

_> RED TEAM SPACE



>>2024_EDITION<<



WINDOWS PROVEERÁ

Living off the land (LOTL)



NAME:

PAOLO BESSOLO | @Ha1x0n



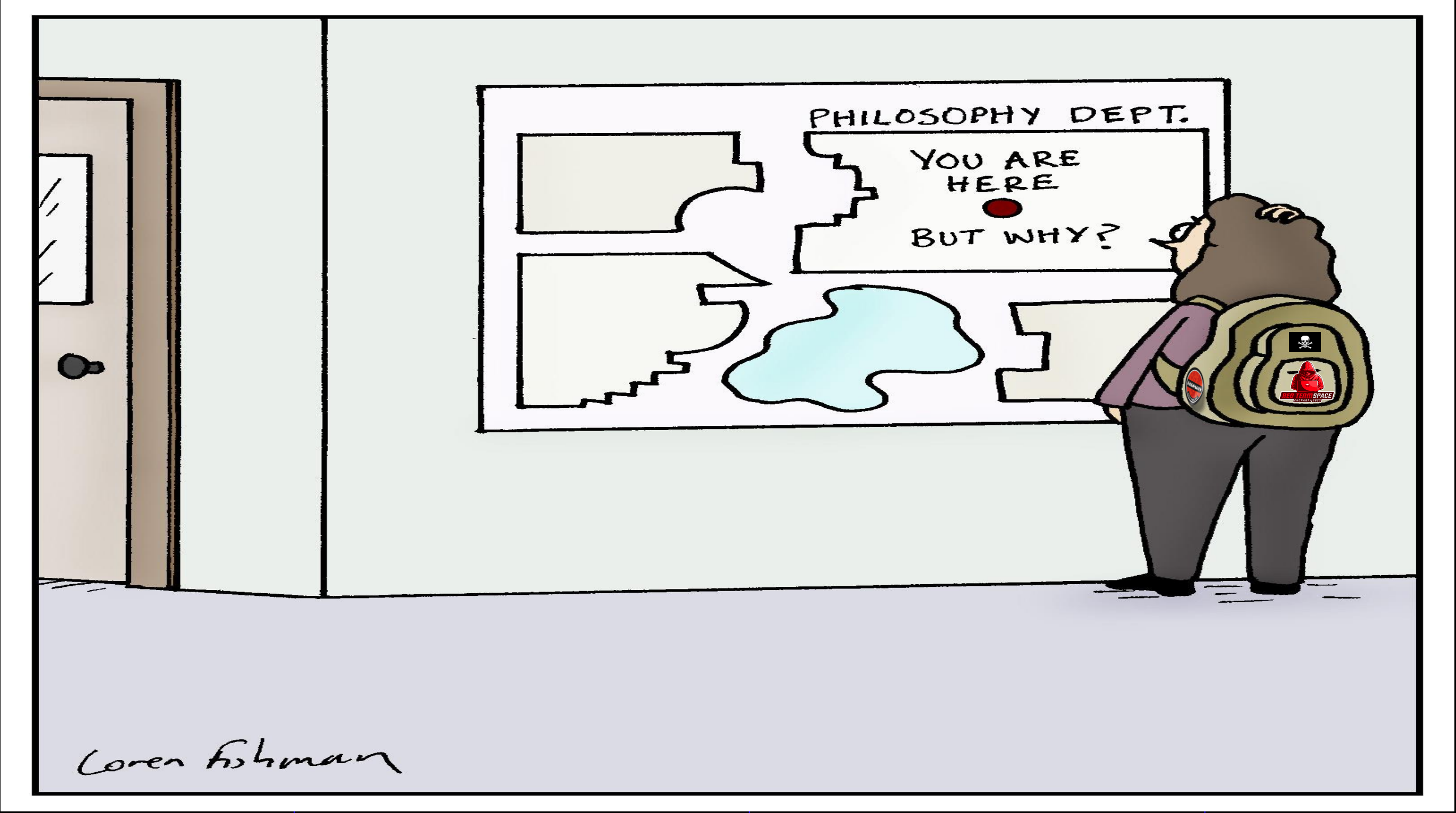
Agenda



1. Escenarios
2. Control de Integridad Obligatorio
3. Recopilación de información
4. LOLBAS
5. Otros Proyectos LOTL
6. Automatización

