

A close-up photograph of a golden retriever's head, looking down at a small brown mouse on a grey concrete surface. The dog's face is in the upper left, and the mouse is in the lower center. The background is a blurred outdoor setting.

HoneyCon - Una nube de
Malware, Por favour!





Carlos Antonini



Trabajo: Ethical Hacker en Prosegur Ciberseguridad

Auditor de hacking ético. Varios años de experiencia en el sector de la seguridad en multiples ámbitos: Seguridad defensiva en IPS/IDS y sistemas de correlación de eventos Alienvault. Seguridad ofensiva con técnicas de hacking en entornos de caja negra y caja blanca con herramientas como Metasploit, Sqlmap, Nikto, Nmap. Soy una persona autodidacta que nunca deja de aprender, Codesarrolador de la herramienta de código abierto 4nonimizer para hacer conexiones anónimas a través de VPN gratuitas, también estoy actualmente como colaborador del blog hackplayers.com, Organizador de la h-c0n

Contacto

Carlos.antonini1@Gmail.com

Formación y Certificaciones:

<https://www.linkedin.com/in/carlos-antonini-cepeda-44356853/>



Lórien



Contacto
@loriendr

Trabajo: Forense y DFIR en Prosegur Ciberseguridad.

Formación: Ing. Informática y Master en Informática Forense y Delitos Informáticos

Certificaciones: unas cuentas de forense y Cloud - Azure.
CHFI, CEH...

Profesor: Curso de análisis forense.

Grupos: #Cibercooperantes, @Cibervoluntario,
@Hack4ensicTeam y @C43S4RS

¿DE QUE VA ESTO?

Blue Team vs Red Team

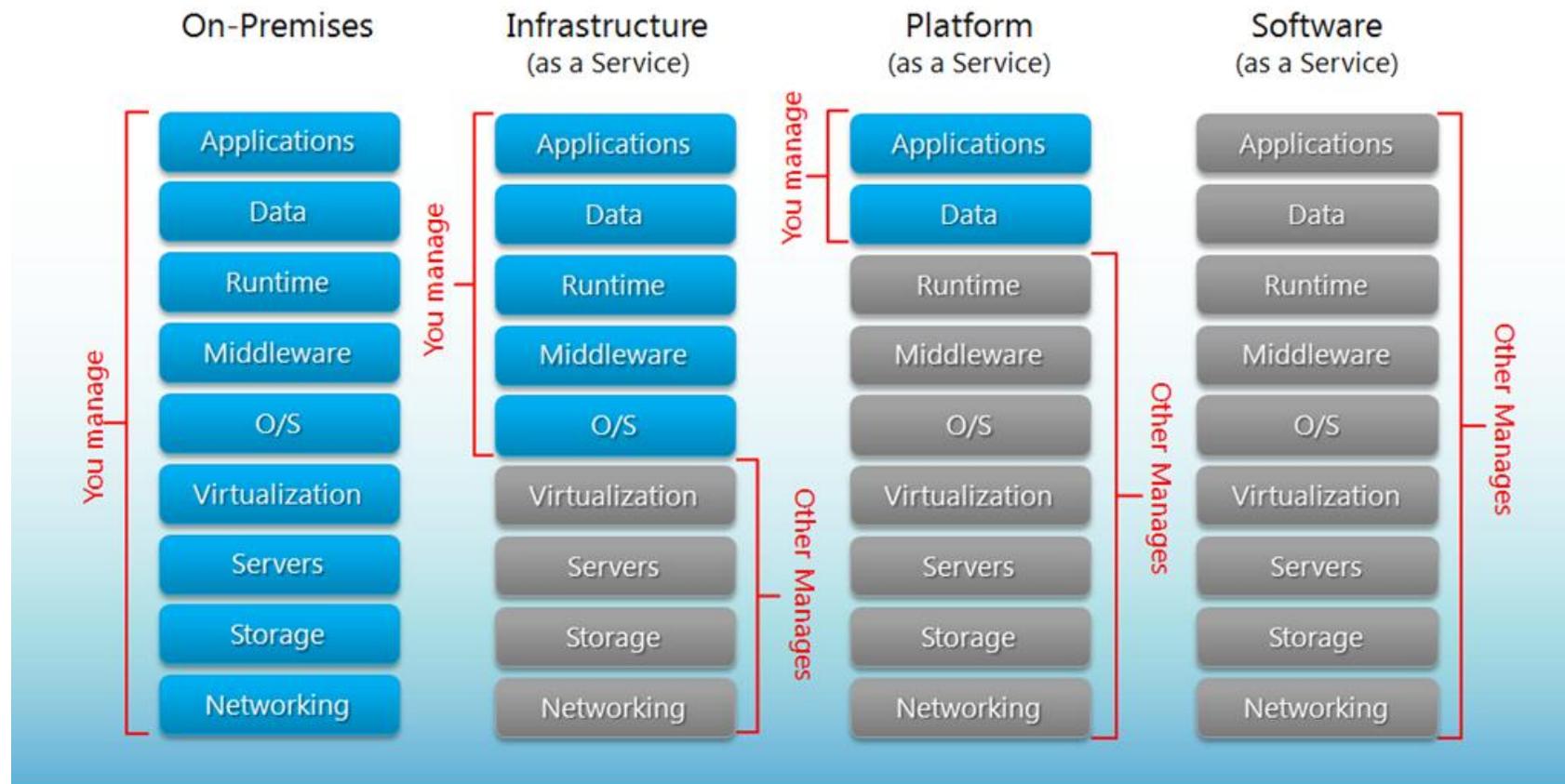
Crear un entorno en la nube.
Ataque y defensa - 6 horas cada uno.

