culorilor pentru Identificare.** Process Explorer folosește culori diferite pentru a marca diferențe tipuri de procese (de exemplu, procesele de sistem, procesele de rețea, etc.). Aceasta poate fi o modalitate rapidă de a identifica procesele care merită investigații suplimentare.
- **Scanarea Online a Proceselor.** Process Explorer permite utilizatorilor să scanzeze procesele cu *VirusTotal* direct din interfață. Aceasta este o modalitate excelentă de a verifica rapid dacă un proces este recunoscut ca fiind malware de către multiple motoare antivirus.

# PROCESS EXPLORER

## UN TASK MANAGER AVANSAT

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-7DCQ40M\Paul]

File Options View Process Find Users Help

Process CPU Private Bytes Working Set PID Description Company Name

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry	5,820 K	48,224 K	100			
System Idle Process	78.87	40 K	4 K	0		
System	2.27	68 K	1,480 K	4		
Interrupts	1.14	0 K	n/a	Hardware Interrupts and DPCs		
smss.exe		312 K	544 K	448		
Memory Compression	< 0.01	1,048 K	38,804 K	1696		
csrss.exe	< 0.01	1,116 K	2,996 K	672		
wininit.exe	1,092 K	2,696 K	760			
services.exe	0.38	3,144 K	5,044 K	972		
svchost.exe	< 0.01	7,460 K	11,860 K	1140 Host Process for Windows S... Microsoft Corporation		
StartMenuExperience...		15,108 K	19,344 K	1276		
RuntimeBroker.exe	4,392 K	4,760 K	1960 Runtime Broker	Microsoft Corporation		
SearchApp.exe	Susp...	92,952 K	49,220 K	2416 Search application	Microsoft Corporation	
RuntimeBroker.exe	12,244 K	24,836 K	4244 Runtime Broker	Microsoft Corporation		
TextInputHost.exe	8,020 K	9,852 K	5636	Microsoft Corporation		
RuntimeBroker.exe	2,856 K	7,332 K	4340 Runtime Broker	Microsoft Corporation		
UserOOBEBroker.exe	1,436 K	3,852 K	4040 User OOBE Broker	Microsoft Corporation		
SettingSyncHost.exe	1,988 K	2,716 K	7748 Host Process for Setting Syn...	Microsoft Corporation		
TlWorker.exe	63,084 K	3,112 K	8016			
WmiPrvSE.exe	3,548 K	9,592 K	8004			
ShellExperienceHost....	Susp...	12,936 K	28,272 K	7832 Windows Shell Experience H...	Microsoft Corporation	
RuntimeBroker.exe	4,272 K	16,804 K	5804 Runtime Broker	Microsoft Corporation		
dllhost.exe	3,228 K	10,400 K	5960 COM Surrogate	Microsoft Corporation		
smartscreen.exe	7,572 K	19,540 K	1396 Windows Defender SmartScr...	Microsoft Corporation		
WmiPrvSE.exe	2,264 K	8,208 K	7244			
SppExtComObj.Exe	1,580 K	8,744 K	596			
svchost.exe	< 0.01	5,172 K	10,164 K	1260 Host Process for Windows S...	Microsoft Corporation	
svchost.exe		45,928 K	34,472 K	1384 Host Process for Windows S...	Microsoft Corporation	
sihost.exe		4,804 K	13,428 K	4672 Shell Infrastructure Host	Microsoft Corporation	

CPU Usage: 21.23% Commit Charge: 49.21% Processes: 99 Physical Usage: 81.87%

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-7DCQ40M\Paul]

File Options View Process Find Users Help

Process CPU Private Bytes Working Set PID Description Company Name

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry	5,840 K	48,268 K	100			
System Idle Process	91.66	40 K	4 K	0		
System	0.38	68 K	1,488 K	4		
Interrupts	0.75	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		312 K	544 K	448		
Memory Compression	< 0.01	1,048 K	36,280 K	1696		
csrss.exe		1,092 K	2,988 K	672		
wininit.exe		1,092 K	2,696 K	760		
services.exe		3,144 K	5,072 K	972		
svchost.exe	< 0.01	7,460 K	11,860 K	1140 Host Process for Windows S... Microsoft Corporation		
StartMenuExperience...		15,108 K	19,344 K	1276		
RuntimeBroker.exe	4,392 K	4,760 K	1960 Runtime Broker	Microsoft Corporation		
SearchApp.exe	Susp...	92,952 K	49,220 K	2416 Search application	Microsoft Corporation	
RuntimeBroker.exe	12,184 K	24,828 K	4244			
TextInputHost.exe	8,084 K	9,852 K	5636	Microsoft Corporation		
RuntimeBroker.exe	2,856 K	7,332 K	4340	Microsoft Corporation		
UserOOBEBroker.exe	1,436 K	3,852 K	4040	Microsoft Corporation		
SettingSyncHost.exe	1,988 K	2,716 K	7748	Microsoft Corporation		
TlWorker.exe	63,084 K	3,112 K	8016			
WmiPrvSE.exe	3,636 K	9,696 K	8004			
ShellExperienceHost....	Susp...	12,936 K	14,088 K	7832		
RuntimeBroker.exe	4,272 K	16,804 K	5804			
dllhost.exe	3,228 K	10,400 K	5960			
smartscreen.exe	7,572 K	19,540 K	1396	Microsoft Corporation		
WmiPrvSE.exe	2,264 K	8,208 K	7244			
SppExtComObj.Exe	1,604 K	8,772 K	596			
svchost.exe	< 0.01	5,156 K	10,148 K	1260		
svchost.exe		46,084 K	34,812 K	1384		
sihost.exe		4,804 K	13,428 K	4672		

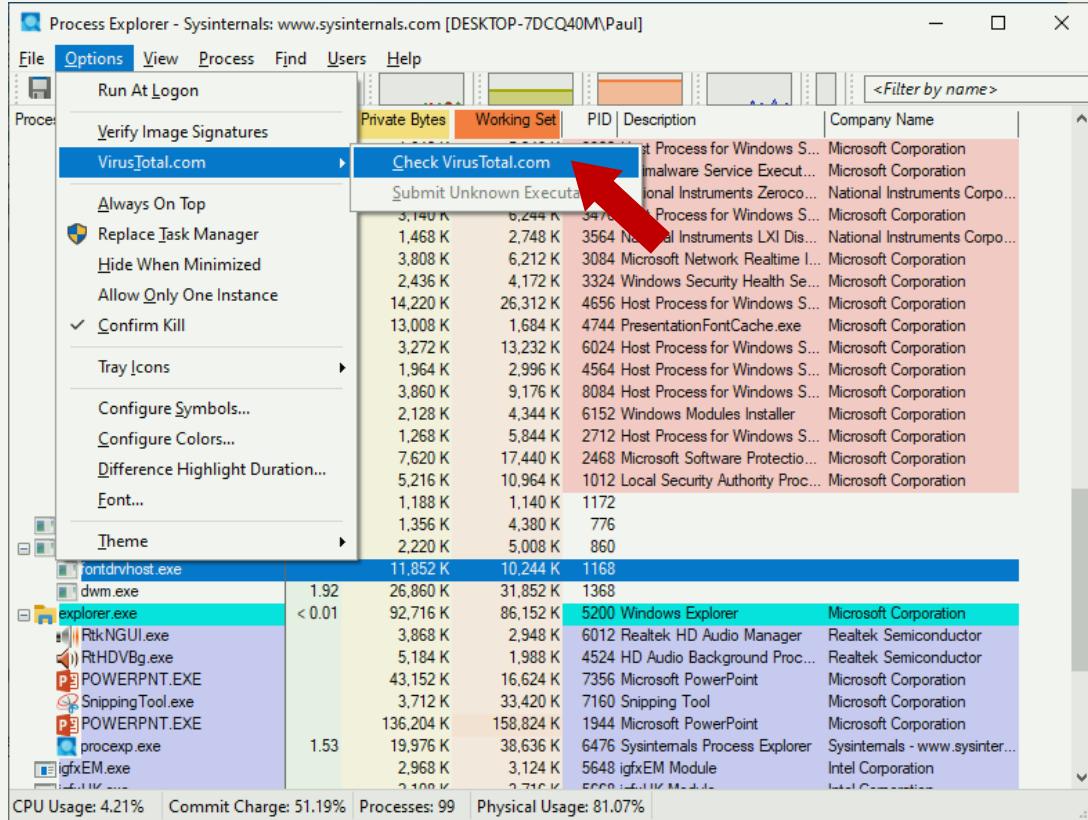
CPU Usage: 9.02% Commit Charge: 51.12% Processes: 99 Physical Usage: 84.1

Context menu options shown for the selected process (svchost.exe, PID 1140):

- Window
- Set Affinity...
- Set Priority
- Kill Process
- Kill Process Tree
- Shift+Del
- Restart
- Suspend
- Create Dump
- Check VirusTotal.com
- Properties...
- Search Online...
- Ctrl+M

# PROCESS EXPLORER

## COLABORAREA CU VIRUSTOTAL

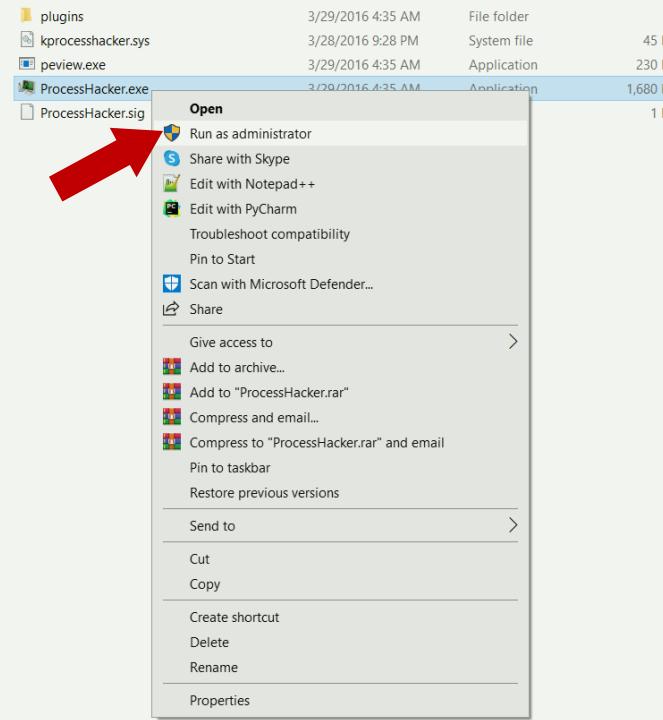


The screenshot shows a list of processes from Process Explorer. The table includes columns for Process, CPU, Private Bytes, Working Set, PID, Description, Company Name, and VirusTotal score. The processes listed are mostly system services and drivers, with some Microsoft and Realtek components.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	VirusTotal
SearchApp.exe	Susp...	92,952 K	3,500 K	2416	Search application	Microsoft Corporation	0/75
RuntimeBroker.exe		12,184 K	8,704 K	4244	Runtime Broker	Microsoft Corporation	0/73
TextInputHost.exe		8,024 K	9,588 K	5636		Microsoft Corporation	0/75
RuntimeBroker.exe		2,856 K	7,044 K	4340	Runtime Broker	Microsoft Corporation	0/73
UserOOBEBroker.exe		1,428 K	3,620 K	4040	User OOBE Broker	Microsoft Corporation	0/75
SettingSyncHost.exe		1,988 K	2,340 K	7748	Host Process for Setting Sync...	Microsoft Corporation	0/75
TlWorker.exe		63,084 K	3,008 K	8016			
WmiPrvSE.exe		3,404 K	9,680 K	8004			
ShellExperienceHost...		12,936 K	7,048 K	7832	Windows Shell Experience H...	Microsoft Corporation	0/75
RuntimeBroker.exe		4,272 K	8,508 K	5804	Runtime Broker	Microsoft Corporation	0/73
dllhost.exe		3,168 K	5,688 K	5960	COM Surrogate	Microsoft Corporation	0/75
smartscreen.exe		7,584 K	9,468 K	1396	Windows Defender SmartScr...	Microsoft Corporation	0/74
SppExtComObj.Exe		1,612 K	8,356 K	596			
svchost.exe	< 0.01	5,176 K	9,624 K	1260	Host Process for Windows S...	Microsoft Corporation	0/77
svchost.exe		45,664 K	17,528 K	1384	Host Process for Windows S...	Microsoft Corporation	0/77
sihost.exe		4,804 K	9,580 K	4672	Shell Infrastructure Host	Microsoft Corporation	0/73
taskhostw.exe		6,404 K	8,568 K	4948	Host Process for Windows T...	Microsoft Corporation	0/74
RtHDVBg.exe	< 0.01	5,360 K	1,332 K	5460	HD Audio Background Proc...	Realtek Semiconductor	0/76
svchost.exe	0.38	45,708 K	26,408 K	1480	Host Process for Windows S...	Microsoft Corporation	0/77
dasHost.exe		2,252 K	4,248 K	1632			
cfdmon.exe		9,164 K	10,772 K	5220			
WUDFHost.exe		1,520 K	3,436 K	1732			
svchost.exe		1,988 K	4,868 K	1740	Host Process for Windows S...	Microsoft Corporation	0/77
svchost.exe		8,556 K	11,256 K	1748	Host Process for Windows S...	Microsoft Corporation	0/77
svchost.exe		17,944 K	11,728 K	1756	Host Process for Windows S...	Microsoft Corporation	0/77
igfxCUIService.exe		11,788 K	13,048 K	1928	Host Process for Windows S...	Microsoft Corporation	0/77
svchost.exe		1,572 K	4,336 K	384	igfxCUIService Module	Intel Corporation	0/76
svchost.exe		1,824 K	4,936 K	936	Host Process for Windows S...	Microsoft Corporation	0/77
svchost.exe		7,556 K	10,656 K	952	Host Process for Windows S...	Microsoft Corporation	0/77
audiogd.exe	< 0.01	5,156 K	9,608 K	2072	Host Process for Windows S...	Microsoft Corporation	0/77
RtkAudioService.exe		60,520 K	40,128 K	7972			
RtHDVBg.exe		1,308 K	3,216 K	2284	Realtek Audio Service	Realtek Semiconductor	0/76
RtHDVBg.exe		5,480 K	1,196 K	2556			
svchost.exe		5,224 K	1,312 K	2568			
svchost.exe		1,328 K	3,424 K	2352	Host Process for Windows S...	Microsoft Corporation	0/77
svchost.exe		2,192 K	5,400 K	2360	Host Process for Windows S...	Microsoft Corporation	0/77

