



Como fazer bug bounty em aplicativos Windows

BUG BOUNTY ALÉM DE WEB

whoami_



Giuliano Sanfins - Campinas/SP



Eng. de Computação - Analista de segurança SiDi



Foco em análises de aplicações Windows



OSED - Offsec Exploit Developer



CVE-2025-36537, CVE-2025-9870, CVE-2025-9871, CVE-2025-9869



LinkedIn_

[/giuliano-sanfins](#)

Twitter_

[@0x_alibabas](#)





Por que
analisar apps
Windows

Fugindo da saturação Web

- **Web:** Você compete contra milhares de hunters, bots e scanners que acham falhas em minutos.
- **Windows:** A barreira de entrada técnica e o medo do desconhecido afasta o pessoal.



500
duples on RXSS

RCE/LPE on
WindowsApps



Web ≠ Windows

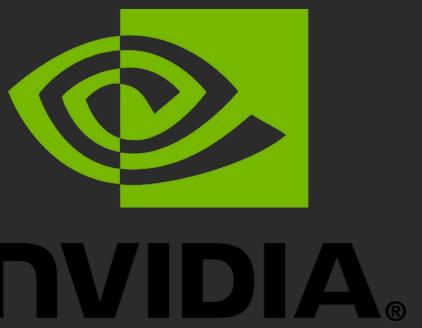
- **Escopo:** Em web você ataca a infraestrutura e dados sensíveis da empresa, em Windows você ataca o software.
- **Recompensa:** Não parece alarmante? Só um RCE? Recompensa menor.



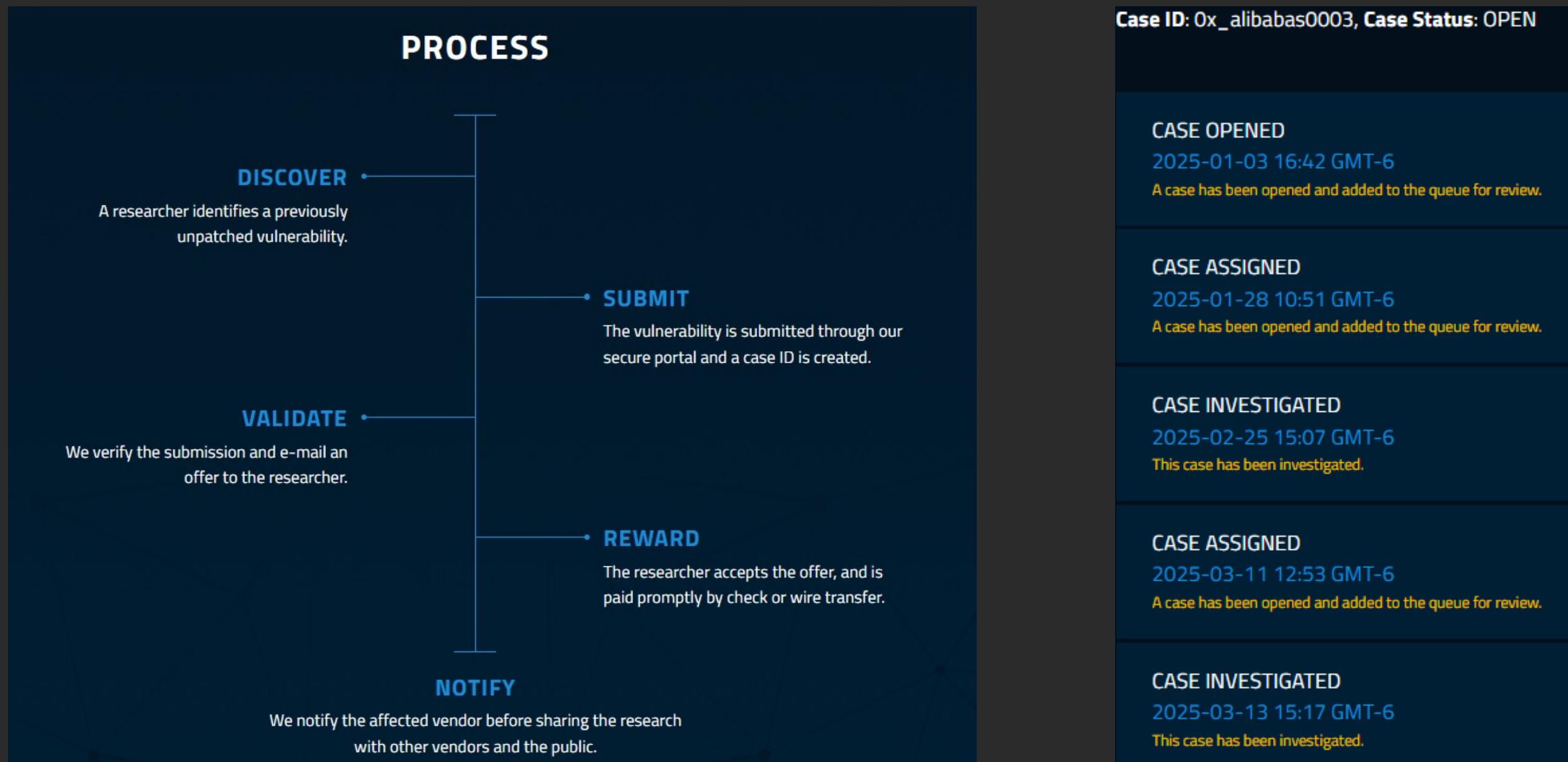
Alguns programas famosos



Programa de Bounty	Recompensa Máxima (USD)
Microsoft Windows Insider Preview	Até \$100,000
Microsoft Hyper-V	Até \$250,000
Microsoft Applications and On-Premises Servers	Até \$30,000
Microsoft Edge (Chromium-based)	Até \$30,000
Windows Defender Application Guard	Até \$30,000
Microsoft 365 Insider	Até \$15,000
Microsoft .NET	Até \$15,000
Microsoft Defender	Até \$20,000