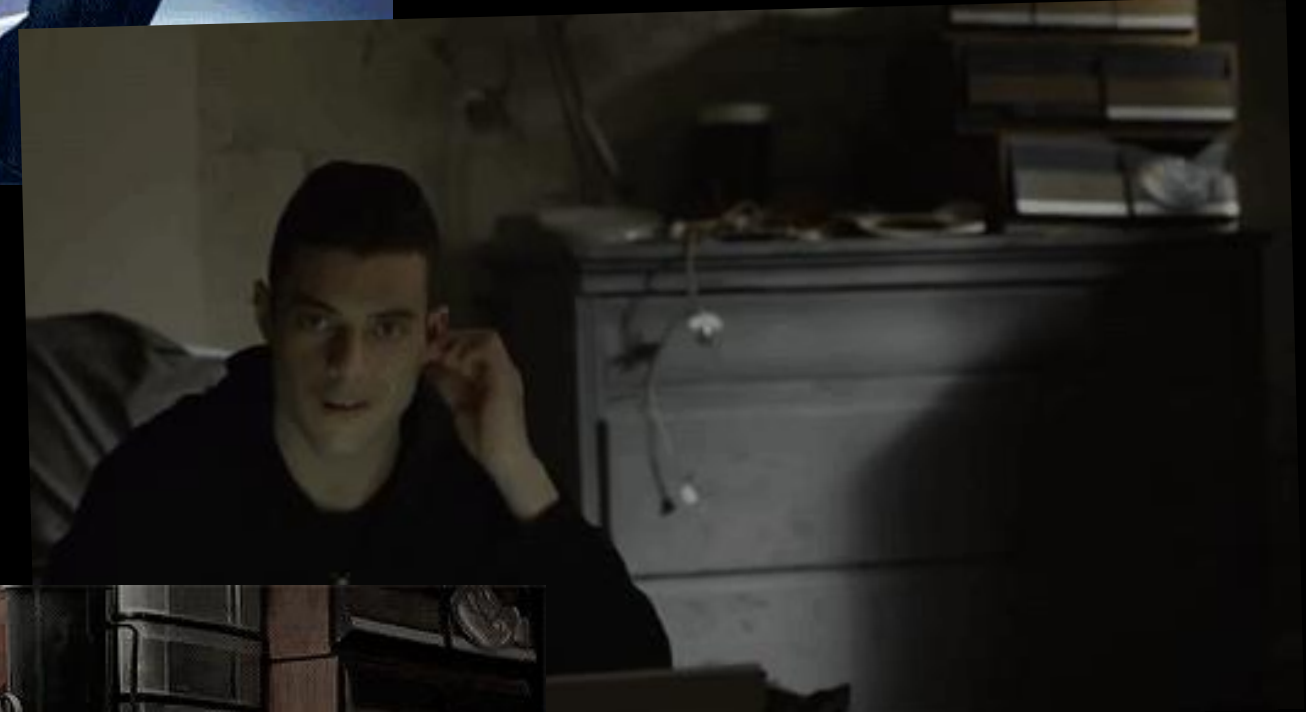


PROLOGO



1. Escenarios

- Mejor
 - Administrador (ID=500)
- Intermedio
 - Pertenece a grupo Administradores
- Peor
 - Usuario estándar



2. MIC (Mandatory Integrity Control)



- SYSTEM (4)

→ System

- High (3)

→ Usuario privilegiado (administrador)

- Medium (2)

→ Usuario estándar

- Low (1)

→ IE (browsers)

- Untrusted (0)

→ Guest



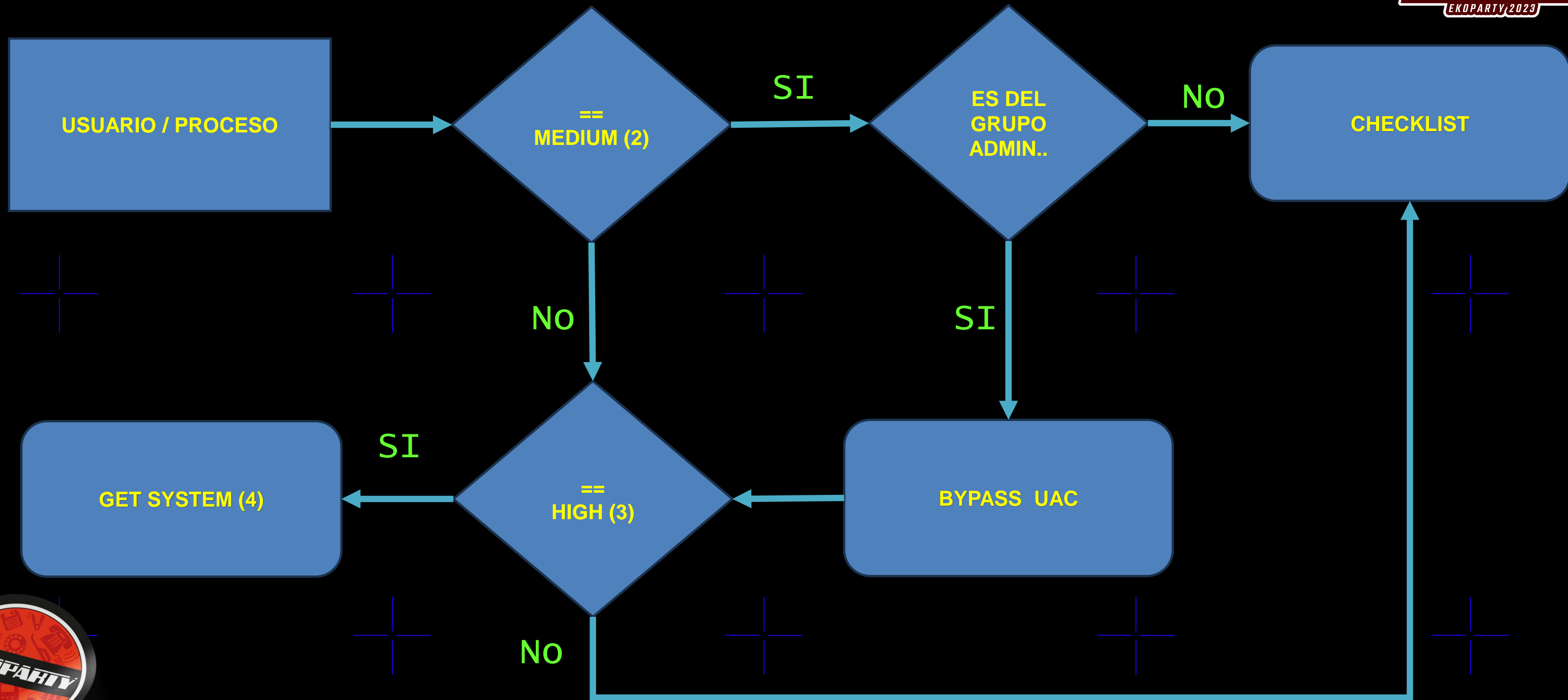
2. MIC (Mandatory Integrity Control)