# PROCESS HACKER

## RULARE (VIZUALIZAREA SECTIUNILOR EXE (PE) INCARCATE IN MEMORIE)



Name	PID	CPU	I/O total r...	Private by...	User name	Description
System Idle Process	0	86.83	60 kB	NT AUTHORITY\SYSTEM		
System	4	0.36	200 kB	NT AUTHORITY\SYSTEM	NT Kernel & System	Windows Session Manager
smsss.exe	448		1.05 MB	NT AUTHORITY\SYSTEM		
Memory Compression	2404		2.62 MB	NT AUTHORITY\SYSTEM		
Interrupts		0.25	0			Interrupts and DPCs
Registry	100	0.02	300 kB/s	9.29 MB	NT AUTHORITY\SYSTEM	Client Server Runtime Process
csrss.exe	624		2.02 MB	NT AUTHORITY\SYSTEM		
wininit.exe	708		1.42 MB	NT AUTHORITY\SYSTEM		Windows Start-Up Application
services.exe	824	0.40		6.29 MB	NT AUTHORITY\SYSTEM	Services and Controller app
svchost.exe	980		16.07 MB	NT AUTHORITY\SYSTEM		Host Process for Windows Serv...
dllhost.exe	6164		3.35 MB	NT AUTHORITY\SYSTEM		COM Surrogate
WmiPrvSE.exe	6388		6.92 MB	NT AUTHORITY\SYSTEM		WMI Provider Host
unsecapp.exe	6648		1.79 MB	NT AUTHORITY\SYSTEM		Sink to receive asynchronous c...
SettingSyncHost.exe	8328		2.75 MB	DESKTOP-II4...\\Elitebook		Host Process for Setting Synchron...
StartMenuExperienc...	9056		33.39 MB	DESKTOP-II4...\\Elitebook		
RuntimeBroker.exe	9200		7.2 MB	DESKTOP-II4...\\Elitebook		Runtime Broker
MoUsOCoreWorker...	7960		21.39 MB	NT AUTHORITY\SYSTEM		MoUSO Core Worker Process
RuntimeBroker.exe	9416		14.25 MB	DESKTOP-II4...\\Elitebook		Runtime Broker
unsecapp.exe	9756		1.42 MB	DESKTOP-II4...\\Elitebook		Sink to receive asynchronous c...
RuntimeBroker.exe	3520		7.73 MB	DESKTOP-II4...\\Elitebook		Runtime Broker
TextInputHost.exe	10652		15.1 MB	DESKTOP-II4...\\Elitebook		
dllhost.exe	11148		8.96 MB	DESKTOP-II4...\\Elitebook		COM Surrogate
dllhost.exe	12824		2.14 MB	DESKTOP-II4...\\Elitebook		COM Surrogate
CompPkgSrv.exe	12344		1.47 MB	DESKTOP-II4...\\Elitebook		Component Package Support ...
ApplicationFrame	1476		18.89 MB	DESKTOP-II4...\\Elitebook		Application Frame Host

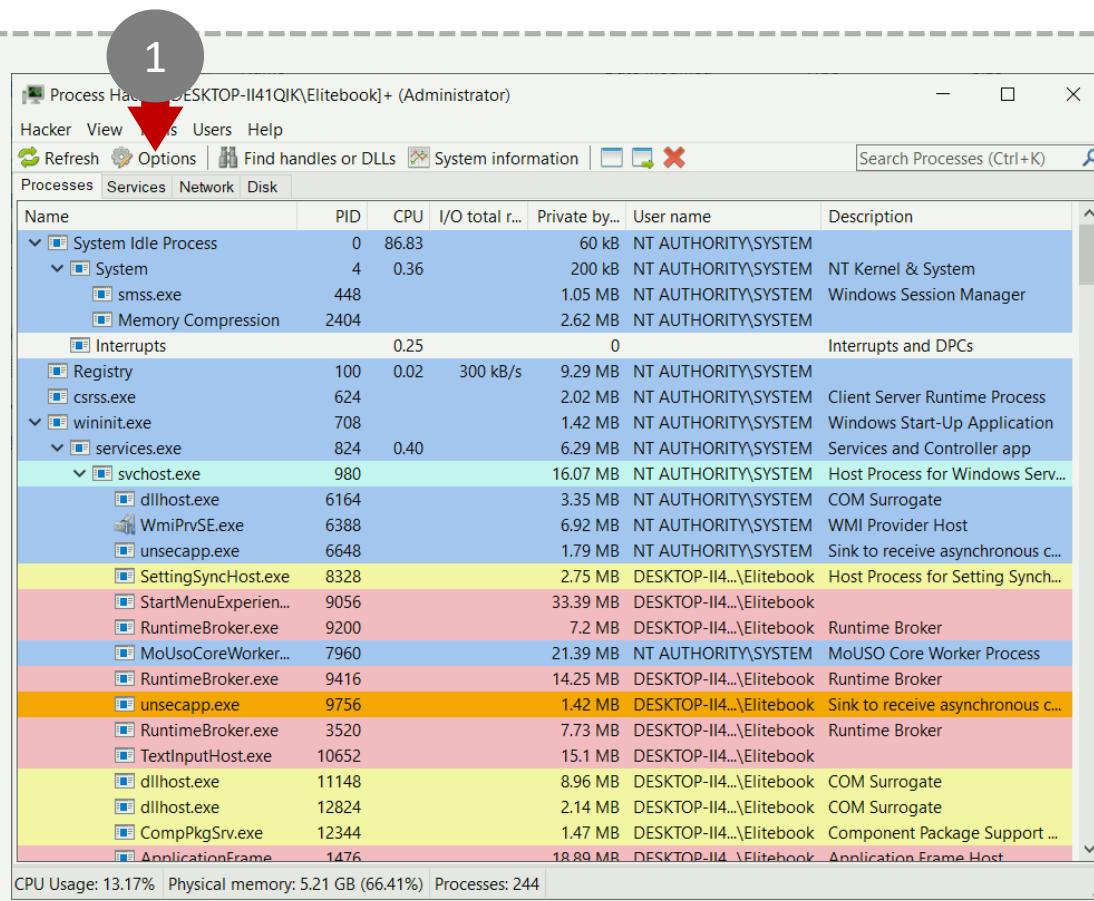
# PROCESS HACKER

## CE URMARIM?

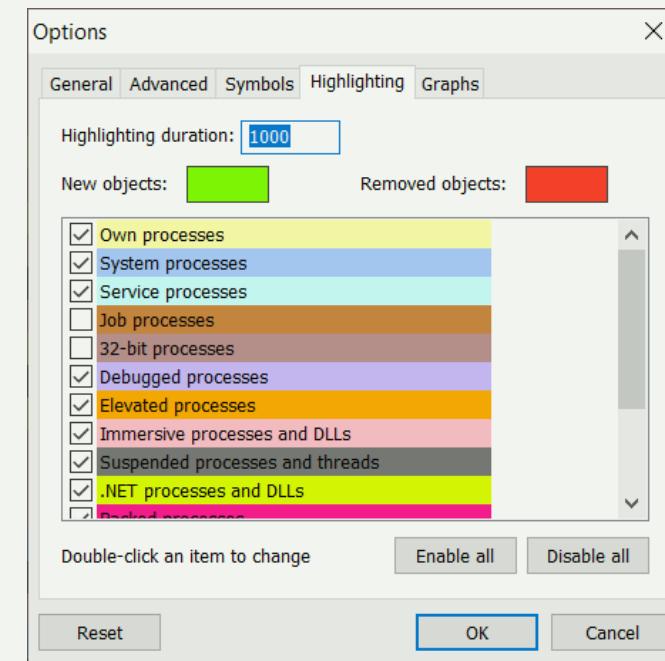
- **Procese neobișnuite sau suspecte.** Urmăriți procesele noi sau neașteptate care apar după executarea malware-ului. Process Hacker oferă detalii extinse despre fiecare proces, inclusiv PID-ul, utilizarea resurselor și parent process. Analizați procesele care nu au o semnătură digitală validă sau care sunt ascunse.
- **Modificări ale regiszrelor.** Monitorizați modificările efectuate în registrul sistemului. Multe tipuri de malware își modifică înregistrările pentru a asigura persistența sau pentru a schimba setările de securitate.
- **Conexiuni de rețea.** Verificați tab-ul de rețea pentru a observa orice conexiune neobișnuită sau neautorizată. Malware-ul poate încerca să comunice cu servere de comandă și control sau să descarce payload-uri suplimentare.
- **Servicii și driver.** Fiți atenți la orice serviciu sau driver nou instalat de malware. Unele malware-uri instalează drivere pentru a obține acces la nivel scăzut la sistemul de operare.
- **Manipularea memoriei.** Observați orice proces care pare să manipuleze memoria altor procese. Multe tipuri de malware încearcă să se injecteze în procese legitime pentru a evita detectarea.
- **Chei de autostart.** Examinati modificările aduse cheilor de autostart în registrul sistemului pentru a identifica metodele de persistență ale malware-ului.
- **Utilizarea resurselor.** Monitorizați utilizarea excesivă a CPU-ului, memoriei sau a discului, deoarece acest lucru poate indica activitatea malware-ului.
- **Fișiere și directoare.** Fiți atenți la orice modificare a sistemului de fișiere, inclusiv fișiere create, modificate sau șterse de malware.