Limitaciones - sólo se puede usar la
extracción forense de la máquina.
Resultados hasta ahora

BLUE TEAM 1 - RED TEAM 0

Modelo de Servicio Cloud (SaaS, PaaS, IaaS) y el FaaS

Separation of Responsibilities





RESOLUCIÓN DE INCIDENCIAS



Forense en IaaS (Azure, AWS y GCP)

Adquisición

Discos virtuales	Logs de los DNS
Snapshots	Logs de la VM
BBDD	Logs del Host
Otros EndPoints	Logs de la API
Workspaces	Logs del portal
Memoria Ram	Logs de la consola
Metadatos de la instancia	Captura de paquetes Registros
Logs de la red	de facturación

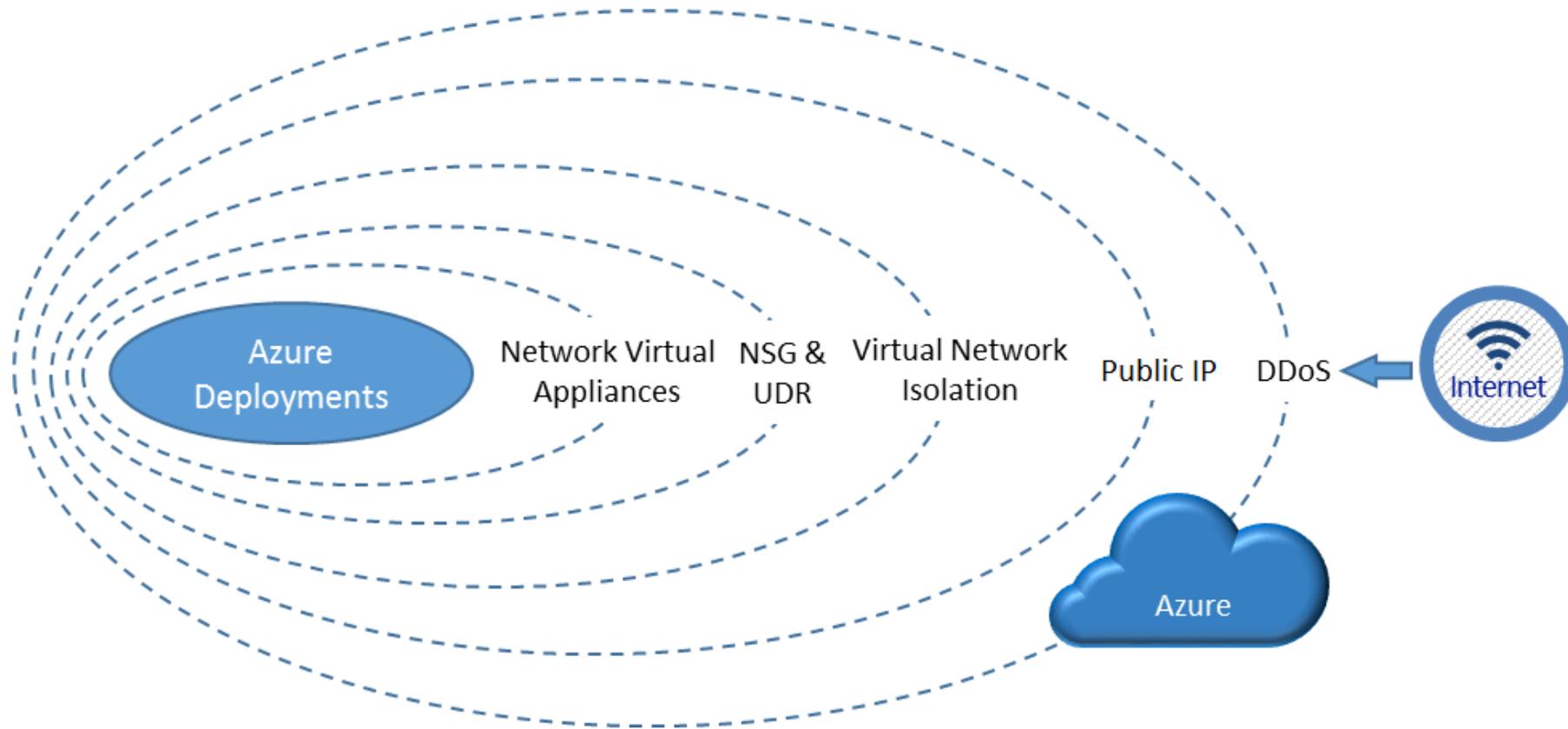
Análisis de las evidencias

Toma de decisión con sus pros y contras:

- ✓ Forense en la nube con una instancia específica
- ✓ Traslado de las evidencias a un entorno de Forense tradicional

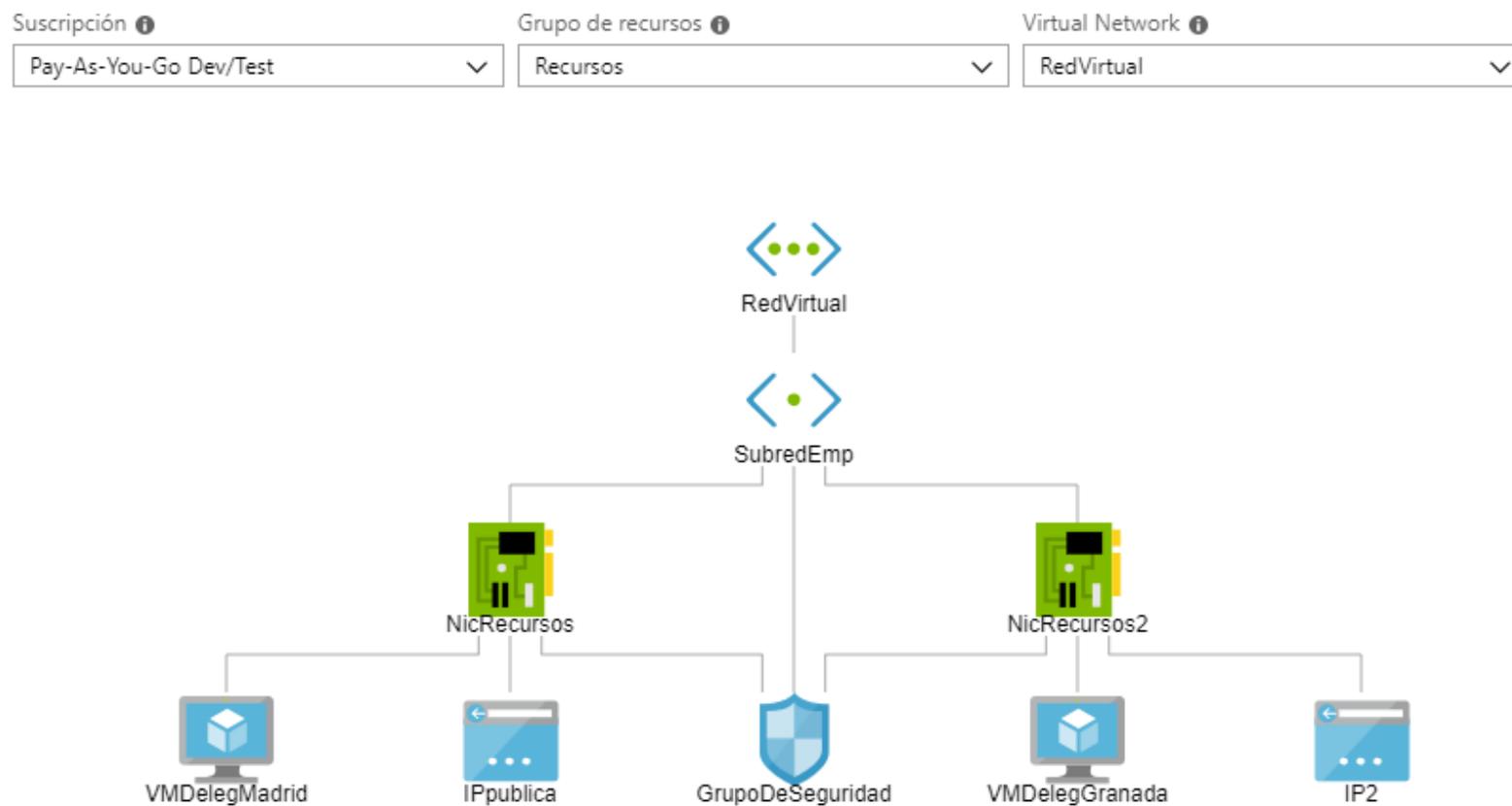


A nivel de seguridad se crean varias capas desde el exterior al interior:





Tenemos un entorno en cloud con diferentes redes y subredes, el esquema queda de esta manera:





Configuración del SecurityGroup

Inicio > GrupoDeSeguridad

GrupoDeSeguridad
Grupo de seguridad de red

Buscar (Ctrl+/)