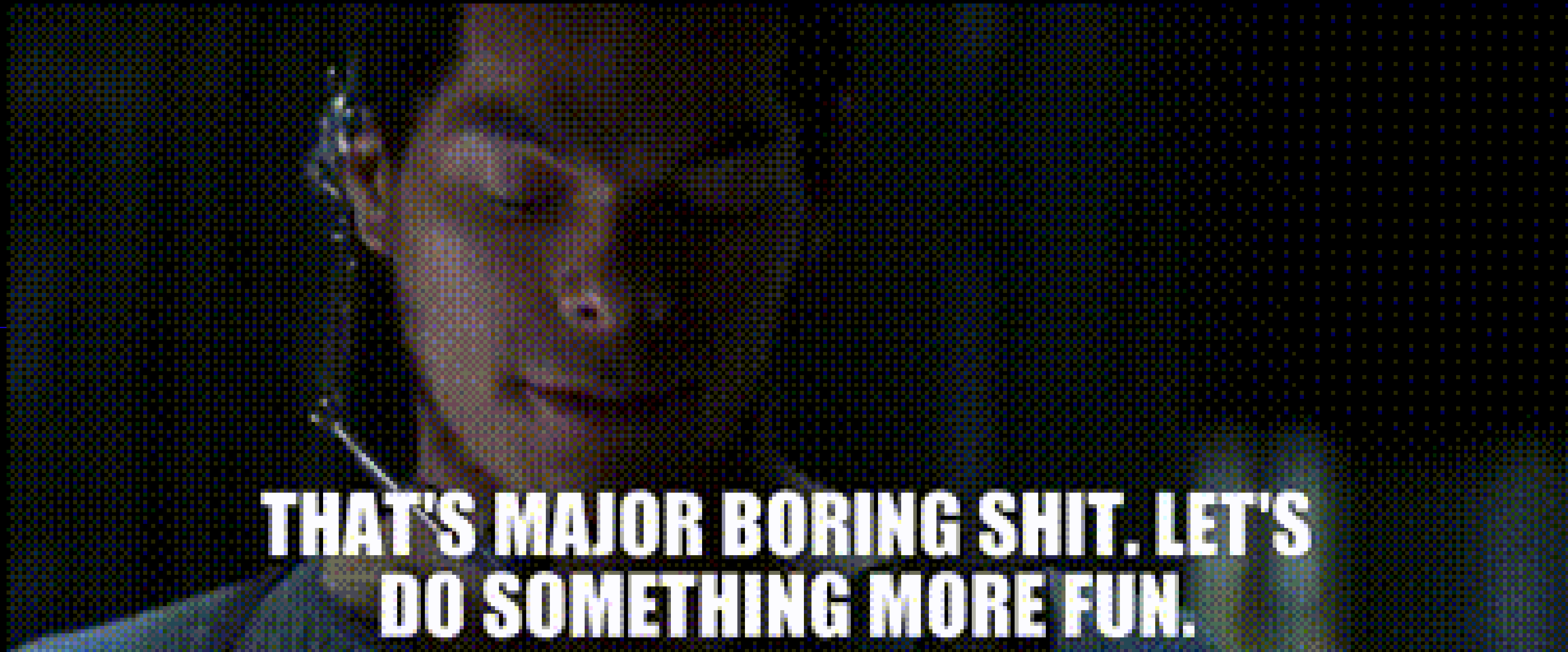
| Process | CPU | Private Bytes | Working Set | PID | Description | Compan... | Integrity |
|---------------------------|--------|---------------|-------------|-------|-----------------|--------------|-----------------------------------|
| fontdrvhost.exe | | 1,292 K | 1,680 K | 704 | | | |
| csrss.exe | < 0.01 | 1,972 K | 2,992 K | 484 | | | |
| winlogon.exe | | 2,520 K | 5,552 K | 568 | | | |
| fontdrvhost.exe | | 3,532 K | 3,528 K | 696 | | | |
| dwm.exe | < 0.01 | 98,588 K | 75,772 K | 884 | | | |
| explorer.exe | < 0.01 | 94,552 K | 118,772 K | 3040 | Explorador ... | Microsoft... | Nivel obligatorio medio |
| SecurityHealthSystray.exe | | 1,768 K | 9,516 K | 4836 | Windows S... | Microsoft... | Nivel obligatorio medio |
| cmd.exe | | 3,896 K | 6,368 K | 996 | Procesador... | Microsoft... | Nivel obligatorio medio |
| conhost.exe | | 9,692 K | 7,960 K | 5288 | Host de ve... | Microsoft... | Nivel obligatorio medio |
| procexp.exe | < 0.01 | 33,704 K | 26,048 K | 10944 | Sysinternals... | Sysintern... | Nivel obligatorio medio |
| notepad.exe | | 3,132 K | 836 K | 4924 | Bloc de notas | Microsoft... | Nivel obligatorio medio |
| cmd.exe | | 3,064 K | 644 K | 3732 | Procesador... | Microsoft... | Nivel obligatorio medio |
| conhost.exe | | 7,336 K | 6,048 K | 7772 | Host de ve... | Microsoft... | Nivel obligatorio medio |
| csrss.exe | < 0.01 | 2,000 K | 1,744 K | 5484 | | | |
| winlogon.exe | | 2,372 K | 2,396 K | 3024 | | | |
| fontdrvhost.exe | | 1,648 K | 1,252 K | 1976 | | | |
| dwm.exe | < 0.01 | 33,612 K | 6,072 K | 2928 | | | |
| LogonUI.exe | | 8,040 K | 3,268 K | 4736 | | | |