Achou em um binário sem BB? ZDI/Pwn2own



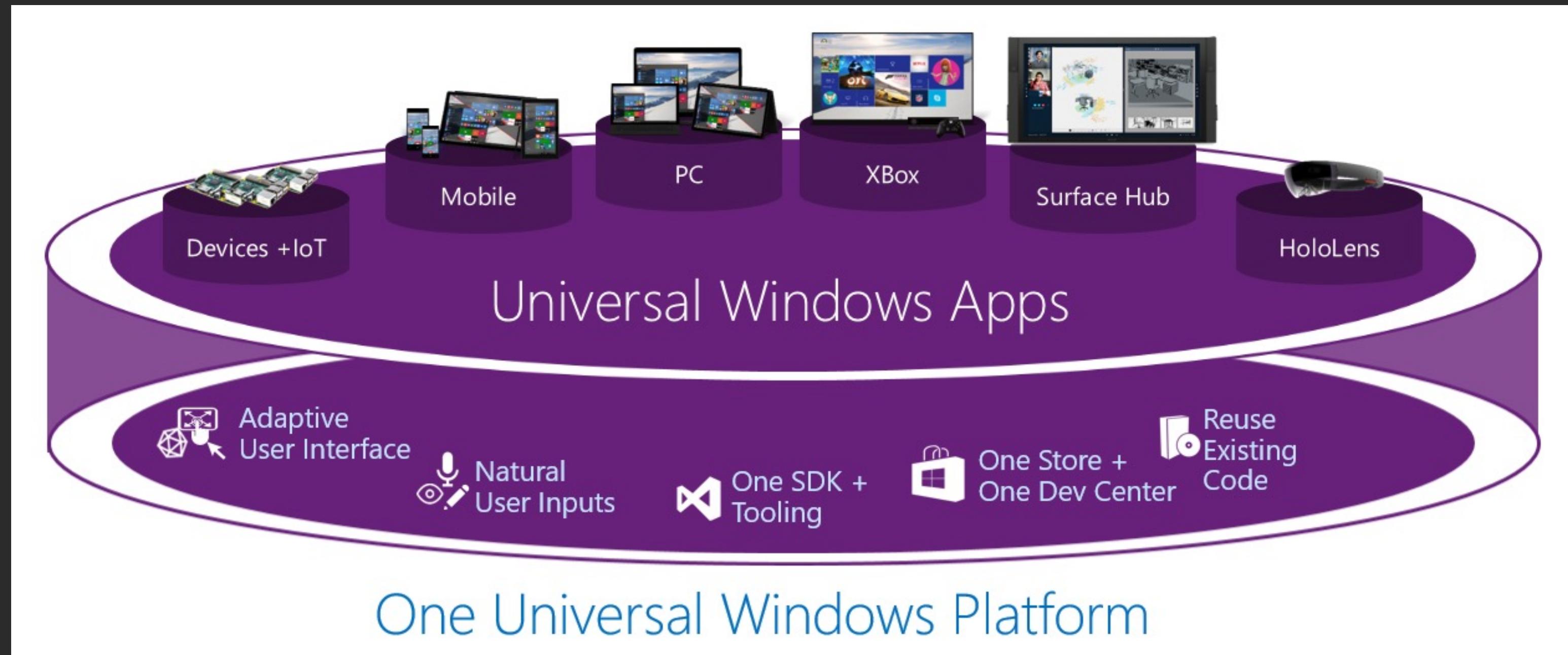


Histórico

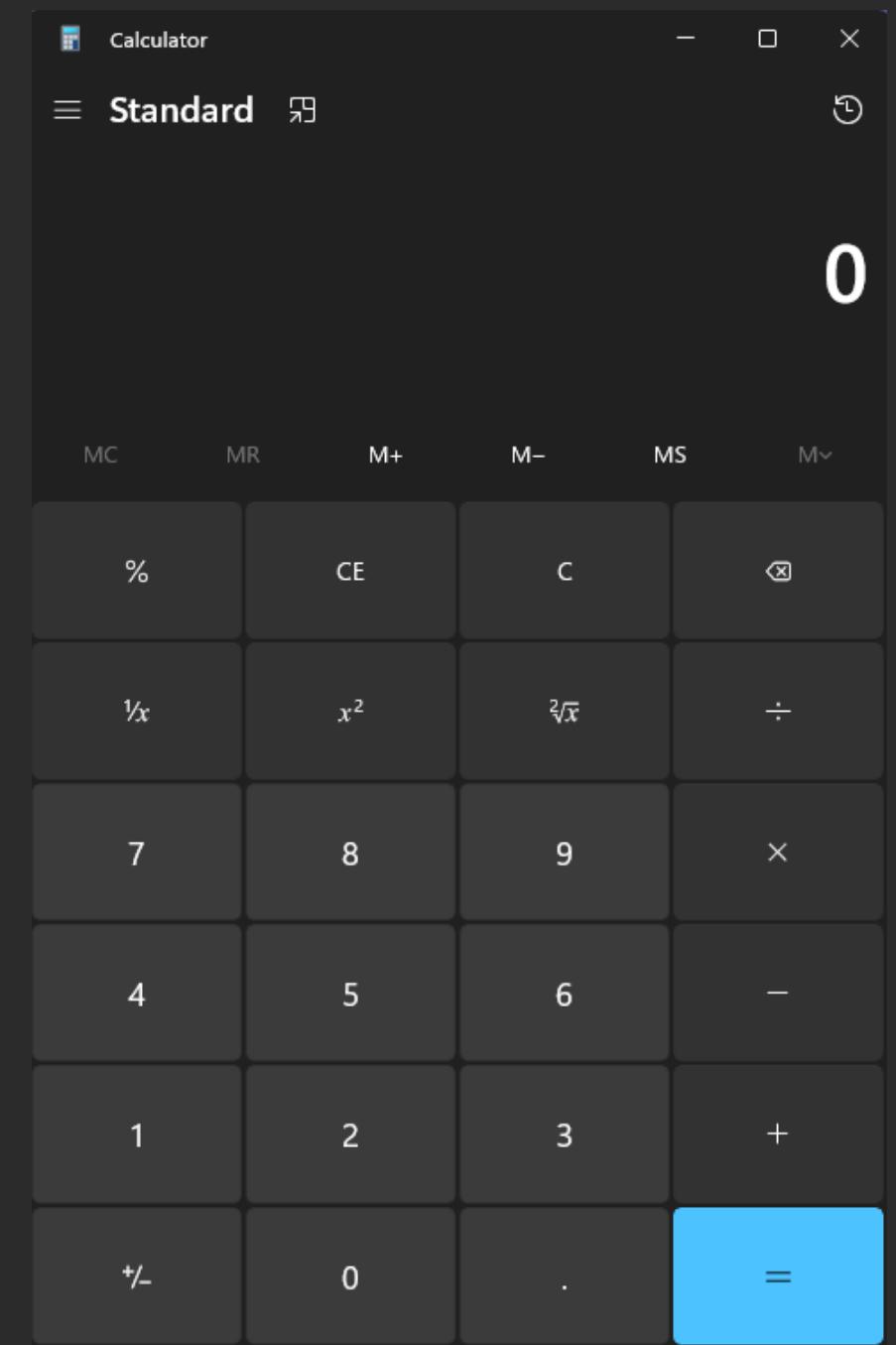
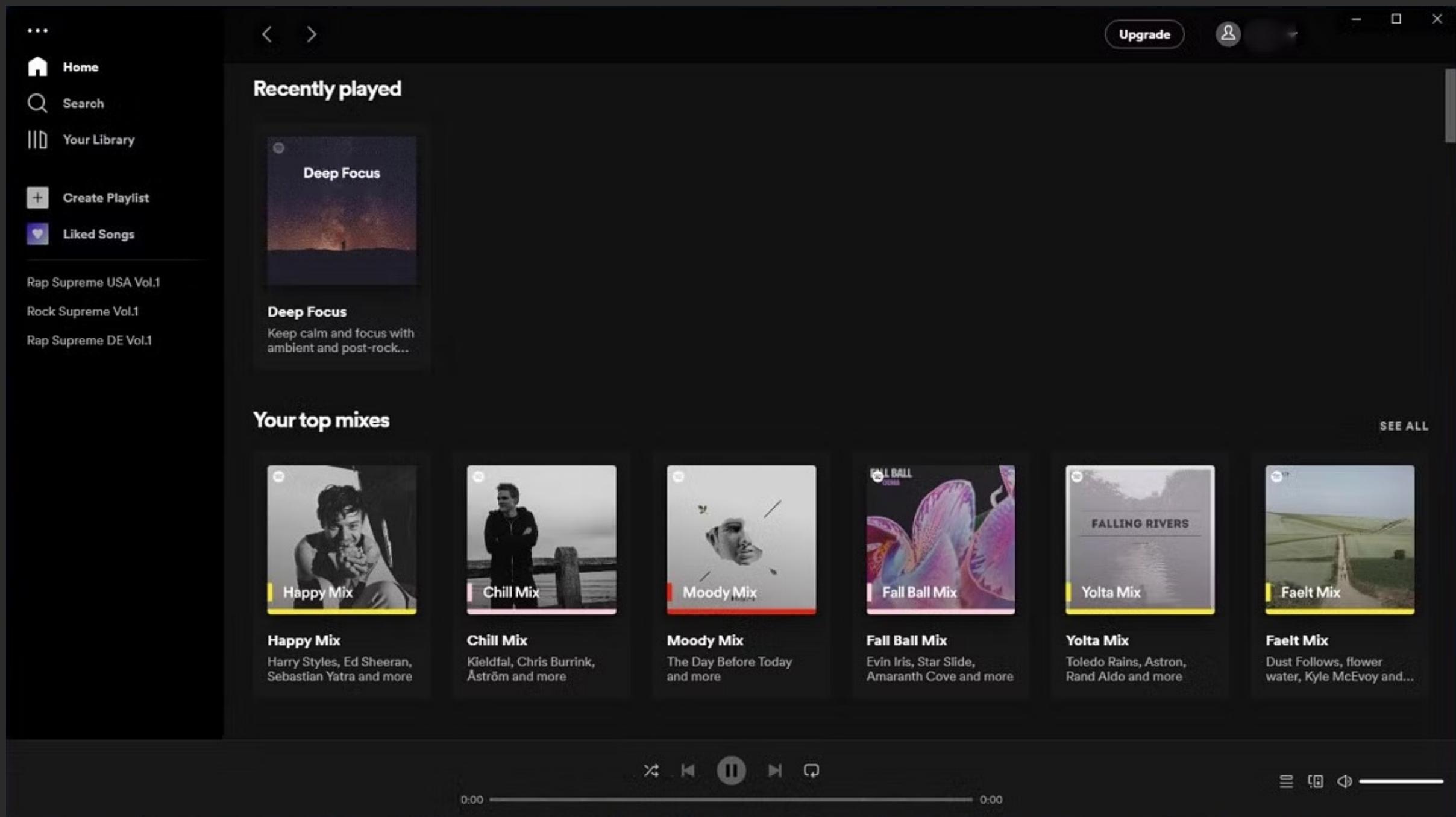
Histórico



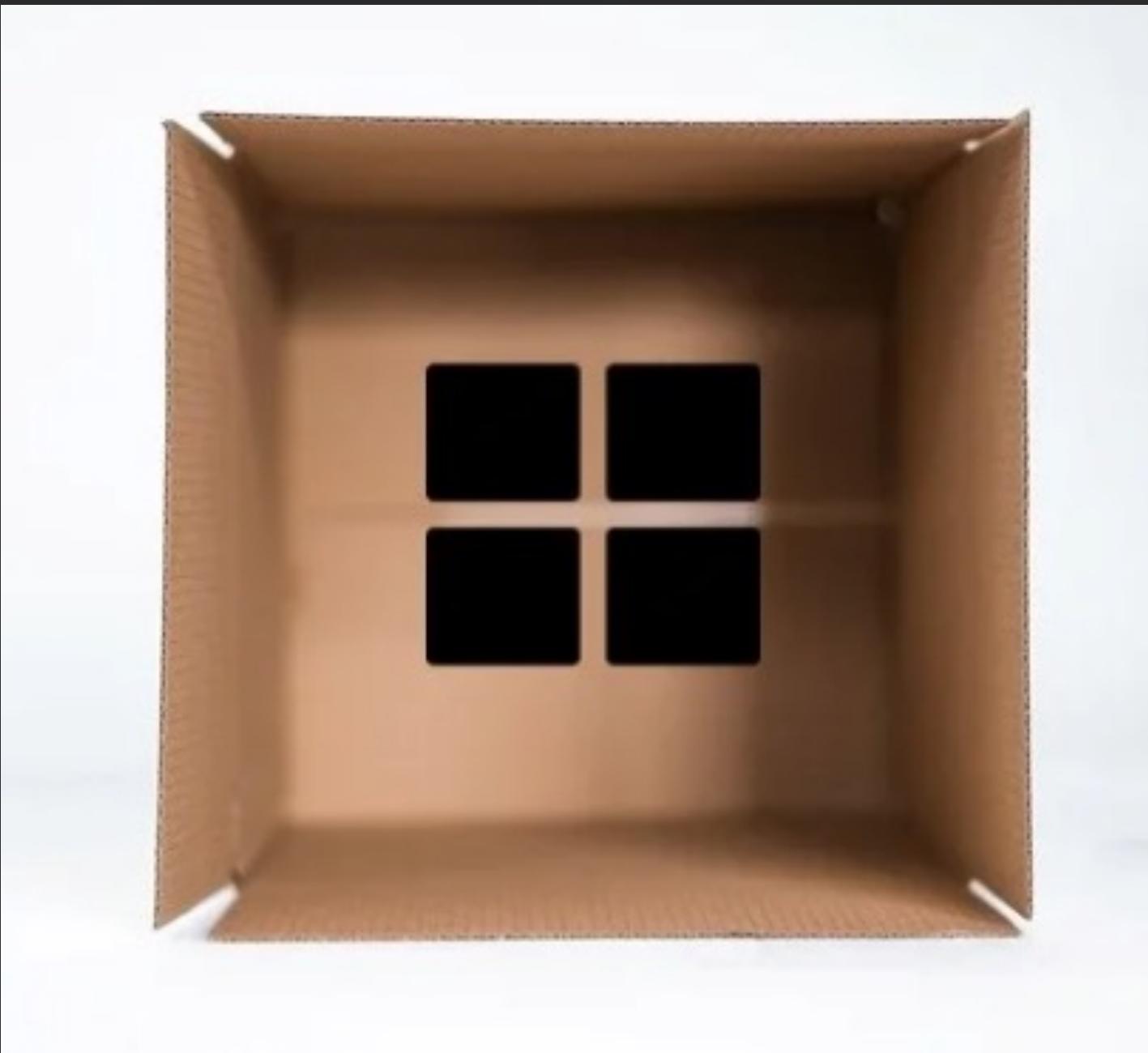
UWP – Universal Windows Platform



UWP apps



UWP Sandbox



Process Hacker [WIN-4K5IL65R91T\computer] (Administrator)

Hacker View Tools Users Help

Refresh Options Find handles or DLLs System information

calculator

Name	PID	CPU	User name	Integrity	Description
RuntimeBroker.exe	5208	0.03	WIN-4K5IL6...\computer	Medium	Runtime Broker
CalculatorApp.exe	4468	0.03	WIN-4K5IL6...\computer	Low	Calculator