# PROCESS HACKER

## CODUL CULORILOR

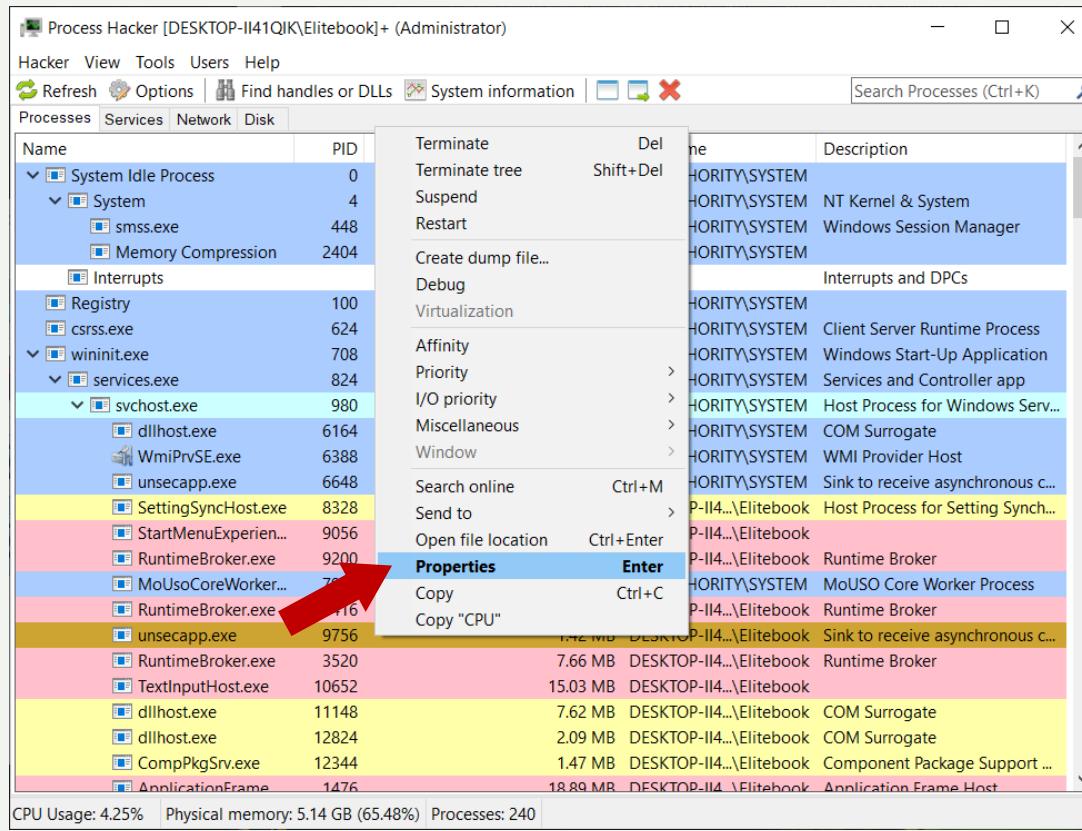


### Codul culorilor:



# PROCESS HACKER

## VISUALIZARE MEMORIE (ÎNCĂRCAREA SECTIUNILOR)



unsecapp.exe (9756) Properties				
General		Handles	GPU	Disk and Network
Base address	Type	Size	Protection	Use
> 0x7ffe0000	Private	4 kB	R	USER_S...
> 0x7ffec000	Private	4 kB	R	
> 0xddde9a00000	Private	2,048 kB	RW	PEB
> 0xddde9b00000	Private	1,024 kB	RW	Stack (...
> 0xddde9c00000	Private	1,024 kB	RW	Stack (...
> 0x26f46c90000	Mapped	4 kB	R	
> 0x26f46ca0000	Mapped	4 kB	R	
> 0x26f46cb0000	Mapped	116 kB	R	
> 0x26f46cd0000	Mapped	16 kB	R	
> 0x26f46ce0000	Mapped	4 kB	R	
> 0x26f46cf0000	Private	8 kB	RW	
> 0x26f46d00000	Mapped	4 kB	R	
> 0x26f46d10000	Mapped	64 kB	RW	Heap (...
> 0x26f46d20000	Mapped	32 kB	R	
> 0x26f46d30000	Private	1,024 kB	RW	Heap (...
> 0x26f46e30000	Mapped	804 kB	R	C:\Win...
> 0x26f46f00000	Private	104 kB	RW	
> 0x26f46f20000	Private	104 kB	RW	
> 0x26f46f40000	Mapped	4 kB	R	
> 0x26f46f50000	Mapped	4 kB	R	
> 0x26f46f60000	Private	4 kB	RW	
> 0x26f46f70000	Private	4 kB	RW	
> 0x26f47030000				

# PROCESS HACKER

## VISUALIZARE MEMORIE (ÎNCĂRCAREA SECTIUNILOR)

LaboratorATMClar.exe (19920) Properties

General Statistics Performance Threads Token Modules Memory Environment Handles GPU Disk and Network Comment

Hide free regions

Strings... Refresh

Base address	Type	Size	Protection	Use
> 0x10000	Mapped	4 kB	R	
> 0x20000	Mapped	4 kB	R	
> 0x30000	Mapped	4 kB	R	
> 0x40000	Mapped	116 kB	R	
> 0x60000	Private	256 kB	RW	Stack (thread 2956)
> 0xa0000	Private	1,024 kB	RW	Stack 32-bit (thread 2956)
> 0x1a000	Mapped	16 kB	R	
> 0x1b0000	Private	8 kB	RW	
> 0x1c0000	Mapped	4 kB	R	
> 0x1d0000	Mapped	4 kB	R	
> 0x1e0000	Mapped	4 kB	R	
> 0x1f0000	Mapped	64 kB	RW	Heap (ID 2)
> 0x200000	Private	2,048 kB	RW	PEB
<b>0x400000</b>	<b>Image</b>	<b>820 kB</b>	<b>WCX</b>	<b>C:\Users\Elitebook\Desktop\LaboratorATMClar.exe</b>
0x400000	Commit	4 kB	R	C:\Users\Elitebook\Desktop\LaboratorATMClar.exe
0x401000	Commit	408 kB	RX	C:\Users\Elitebook\Desktop\LaboratorATMClar.exe
0x467000	Commit	4 kB	RW	C:\Users\Elitebook\Desktop\LaboratorATMClar.exe
0x468000	Commit	404 kB	R	C:\Users\Elitebook\Desktop\LaboratorATMClar.exe
> 0x4d0000	Mapped	804 kB	R	C:\Windows\System32\locale.nls
> 0x5a0000	Private	64 kB	RW	Heap (ID 1)
> 0x630000	Private	56 kB	RW	
> 0x680000	Mapped	32 kB	R	
> 0x690000	Private	4 kB	RW	
> 0x6a0000	Private	64 kB	RW	
> 0x6b0000				

Close

LaboratorATMClar.exe (19920) (0x400000 - 0x401000)

00000000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....@.....

00000000 b8 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 ..L.!Th.....

00000030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..!..

00000040 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 .....!Th.....

00000050 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f is program canno.....

00000060 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 t be run in DOS.....\$.....

00000070 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 mode.....\$.....

00000080 8f 8a f9 db cb eb 97 88 cb eb 97 88 cb eb 97 88 .....

00000090 48 f7 99 88 ca eb 97 88 a2 f4 9e 88 ca eb 97 88 H.....

000000a0 22 f4 9a 88 ca eb 97 88 52 69 63 68 cb eb 97 88 ".....Rich.....

000000b0 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 .....PE..L.....

000000c0 d5 17 f6 65 00 00 00 00 00 00 e0 00 0f 01 ..e.....

000000d0 0b 01 06 00 00 60 06 00 00 60 06 00 00 00 00 ..`.....

000000e0 90 11 00 00 00 10 00 00 00 70 06 00 00 00 40 00 ..P..@.....

000000f0 00 10 00 00 00 10 00 00 04 00 00 00 01 00 00 00 ..`.....

00000100 04 00 00 00 00 00 00 00 d0 0c 00 00 10 00 00 ..`.....

00000110 12 0a 0d 00 02 00 00 00 00 10 00 00 10 00 00 ..`.....

00000120 00 00 10 00 00 10 00 00 00 00 00 10 00 00 ..`.....

00000130 00 00 00 00 00 00 00 00 74 63 06 00 28 00 00 00 ..tc..(.....

00000140 00 80 06 00 9c 48 06 00 00 00 00 00 00 00 00 00 ..H.....

00000150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..`.....

00000160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..`.....

00000170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..`.....

00000180 00 00 00 00 00 00 00 00 28 02 00 00 20 00 00 00 ..`.....

00000190 00 10 00 00 98 00 00 00 00 00 00 00 00 00 00 00 ..`.....

000001a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..`.....

000001b0 2e 74 65 78 74 00 00 00 68 56 06 00 00 10 00 00 ..text..hv.....

000001c0 00 60 06 00 00 10 00 00 00 00 00 00 00 00 00 00 ..`.....

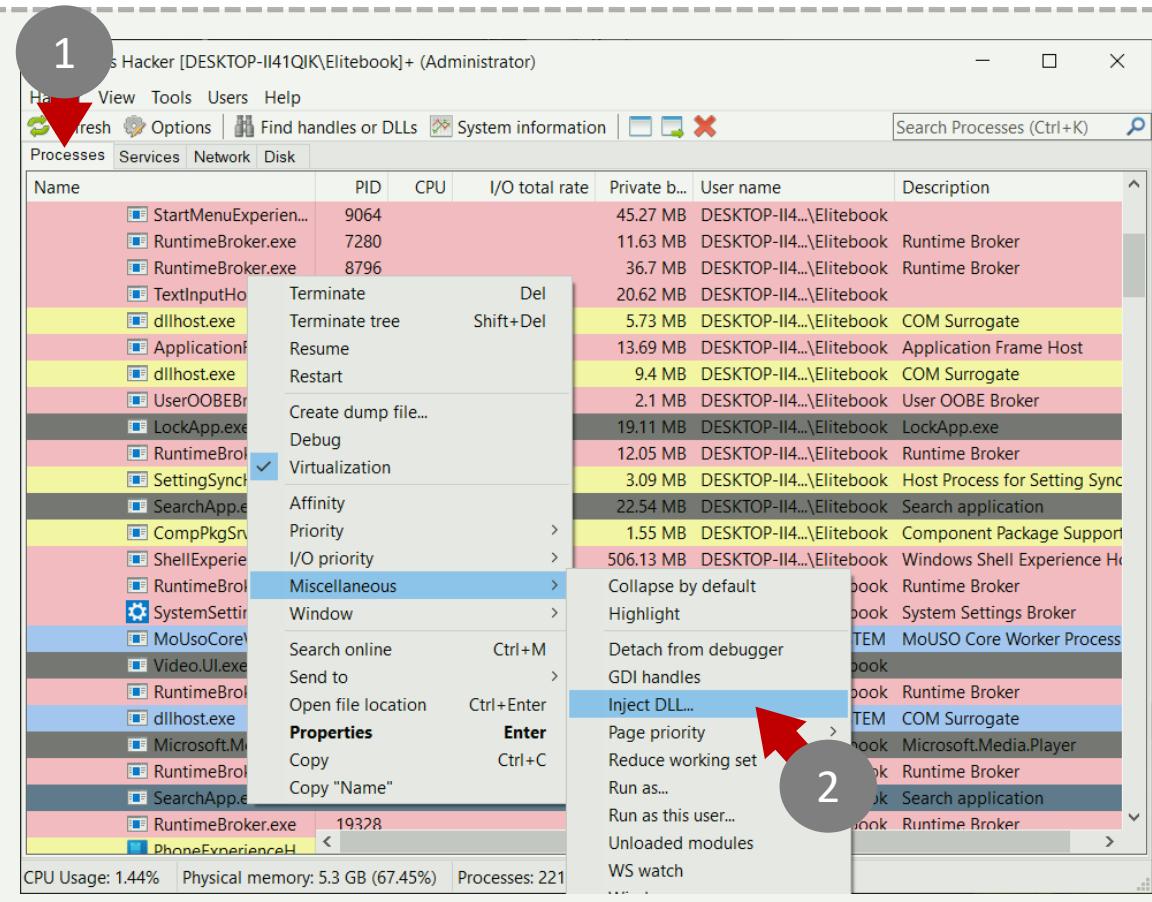
000001d0 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 ..`.....data.....

Re-read Write Go to... 16 bytes per row Save... Close

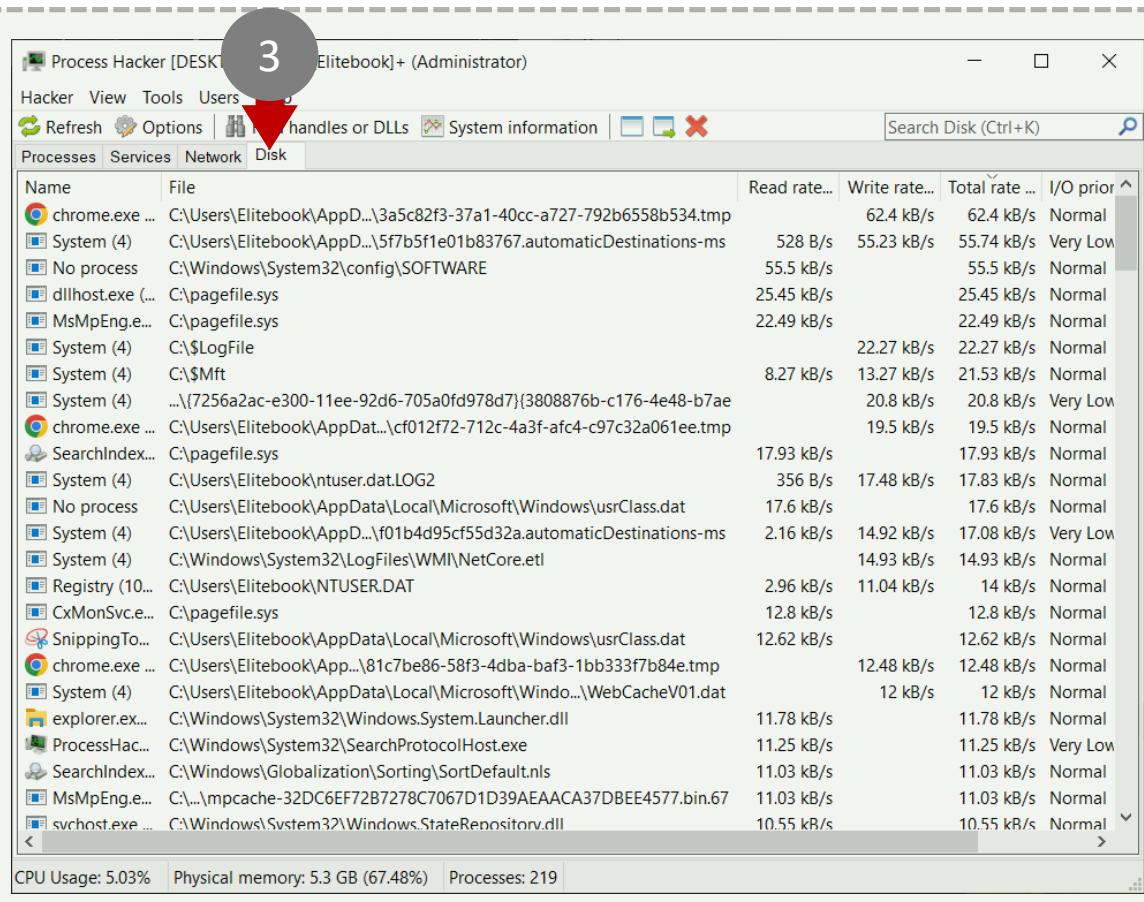
Exemplu de executabil compilat și rulat în laborator