| explorer.exe | < 0.01 | 71,788 K | 225,528 K | 7712 | | | |
| SecurityHealthSystray.exe | | 1,792 K | 3,192 K | 9120 | | | |
| OneDrive.exe | | 43,384 K | 23,856 K | 10992 | | | |
| cmd.exe | | 4,508 K | 744 K | 9448 | Procesador... | Microsoft... | Nivel obligatorio medio |
| conhost.exe | | 7,132 K | 4,872 K | 2612 | Host de ve... | Microsoft... | Nivel obligatorio medio |
| notepad.exe | | 2,568 K | 752 K | 8240 | Bloc de notas | Microsoft... | Nivel obligatorio medio |
| ftp.exe | | 984 K | 256 K | 5968 | Programa d... | Microsoft... | Nivel obligatorio medio |
| OneDrive.exe | | 43,192 K | 4,492 K | 12032 | Microsoft O... | Microsoft... | Nivel obligatorio medio |
| firefox.exe | < 0.01 | 145,004 K | 226,428 K | 6616 | Firefox | Mozilla C... | Nivel obligatorio medio |
| firefox.exe | | 146,204 K | 78,272 K | 7880 | Firefox | Mozilla C... | Nivel obligatorio bajo |
| firefox.exe | | 20,616 K | 15,940 K | 8300 | Firefox | Mozilla C... | Nivel obligatorio de no confianza |
| firefox.exe | < 0.01 | 35,460 K | 61,060 K | 11400 | Firefox | Mozilla C... | Nivel obligatorio bajo |
| firefox.exe | | 35,780 K | 51,868 K | 6640 | Firefox | Mozilla C... | Nivel obligatorio bajo |
| firefox.exe | | 21,096 K | 14,448 K | 3352 | Firefox | Mozilla C... | Nivel obligatorio de no confianza |
| firefox.exe | | 49,772 K | 84,540 K | 11916 | Firefox | Mozilla C... | Nivel obligatorio bajo |
| firefox.exe | | 26,584 K | 28,388 K | 10644 | Firefox | Mozilla C... | Nivel obligatorio bajo |
| firefox.exe | | 26,584 K | 28,372 K | 11128 | Firefox | Mozilla C... | Nivel obligatorio bajo |
| firefox.exe | | 26,576 K | 28,332 K | 5652 | Firefox | Mozilla C... | Nivel obligatorio bajo |