Mover Eliminar Actualizar

PRIORIDAD	NOMBRE	PUERTO	PROTOCOLO	ORIGEN	DESTINO	ACCIÓN
1001	ReglaWEB	80	TCP	Cualquiera	Cualquiera	✔ Permitir ...
1002	⚠ ReglaRDP	3389	TCP	Cualquiera	Cualquiera	✔ Permitir ...
1012	Port_8080	8080	Cualquiera	Cualquiera	Cualquiera	✔ Permitir ...
1022	Port_serv	5000	Cualquiera	Cualquiera	Cualquiera	✔ Permitir ...
65000	AllowVnetInBound	Cualquiera	Cualquiera	VirtualNetwork	VirtualNetwork	✔ Permitir ...
65001	AllowAzureLoadBalancerInBo...	Cualquiera	Cualquiera	AzureLoadBala...	Cualquiera	✔ Permitir ...
65500	DenyAllInBound	Cualquiera	Cualquiera	Cualquiera	Cualquiera	✘ Denegar ...

Reglas de seguridad de salida

PRIORIDAD	NOMBRE	PUERTO	PROTOCOLO	ORIGEN	DESTINO	ACCIÓN
65000	AllowVnetOutBound	Cualquiera	Cualquiera	VirtualNetwork	VirtualNetwork	✔ Permitir ...
65001	AllowInternetOutBound	Cualquiera	Cualquiera	Cualquiera	Internet	✔ Permitir ...
65500	DenyAllOutBound	Cualquiera	Cualquiera	Cualquiera	Cualquiera	✘ Denegar ...

Información general
 Registro de actividad
 Control de acceso (IAM)
 Etiquetas
 Diagnosticar y solucionar pr...
 Configuración
 Reglas de seguridad de ent...
 Reglas de seguridad de sali...
 Interfaces de red
 Subredes
 Propiedades
 Bloqueos
 Script de automatización
 Supervisión
 Configuración de diagnóstico



Vemos que en el sistema está totalmente actualizado y el antivirus activado

The screenshot shows two windows from a Windows 10 desktop. On the left is the 'Administrator: Command Prompt' window displaying system information. On the right is the 'Windows Defender Security Center' window, which is open to the 'Settings' pane. The Security Center shows that the device is protected, with all four main protection areas (Virus & Threat Protection, Firewall & Network Protection, Device performance & Health, and App & Browser Control) having green checkmarks and 'No action needed' status. The 'About' section of the Settings pane shows the device name 'MVNegocio' and various specifications.

```
Administrator: Command Prompt
Registered Organization: N/A
Product ID: 00331-10000-00001-AA821
Original Install Date: 3/12/2018, 6:45:49 PM
System Boot Time: 3/13/2018, 8:28:30 AM
System Manufacturer: Microsoft Corporation
System Model: Virtual Machine
System Type: x64-based PC
Processor(s): 1 Processor(s) Installed.
[01]: Intel64 Family 6 Model 63 Stepping 2 GenuineIntel ~2394
BIOS Version: American Megatrends Inc. 090007 , 6/2/2017
Windows Directory: C:\Windows
System Directory: C:\Windows\system32
Boot Device: \Device\HarddiskVolume1
System Locale: en-us;English (United States)
Input Locale: en-us;English (United States)
Time Zone: (UTC) Coordinated Universal Time
Total Physical Memory: 768 MB
Available Physical Memory: 63 MB
Virtual Memory: Max Size: 2,752 MB
Virtual Memory: Available: 1,437 MB
Virtual Memory: In Use: 1,315 MB
Page File Location(s): D:\pagefile.sys
Domain: WORKGROUP
Logon Server: \\MVNegocio
Hotfix(s): 3 Hotfix(s) Installed.
[01]: KB4056887
[02]: KB4087256
[03]: KB4074588
Network Card(s): 1 NIC(s) Installed.
[01]: Microsoft Hyper-V Network Adapter
Connection Name: Ethernet
DHCP Enabled: Yes
DHCP Server: 168.63.129.16
IP address(es)
[01]: 192.168.1.8
[02]: fe80::3c43:bd7:9325:6aa1
Hyper-V Requirements: A hypervisor has been detected. Features required for Hyper-V
played.
C:\Users\azureuser>
```

Windows Defender Security Center

Your device is being protected.

Last threat scan: Not available
Last threat definition update: 3/13/2018
Last health scan: 3/13/2018

Settings

About

Your PC is monitored and protected.

- ✓ Virus & Threat Protection
- ✓ Firewall & Network Protection
- ✓ Device performance & Health
- ✓ App & Browser Control

[See details in Windows Defender](#)

Device specifications

Device name	MVNegocio
Processor	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz 2.39 GHz
Installed RAM	768 MB (768 MB usable)
Device ID	E1C562DF-47D4-4BB3-B3A6-2D86199DF365
Product ID	00331-10000-00001-AA821
System type	64-bit operating system, x64-based processor
Pen and touch	No pen or touch input is available for this displ

[Rename this PC](#)

9:06 AM
3/13/2018



¿Empezamos con el ejercicio?