# PROCESS HACKER

## PROCESE ȘI ACCES LA DISC ÎN TIMP REAL



## Procese



# Access la disc

# PROCESS HACKER

## SERVICIU SI REȚEA

1

Name	Display name	Type	Status	Start type	PID
1394ohci	1394 OHCI Compliant Host Controller	Driver	Stopped	Demand start	
3ware	3ware	Driver	Stopped	Demand start	
AarSvc	Agent Activation Runtime	User share proc...	Stopped	Demand start	
AarSvc_a244b	Agent Activation Runtime_a244b	User share proc...	Stopped	Demand start	
Accelerometer	HP Mobile Data Protection Sensor	Driver	Running	Demand start	
ACPI	Microsoft ACPI Driver	Driver	Running	Boot start	
AcpiDev	ACPI Devices driver	Driver	Stopped	Demand start	
acpiex	Microsoft ACPIEx Driver	Driver	Running	Boot start	
acpipagr	ACPI Processor Aggregator Driver	Driver	Running	Demand start	
AcpiPmi	ACPI Power Meter Driver	Driver	Stopped	Demand start	
acpitime	ACPI Wake Alarm Driver	Driver	Stopped	Demand start	
Acx01000	Acx01000	Driver	Stopped	Demand start	
ADP80XX	ADP80XX	Driver	Stopped	Demand start	
AFD	Ancillary Function Driver for Winsock	Driver	Running	System start	
afunix	afunix	Driver	Running	System start	
ahcache	Application Compatibility Cache	Driver	Running	System start	
AJRouter	AllJoyn Router Service	Share process	Stopped	Demand start (trigger)	
ALG	Application Layer Gateway Service	Own process	Stopped	Demand start	
amdgpio2	AMD GPIO Client Driver	Driver	Stopped	Demand start	
amdi2c	AMD I2C Controller Service	Driver	Stopped	Demand start	
AmdK8	AMD K8 Processor Driver	Driver	Stopped	Demand start	
AmdPPM	AMD Processor Driver	Driver	Stopped	Demand start	
amdsata	amdsata	Driver	Stopped	Demand start	
amdsbs	amdsbs	Driver	Stopped	Demand start	
amdyata	amdyata	Driver	Stopped	Demand start	

CPU Usage: 9.36% Physical memory: 5.15 GB (65.62%) Processes: 216

Servicii

2

Name	Local address	Local ...	Remote address	Remo...	Prot...	State	Owner
chrome.exe (12680)	DESKTOP-II41QIK	5353			UDP		
chrome.exe (12680)	DESKTOP-II41QIK	5353			UDP6		
chrome.exe (12680)	DESKTOP-II41QIK	1033	wf-in-f188.1e100.net	5228	TCP	Established	
chrome.exe (12680)	DESKTOP-II41QIK	1034	bud02s27-in-f14.1e...	443	TCP	Established	
chrome.exe (12680)	DESKTOP-II41QIK	1040	bud02s38-in-f14.1e...	443	TCP	Established	
chrome.exe (12680)	DESKTOP-II41QIK	1042	141.85.223.62	443	TCP	Established	
chrome.exe (12680)	DESKTOP-II41QIK	1047	104.18.37.228	443	TCP	Established	
chrome.exe (12680)	DESKTOP-II41QIK	1048	104.18.32.115	443	TCP	Established	
chrome.exe (12680)	DESKTOP-II41QIK	1049	104.18.37.228	443	TCP	Established	
chrome.exe (12680)	DESKTOP-II41QIK	1050	104.18.32.115	443	TCP	Established	
chrome.exe (12680)	DESKTOP-II41QIK	1036	2603:1030:807:3::112	443	TCP6	Established	
chrome.exe (3596)	DESKTOP-II41QIK	5353			UDP		
chrome.exe (3596)	DESKTOP-II41QIK	5353			UDP6		
jhi_service.exe (5072)	DESKTOP-II41QIK	49669			TCP6	Listen	jhi_service
lsass.exe (852)	DESKTOP-II41QIK	49664			TCP	Listen	
lsass.exe (852)	DESKTOP-II41QIK	49664			TCP6	Listen	
MpDefenderCoreService.exe (312...	DESKTOP-II41QIK	1052	2603:1063:31:108::	443	TCP6	SYN sent	MDCoreSvc
SearchApp.exe (14936)	DESKTOP-II41QIK	24739	a92-123-103-74.de...	443	TCP	Close wait	
services.exe (844)	DESKTOP-II41QIK	49670			TCP	Listen	
services.exe (844)	DESKTOP-II41QIK	49670			TCP6	Listen	
spoolsv.exe (3192)	DESKTOP-II41QIK	49668			TCP	Listen	Spooler
spoolsv.exe (3192)	DESKTOP-II41QIK	49668			TCP6	Listen	Spooler
svchost.exe (11636)	DESKTOP-II41QIK	123			UDP	W32Time	
svchost.exe (11636)	DESKTOP-II41QIK	123			UDP6	W32Time	
svchost.exe (11860)	DESKTOP-II41QIK	7680			TCP	Listen	DoSvc

CPU Usage: 26.36% Physical memory: 5.31 GB (67.59%) Processes: 219

Rețea

# CARE ESTE DIFERENTA DIN TRE PROCESS MONITOR, PROCESS EXPLORER SI PROCESS HACKER?

## Process Monitor

- Funcționalitate. Process Monitor este o unealtă avansată de monitorizare care combină caracteristicile de la două unelte mai vechi, Filemon și Regmon. Oferă o monitorizare în timp real a activității sistemului de fișiere, a registrului și a proceselor/thread-urilor, inclusiv a activității de rețea. Este util pentru captarea unei imagini cuprinzătoare a tuturor activităților care au loc pe sistem.
- Cazuri de utilizare. Ideal pentru depistarea problemelor complexe de sistem, inclusiv probleme de performanță, erori de aplicații și probleme de înregistrare.

## Process Explorer

- Funcționalitate. Process Explorer oferă o vedere mai detaliată asupra proceselor care rulează decât Managerul de sarcini Windows standard. Afisează informații despre procesele active, inclusiv mapele de manipulare și DLL-urile încărcate. Oferă, de asemenea, o reprezentare vizuală a relațiilor dintre procese, permitând utilizatorilor să vadă rapid care procese sunt legate.
- Cazuri de utilizare. Foarte util pentru identificarea proceselor care consumă resurse și pentru analiza relațiilor dintre procese. Este adesea folosit pentru troubleshooting și analiză preliminară a malware-ului.

## Process Hacker

- Funcționalitate. Process Hacker este o unealtă open-source care oferă funcționalități similare cu Process Explorer, dar cu caracteristici suplimentare avansate. Include o vedere detaliată a serviciilor, conexiunilor de rețea, sesiunilor de utilizator, și permite utilizatorilor să manipuleze procese, thread-uri și multe altele. Oferă, de asemenea, un monitorizor de sistem care poate afișa activitatea în timp real.
- Cazuri de utilizare. Recomandat pentru utilizatori tehnici sau analiști de securitate care au nevoie de funcții avansate pentru depanare, analiza malware-ului și optimizarea performanței sistemului.

# DIFERENȚE CHEIE

- **Complexitate și Public Țintă:** Process Monitor este cel mai bun pentru captarea unui flux de date detaliat despre activitatea sistemului, ideal pentru analiza profundă. Process Explorer este mai ușor de utilizat pentru o privire generală asupra proceselor și DLL-urilor. Process Hacker oferă cele mai avansate funcționalități, fiind preferat de profesioniștii în IT și de analiștii de securitate pentru analize detaliate și intervenții.
- **Funcționalități Unice:** Deși toate trei pot fi utilizate pentru monitorizarea proceselor și a activității sistemului, Process Hacker și Process Explorer oferă o analiză mai profundă a relațiilor dintre proceze, în timp ce Process Monitor se concentrează pe evenimentele sistemului în timp real.
- **Interfață și Ușurință de Utilizare:** Process Explorer are o interfață relativ simplă și ușor de înțeles, comparativ cu Process Hacker care oferă mai multe opțiuni avansate și o personalizare mai detaliată, ceea ce poate fi intimidant pentru utilizatorii noi sau neexperimentați. Process Monitor are o abordare unică, concentrându-se pe monitorizarea evenimentelor și oferind filtre puternice pentru analiza datelor.

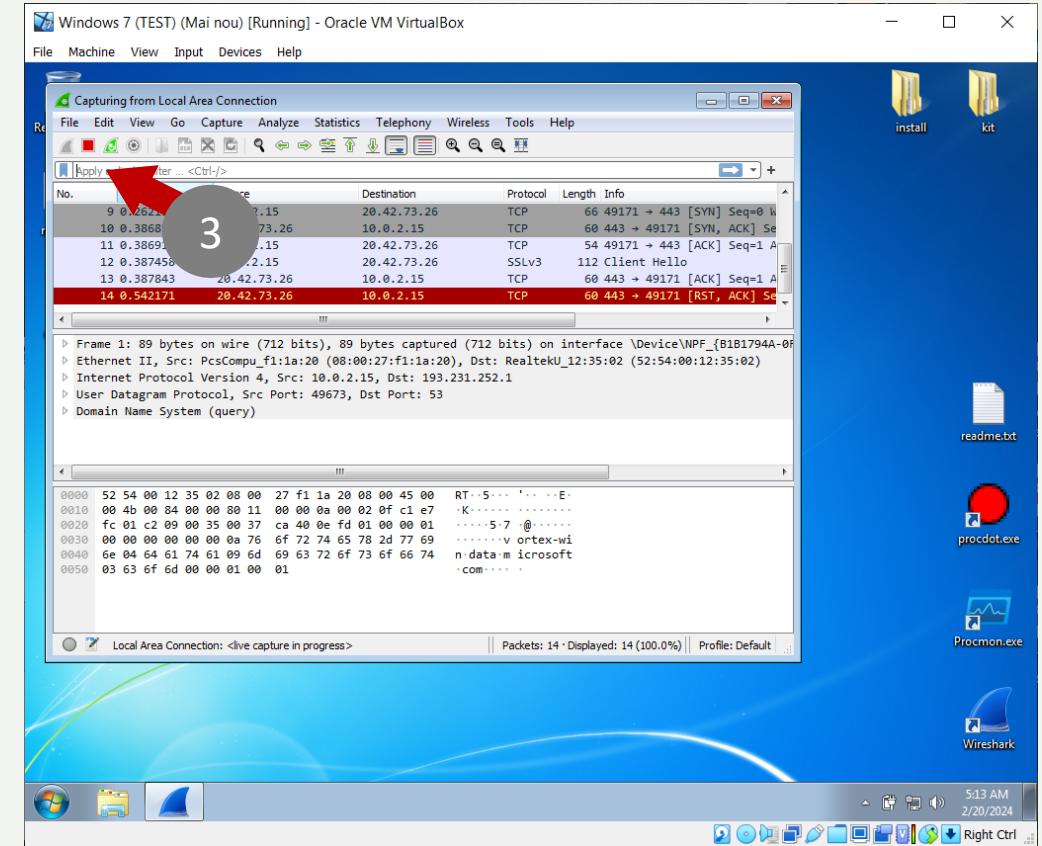
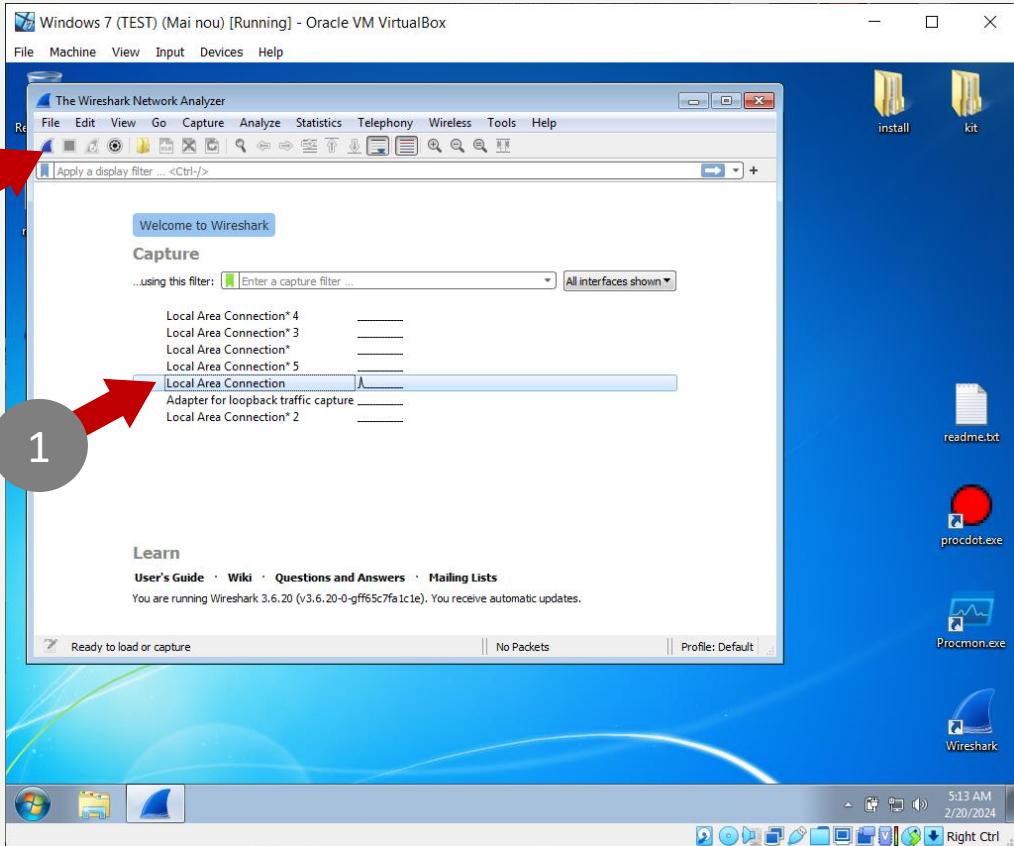
# COD MALIȚIOS: INSTRUMENTE DE ANALIZĂ