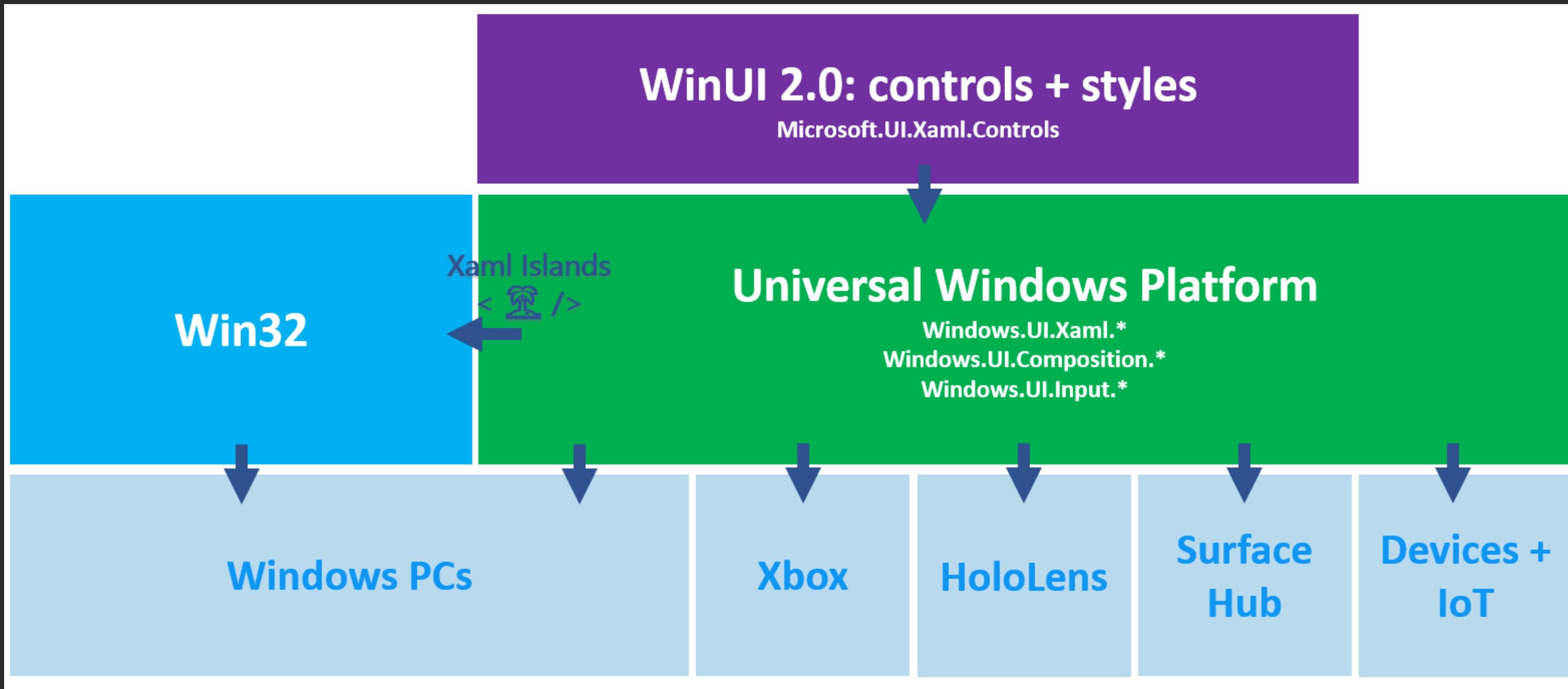
CPU Usage: 5.72% Physical memory: 13.94 GB (21.90%) Processes: 323

0

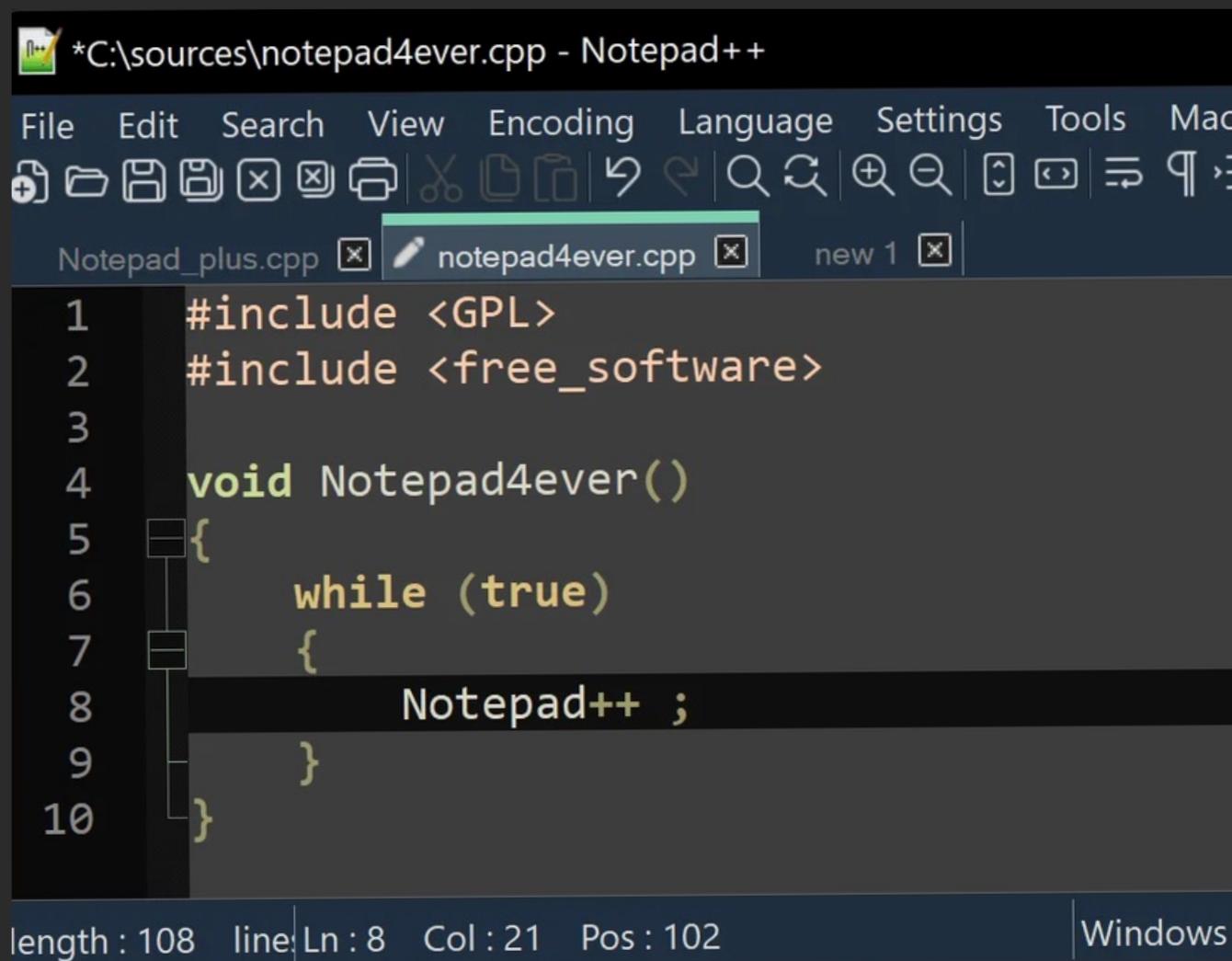
MC	MR	M+	M-	MS	M ^v
%	CE	C	\otimes		
$1/x$	x^2	$\sqrt[3]{x}$	\div		
7	8	9	\times		
4	5	6	-		
1	2	3	+		



Win32



Win32 apps



A screenshot of the Notepad++ text editor. The title bar reads "*C:\sources\notepad4ever.cpp - Notepad++". The menu bar includes File, Edit, Search, View, Encoding, Language, Settings, Tools, and Mac. The toolbar contains various icons for file operations like Open, Save, Find, and Print. The status bar at the bottom shows "length : 108 line: Ln : 8 Col : 21 Pos : 102" and "Windows". The main window displays the following C++ code:

```
1 #include <GPL>
2 #include <free_software>
3
4 void Notepad4ever()
5 {
6     while (true)
7     {
8         Notepad++ ;
9     }
10 }
```