2. MIC (Mandatory Integrity Control)



2. MIC (Mandatory Integrity Control)



3. Recopilación de Información



1. ¿Quién somos?

2. ¿Dónde estamos?

3. ¿Qué hacemos ahora?



3. Recopilación de Información



1. ¿Quién somos?

- whoami /all
- net user/localgroup
- Get-LocalUser
- set

```
C:\>whoami /priv
```

INFORMACIÓN DE PRIVILEGIOS

| Nombre de privilegio | Descripción | Estado |
|-------------------------------|--|---------------|
| ===== | ===== | ===== |
| SeShutdownPrivilege | Apagar el sistema | Deshabilitado |
| SeChangeNotifyPrivilege | Omitir comprobación de recorrido | Habilitada |
| SeUndockPrivilege | Quitar equipo de la estación de acoplamiento | Deshabilitado |
| SeIncreaseWorkingSetPrivilege | Aumentar el espacio de trabajo de un proceso | Deshabilitado |
| SeTimeZonePrivilege | Cambiar la zona horaria | Deshabilitado |



3. Recopilación de Información



2. ¿Dónde estamos?

- systeminfo
- driverquery
- fsutil fsinfo drives
- ipconfig
- netstat
- wmic useraccount

C:\>systeminfo

```
Nombre de host:                DESKTOP-I7N4DLH
Nombre del sistema operativo:   Microsoft Windows 10 Pro N
Versión del sistema operativo:  10.0.19045 N/D Compilación 19045
Fabricante del sistema operativo: Microsoft Corporation
Configuración del sistema operativo: Estación de trabajo independiente
Tipo de compilación del sistema operativo: Multiprocessor Free
Propiedad de:                  Terry
Organización registrada:
Id. del producto:              00331-60000-00000-AA739
Fecha de instalación original:  6/2/2024, 19:14:25
Tiempo de arranque del sistema:  14/2/2024, 10:25:18
Fabricante del sistema:        innotek GmbH
Modelo del sistema:            VirtualBox
Tipo de sistema:               x64-based PC
Procesador(es):                1 Procesadores instalados.
                                [01]: Intel64 Family 6 Model 154 Ste
                                innotek GmbH VirtualBox, 1/12/2006
Versión del BIOS:
Directorio de Windows:         C:\Windows
Directorio de sistema:         C:\Windows\system32
Dispositivo de arranque:        \Device\HarddiskVolume1
Configuración regional del sistema: 580a
Idioma de entrada:             es-mx;Español (México)
Zona horaria:                  (UTC-04:00) Santiago
```



3. Recopilación de Información



3. ¿Qué hacemos ahora?



3. Recopilación de Información



3. ¿Qué hacemos ahora?

- Buscar Contraseñas, credenciales e información sensible.
- Obtener información de procesos, servicios y tareas.
- Buscar sesiones que se puedan comprometer.
- Identificar software con vulnerabilidades.



3. Recopilación de Información - Servicios



Desde `services.msc` o a través de la herramienta de línea de comandos `sc` o desde `powershell` podemos listarlos.

```
NOMBRE_MOSTRAR : Administrador de credenciales
TIPO           : 20  WIN32_SHARE_PROCESS
ESTADO         : 4   RUNNING
                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
CÓD_SALIDA_WIN32 : 0   (0x0)
CÓD_SALIDA_SERVICIO: 0   (0x0)
PUNTO_COMPROB.  : 0x0
INDICACIÓN_INICIO : 0x0

NOMBRE_SERVICIO: W32Time
NOMBRE_MOSTRAR : Hora de Windows
TIPO           : 20  WIN32_SHARE_PROCESS
ESTADO         : 4   RUNNING
                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
CÓD_SALIDA_WIN32 : 0   (0x0)
CÓD_SALIDA_SERVICIO: 0   (0x0)
PUNTO_COMPROB.  : 0x0
INDICACIÓN_INICIO : 0x0

NOMBRE_SERVICIO: W3SVC
NOMBRE_MOSTRAR : Servicio de publicación World Wide Web
TIPO           : 20  WIN32_SHARE_PROCESS
ESTADO         : 4   RUNNING
                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
CÓD_SALIDA_WIN32 : 0   (0x0)
CÓD_SALIDA_SERVICIO: 0   (0x0)
PUNTO_COMPROB.  : 0x0
INDICACIÓN_INICIO : 0x0

NOMBRE_SERVICIO: WaaSMedicSvc
NOMBRE_MOSTRAR : Servicio de Windows Update Medic
TIPO           : 20  WIN32_SHARE_PROCESS
ESTADO         : 4   RUNNING
                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
CÓD_SALIDA_WIN32 : 0   (0x0)
CÓD_SALIDA_SERVICIO: 0   (0x0)
PUNTO_COMPROB.  : 0x0
INDICACIÓN_INICIO : 0x0
```



3. Recopilación de Información - Servicios



- Automático: el servicio se inicia inmediatamente al arrancar
- Automático (inicio retrasado): el servicio espera un breve período de tiempo después del arranque antes de iniciarse (principalmente una opción heredada para ayudar a que el escritorio se cargue más rápido).
- Manual: el servicio solo se iniciará cuando se solicite específicamente
- Deshabilitado: el servicio está deshabilitado y no se ejecutará



3. Recopilación de Información - Servicios



Es cuando la ruta al binario del servicio no está entre comillas.

¿Por qué eso es un problema? Por sí mismo no lo es, pero bajo condiciones específicas puede conducir a una elevación de privilegio.