# WIRESHARK

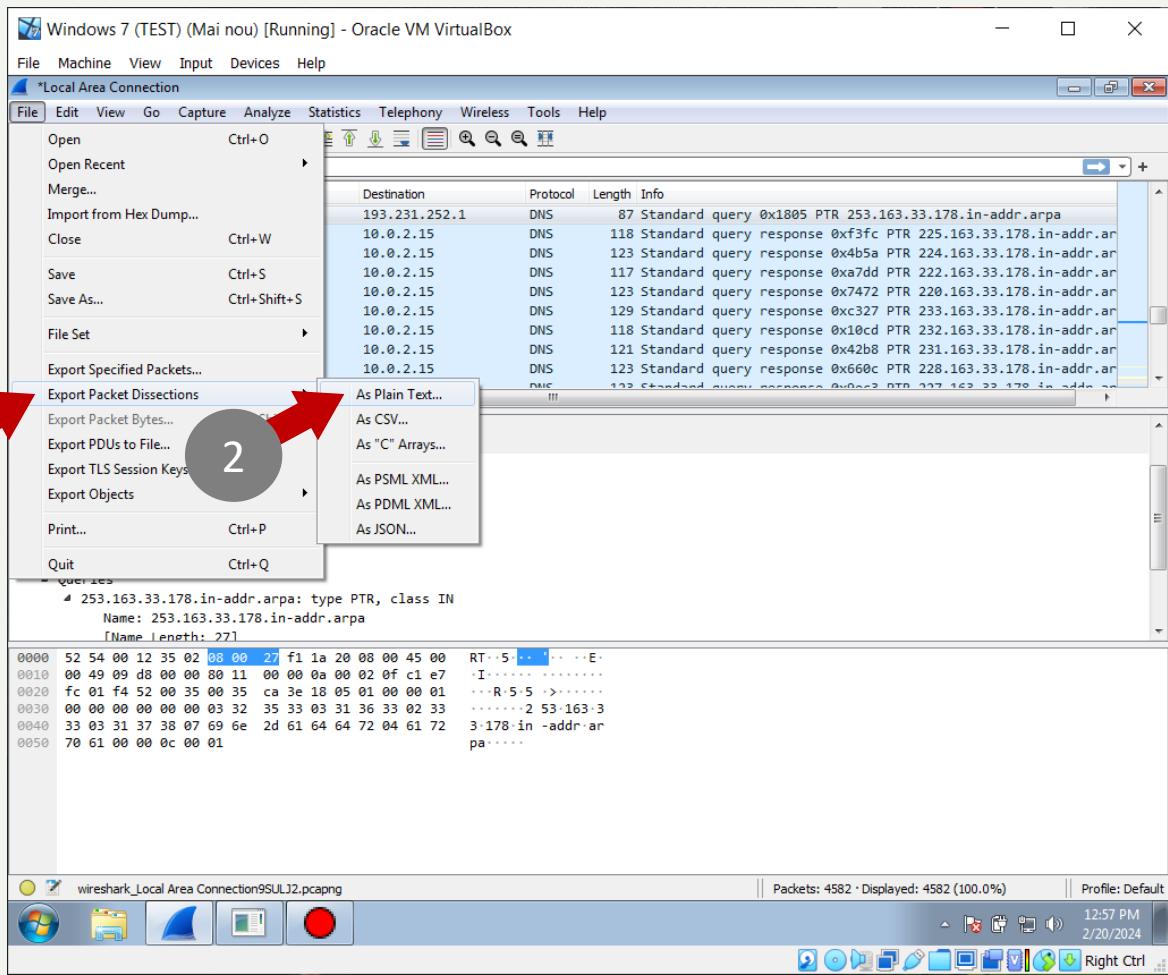
## PORNIRE (FILTRU; SMTP;HTTP)

- 1) Selectare adaptor de rețea
- 2) Pornire wireshark
- 3) Aplicare de filtre



# SALVAȚI JURNALUL CA TEXT PENTRU A FI UTILIZAT DE CĂTRE PROCDOT WIRESHARK

Moduri concise de a utiliza Wireshark pentru detectarea malware-ului:



**Trafic Neobișnuit.** Monitorizați volumul de trafic pentru a identifica orice creștere neașteptată, care poate indica activitatea unui malware ce încearcă să comunice cu serverul de comandă și control (C&C).

**Destinații Suspecte.** Verificați adresele IP și domeniile către care sunt direcționate pachetele de date. Comunicările cu adrese IP sau domenii cunoscute pentru a fi asociate cu activități malware ar trebui investigate.

**Protocole Neașteptate.** Urmăriți utilizarea protocolelor neobișnuite sau neașteptate pentru mediul de rețea respectiv. Malware-ul poate folosi protocole inedite pentru a evita detectarea.

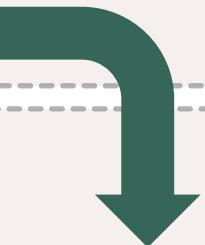
**Pachete Mici Repetate.** O serie de pachete mici și frecvente trimise către o anumită destinație poate fi un indicator al unui canal de exfiltrare a datelor.

**Trafic Criptat Nejustificat.** Monitorizați cantitatea de trafic criptat. Deși criptarea este comună, o cantitate excesivă de trafic criptat, în special în locuri neașteptate, poate fi suspectă.

**Analiza Conținutului Pachetului.** Examinarea conținutului pachetelor poate dezvălui string-uri suspecte, chei de malware sau alte semnături ale software-ului rău intenționat.

**Anomaliiile DNS.** Verificați cererile DNS pentru a identifica rezolvări neobișnuite sau frecvente către domenii suspecte, care pot indica activitatea de C&C sau tentativa de exfiltrare a datelor.

# COD MALIȚIOS: INSTRUMENTE DE ANALIZĂ

- PEStudio
  - Bcompare
  - Cutter & IDA & x64dbg
- 
- Sysinternals
  - Wireshark
  - **procDOT**
- 

Analiză Statică

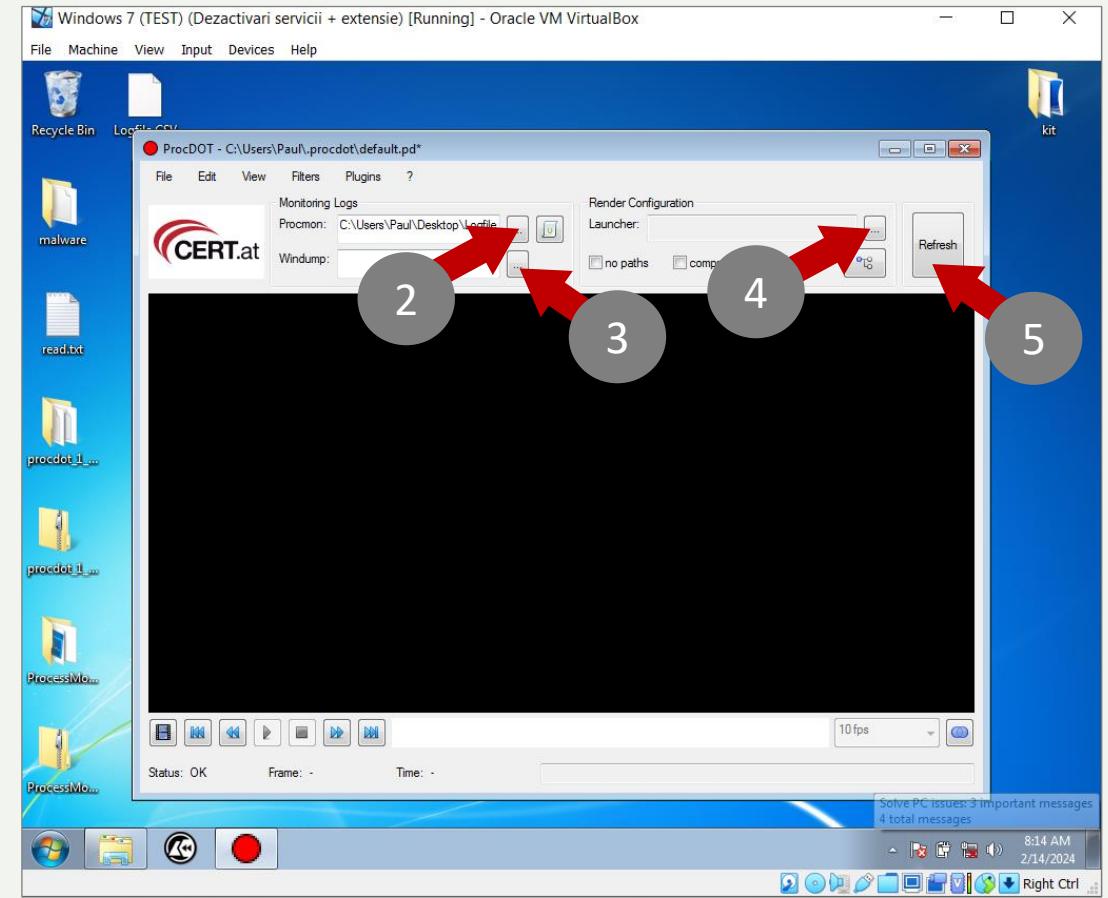
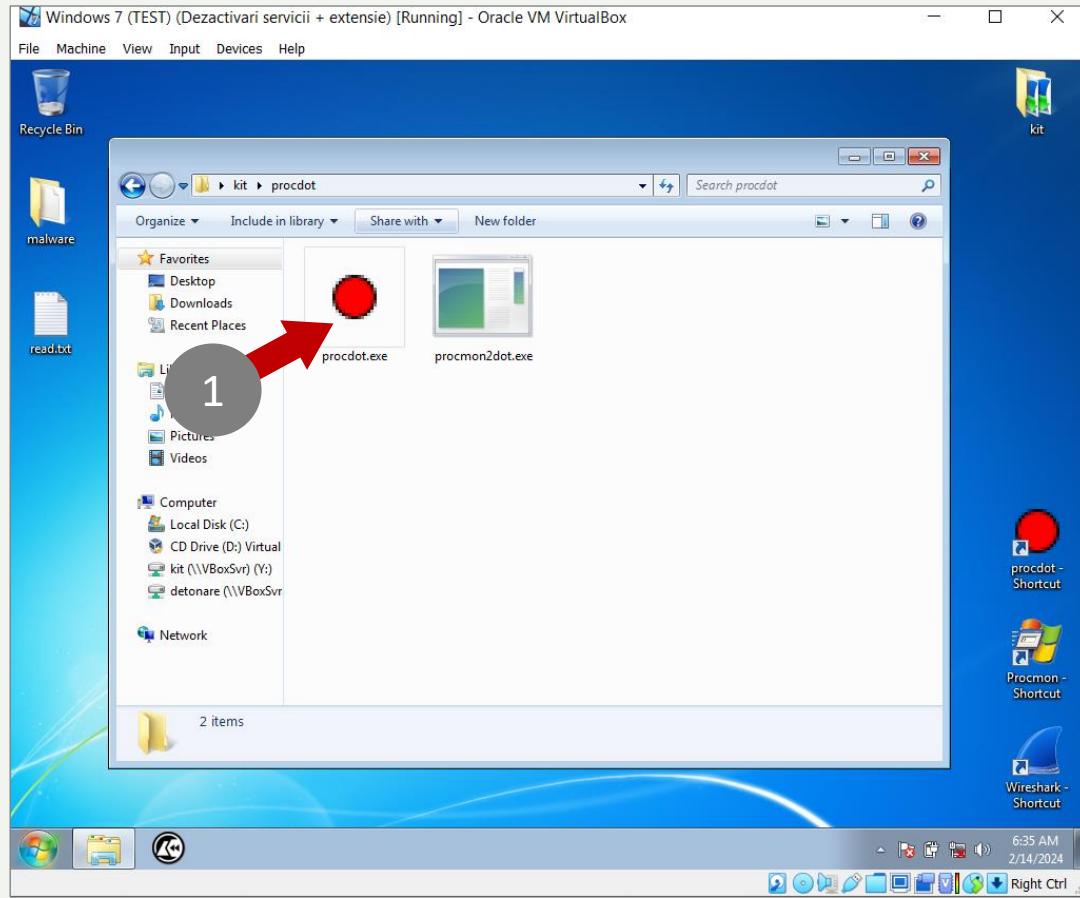
Analiză Dinamică