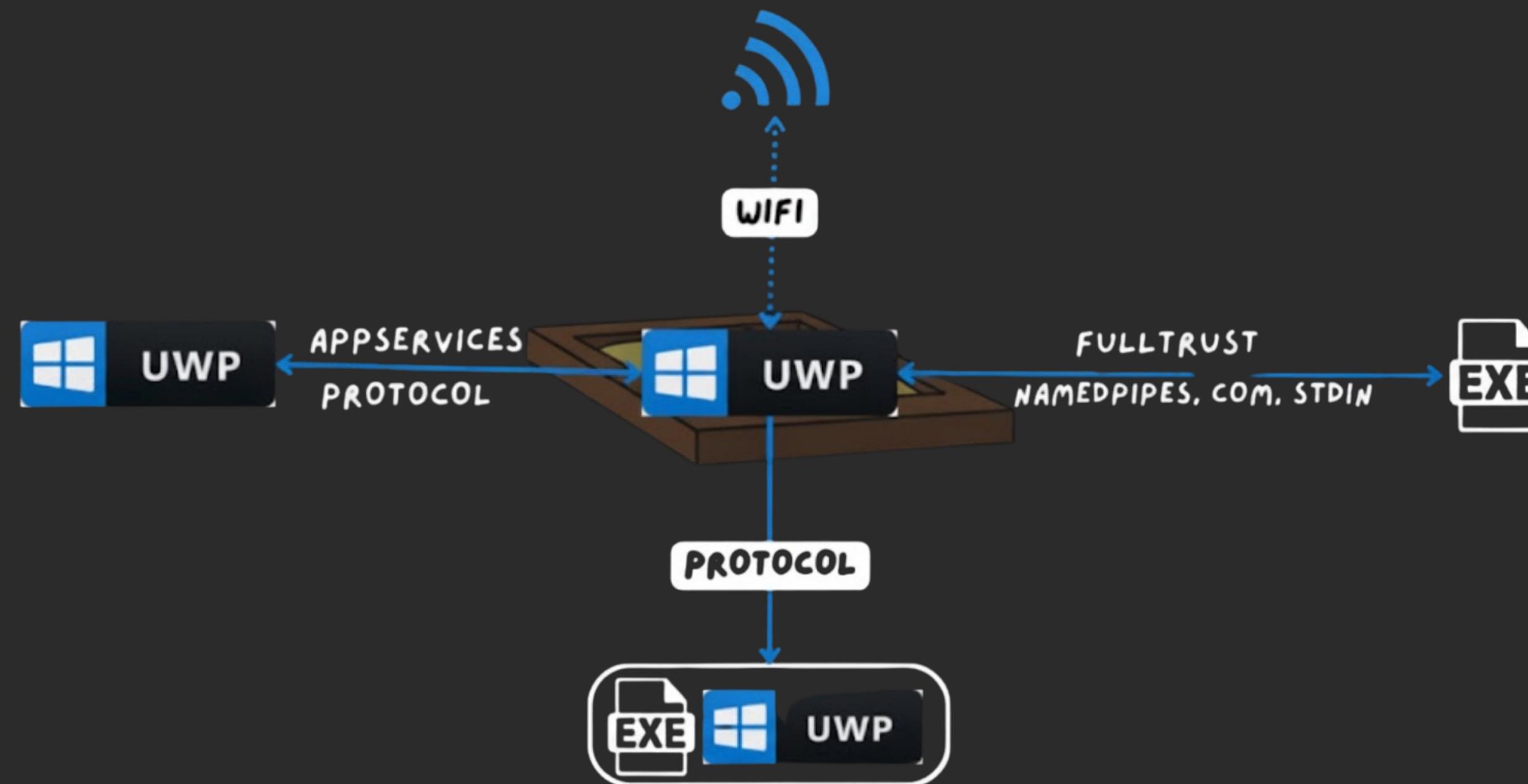
Win32





Entrypoints e Integrity Levels

Entrypoints



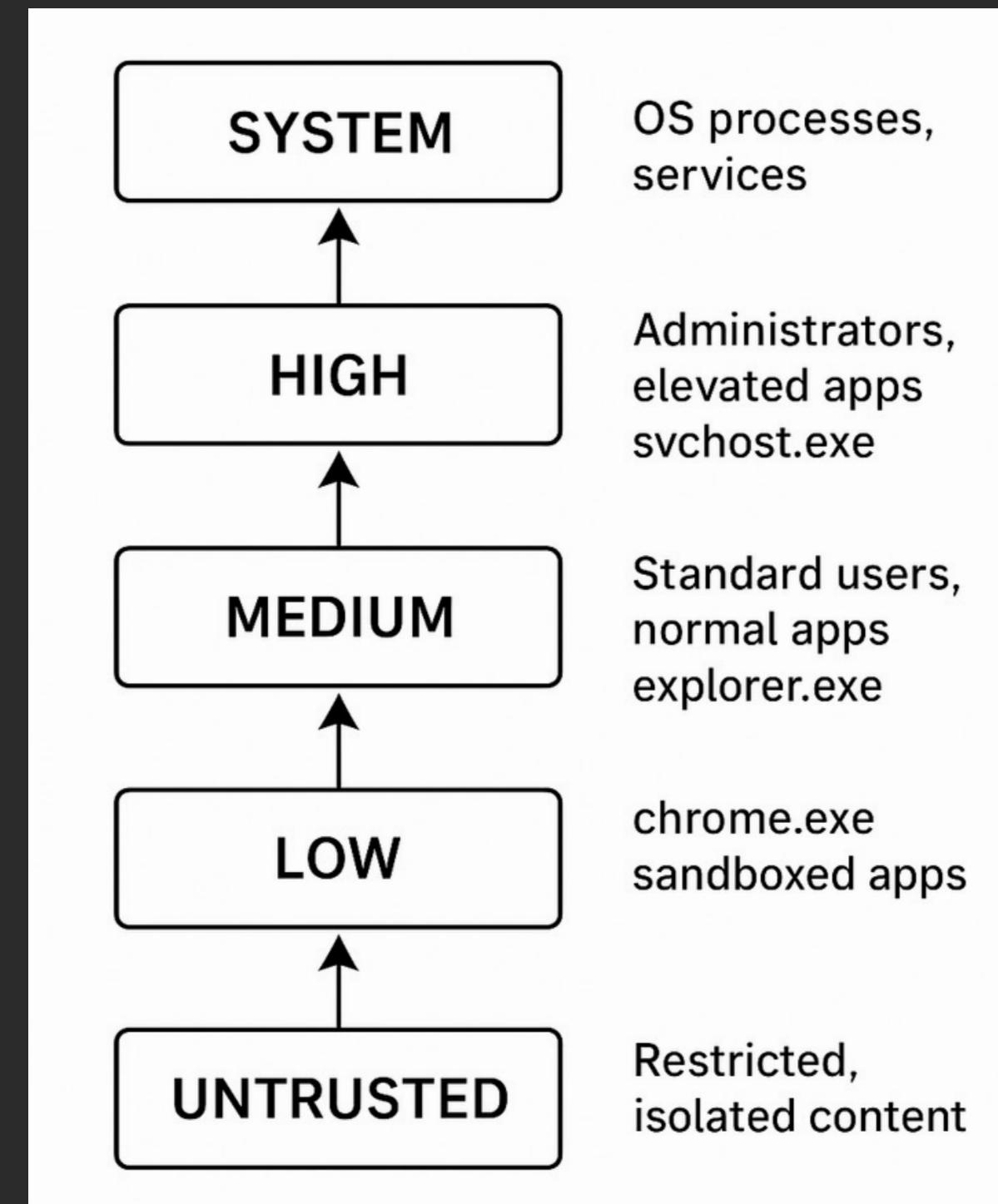
Integrity level

System Informer [DESKTOP-6KV6Q98\0x_alibabas] (Administrator)

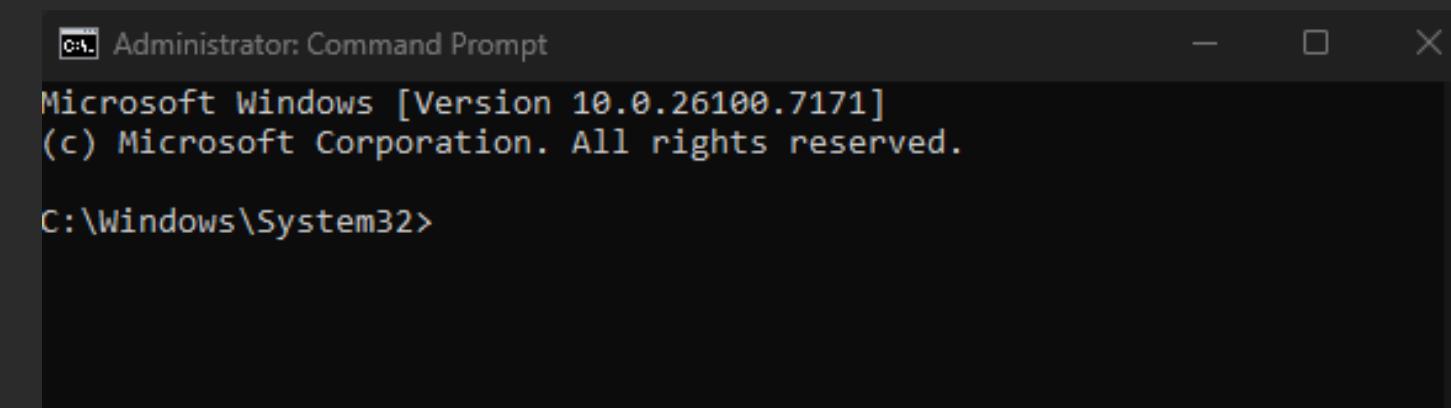
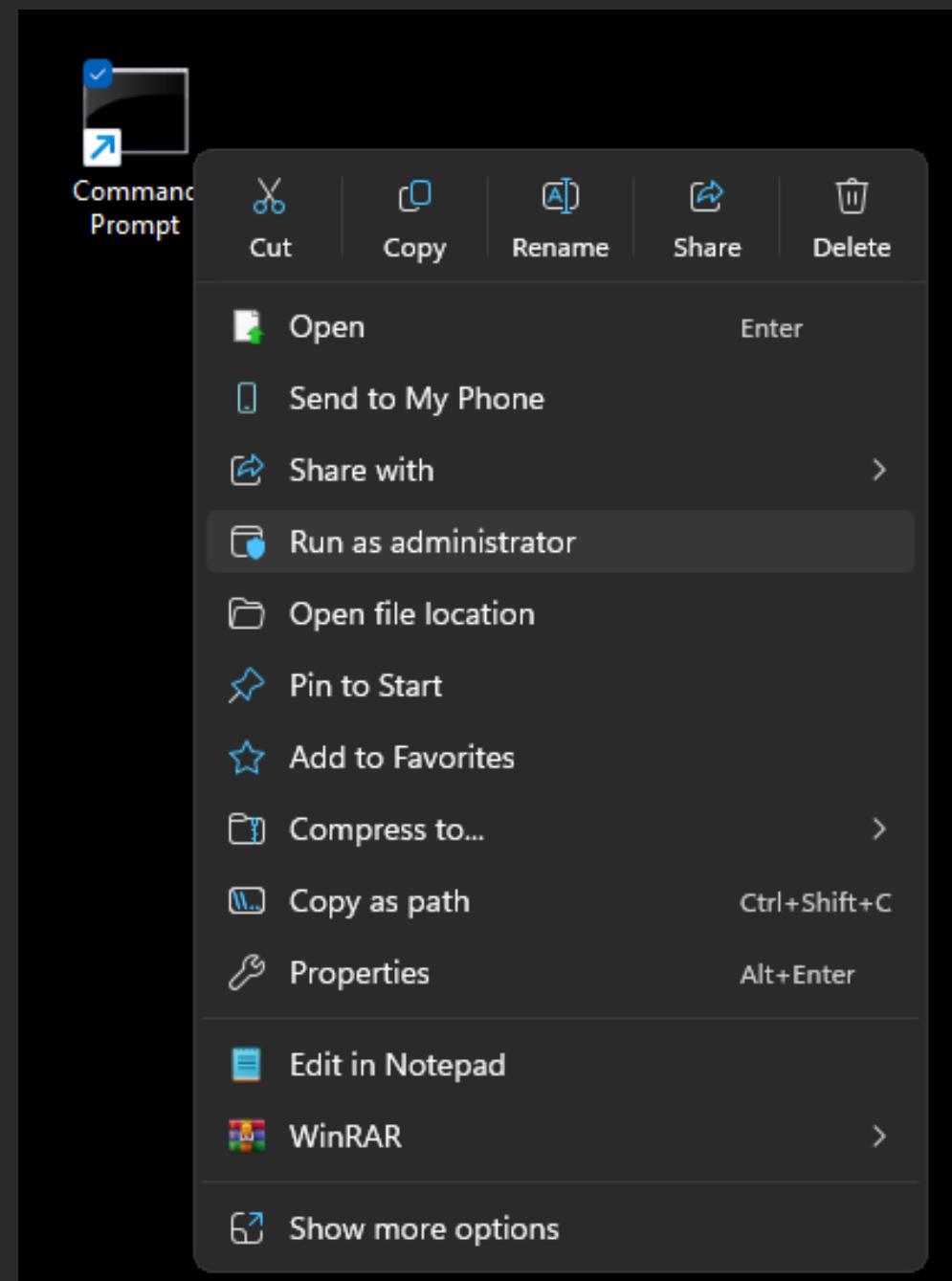
Processes Services Network Disk Firewall Devices

Name	PID	Integrity
Lsalso.exe	1372	System
services.exe	1328	System
winlogon.exe	1304	System
csrss.exe	1208	System
wininit.exe	1200	System
csrss.exe	1116	System
smss.exe	700	System
svchost.exe	684	System
Registry	184	System
Secure System	140	System
taskhostw.exe	24412	High
ctfmon.exe	15576	High
TabTip.exe	12940	High
ArmourySocketServer.exe	10376	High
SystemInformer.exe	8060	High
AcPowerNotification.exe	5832	High
vmmemWSL	4940	High
vmwp.exe	996	High
msedge.exe	27640	Medium
msedge.exe	26508	Medium
svchost.exe	26076	Medium
OpenConsole.exe	25288	Medium
	21612	Medium

CPU usage: 8.39% Physical memory: 12.06 GB (76.88%) Free memory: 3.62 GB (23.12%)



Name	PID	Integrity	User ...	Description	P
NordUpdateService.exe	6744	System	...\SYST	NordSec Update ...	
nordvpn-service.exe	5888	System	...\SYST	nordvpn-service	
NordVPN.exe	2404	Medium	...\0x_al	NordVPN	



Administrator: Command Prompt
Microsoft Windows [Version 10.0.26100.7171]
(c) Microsoft Corporation. All rights reserved.
C:\Windows\System32>