Ruta del Servicio

C:\Program Files\PROGRAMA\Remote Server\Remots.exe

1. C:\Program.exe
2. C:\Program Files\PROGRAMA\Remote.exe
3. C:\Program Files\PROGRAMA\Remote Server\Remots.exe



4. LOLBAS (Living Off The Land Binaries, Scripts and Libraries)



LOLBAS

☆ Star 6,389



Living Off The Land Binaries, Scripts and Libraries

For more info on the project, click on the logo.

If you want to [contribute](#), check out our [contribution guide](#). Our [criteria list](#) sets out what we define as a LOLBin/Script/Lib. More information on programmatically accessing this project can be found on the [API page](#).

MITRE ATT&CK® and ATT&CK® are registered trademarks of The MITRE Corporation. You can see the current ATT&CK® mapping of this project on the [ATT&CK® Navigator](#).

If you are looking for UNIX binaries, please visit [gtfobins.github.io](#).
If you are looking for drivers, please visit [loldrivers.io](#).

Search among 198 binaries by name (e.g. 'MSBuild'), function (e.g. '/execute'), type (e.g. '#Script') or ATT&CK info (e.g. 'T1218')

| Binary | Functions | Type | ATT&CK® Techniques |
|-------------------------------------|---|----------|--|
| AddinUtil.exe | Execute | Binaries | T1218: System Binary Proxy Execution |
| AppInstaller.exe | Download | Binaries | T1105: Ingress Tool Transfer |
| Aspnet_Compiler.exe | AWL bypass | Binaries | T1127: Trusted Developer Utilities Proxy Execution |
| At.exe | Execute | Binaries | T1053.002: At |
| Atbroker.exe | Execute | Binaries | T1218: System Binary Proxy Execution |
| Bash.exe | Execute AWL bypass | Binaries | T1202: Indirect Command Execution |

<https://lolbas-project.github.io/#>



4. LOLBAS (Living Off The Land Binaries, Scripts and Libraries)



- Ejecutar código de programa o scripts
- Compilando el código del programa
- Omitir el control de cuentas de usuario
- Lectura de tráfico de red o actividad del usuario
- DLL de carga lateral o secuestro
- Volcado de memoria de proceso
- Lectura de credenciales de inicio de sesión
- Operaciones de archivos como descargas y cargas de archivo.



4. LOLBAS (Living Off The Land Binaries, Scripts and Libraries)



.. /Ftp.exe ☆ Star 6,393

Execute Download

A binary designed for connecting to FTP servers

Paths:

C:\Windows\System32\ftp.exe
C:\Windows\SysWOW64\ftp.exe

Resources:

- <https://twitter.com/OxAmit/status/1070063130636640256>
- <https://medium.com/@Oxamit/lets-talk-about-security-research-discoveries-and-proper-discussion-etiquette-on-twitter-10f9be6d1939>
- <https://ss64.com/nt/ftp.html>
- <https://www.asafety.fr/vuln-exploit-poc/windows-dos-powershell-upload-de-fichier-en-ligne-de-commande-one-liner/>

Acknowledgements:

- Casey Smith (@subtee)
- BennyHusted ()
- Amit Serper (@OxAmit)

Detection:

- Sigma: [proc_creation_win_lolbin_ftp.yml](#)
- IOC: cmd /c as child process of ftp.exe

Execute

Executes the commands you put inside the text file.

```
echo !calc.exe > ftpcommands.txt && ftp -s:ftpcommands.txt
```

Usecase: Spawn new process using ftp.exe. Ftp.exe runs cmd /C YourCommand

Privileges required: User


OS: Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11

MITRE ATT&CK®: [T1202: Indirect Command Execution](#)



5. Otros proyectos LOTL





Search site

AboutHTA GeneratorPremium

Living Off The Land Drivers

Living Off The Land Drivers is a curated list of Windows drivers used by adversaries to bypass security controls and carry out attacks. The project helps security professionals stay informed and mitigate potential threats.

!

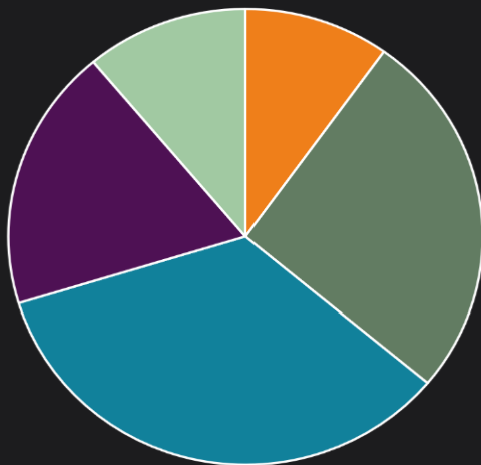
Feel free to open a [PR](#), raise an [Issue\(s\)](#) or request new driver(s) be added.