- Analiza malware in Cloud

Analiză Cloud

# PROCDOT

## RULAREA ȘI UTILIZAREA JURNALELOR PROCMON ȘI WIRESHARK



# PROCDOT

## REZULTAT FINAL

### Pornire rapidă în ProcDOT

=====

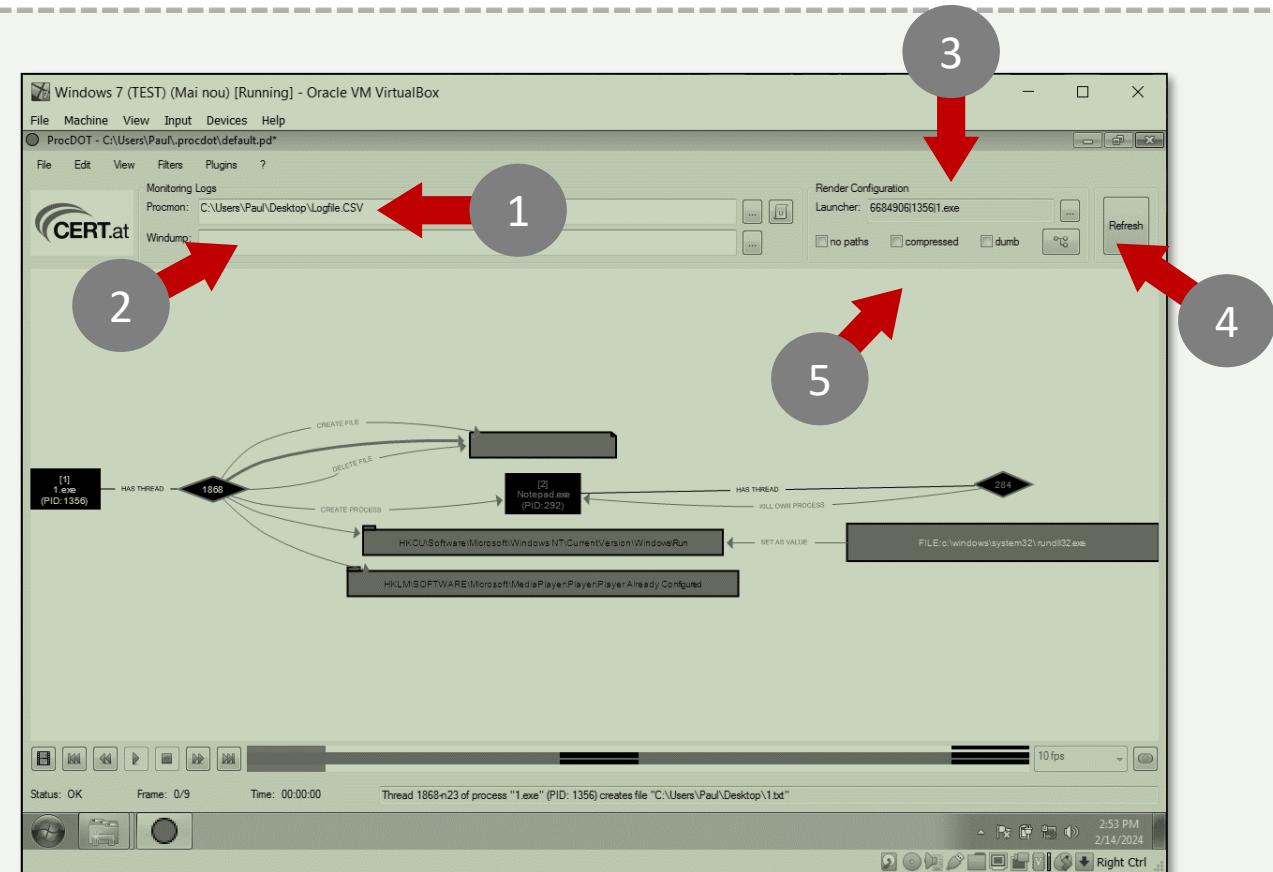
- 1) Selectați fișierele de jurnal (trist, dar adevărat, specificațiile pentru formatul de fișier nativ al Procmon (.PML) nu sunt disponibile (public). Prin urmare, trebuie să exportați fișierul dvs. .PML în .CSV, ceea ce se poate face cu ușurință prin „Salvare”.,, element de meniu din Procmon. Asigurați-vă că selectați „toate evenimentele”.)

- 2) Alegeți modul de reprezentare grafică (fără căi, comprimat)

- 3) Selectați primul proces relevant (malițios) (proces de lansare)

- 4) Faceți clic pe „Reîmprospătare”

dot.exe îl gasiți în graphviz

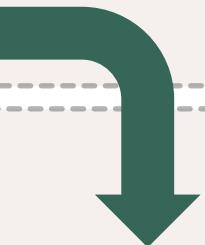


# ANALIZA IN CLOUD:



In registrare/Analiza la distanza

# COD MALIȚIOS: INSTRUMENTE DE ANALIZĂ

- PEStudio
  - Bcompare
  - Cutter & IDA & x64dbg
- 
- Sysinternals
  - Wireshark
  - procDOT
- ■ **Analiza malware in Cloud**

Analiză Statică

Analiză Dinamică

Analiză Cloud



# VIRUSTOTAL

Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

FILE

URL

SEARCH



Choose file

1

By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Policy](#), and to the **sharing of your Sample submission with the security community**. Please do not submit any personal information;

VirusTotal is not responsible for the contents of your submission. [Learn more](#).



# HYBRID ANALYSIS

File/URL

File Collection

Report Search

YARA Search

String Search

This is a free malware analysis service for the community that detects and analyzes unknown threats using a unique Hybrid Analysis technology.



Drag & Drop For Instant Analysis

or

<http://www.example.com/suspicious.zip>



Analyze

2

Maximum upload size is 100 MB.

Powered by **CrowdStrike Falcon® Sandbox**.

Interested in a free trial?

# Triage

- Triage dispune de o interfață care facilitează analiza amenințărilor chiar și pentru utilizatorii mai puțin tehnici.
- Permite analiza automatizată a fișierelor suspecte și a URL-urilor pentru a identifica comportamentele malicioase.
- Utilizează tehnici de sandboxing și emulare pentru a observa comportamentul fișierelor într-un mediu controlat.

The image consists of four screenshots of the Recorded Future Triage web application, arranged in a 2x2 grid. Each screenshot includes a numbered callout (1, 2, or 3) indicating a specific action or feature.

- Screenshot 1:** Submission page. Shows a file named "Executabil\_B.exe" with a score of 3/10. The "Platforms" section lists various operating systems and their architectures (Windows 7-x64, Windows 10-1703-x64, Windows 10-2004-x64, macOS 10.15-arm64, macOS 11-x64, Android 10-x64, Android 11-x64, Android 13-x64, Linux 12-armhf, Linux 9-mipsel, Linux 9-armhf, Linux 18.04-amd64). A red arrow points from the number 1 to the "Analyze" button at the bottom right of the platforms section.
- Screenshot 2:** Live Monitor page for the "Executabil\_B.exe" sample. It shows a screenshot of a Windows 7 desktop with various icons. Below the screenshot are buttons for "Extend analysis", "Terminate", "Mouse Simulation", and "Fullscreen". Session length is 00:55 and time remaining is 01:35. Task is labeled "behavioral1". A red arrow points from the number 2 to the "Terminate" button.
- Screenshot 3:** Live Monitor page showing the analysis progress. It says "This analysis is finished." and has a blue "Open Report" button. A red arrow points from the number 3 to the "Open Report" button.
- Screenshot 4:** Reports page for the "Executabil\_B.exe" sample. It shows a "General" section with target, size, MD5, SHA1, SHA256, SHA512, and SSDEEP details. An "Analysis" section lists max kernel time (31s), max time network (18s), and platform (windows7-x64). A "Score" section shows a score of 1/10. A red arrow points from the number 4 to the "Report" button at the top right.

C.5.3

# AUTOMATIZAREA MAȘINII VIRTUALE



# AUTOMATIZAREA MASINII VIRTUALE

## ACEASTA ESTE O PARTE DINTR-UN SCRIPT POWERSHELL

### AJUSTAȚI NUMELE MAȘINII VIRTUALE ȘI CĂILE CĂtre EXECUTABILE AFERENTE

- Mai jos este un exemplu de script PowerShell care ar putea face ceea ce ați descris, presupunând că aveți setările necesare deja configurate în VirtualBox, inclusiv un folder partajat, și că aveți deja instalate Process Monitor și Wireshark pe mașina virtuală. De asemenea, presupun că există mecanisme automate pentru a porni Process Monitor și Wireshark la pornirea mașinii virtuale sau la executarea unui script inițializat automat.

Conectare la mașina virtuală pentru a executa scriptul de pornire a Process Monitor și Wireshark. Presupunem că există un script pe VM care face acest lucru și că avem acces la VM prin PSRemoting.

- Acest script este doar un exemplu și poate necesita ajustări pentru a funcționa într-un mediu real, inclusiv gestionarea permisiunilor, configurarea rețelei și politici de securitate. De asemenea, este nevoie să verificați dacă PowerShell Remoting este activat și configurat pe mașina virtuală, care de asemenea, ar trebui să permită scripturilor să ruleze fără intervenție manuală.