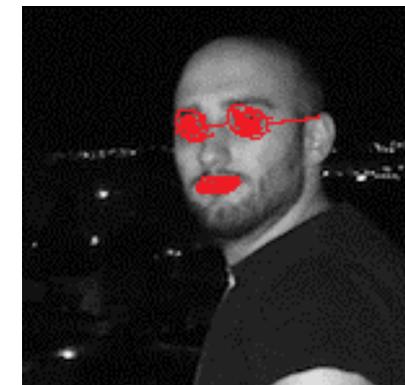




¿Qué me encuentro?



Servicio expuesto a internet basado desde el entorno cloud:
dnspub.westeurope.cloudapp.azure.com:5000



Tiene una apariencia como esta:



PROSEGUR CIBERSEGURIDAD

 **PROSEGUR**
Seguridad de confianza

Acceso al servicio

Username:

Password:

ACEPTAR

Microsoft Azure

- Crear un recurso
- Todos los servicios
- FAVORITOS
- Panel
- Grupos de recursos
- Todos los recursos
- Recientes
- App Services
- Máquinas virtuales
- Suscripciones
- Monitor
- Security Center
- Asesor
- Discos
- Instantáneas
- Direcciones IP públicas
- Alertas
- Cuentas de almacenami...
- Administración de costo...
- Máquinas virtuales (clási...
- SQL Database

Inicio > Todos los recursos

Todos los recursos

+ Agregar
≡ Editar columnas
↻ Actualizar
🏷️ Asignar etiquetas
🗑️ Eliminar
💬 Comentarios
ℹ️ Información de versión preli...
👉 Salir de la versión preliminar

Restablecer filtros

Suscripción

Mostrar tipos ocultos

Grupo de recursos

recursos (12)

cloud-shell-storage-westeur... (1)

Tipo

Disco (3)

Máquina virtual (2)

Interfaz de red (2)

Dirección IP pública (2)

Conjunto de disponibilidad (1)

Buscando tipos de recursos...

Ubicación

Oeste de Europa (13)

Mostrando de 1 a 13 de 13 registros.

< Anterior
Página 1 de 1
Siguiente >

<input type="checkbox"/>	NOMBRE ↑↓	GRUPO DE RE... ↑↓	UBICACIÓN ↑↓	SUSCRIPCIÓN ↑↓	ETIQUETAS	IDENTIFICAD... ↑↓	TIPO ↑↓	TIPO ↑↓
<input type="checkbox"/>	ConjuntoDispo	recursos	Oeste de Europa	Pay-As-You-Go D...		/subscriptions/d7...	microsoft.comput...	Conjunto de disp...
<input type="checkbox"/>	csbd72bc2388164x47d3x878	cloud-shell-stora...	Oeste de Europa	Pay-As-You-Go D...	ms-reso...	/subscriptions/d7...	microsoft.storage...	Cuenta de almace...
<input type="checkbox"/>	DFIR	recursos	Oeste de Europa	Pay-As-You-Go D...		/subscriptions/d7...	microsoft.comput...	Disco
<input type="checkbox"/>	DISCO_1	recursos	Oeste de Europa	Pay-As-You-Go D...		/subscriptions/d7...	microsoft.comput...	Disco
<input type="checkbox"/>	DISCO_2	recursos	Oeste de Europa	Pay-As-You-Go D...		/subscriptions/d7...	microsoft.comput...	Disco
<input type="checkbox"/>	GrupoDeSeguridad	recursos	Oeste de Europa	Pay-As-You-Go D...		/subscriptions/d7...	microsoft.network...	Grupo de segurid...
<input type="checkbox"/>	IP2	recursos	Oeste de Europa	Pay-As-You-Go D...		/subscriptions/d7...	microsoft.network...	Dirección IP públi...
<input type="checkbox"/>	IPpublica	recursos	Oeste de Europa	Pay-As-You-Go D...		/subscriptions/d7...	microsoft.network...	Dirección IP públi...
<input type="checkbox"/>	NicRecursos	recursos	Oeste de Europa	Pay-As-You-Go D...		/subscriptions/d7...	microsoft.network...	Interfaz de red
<input type="checkbox"/>	NicRecursos2	recursos	Oeste de Europa	Pay-As-You-Go D...		/subscriptions/d7...	microsoft.network...	Interfaz de red
<input type="checkbox"/>	RedVirtual	recursos	Oeste de Europa	Pay-As-You-Go D...		/subscriptions/d7...	microsoft.network...	Red virtual
<input type="checkbox"/>	VMDelegGranada	recursos	Oeste de Europa	Pay-As-You-Go D...		/subscriptions/d7...	microsoft.comput...	Máquina virtual
<input type="checkbox"/>	VMDelegMadrid	recursos	Oeste de Europa	Pay-As-You-Go D...		/subscriptions/d7...	microsoft.comput...	Máquina virtual



¿Qué pasó hermano?