i

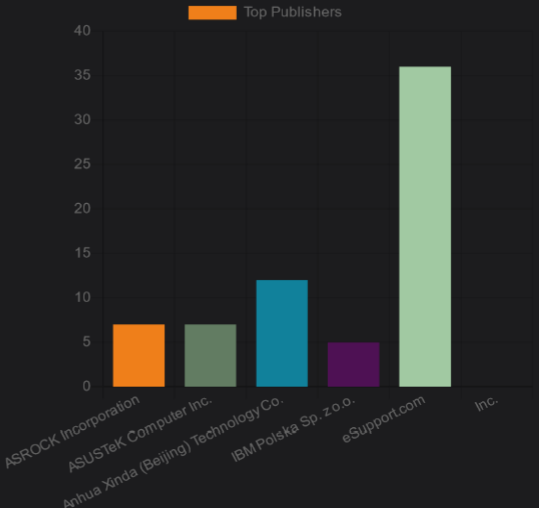
You can also get the malicious driver list via API using [CSV](#) or [JSON](#). Sysmon users check out the pre-built [config](#). There is a [Sigma rule](#) for SIEMs. If you've found this project valuable, you'll absolutely love our sister projects, [LOLBAS](#) and [GTFBins](#), check them out!

Top Products

CDRToolsCPUID serviceNTIOLibNovell XTiermimidrv (mimikatz)



Top Publishers



Filter Table Values

| Tag | SHA256 | Category | Created |
|--------------------------------------|--|-------------------|------------|
| SysInfoDetectorX64.sys | 45e5977b8d5baec776eb2e62a84981a8e46f6ce17947c9a76fa1f955dc547271 | Vulnerable driver | 2023-11-02 |
| NTIOLib.sys | 09bedbf7a41e0f8dabe4f41d331db58373ce15b2e9204540873a1884f38bdde1 | Vulnerable driver | 2023-01-09 |
| Proxy32.sys | 49ed27460730b62403c1d2e4930573121ab0c86c442854bc0a62415ca445a810 | Vulnerable driver | 2023-01-09 |
| TGSafe.sys | 3a95cc82173032b82a0ffc7d2e438df64c13bc16b4574214c9fe3be37250925e | Vulnerable driver | 2023-01-09 |
| c94f405c5929cfcccc8ad00b42c95083.sys | da70fa44290f949e9b3e0fcfe0503de46e82e0472e8e3c360da3fd2bfa364eee | Malicious | 2023-07-31 |
| wsdkd.sys | 6278bc785113831b2ec3368e2c9c9e89e8aca49085a59d8d38dac651471d6440 | Vulnerable driver | 2023-09-12 |
| DhKernel.sys | bb50818a07b0eb1bd317467139b7eb4bad6cd89053fecdbfeae11689825955 | Vulnerable driver | 2023-01-09 |

<https://www.lo1drivers.io/>



5. Otros proyectos LOTL

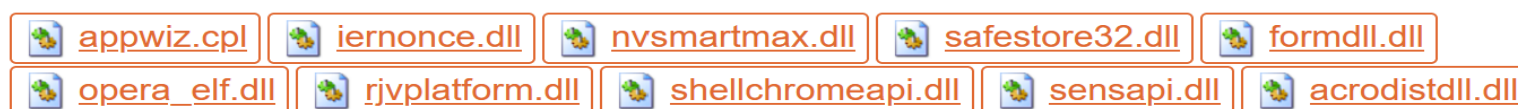


HijackLibs

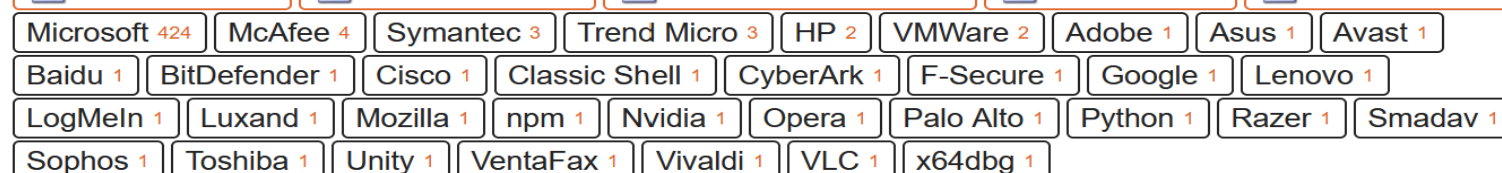
Enter the name of a DLL or EXE here...

☒ Sideload ☒ Environment Variable ☒ Phantom ☒ Search Order

Latest entries:



By vendor:



The database contains 388 *Sideload*, 89 *Environment Variable*, 13 *Phantom* and 9 *Search Order* entries. To see all available DLL hijacking entries, click [here](#).

What is DLL Hijacking?

DLL Hijacking is, in the broadest sense, tricking a legitimate/trusted application into loading an arbitrary **DLL**. Defensive measures such as AV and EDR solutions may not pick up on this activity out of the box, and allow-list applications such as AppLocker may not block the execution of the untrusted code. There are numerous examples of threat actors that have been observed to leverage DLL Hijacking to achieve their objectives.