High IL



Integrity level



Low

Medium

High

SYSTEM



Inter-Process Communication

IPC Mechanism	Descrição / Caso de Uso
WinRT / UWP App Services	Comunicação de aplicativo moderno (UWP para UWP/Win32)
COM / DCOM	Component Object Model (objetos locais e remotos)
RPC (Remote Procedure Call)	Executar código em máquinas/processos remotos
Named Pipes	Fluxo de dados confiável, bidirecional e ordenado
Windows Sockets (Winsock)	Rede TCP/UDP padrão
Shared Memory (File Mapping)	Método mais rápido para compartilhamento de dados
Window Messages (HWND)	Comunicação de thread de UI (SendMessage)
Mailslots	Comunicação de transmissão unidirecional
Events / Mutexes / Semaphores	Sincronização e sinalização





Falhas Comuns

Falhas comuns

- Aplicações com alto privilégio fazendo operações de arquivo em caminhos controláveis por usuários sem privilégio - também válido para registro (HKCU vs HKLM)
- Má configuração de IPCs: NamedPipes sem permissões corretas, COM exportados, checagem de assinatura/hash mal feitos

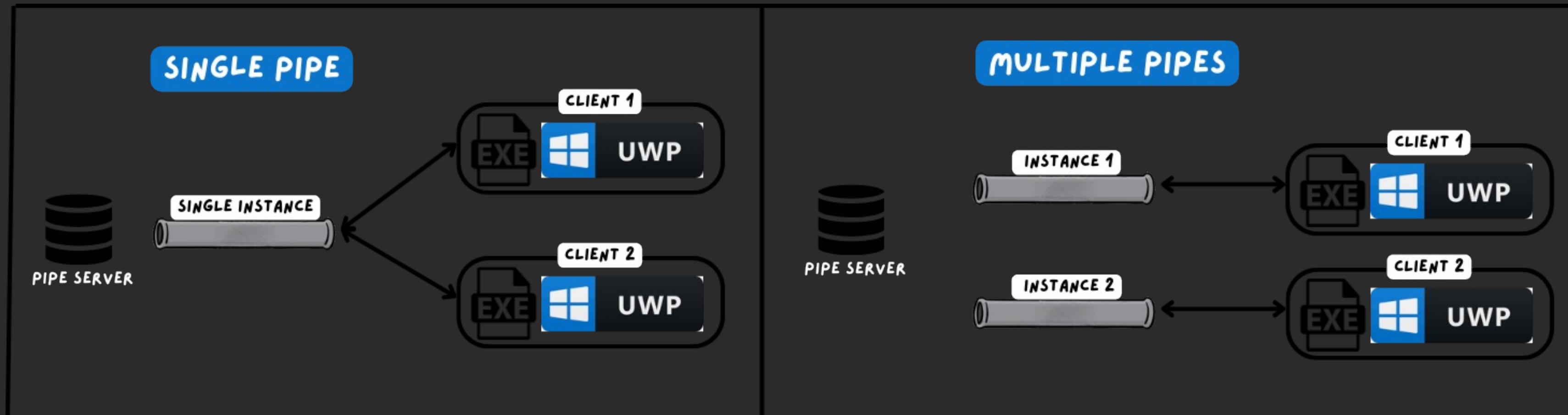




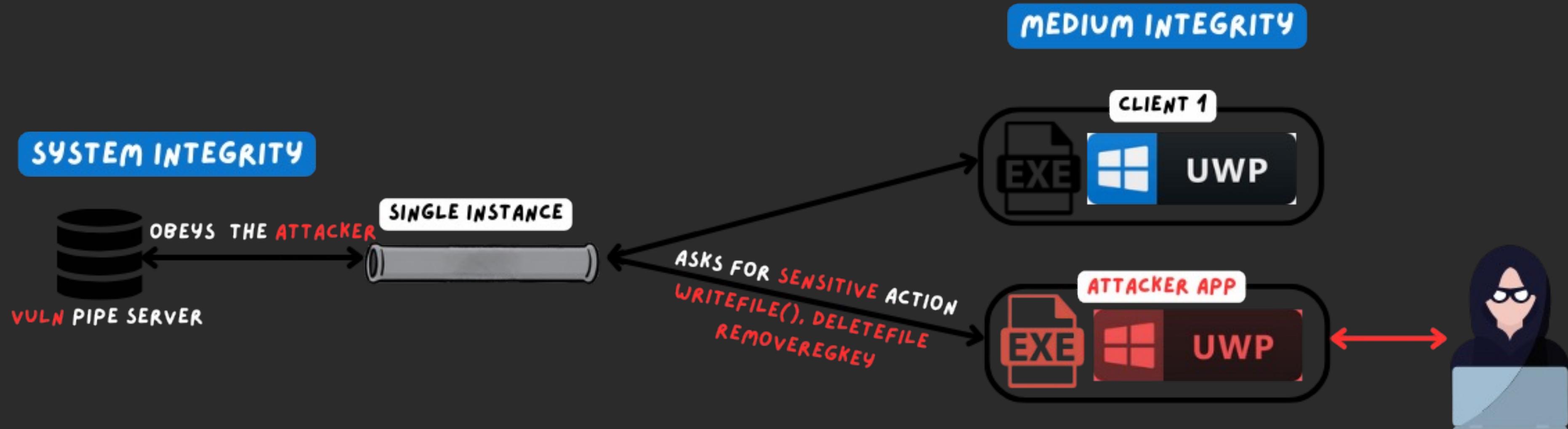
NamedPipes

NamedPipes

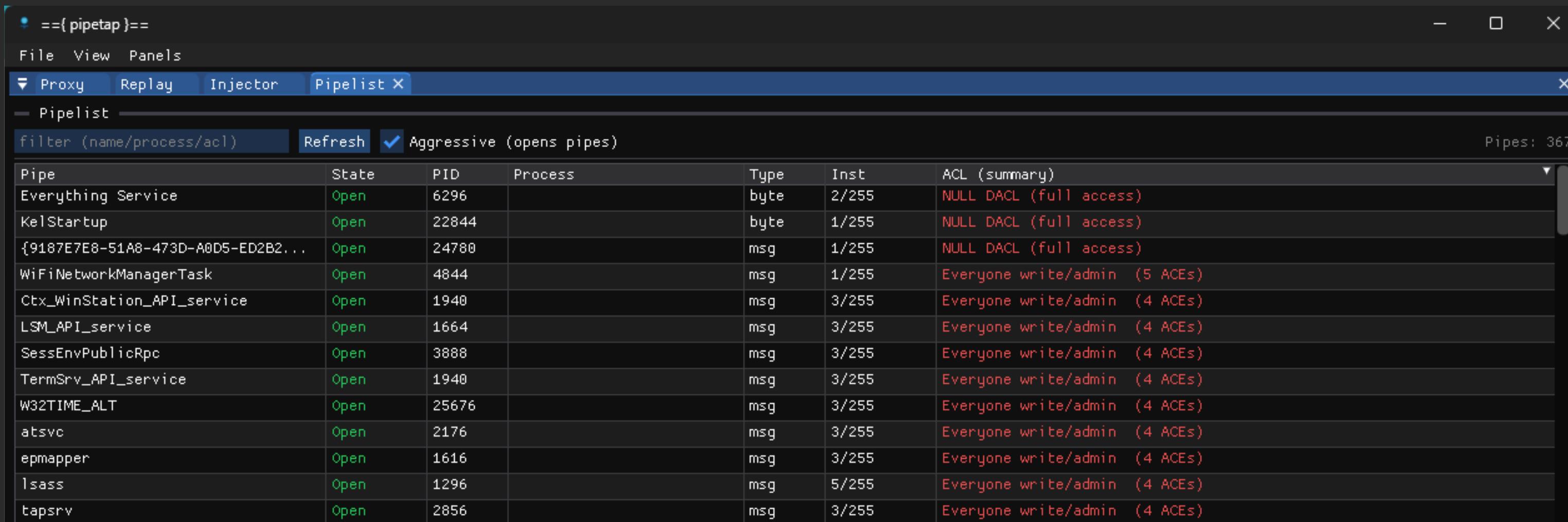
- São como arquivos no filesystem
- Seguem o padrão: \\.\pipe\PipeName (. sendo PC local)
- Desenvolvedor precisa configurar a permissão corretamente



NamedPipes



Permissões NamedPipes



The screenshot shows the pipetap application interface. The title bar says "pipetap". The menu bar includes File, View, Panels, Proxy, Replay, Injector, and Pipelist (which is selected). Below the menu is a toolbar with a Refresh button and a checked checkbox for "Aggressive (opens pipes)". A status bar at the bottom right shows "Pipes: 367". The main area is a table titled "Pipelist" with columns: Pipe, State, PID, Process, Type, Inst, and ACL (summary). The table lists 367 entries, each detailing an open named pipe with its process ID and type, and its current access control list.

Pipe	State	PID	Process	Type	Inst	ACL (summary)
Everything Service	Open	6296		byte	2/255	NULL DACL (full access)
KelStartup	Open	22844		byte	1/255	NULL DACL (full access)
{9187E7E8-51A8-473D-A0D5-ED2B2...	Open	24780		msg	1/255	NULL DACL (full access)
WiFiNetworkManagerTask	Open	4844		msg	1/255	Everyone write/admin (5 ACEs)
Ctx_WinStation_API_service	Open	1940		msg	3/255	Everyone write/admin (4 ACEs)
LSM_API_service	Open	1664		msg	3/255	Everyone write/admin (4 ACEs)
SessEnvPublicRpc	Open	3888		msg	3/255	Everyone write/admin (4 ACEs)
TermSrv_API_service	Open	1940		msg	3/255	Everyone write/admin (4 ACEs)
W32TIME_ALT	Open	25676		msg	3/255	Everyone write/admin (4 ACEs)
atsvc	Open	2176		msg	3/255	Everyone write/admin (4 ACEs)
epmapper	Open	1616		msg	3/255	Everyone write/admin (4 ACEs)
lsass	Open	1296		msg	5/255	Everyone write/admin (4 ACEs)
tapsrv	Open	2856		msg	3/255	Everyone write/admin (4 ACEs)

Accesschk v6.15 – Reports effective permissions for securable objects
Copyright (C) 2006–2022 Mark Russinovich
Sysinternals – www.sysinternals.com

```
\.\Pipe\eventlog
RW Everyone
RW NT SERVICE\EventLog
R OWNER RIGHTS
R NT AUTHORITY\LOCAL SERVICE
```

=={pipetap}==

File View Panels Administrator

Proxy Replay Injector X Pipelist

- Target Process

image

Refresh

Name	User	PID	Arch	IL	Session	System
ImageService.exe	NT AUTHORITY\SYSTEM	7864	x86	System	8	SYSTEM

- Parameters -

7864 PID C:\Users\0x_alibabas\Downloads\pipetap-1.0.1-x86\pipetap-dll.dll Use Default Auto-connect proxy Inject Support DLL