Abrimos la carpeta con la extracción de las evidencias realizadas con la tool Live Response Collection de @BriMorLabs y repasamos los ficheros más relevantes mientras ponemos en marcha Volatility

- BasicInfo
- CopiedFiles
- NetworkInfo**
- PersistenceMechanisms
- UserInfo

- cports.html
- Gateway_ARP_Lookup.txt
- nbtstat.txt
- NetBIOS_sessions.txt
- netstat_anb_results.txt
- TCPView.txt

- amcache
- chrome
- eventlogs
- firefox
- hosts
- ie
- logfile
- mft
- prefetch
- registry
- SRUMDB
- usnrjnl
- forecopy_handy.log

- autorunsc.csv
- autorunsc.txt
- Driver_group_load_order_wmic.txt
- Loaded_dlls.txt
- scheduled_tasks.txt
- services_aw_processes.txt
- Startup_wmic.txt

- DiskDriveList_wmic.txt
- Full_file_listing.txt
- Hashes_md5_Startup_and_Dates.txt
- Hashes_md5_System_TEMP_AllFiles_and_Dates.txt
- Hashes_md5_System32_AllFiles_and_Dates.txt
- Hashes_md5_User_TEMP_AllFiles_and_Dates.txt
- Hashes_sha256_Startup_and_Dates.txt
- Hashes_sha256_System_TEMP_AllFiles_and_Dates.txt
- Hashes_sha256_System32_AllFiles_and_Dates.txt
- Hashes_sha256_User_TEMP_AllFiles_and_Dates.txt
- Installed_software_wmic.txt
- LastActivityView.html**
- List_hidden_directories.txt
- Loaded_system_drivers_wmic.txt
- LogicalDisk_name_wmic.txt
- LogicalDisk_size_caption_wmic.txt
- Possible_unicode_files_and_directories.txt
- PrcView_extended.txt
- PrcView_extended_long.txt
- psfile.txt
- psinfo.txt
- PsList.txt
- PsLoggedon.txt



¿Qué pasó hermano?



Vamos a utilizar ParrotOS y la última versión de Volatility descargada desde GitHub y sacamos el perfil de la máquina: **Win10x64_14393** con el comando: `volatility -f VMDelegM.dmp imageinfo`

```
[x]-[root@parrot]-[/home/lord4/evidencias]
#volatility -f VMDelegM.dmp imageinfo
Volatility Foundation Volatility Framework 2.6
INFO      : volatility.debug      : Determining profile based on KDBG search...
Suggested Profile(s) : Win10x64_10586, Win10x64_14393, Win10x64, Win2016x64_14393, Win10x64_15063
Win10x64_15063)
AS Layer1 : SkipDuplicatesAMD64PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (/home/lord4/evidencias/VMDelegM.dmp)
PAE type  : No PAE
DTB       : 0x1aa000L
KDBG      : 0xf80114f0c8e0L
Number of Processors : 2
Image Type (Service Pack) : 0
KPCR for CPU 0 : 0xfffff80114f5e000L
KPCR for CPU 1 : 0xffff96000d027000L
KUSER_SHARED_DATA : 0xfffff78000000000L
Image date and time : 2018-11-04 16:41:13 UTC+0000
Image local date and time : 2018-11-04 16:41:13 +0000
```

`git clone https://github.com/volatilityfoundation/volatility.git`



¿Qué pasó hermano?



¿Qué tenemos hasta ahora?

Una imagen abierta con el programa Paint, con la imagen de un conocido Ransomware. **Pero abierto con el Paint???**

¿Cómo planteamos el DFIR?

Búsqueda de evidencias en los procesos

Búsqueda de conexiones de entrada/salida

Objetivo:

Si hay infección que no se extienda más aún. (Identificación y Contención)

Obtención de información sobre las conexiones con la máquina



¿Qué pasó hermano?