Notă: Scriptul de mai jos presupune că este permis PSRemoting între gazdă și mașina virtuală și că sunt configurate corect politicile de execuție PowerShell și setările de rețea.

```
# Înlocuiți 'NumeMasinaVirtuala' cu numele mașinii dvs. virtuale din VirtualBox
$NumeMasinaVirtuala = "NumeMasinaVirtuala"

# Calea locală către executabilul care va fi copiat în directorul partajat
$CaleExecutabilLocal = "C:\calea\locala\spre\executabil.exe"

# Calea către directorul partajat 'detonare' de pe mașina virtuală
$CaleDirectorPartajatVM = "\\vm\detonare"

# Pornirea mașinii virtuale
Write-Host "Pornirea mașinii virtuale..."
Start-Process "C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" -ArgumentList "startvm $NumeMasinaVirtuala --type headless"

# Așteptăm să se inițializeze mașina virtuală (ajustați timpul conform necesității)
Start-Sleep -Seconds 60

# Copierea executabilului în directorul partajat 'detonare'
Write-Host "Copierea executabilului în directorul partajat 'detonare'..."
Copy-Item -Path $CaleExecutabilLocal -Destination $CaleDirectorPartajatVM -Force

# Înlocuiți 'NumeUtilizator' și 'Parola' cu credențialele pentru VM
$NumeUtilizator = "NumeUtilizator"
$Parola = ConvertTo-SecureString "Parola" -AsPlainText -Force
$CredentialeVM = New-Object System.Management.Automation.PSCredential($NumeUtilizator, $Parola)

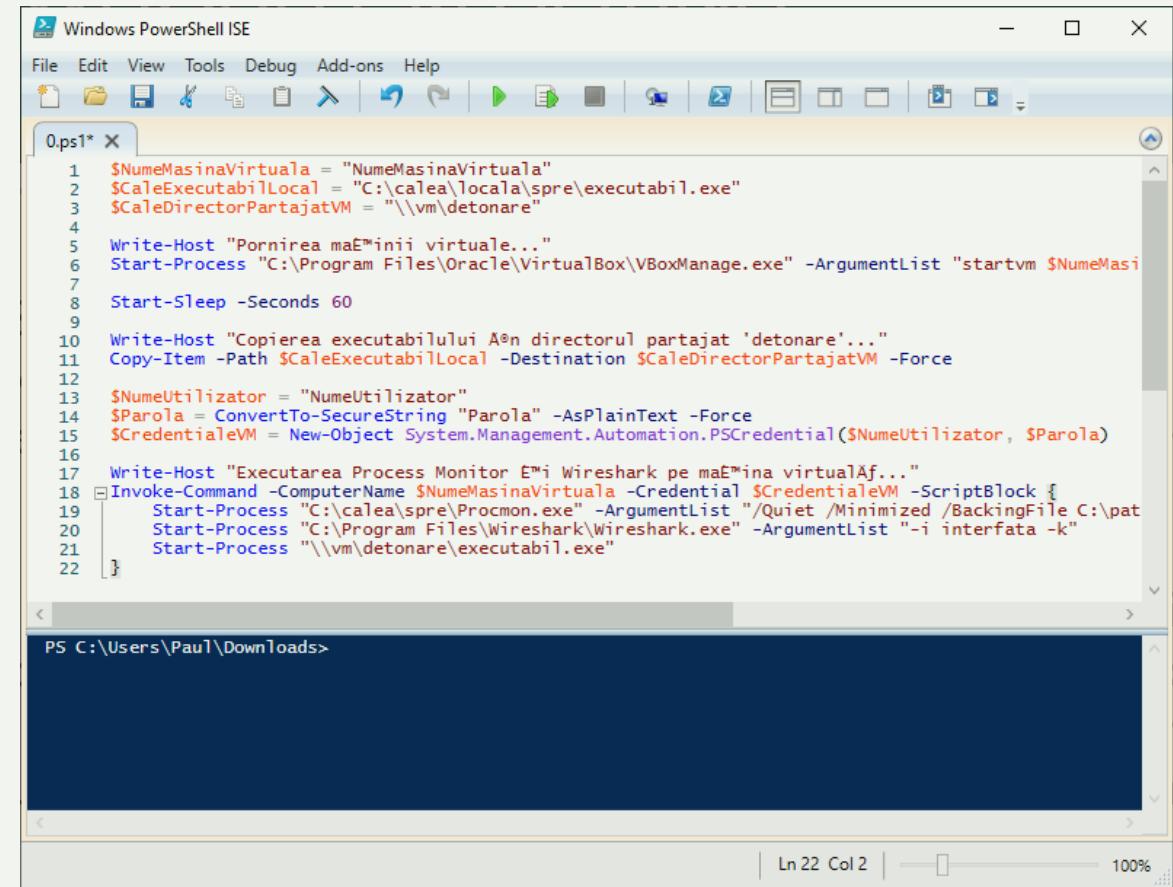
# Această parte presupune că PSRemoting este activat și configurat pe VM
Write-Host "Executarea Process Monitor și Wireshark pe mașina virtuală..."
Invoke-Command -ComputerName $NumeMasinaVirtuala -Credential $CredentialeVM -ScriptBlock {
    # Pornirea Process Monitor
    Start-Process "C:\calea\spre\Procmon.exe" -ArgumentList "/Quiet /Minimized /BackingFile C:\path\spre\log.pml"

    # Pornirea Wireshark în capture mode (înlocuiți 'interfata' cu numele interfeței de rețea)
    Start-Process "C:\Program Files\Wireshark\Wireshark.exe" -ArgumentList "-i interfata -k"

    # Executarea executabilului
    Start-Process "\\vm\detonare\executabil.exe"
}
```

# POWERSHELL REMOTING (PE SCURT)

- PSRemoting, sau PowerShell Remoting, permite rularea comenziilor PowerShell pe mașini îndepărtate. Acesta folosește *Windows Remote Management* (WinRM), care este o implementare a protocolului WS-Management și permite comunicația securizată prin rețea cu alte calculatoare care rulează PowerShell.
- Cu PSRemoting, puteți intra într-o sesiune pe un computer îndepărtat și rula comenzi ca și cum ați fi local pe acel computer. Vă permite, de asemenea, să trimiteți un script sau o comandă pentru a fi executată pe unul sau mai multe computere îndepărtate fără a fi nevoie să intrați într-o sesiune interactivă. Aceasta este o funcție puternică pentru administrarea de rețea și automatizare în medii de tip enterprise.



The screenshot shows the Windows PowerShell Integrated Scripting Environment (ISE). The title bar reads "Windows PowerShell ISE". The menu bar includes File, Edit, View, Tools, Debug, Add-ons, and Help. The toolbar contains various icons for file operations like Open, Save, Copy, Paste, and Run. A ribbon bar with tabs like Home, Insert, Tools, and Help is visible. The main area displays a PowerShell script named "0.ps1" with the following content:

```
$NumeMasinaVirtuala = "NumeMasinaVirtuala"
$CaleExecutabilLocal = "C:\calea\locala\spre\executabil.exe"
$CaleDirectorPartajatVM = "\\vm\detonare"
Write-Host "Pornirea mașinii virtuale..."
Start-Process "C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" -ArgumentList "startvm $NumeMasinaVirtuala"
Start-Sleep -Seconds 60
Write-Host "Copierea executabilului din directorul partajat 'detonare'..."
Copy-Item -Path $CaleExecutabilLocal -Destination $CaleDirectorPartajatVM -Force
$NumeUtilizator = "NumeUtilizator"
$Parola = ConvertTo-SecureString "Parola" -AsPlainText -Force
$CredentialeVM = New-Object System.Management.Automation.PSCredential($NumeUtilizator, $Parola)
Write-Host "Executarea Process Monitor și Wireshark pe mașina virtuală..."
Invoke-Command -ComputerName $NumeMasinaVirtuala -Credential $CredentialeVM -ScriptBlock {
    Start-Process "C:\calea\spre\Procmon.exe" -ArgumentList "/Quiet /Minimized /BackingFile C:\patrulla\procmon.log"
    Start-Process "C:\Program Files\Wireshark\Wireshark.exe" -ArgumentList "-i interfata -k"
    Start-Process "\\vm\detonare\executabil.exe"
}
```

The bottom pane shows the PowerShell prompt: "PS C:\Users\PauT\Downloads>". The status bar at the bottom right indicates "Ln 22 Col 2" and "100%".

# ADMINISTRAREA LA DISTANȚĂ A MAȘINILOR

## EXECUTAREA DE SCRIPTURI PE ACESTEA PRIN SESIUNI DE POWERSHELL

Pentru a utiliza PSRemoting, care este un feature al PowerShell ce permite administrarea la distanță a mașinilor și executarea de scripturi pe acestea prin sesiuni de PowerShell, trebuie să faceți câteva setări speciale pe mașina virtuală:

- **Activarea PSRemoting.** Trebuie să activați PSRemoting pe mașina virtuală cu Windows 7. Acest lucru se poate face prin executarea comenzi *Enable-PSRemoting* într-o sesiune PowerShell cu drepturi de administrator.
- **Configurarea firewall-ului.** Trebuie să asigurați că firewall-ul Windows permite conexiuni pentru PSRemoting. De obicei, rularea comenzi *Enable-PSRemoting* configura automat regulile firewall necesare.
- **Configurarea WinRM.** PSRemoting folosește serviciul Windows Remote Management (WinRM) pentru a gestiona sesiunile la distanță. Acest serviciu trebuie să fie activat și configurat corespunzător. Comanda *Enable-PSRemoting* de obicei se ocupă și de această parte.
- **Politica de execuție.** Politica de execuție PowerShell trebuie să permită executarea scripturilor. Puteți seta aceasta folosind *Set-ExecutionPolicy*, de exemplu: *Set-ExecutionPolicy RemoteSigned*.
- **Autentificarea.** Pentru a vă conecta la o mașină la distanță, trebuie să utilizați credențiale valide. În cazul unei mașini virtuale, acestea ar putea fi credențialele de administrator ale mașinii virtuale.
- **Trusted Hosts.** Dacă mașina gazdă și mașina virtuală nu fac parte din același domeniu sau nu sunt pe aceeași rețea de încredere, este posibil să fie necesar să adăugați adresa gazdei la lista de gazde de încredere pe mașina virtuală, folosind *Set-Item WSMan:\localhost\Client\TrustedHosts -Value "numele\_sau\_IP-ul\_gazdei"*.
- **Credențialele.** Dacă utilizați autentificarea pe bază de username și parolă, asigurați-vă că transmiteți credențialele într-o manieră securizată.

C.5.4

# MOSTRE MALWARE & PROTOCOALE DE MANIPULARE



## PAROLA DE LA BANCA MALWARE BANCA~~M~~ALWARE.ZIP (DIRECTORUL DETONARE)

- DETONARE
- BancaMalware.zip (parola: infectie)

## SSTRUCTURA BANCII MALWARE (DETONARE – MOODLE)

BancaMalware.zip:

- Bazar (versiuni mai noi)
- VIRUSI ANALIZATI (Scut Antivirus)
- VX (VX Heaven)
- theZoo-master.zip (colectare variată de probe pentru detonare; **parola: infected**)
- Worm.Win32.Kebede.H@mm (binary si cod sursa in VB6)

# MOSTRE MALWARE ONLINE – SURSE DE INCREDERE

Name	URL	Description
<b>Virus Samples</b>	<a href="https://virussamples.com">https://virussamples.com</a>	Fluxuri Enterprise și gratuite disponibile. Arhivă și depozit masiv.
<b>VirusShare</b>	<a href="https://virusshare.com/">https://virusshare.com/</a>	VirusShare este un serviciu găzduit și întreținut de <i>Corvus Forensics</i> .
<b>MalQuarium</b>	<a href="https://malquarium.org/">https://malquarium.org/</a>	Arhivă mică de mostre, în mare parte de la <i>MalShare</i> și URLHaus. Depozit de malware bazat pe web.
<b>MalShare</b>	<a href="https://malshare.com">https://malshare.com</a>	Depozit gratuit de programe malware condus de <i>Silas Cutler</i> .
<b>Contagio</b>	<a href="http://contagiadump.blogspot.com/">http://contagiadump.blogspot.com/</a>	Blog care este actualizat din când în când cu mostre interesante. Nu o arhivă.
<b>PolySwarm</b>	<a href="https://polyswarm.io">https://polyswarm.io</a>	Motor de agregare antivirus bazat pe blockchain care vă permite să descărcați anumite mostre cu înregistrarea.
<b>VirusTotal</b>	<a href="https://www.virustotal.com">https://www.virustotal.com</a>	Motor de agregare antivirus care vă permite să descărcați anumite mostre cu înregistrarea.
<b>VirusBay</b>	<a href="https://beta.virusbay.io/">https://beta.virusbay.io/</a>	O comunitate mică conduce colecția de programe malware.
<b>VirusSign</b>	<a href="https://virussign.com">https://virussign.com</a>	VirusSign oferă o colecție de mostre de malware de înaltă calitate, în diferite categorii. 500/zi sunt gratuite.

# ETICA ÎN INGINERIA INVERSĂ ÎN CONTEXT MILITAR

## Definirea Ingineriei Inverse

- Procesul de analiză a software-ului sau hardware-ului pentru a determina designul, funcționarea și potențialul de exploatare.

## Utilizare în Context Militar

- Ingineria inversă este utilizată pentru a înțelege și contracara tehnologiile adversarilor.

## Considerații Etice

- Responsabilitate, Legalitate, Confidențialitate.
- Echilibrul între necesitățile strategice și etica profesională este esențial.

# PROBLEME ETICE

## ÎN CREAREA ȘI UTILIZAREA MALWARE-ULUI

### Definirea Malware-ului

- Software creat pentru a dăuna sau a exploata sisteme informatiche.

### Utilizare în Scopuri Militare și de Securitate

- Dezvoltarea și utilizarea malware-ului pentru operațiuni de cyber-război.

### Considerații Etice

- Intenție, Impact asupra Civililor, Consecințe pe Termen Lung.
- Crearea și utilizarea malware-ului ridică întrebări etice profunde, necesitând principii etice solide.