Injector Status Clear

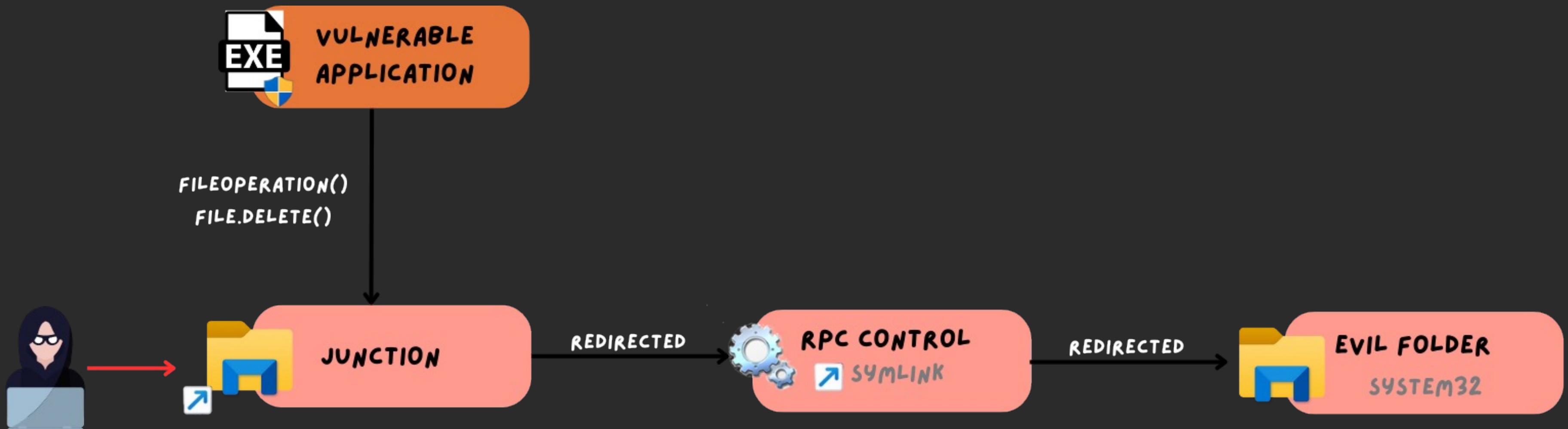


Symbolic Links

Symbolic Links



Symbolic Links



307

X

Windows

X | +



307

Search 307



+ New



Sort



Viewer



Ho

Gal

I

D

I

F

F

F

F

F

F

F

F

F

F

This

Net

Lin



307.jpg



307 - Copy.jpg

Symbolic Links

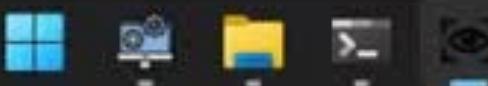
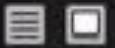
Delete

Move

Rename

SetSecurityFile

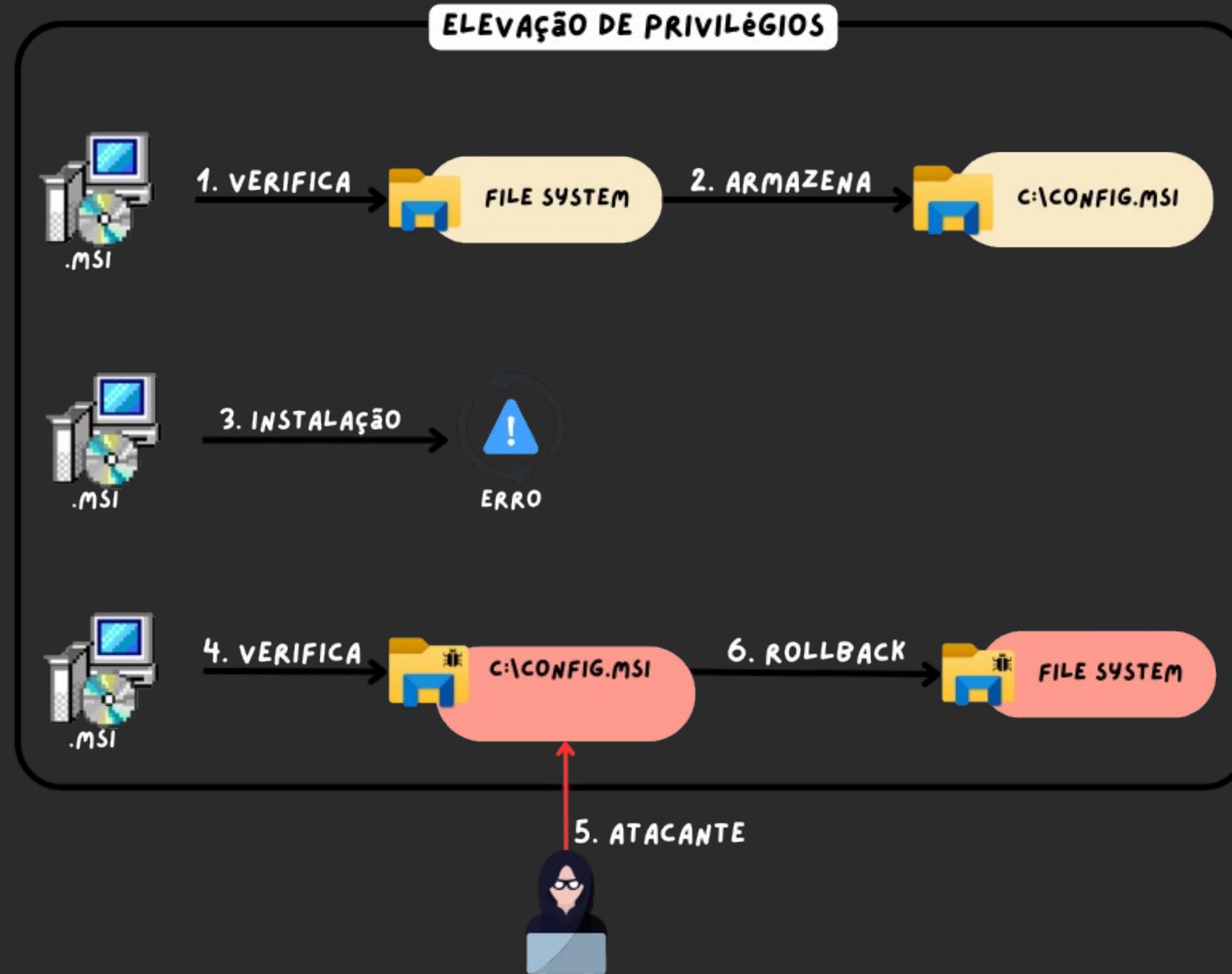
2 items |



Deleção arbitrária



Deleção arbitrária



Impacto





Oplocks

The image shows two separate Command Prompt windows running on a Windows operating system. Both windows have a dark theme.

Left Window (Command Prompt):

- Output of `echo a > a.txt`:
C:\Temp>echo a > a.txt
- Output of `SetOpLock.exe`:
C:\Temp>SetOpLock.exe
Usage: SetOpLock target [rwdx]
Share Mode:
r - FILE_SHARE_READ
w - FILE_SHARE_WRITE
d - FILE_SHARE_DELETE
x - Exclusive lock
- Output of `SetOpLock.exe "a.txt" w`:
C:\Temp>SetOpLock.exe "a.txt" w

Right Window (Command Prompt - type a.txt):

- Output of `echo a > a.txt`:
C:\Temp>echo a > a.txt
- Output of `type a.txt`:
a
- Output of `echo a >> a.txt`:
C:\Temp>echo a >> a.txt
- Output of `type a.txt`:
a
a
- Final prompt:
C:\Temp>

Demo



```
Microsoft Visual Studio Debug + | v
[+] Config.msi directory created!
[+] File to export macro: C:\windows\temp\92075f2e-d674-4011-a9ea-62886b86538b\1.xml
[+] File C:\windows\temp\92075f2e-d674-4011-a9ea-62886b86538b\1.xml.tmp created!
[*] MSI file: C:\windows\temp\MSIA03E.tmp
[+] Rollback script overwritten!
Error: 4390
error :2

C:\Users\computer\Desktop\RazerEoP2\RazerEoP2\x64\Release\RazerEoP.exe (process 30640) exited with code 0.
To automatically close the console when debugging stops, enable Tools->Options->Debugging->Automatically close the console when debugging stops.
Press any key to close this window . . .|
```

```
Administrator: C:\windows\system32\cmd.exe
Microsoft Windows [Version 10.0.22621.3085]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>whoami
nt authority\system

C:\Windows\System32>whoami /priv

PRIVILEGES INFORMATION
-----

Privilege Name          Description          State
-----
SeAssignPrimaryTokenPrivilege Replace a process level token      Disabled
SeLockMemoryPrivilege    Lock pages in memory       Enabled
SeIncreaseQuotaPrivilege Adjust memory quotas for a process  Disabled
SeTcbPrivilege           Act as part of the operating system  Enabled
SeSecurityPrivilege     Manage auditing and security log  Enabled
SeTakeOwnershipPrivilege Take ownership of files or other objects  Disabled
SeLoadDriverPrivilege   Load and unload device drivers  Disabled
SeProfileSingleProcessPrivilege Profile single process        Enabled
SeIncreaseBasePriorityPrivilege Increase scheduling priority  Enabled
SeCreatePagefilePrivilege Create a pagefile            Enabled
SeCreatePermanentPrivilege Create permanent shared objects  Enabled
SeBackupPrivilege         Back up files and directories  Disabled
SeRestorePrivilege        Restore files and directories  Disabled
SeShutdownPrivilege      Shut down the system        Disabled
SeAuditPrivilege          Generate security audits     Enabled
SeChangeNotifyPrivilege   Bypass traverse checking    Enabled
SeImpersonatePrivilege   Impersonate a client after authentication  Enabled
SeCreateGlobalPrivilege   Create global objects        Enabled
SeCreateSymbolicLinkPrivilege Create symbolic links       Enabled

C:\Windows\System32>
```