volatility -f VMDelegM.dmp --profile=Win10x64_14393 pslist

```

#volatility -f VMDelegM.dmp --profile=Win10x64_14393 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V) Name PID PPID Thds Hnds Sess Wow64 Start
-----
0xffffe08872c98700 System 4 0 111 0 0 0 0 2018-11-04 14:15:58 UTC+0000
0xffffe08873577840 smss.exe 308 4 2 0 0 0 0 2018-11-04 14:15:58 UTC+0000
0xffffe088741c1700 csrss.exe 408 400 12 0 0 0 0 2018-11-04 14:16:02 UTC+0000
0xffffe08874398080 smss.exe 484 308 0 0 1 0 0 2018-11-04 14:16:02 UTC+0000
0xffffe08874392080 wininit.exe 492 400 3 0 0 0 0 2018-11-04 14:16:02 UTC+0000
0xffffe0887438f100 csrss.exe 500 484 11 0 1 0 0 2018-11-04 14:16:02 UTC+0000
0xffffe08874257080 winlogon.exe 552 484 2 0 1 0 0 2018-11-04 14:16:02 UTC+0000
0xffffe088743f8840 services.exe 620 492 7 0 0 0 0 2018-11-04 14:16:03 UTC+0000
0xffffe08874720080 lsass.exe 628 492 8 0 0 0 0 2018-11-04 14:16:03 UTC+0000
0xffffe08874744080 svchost.exe 712 620 21 0 0 0 0 2018-11-04 14:16:03 UTC+0000
0xffffe08874782840 svchost.exe 768 620 13 0 0 0 0 2018-11-04 14:16:03 UTC+0000
0xffffe0887475c080 LogonUI.exe 876 552 12 0 1 0 0 2018-11-04 14:16:04 UTC+0000
0xffffe088747c8080 dwm.exe 884 552 12 0 1 0 0 2018-11-04 14:16:04 UTC+0000
0xffffe0887477e840 svchost.exe 936 620 39 0 0 0 0 2018-11-04 14:16:04 UTC+0000
0xffffe0887477c840 svchost.exe 964 620 28 0 0 0 0 2018-11-04 14:16:04 UTC+0000
0xffffe08874778840 svchost.exe 1012 620 16 0 0 0 0 2018-11-04 14:16:04 UTC+0000
0xffffe08873446080 svchost.exe 336 620 16 0 0 0 0 2018-11-04 14:16:04 UTC+0000
0xffffe08874772840 svchost.exe 1044 620 20 0 0 0 0 2018-11-04 14:16:05 UTC+0000
0xffffe088748583c0 svchost.exe 1104 620 46 0 0 0 0 2018-11-04 14:16:05 UTC+0000
0xffffe0887476e840 svchost.exe 1112 620 18 0 0 0 0 2018-11-04 14:16:05 UTC+0000
0xffffe0887476a840 svchost.exe 1236 620 21 0 0 0 0 2018-11-04 14:16:05 UTC+0000
0xffffe08874769680 svchost.exe 1244 620 10 0 0 0 0 2018-11-04 14:16:05 UTC+0000
0xffffe088742af840 VSSVC.exe 1252 620 4 0 0 0 0 2018-11-04 14:16:05 UTC+0000
0xffffe08874654080 svchost.exe 1852 620 4 0 0 0 0 2018-11-04 14:16:06 UTC+0000

```



¿Qué pasó hermano?