There are various subtypes of DLL Hijacking; this project distinguishes between the following types:


- **DLL Sideload** ([T1574.002](#)): By copying (and optionally renaming) a vulnerable application to a user-writable folder, alongside a malicious DLL, arbitrary code can be executed through the legitimate application.
- **Phantom DLL Hijacking**: By copying a malicious DLL to a specific location, vulnerable applications will load and execute the (normally non-existent) DLL upon normal execution.
- **DLL Search Order Hijacking** ([T1574.001](#)): DLLs specified by an application without a path are searched for in fixed locations in a **specific order**. By putting a malicious DLL in a location that is searched in before the

<https://hijacklibs.net/>



5. Otros proyectos LOTL





Living Off Trusted Sites (LOTS) Project

Attackers are using popular legitimate domains when conducting phishing, C&C, exfiltration and downloading tools to evade detection. The list of websites below allow attackers to use their domain or subdomain. Website design credits: [LOLBAS](#) & [GTFOBins](#).

| Website | Tags | Service Provider ▾ |
|---|------------------------------------|--------------------|
| raw.githubusercontent.com | Phishing C&C Download | Github |
| github.com | Phishing Download | Github |
| 1drv.ms | Phishing | Microsoft |
| 1drv.com | Phishing Download | Microsoft |
| docs.google.com | Phishing C&C | Google |
| drive.google.com | Phishing Download Exfiltration | Google |
| *.azurewebsites.net | Phishing Download Exfiltration C&C | Microsoft |
| | Phishing Download Exfiltration | |

<https://lots-project.com/>



5. Otros proyectos LOTL



WADComs

☆ Star 1,257NIGHTMODE

WADComs is an interactive cheat sheet, containing a curated list of offensive security tools and their respective commands, to be used against Windows/AD environments.

If you hate constantly looking up the right command to use against a Windows or Active Directory environment (like me), this project should help ease the pain a bit. Just select what information you currently have related to the Windows machine (passwords, usernames, services, etc.), and it will display a list of tools you can try against the machine, along with a template command for easy copy/pasting. See the full list of [items](#) and [filters](#).

This project was created by [John Woodman](#) and was inspired by [GTFOBins](#) and [LOLBAS](#). I relied heavily on [GTFOBins](#)' site template to make this one.

I'm hoping to make WADComs a [collaborative project](#), so please feel free to [contribute](#) your commands.

What you have:

UsernamePasswordNo CredsHashTGS

TGT

PFXShell

Services:

SMBWMI

DCOMKerberosRPCLDAP

NTLMDNS

Attack Type:

Enumeration✓ExploitationPersistence

Privilege Escalation

OS:

LinuxWindows

+Enumeration

Command

```
python3 windapsearch --dc-ip 10.10.10.1 -u test.local\\john -p password123 -U -G --da -m "Remote Desktop Users" -C -r
```

EnumerationUsernamePasswordLinuxWindows

```
Snaffler.exe -s -o snaffler_output.log -d test.local -c 10.10.10.1
```

EnumerationShellSMBWindows

<https://wadcoms.github.io>










5. Otros proyectos LOTL



Living Off the Living Off the Land



A great collection of resources to thrive off the land

| logo | link | description |
|---|---|---|
|  | https://br0k3nlab/LoFP/ | Living off the False Positive is an autogenerated collection of false positives sourced from some of the most popular rule sets. The information is categorized along with ATT&CK techniques, rule source, and data source. |
|  | https://loldrivers.io | Living Off The Land Drivers is a curated list of Windows drivers used by adversaries to bypass security controls and carry out attacks |
|  | https://gtfobins.github.io | GTFOBins is a curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured systems |
|  | https://lolbas-project.github.io | The goal of the LOLBAS project is to document every binary, script, and library that can be used for Living Off The Land techniques |
|  | https://lots-project.com | Attackers are using popular legitimate domains when conducting phishing, C&C, exfiltration and downloading tools to evade detection. The list of websites below allow attackers to use their domain or subdomain |
|  | https://filesec.io | File extensions being used by attackers |
|  | https://malapi.io | MalAPI.io maps Windows APIs to common techniques used by malware |

<https://lolol.farm/>



5. Automatización



- PowerUp:
 - <https://github.com/HarmJ0y/PowerUp>
- WinPeas:
 - <https://github.com/carlospolop/PEASS-ng/tree/master/winPEAS>
- Windows Exploit Suggester – Next Generation (WES-NG):
 - <https://github.com/bitsadmin/wesng>
- GhostPack
 - <https://github.com/GhostPack/>
- PowerSploit:
 - <https://github.com/PowerShellMafia/PowerSploit>
- Privesc:
 - <https://github.com/enjoiz/Privesc>
- Lazagne:
 - <https://github.com/AlessandroZ/Lazagne>
- SessionGopher:
 - <https://github.com/Arvanaghi/SessionGopher>





ABOUT ME



<https://EH337.net>

Paolo Bessolo

Ethical Hacker | Pentester | Red Team |
cybersec | cntr011z | cypherpunk

@Halx0n