Casos reais

Caso 1 - Redacted

Caso 2 - Redacted

Caso 3 - Redacted

Tools



PipeTap

<https://github.com/sensepost/pipetap>

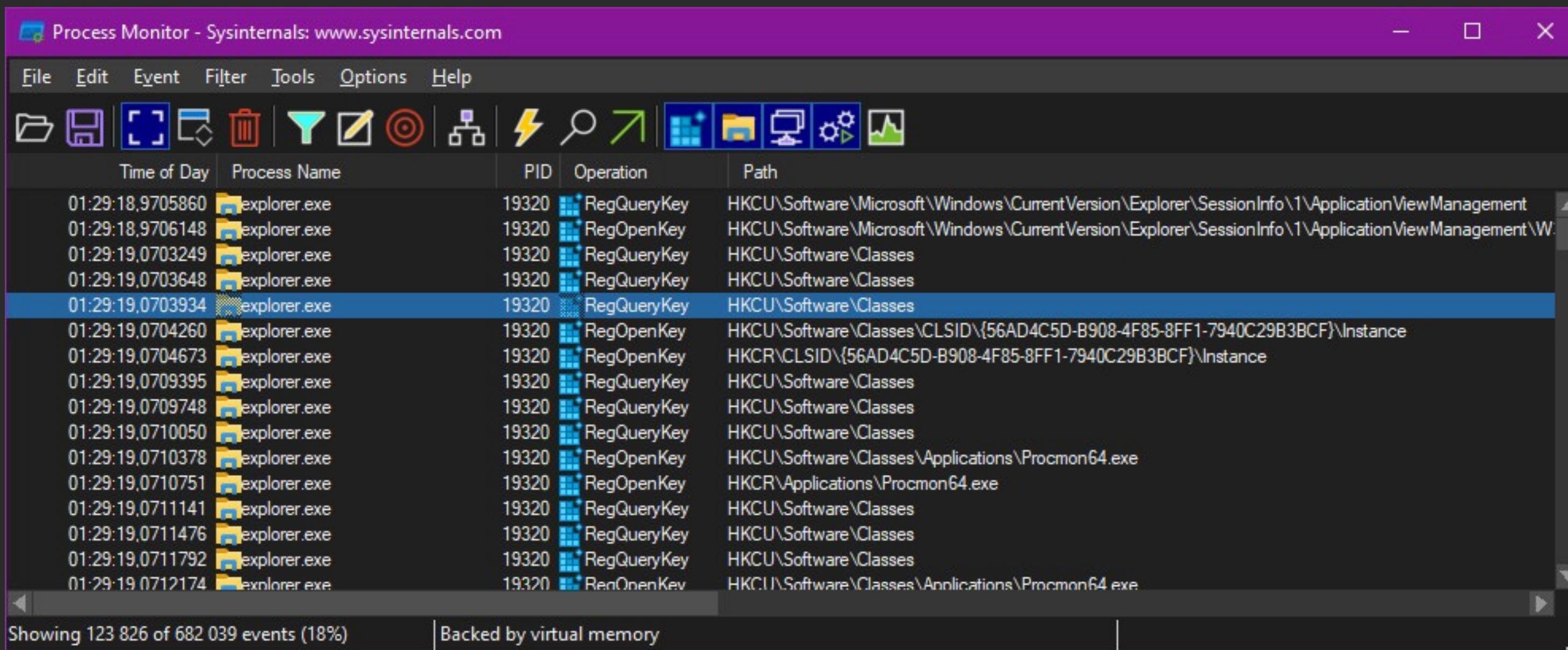
The screenshot shows the PipeTap application window. At the top, there's a toolbar with icons for file operations, a status bar indicating "Administrator", and a menu bar with "File", "View", and "Panels". Below the menu is a tab bar with "Proxy" (selected), "Replay", "Injector", and "Pipelists". A panel below the tabs shows a target process with PID 7784, labeled as connected. There are buttons for "Edit requests" and "Edit responses". A "Selection Data" section contains a hex dump of memory starting at address 00000000, showing bytes EF BB BF. At the bottom is a "Traffic Log" table with columns: ID, Time, D..., Pipe, API, Peer Image, Peer PID, Size, and Data. The log lists several events related to a pipe named '\imagepipe' between processes like pipetap-gui.exe, ImageService.exe, cmd.exe, and FullTrust.exe.

ID	Time	D...	Pipe	API	Peer Image	Peer PID	Size	Data
8	09:39:29	<-	\imagepipe	NtReadFile	pipetap-gui.exe	25532	4	a ..
7	09:33:28	--	\imagepipe	NtCreateNamedPi	ImageService.exe	7784	-	
6	09:33:28	--	\imagepipe	NtClose	cmd.exe	25020	-	
5	09:33:28	<-	\imagepipe	NtReadFile	cmd.exe	25020	4	a ..
4	09:31:33	--	\imagepipe	NtCreateNamedPi	ImageService.exe	7784	-	
3	09:31:33	--	\imagepipe	NtClose	FullTrust.exe	20424	-	
2	09:31:33	<-	\imagepipe	NtReadFile	FullTrust.exe	20424	62	deleC:\Users\0x_alibabas\Desktop\307\UWP (4) (1) - Copy.
1	09:31:33	<-	\imagepipe	NtReadFile	FullTrust.exe	20424	3	...



Process Monitor

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



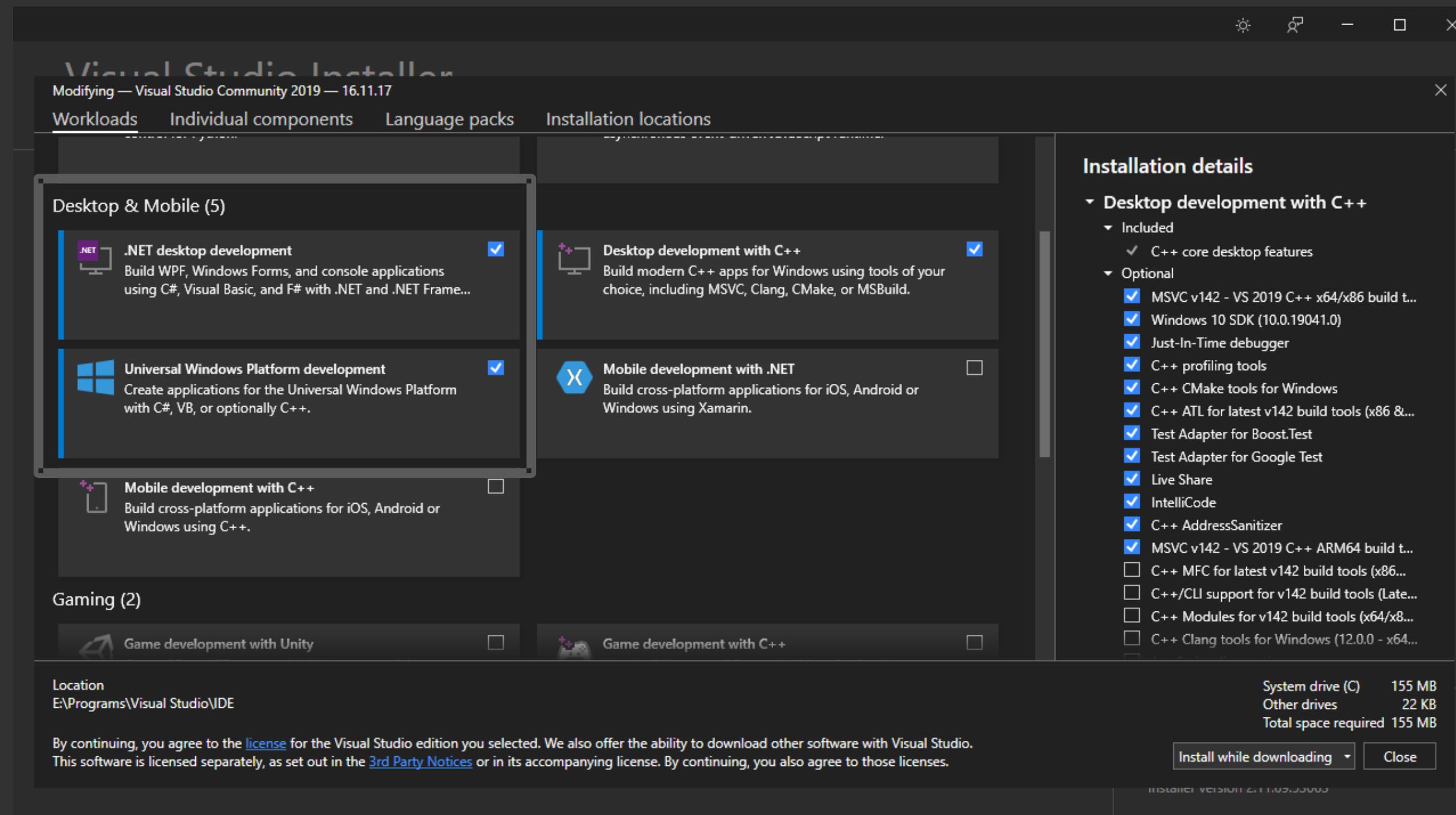
The screenshot shows the Process Monitor application interface. The main window displays a list of registry events captured by the tool. The columns in the table are: Time of Day, Process Name, PID, Operation, and Path. The rows show multiple entries for the process 'explorer.exe' with PID 19320, performing various registry operations like RegQueryKey and RegOpenKey across different registry keys under HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement and HKCU\Software\Classes.

Time of Day	Process Name	PID	Operation	Path
01:29:18,9705860	explorer.exe	19320	RegQueryKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement
01:29:18,9706148	explorer.exe	19320	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W...
01:29:19,0703249	explorer.exe	19320	RegQueryKey	HKCU\Software\Classes
01:29:19,0703648	explorer.exe	19320	RegQueryKey	HKCU\Software\Classes
01:29:19,0703934	explorer.exe	19320	RegQueryKey	HKCU\Software\Classes
01:29:19,0704260	explorer.exe	19320	RegOpenKey	HKCU\Software\Classes\CLSID\{56AD4C5D-B908-4F85-8FF1-7940C29B3BCF}\Instance
01:29:19,0704673	explorer.exe	19320	RegOpenKey	HKCR\CLSID\{56AD4C5D-B908-4F85-8FF1-7940C29B3BCF}\Instance
01:29:19,0709395	explorer.exe	19320	RegQueryKey	HKCU\Software\Classes
01:29:19,0709748	explorer.exe	19320	RegQueryKey	HKCU\Software\Classes
01:29:19,0710050	explorer.exe	19320	RegQueryKey	HKCU\Software\Classes
01:29:19,0710378	explorer.exe	19320	RegOpenKey	HKCU\Software\Classes\Applications\Procmon64.exe
01:29:19,0710751	explorer.exe	19320	RegOpenKey	HKCR\Applications\Procmon64.exe
01:29:19,0711141	explorer.exe	19320	RegQueryKey	HKCU\Software\Classes
01:29:19,0711476	explorer.exe	19320	RegQueryKey	HKCU\Software\Classes
01:29:19,0711792	explorer.exe	19320	RegQueryKey	HKCU\Software\Classes
01:29:19,0712174	explorer.exe	19320	RegOpenKey	HKCU\Software\Classes\Applications\Procmon64.exe