# MOODLE:

## DETTONARE

- Directorul denumit "DETTONARE" este conceput ca o resursă educațională pentru studiul și analiza malware. În interiorul acestui director se găsesc mostre de malware de diverse tipuri, organizate cu scopul de a oferi studenților din domeniul securității cibernetice accesul la exemple reale de software malicioș pentru analiză și învățare. Aceste mostre pot include, dar nu sunt limitate la, troieni, viruși, viermi (se poate folosi și termenul de "wormi"), ransomware, spyware și adware, fiecare reprezentând diferite tehnici și metode utilizate de atacatori pentru a compromite sistemele informatiche.
- Directorul este structurat într-un mod care facilitează navigarea și selecția specifică a tipurilor de malware pentru studiu. Fiecare moștră este încapsulată într-un mod care previne declanșarea accidentală sau răspândirea malware-ului în rețeaua utilizatorului, asigurând un mediu sigur pentru analiză.
- De obicei, aceste mostre sunt însoțite de documentație sau descrieri care detaliază comportamentul lor, tehniciile de evaziune detectate și impactul potențial asupra sistemelor infectate.
- Utilizarea acestui director presupune o înțelegere solidă a măsurilor de precauție în manipularea malware-ului, inclusiv utilizarea unor mediilor izolate, cum ar fi mașinile virtuale, și instrumente de securitate dedicate pentru a preveni infectarea accidentală și minimizarea riscurilor. Scopul directorului "DETTONARE" este de a îmbunătăți competențele practice ale celor interesați de securitatea cibernetică prin experiența directă cu amenințările reale, permitându-le să înțeleagă mai bine strategiile și tehniciile folosite de atacatori și să dezvolte strategii eficiente de apărare și răspuns la incidente.

# MANIPULAREA SIGURĂ A FIŞIERELOR MALWARE

## ■ Importanța Precauției

- Manipularea fișierelor malware necesită precauții stricte pentru a preveni infectarea accidentală a sistemului gazdă sau a rețelei.

## ■ Schimbarea Extensiei Fișierelor

- O metodă simplă, dar eficientă, este modificarea extensiei fișierelor suspecte din ".exe" în ".exe". Această schimbare împiedică execuția accidentală a fișierului pe sistemele Windows.

## ■ Arhivarea cu Parolă

- O altă stratagemă de siguranță este arhivarea fișierelor malware într-o arhivă protejată cu parolă. Acest lucru previne accesul neautorizat și reduce riscul de detonare neintenționată.

## ■ Măsuri de Protecție

- Utilizarea software-ului antivirus actualizat, a firewall-urilor și a altor tehnologii de securitate pentru a scana și izola fișierele suspecte.

# DETONAREA CONTROLATĂ A MALWARE-ULUI

- **Prepararea pentru Detonare**
  - Înainte de a analiza sau de a "detona" malware-ul, asigurați-vă că acesta se află într-un mediu controlat, de preferință o mașină virtuală izolată de restul rețelei.
- **Schimbarea Înapoi a Extensiei**
  - Pentru a analiza comportamentul malware-ului, extensia fișierului poate fi schimbată înapoi în ".exe" doar în cadrul mașinii virtuale sigure.
- **Analiza și Investigația**
  - Utilizați unelte specializate de analiză malware pentru a studia comportamentul și impactul potențial al fișierului executabil asupra sistemelor.
- **Conștientizarea Riscurilor**
  - Fiți conștienți de risurile asociate cu detonarea malware-ului, inclusiv posibilitatea de a eluda măsurile de securitate ale mașinii virtuale. Asigurați-vă că aveți măsuri de recuperare și de restaurare a sistemului.

## Notă

- Educația și precauția sunt esențiale în manipularea malware-ului. Respectând aceste practici de siguranță, studenții ATM pot analiza în siguranță amenințările cibernetice, contribuind la dezvoltarea de soluții de securitate mai robuste.

## REGULI FINALE PENTRU FIŞIERELE MALWARE

- Fişierele executabile sunt păstrate în fişiere comprimate cu o parolă.
- Pentru fişierele executabile, extensia este modificată prin adăugarea caracterului "\_". Ex. "file.exe" este stocat ca "file.\_exe" (previne detonarea accidentală. Pentru a detona, ştergeţi caracterul "\_" din extensia fişierului).
- Mutarea unui fişier malware pe maşina gazdă pentru alte tipuri de studii care nu pot fi efectuate pe MV, se face prin aplicarea aceleiaşi metode de modificare a extensiei, în prealabil.

# MOODLE: HONEYBOT

- Directorul "Honeypot" este conceput ca un mediu experimental controlat, destinat studiului comportamentului malware-ului într-un context securizat. Acesta include două subdirectoare principale, "Curat" și "Infectat", fiecare conținând 65 de executabile inițial neinfectate. Scopul acestei structuri este de a oferi o platformă pentru observarea directă a modului în care diferite tipuri de malware identifică și interacționează cu fișierele executabile, în funcție de extensiile lor și de prezența într-un mediu potențial vulnerabil.
- **Directorul Curat.** Acest subdirector conține executabilele cu extensia modificată în ".\_exe", în încercarea de a evita detectarea și infecția automată de către viruși. Modificarea extensiei este o tactică utilizată pentru a testa dacă malware-ul vizează specific fișierele executabile prin extensia lor standard ".exe".
- **Directorul Infectat.** În contrast, acest subdirector conține același set de executabile, dar cu extensia standard ".exe". Acesta servește ca un mediu țintă pentru detonarea intenționată a malware-ului, oferind o perspectivă asupra eficacității acestuia în recunoașterea și infectarea fișierelor cu extensii cunoscute.
- Prin compararea rezultatelor interacțiunii malware-ului cu fișierele din aceste două directoare, studenții pot obține înțelegere valoroasă asupra tacticii de evitare a detecției utilizate de viruși, precum și asupra măsurilor de securitate care ar putea fi implementate pentru protecția împotriva acestora. Această abordare practică îi ajută pe studenți să dezvolte competențe esențiale în analiza malware-ului și în strategiile de apărare cibernetică.

- [AMAAaaS](#) (fișiere Android)
- [Any.run](#) (versiune gratuită)
- [Binary Guard True Bare Metal](#)
- [Intezer Analyze](#) (ediția comunitară)
- [CAPE Sandbox](#)
- [Comodo Valkyrie](#)
- [Detux Sandbox](#) (binare Linux)
- [FileScan.IO](#) (analiză și emulare statică)
- [Gatewatcher Intelligence](#)
- [Hatching Triage](#) (licențe individuale și de cercetător)
- [IRIS-H](#) (se concentrează pe fișierele documentelor)
- [Hybrid Analysis](#)
- [InQuest Labs Deep File Inspection](#)
- [Joe Sandbox Cloud](#) (ediția comunitară)
- [Manalyzer](#) (analiză statică)
- [sandbox.pikker.ee](#)
- [SandBlast Analysis](#)
- [SecondWrite](#) (versiune gratuită)
- [SNDBOX](#)
- [ThreatConnect](#)
- [ThreatZone](#)
- [VirusTotal](#)
- [Yomi](#)

## Platforme de scanare în cloud

O listă cuprinzătoare de servicii gratuite, găzduite, care efectuează scanări automate de malware.

# SANDBOX PLATFORMS

Name	URL	Description
<b>Any.run</b>	<a href="https://app.any.run">https://app.any.run</a>	Interactive online sandbox with lots of options.
<b>Hatching Triage</b>	<a href="https://tria.ge/dashboard">https://tria.ge/dashboard</a>	Sandbox where you can submit files of your own and download others.
<b>Hybrid Analysis</b>	<a href="https://www.hybrid-analysis.com/">https://www.hybrid-analysis.com/</a>	Free malware analysis service for the community that detects and analyzes owned by Crowdstrike.
<b>SNDBOX</b>	<a href="https://app.sndbox.com/">https://app.sndbox.com/</a>	Currently under maintenance.

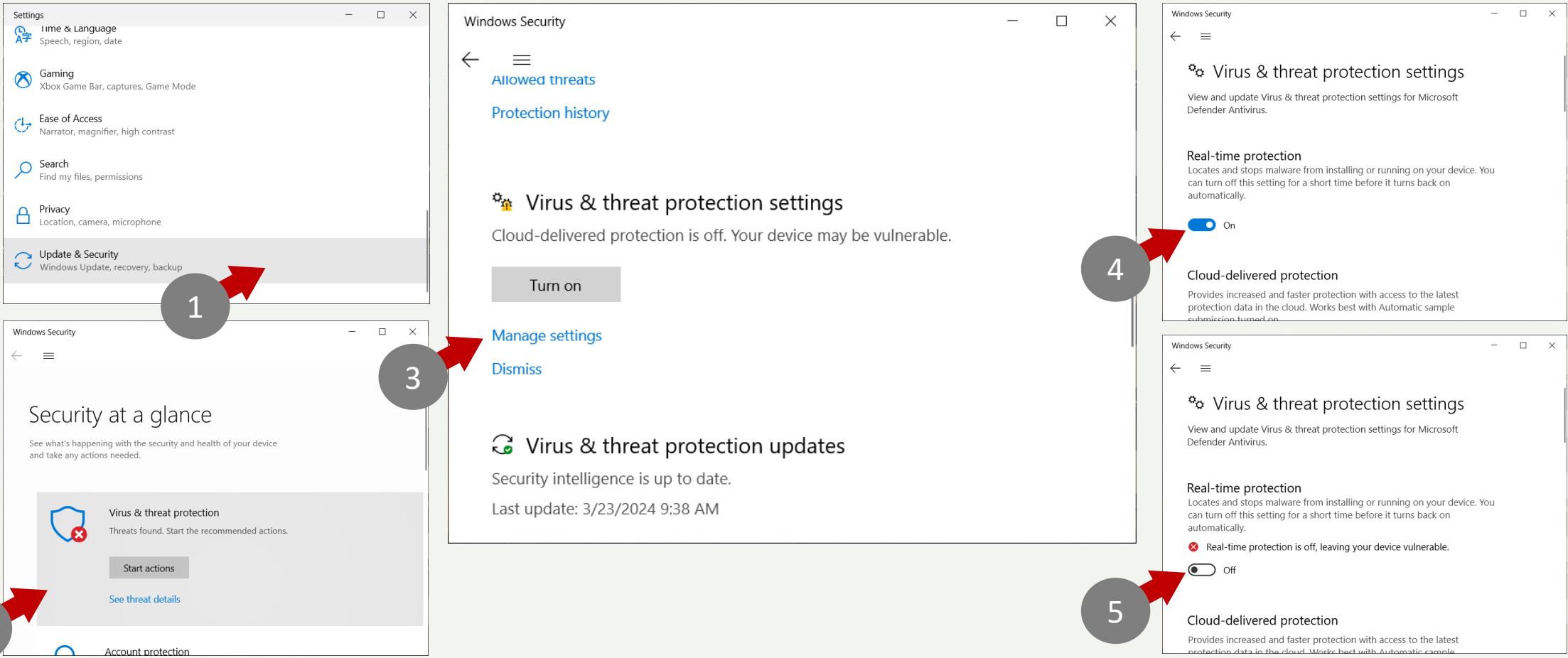
Platforme Sandbox vs. Platforme de scanare în cloud?

# INSTALAREA BĂNCII DE MALWARE DIN MOODLE PE MAŞINA VIRTUALĂ

- Dezactivați Windows Defender (temporar)
- Descărcați *BancaMalware.zip* de pe Moodle pe mașina gazdă
- Copiați fișierul *BancaMalware.zip* din locația de descărcare în directorul DETONATION
- Porniți mașina virtuală
- În Mașina Virtuală, copiați fișierul *BancaMalware.zip* din directorul partajat „DETTONARE”, într-un director nou creat pe desktop, numit „malware”
- Activați Windows Defender pe mașina gazdă.
- În laboratorul următor, aceste mostre vor fi extrase din *BancaMalware.zip*, folosind parola „infectie”

# WINDOWS DEFENDER

## ACTIVARE / DEZACTIVARE



# BIBLIOGRAFIE / RESURSE

- Paul A. Gagniuc. *Antivirus Engines: From Methods to Innovations, Design, and Applications*. Cambridge, MA: Elsevier Syngress, 2024. pp. 1-656.
- Paul A. Gagniuc. *An Introduction to Programming Languages: Simultaneous Learning in Multiple Coding Environments*. Synthesis Lectures on Computer Science. Springer International Publishing, 2023, pp. 1-280.
- Paul A. Gagniuc. *Coding Examples from Simple to Complex - Applications in MATLAB*, Springer, 2024, pp. 1-255.
- Paul A. Gagniuc. *Coding Examples from Simple to Complex - Applications in Python*, Springer, 2024, pp. 1-245.
- Paul A. Gagniuc. *Coding Examples from Simple to Complex - Applications in Javascript*, Springer, 2024, pp. 1-240.
- Paul A. Gagniuc. *Markov chains: from theory to implementation and experimentation*. Hoboken, NJ, John Wiley & Sons, USA, 2017, ISBN: 978-1-119-38755-8.

<https://github.com/gagniuc>