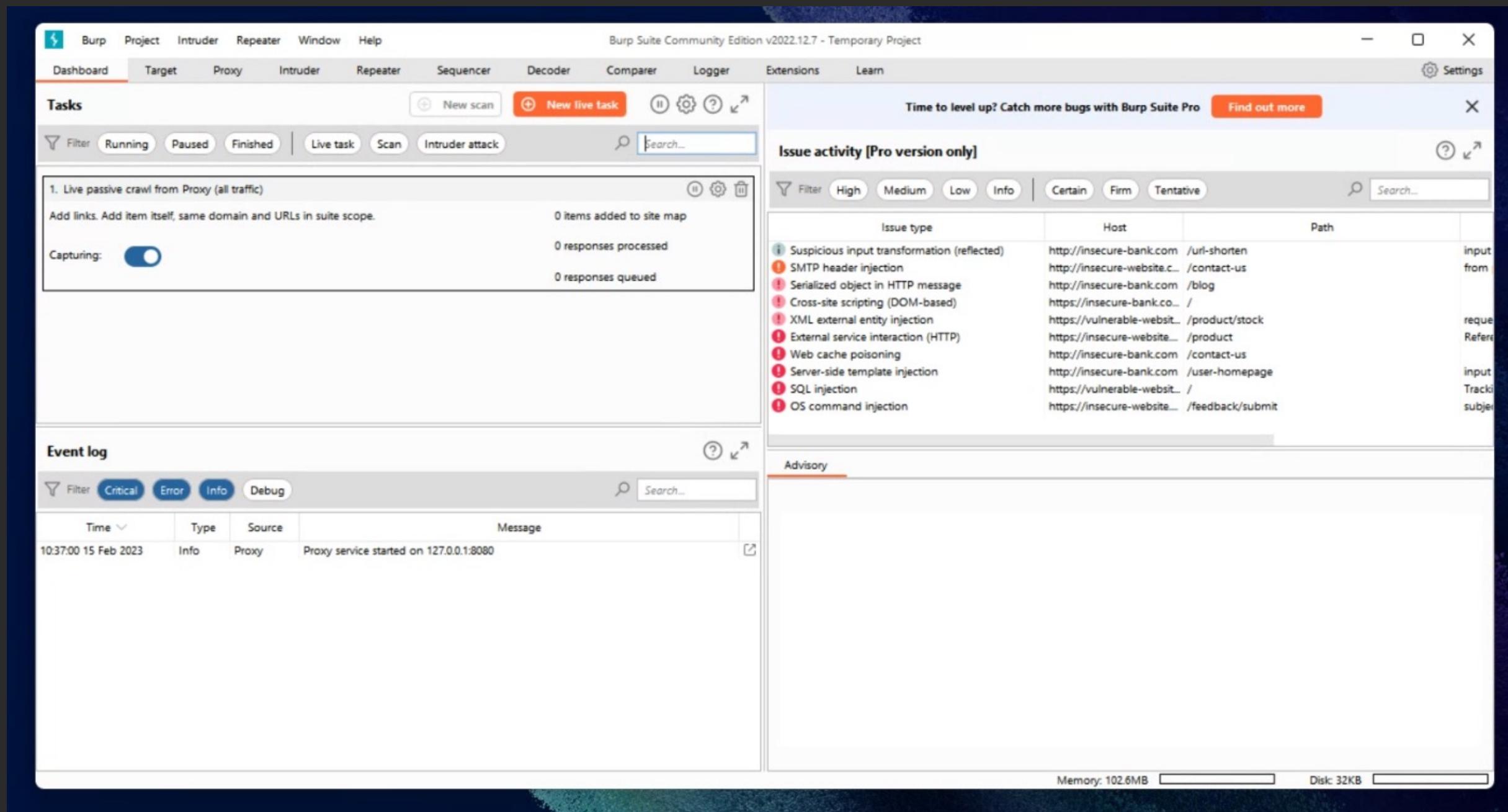
Visual Studio

<https://visualstudio.microsoft.com/>



Burp Suite

<https://portswigger.net/burp>



Process Explorer / System Informer

<https://learn.microsoft.com/en-us/sysinternals/downloads/process-explorer>

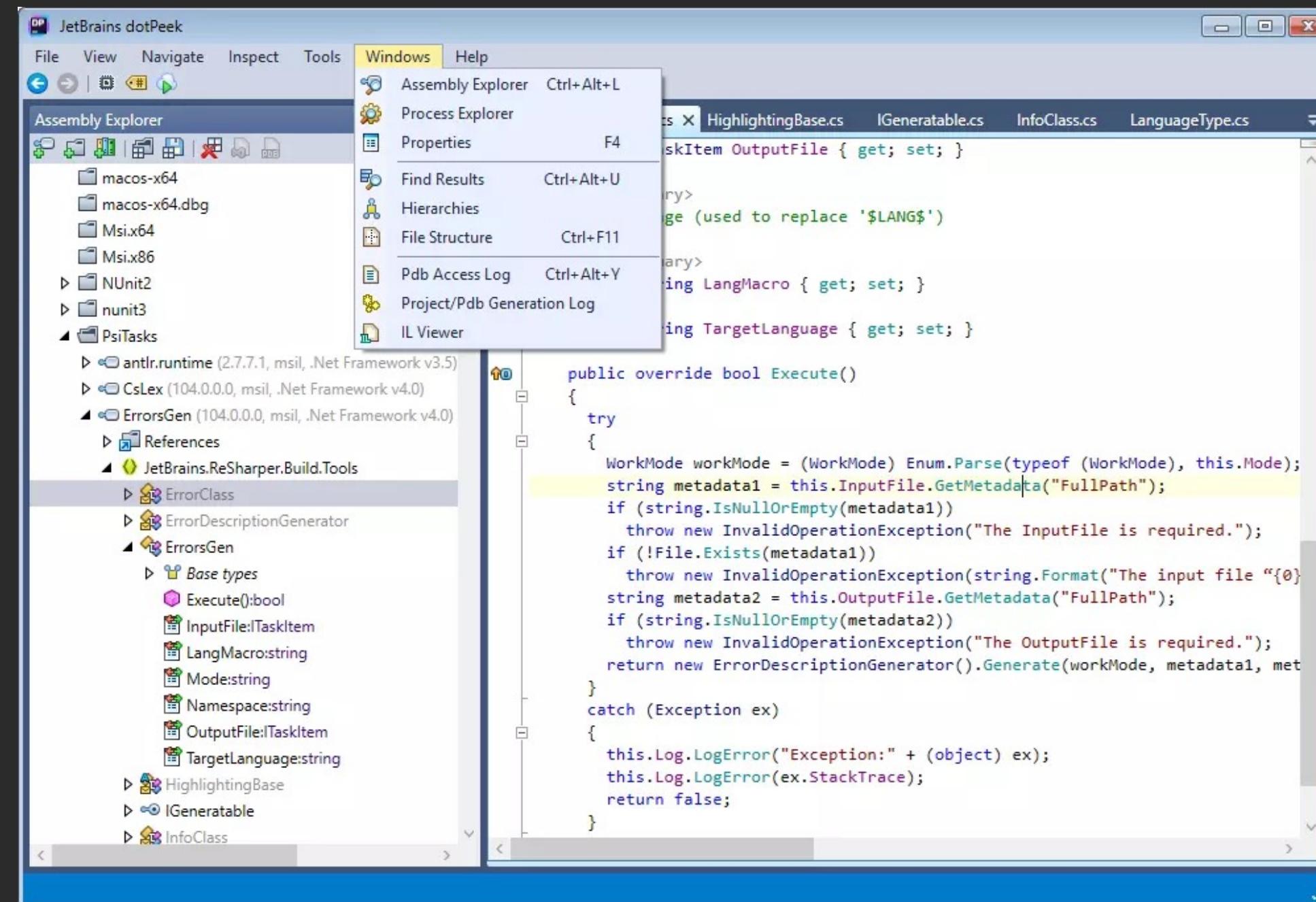
<https://systeminformer.sourceforge.io/>

Name	PID	CPU	I/O total rate	Private bytes	User name	Description
System Idle Process	89.08	0.53		60 kB	NT AUTHORITY\SYSTEM	
System	4			68 kB	NT AUTHORITY\SYSTEM	NT Kernel & System
Secure System	140			184 kB	NT AUTHORITY\SYSTEM	
Registry	188			23.73 MB	NT AUTHORITY\SYSTEM	
smss.exe	756			1.15 MB	NT AUTHORITY\SYSTEM	Windows Session Manager
Memory Compression	3084			296 kB	NT AUTHORITY\SYSTEM	
Interrupts		0.82		0		Interrupts and DPCs
csrss.exe	968			2.29 MB	NT AUTHORITY\SYSTEM	Client Server Runtime Process
wininit.exe	848			1.45 MB	NT AUTHORITY\SYSTEM	Windows Start-Up Application
services.exe	1076	0.13		6.93 MB	NT AUTHORITY\SYSTEM	Services and Controller app
svchost.exe	1228			10.42 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Services
SearchHost.exe	11532			164.18 MB	JXY-DESKTOP\jxy	
StartMenuExperienc...	11556			49.69 MB	JXY-DESKTOP\jxy	Windows Start Experience Host
Widgets.exe	11672			8.1 MB	JXY-DESKTOP\jxy	
msedgewebviewhost...	11896			40.34 MB	JXY-DESKTOP\jxy	Microsoft Edge WebView2
msedgewe...	12824			1.9 MB	JXY-DESKTOP\jxy	Microsoft Edge WebView2
msedgewe...	15772			241.26 MB	JXY-DESKTOP\jxy	Microsoft Edge WebView2
msedgewe...	2892			11.25 MB	JXY-DESKTOP\jxy	Microsoft Edge WebView2
msedgewe...	22144			7.39 MB	JXY-DESKTOP\jxy	Microsoft Edge WebView2
msedgewe...	10524			112.8 MB	JXY-DESKTOP\jxy	Microsoft Edge WebView2
RuntimeBroker.exe	11760			11.22 MB	JXY-DESKTOP\jxy	Runtime Broker
RuntimeBroker.exe	11872			3.35 MB	JXY-DESKTOP\jxy	Runtime Broker
ShellExperienceHost...						



dotPeek

<https://www.jetbrains.com/decompiler/>



The screenshot shows the JetBrains dotPeek interface. The left pane is the Assembly Explorer, displaying a tree of assembly components. The right pane is the code editor, showing C# source code for a class named `ErrorsGen`. The code implements the `IErrorGenerator` interface and overrides the `Execute` method. The code checks for required input and output files and logs errors if they are missing. The assembly explorer shows various assemblies like `antlr.runtime`, `CsLex`, and `ErrorsGen`.

```
public override bool Execute()
{
    try
    {
        WorkMode workMode = (WorkMode) Enum.Parse(typeof(WorkMode), this.Mode);
        string metadata1 = this.InputFile.GetMetadata("FullPath");
        if (string.IsNullOrEmpty(metadata1))
            throw new InvalidOperationException("The InputFile is required.");
        if (!File.Exists(metadata1))
            throw new InvalidOperationException(string.Format("The input file '{0}' does not exist.", metadata1));
        string metadata2 = this.OutputFile.GetMetadata("FullPath");
        if (string.IsNullOrEmpty(metadata2))
            throw new InvalidOperationException("The OutputFile is required.");
        return new ErrorDescriptionGenerator().Generate(workMode, metadata1, metadata2);
    }
    catch (Exception ex)
    {
        this.Log.LogError("Exception: " + (object) ex);
        this.Log.LogError(ex.StackTrace);
        return false;
    }
}
```



x64dbg

<https://github.com/x64dbg/x64dbg>

The screenshot shows the x64dbg debugger interface with the following details:

- Assembly View:** The main pane displays assembly code for the module `x64dbg.exe`. A specific entry point `00007FF751FA2440` is highlighted. The assembly code includes various instructions like `call`, `add`, `jmp`, and `int3`, along with memory addresses and register values.
- Registers View:** To the right of the assembly view, the CPU register pane shows values for RAX, RBX, RCX, RDX, RBP, RSP, RSI, and RDI. The RAX register contains the value `00007FF751FA2440`.
- Memory Dump View:** Below the assembly view, there are two memory dump panes. The left pane shows a dump of memory starting at address `00007FF751FA32D0`, and the right pane shows a dump starting at `00007FF9B2AC7034`. Both panes show ASCII and hex representations of the memory contents.
- Status Bar:** At the bottom, the status bar indicates the current state as "Paused" and provides the command history: `x64dbg.exe: 00007FF751FA3328 -> 00007FF751FA3338 (0x00000011 bytes)`. It also shows the time spent debugging: `Time Wasted Debugging: 9:01:24:07`.



Obrigado!

[LinkedIn_](#)

/giuliano-sanfins

[Twitter_](#)

@0x_alibabas