volatility -f VMDelegM.dmp --profile=Win10x64_14393 pslist

```

0xffffe08874c6a840 rundll32.exe 0.0.0.0 4008 32 1104 19565 4 0 0 0 2018-11-04 14:16:22 UTC+0000
0xffffe08876745840 MpCmdRun.exe 168.1.4.50 2096 1540 60 118 70 0 220 440 E504 2018-11-04 14:17:12 UTC+0000
0xffffe088767d7440 msdtc.exe 192.168.1.4:50 3592 620 969 254 109 254 00 0 0 0 2018-11-04 14:18:13 UTC+0000
0xffffe08876959840 svchost.exe 2.168.1.4:50 1712 620 668 63 120 16 800 0 0 0 0 2018-11-04 14:19:44 UTC+0000
0xffffe088748b4080 svchost.exe 0.0.0.0 1528 620 3 0 0 0 0 0 0 0 2018-11-04 14:26:44 UTC+0000
0xffffe08874c7a840 smss.exe 0.0.0.0 3168 308 0 0 0 0 0 0 0 0 2018-11-04 14:26:59 UTC+0000
0xffffe0887672c840 csrss.exe 0.0.0.0:54383 3232 3168 12 0 0 0 2 0 0 0 2018-11-04 14:26:59 UTC+0000
0xffffe08876e35840 winlogon.exe 54383 3688 3168 5 0 0 2 0 0 0 0 2018-11-04 14:26:59 UTC+0000
0xffffe08876e77080 dwm.exe 0.0.0.0:0 720 3688 13 0 0 0 2 0 0 0 2018-11-04 14:27:00 UTC+0000
0xffffe08876fab440 rdpclip.exe 2.168.1.4:32 4104 936 112 187 250 205 53 277 0 E504 2018-11-04 14:27:05 UTC+0000
0xffffe08876fdb840 RuntimeBroker? 0.0.0.0 4132 712 19 0 0 0 2 0 0 0 0 2018-11-04 14:27:06 UTC+0000
0xffffe08876fd9840 svchost.exe 0.0.0.0 4216 620 6 0 0 0 2 0 0 0 0 2018-11-04 14:27:07 UTC+0000
0xffffe08876fd7840 sihost.exe 92.168.1.4:50 4224 1104 80 77 226 0 250 442 0 0 0 0 2018-11-04 14:27:07 UTC+0000
0xffffe08873504080 taskhostw.exe 0.0.0.0 4260 1104 14 0 0 0 2 0 0 0 0 2018-11-04 14:27:07 UTC+0000
0xffffe0887680e080 userinit.exe 0.0.0.0 4548 3688 0 0 0 0 2 0 0 0 0 2018-11-04 14:27:09 UTC+0000
0xffffe088748e7080 explorer.exe 0.0.1:1900 4572 4548 203 0 0 0 2 0 0 0 0 2018-11-04 14:27:09 UTC+0000
0xffffe08876fc7840 ShellExperienc 0.1.4:40 4864 712 22 2 239 140 196 123 0 E504 2018-11-04 14:27:16 UTC+0000
0xffffe08876fc3840 SearchUI.exe idencias 5016 712 31 0 0 0 2 0 0 0 0 2018-11-04 14:27:18 UTC+0000
0xffffe08875b4b080 conhost.exe mp --profile 2624 10x2584 7134 n0 0 0 0 0 0 0 0 0 2018-11-04 15:13:12 UTC+0000
0xffffe08876152840 mspaint.exe ty Framework 2940 3200 3 0 0 2 1 2018-11-04 15:16:35 UTC+0000
0xffffe08876163080 svchost.exe idencias 2928 620 9 0 0 0 0 0 0 0 0 2018-11-04 15:16:35 UTC+0000
0xffffe088788d9200 ApplicationFra --profile 1092 10x6712 7134 n2 find -b / 2 0 0 0 0 2018-11-04 15:58:27 UTC+0000
0xffffe0887663d080 WmiPrvSE.exe Framework 3620 712 7 0 0 0 0 0 0 0 0 2018-11-04 16:26:11 UTC+0000
0xffffe0887933f780 WmiPrvSE.exe idencias 3744 712 4 0 0 0 1 2018-11-04 16:26:53 UTC+0000
0xffffe088793f91c0 mmc.exe VM.dmp --profile 2960 10x4132 7134 n7 find -b /home/2ord4/e0 2018-11-04 16:37:23 UTC+0000
0xffffe088774824c0 vds.exe tility Framework 2904 620 16 0 0 0 0 0 0 0 0 2018-11-04 16:37:23 UTC+0000
0xffffe08878d28080 smartscreen.ex idencias 1284 712 7 0 0 2 0 0 0 0 0 2018-11-04 16:40:17 UTC+0000
0xffffe08878347280 cmd.exe VM.dmp --profile 2912 10x4392 7134 n1 find -b /home/2ord4/e1 2018-11-04 16:41:12 UTC+0000

```



¿Qué pasó hermano?



volatility -f VMDelegM.dmp --profile=Win10x64_14393 pstree

```
#volatility -f VMDelegM.dmp --profile=Win10x64_14393 pstree
Volatility Foundation Volatility Framework 2.6
Name 00e08874a0e5d0 4 0 R--r-d \Device\Hardd PidId PPidWinThds S Hnds Time ps.dll
-----
0xfffffe08874392080:wininit.exe 0 R--r-d \Device\Hardd 492 0 lum 400 Window 3 \System 0 2018-11-04 14:16:02 UTC+0000
0xfffffe088743f8840:services.exe R--r-d \Device\Hardd 620 0 lum 492 Window 7 \System 0 2018-11-04 14:16:03 UTC+0000
0xfffffe08874782840:svchost.exe R--r-d \Device\Afd\En 768 int 620 13 0 2018-11-04 14:16:03 UTC+0000
0xfffffe088767d7440:msdtc.exe 1 R--r-w- \Device\Hardd 3592 0 lum 620 Window 9 \System 0 2018-11-04 14:18:13 UTC+0000
0xfffffe08874693840:MsMpEng.exe R--r-d \Device\Hardd 1880 0 lum 620 Window 25 \System 0 2018-11-04 14:16:07 UTC+0000
0xfffffe08874772840:svchost.exe R--r-d \Device\Device 1044 \CMP 620 fy 20 0 2018-11-04 14:16:05 UTC+0000
0xfffffe0887468f840:WindowsAzureTe rd \Device\Hardd 2072 0 lum 620 \Dire 17 ory 0 2018-11-04 14:16:07 UTC+0000
0xfffffe08874663300:spoolsv.exe RW--r-d \Device\Hardd 1948 0 lum 620 Window 16 \Servi 0 2018-11-04 14:16:07 UTC+0000
0xfffffe08876959840:svchost.exe R--r-d \Device\Device 1712 \CMP 620 fy 6 0 2018-11-04 14:19:44 UTC+0000
0xfffffe088746e0680:WindowsAzureGu R--r-d \Device\Device 1096 \CMP 620 fy 16 0 2018-11-04 14:16:07 UTC+0000
0xfffffe08874bfc5c0:NisSrv.exe R--r-d \Device\Hardd 3000 0 lum 620 Window 7 \System 0 2018-11-04 14:16:14 UTC+0000
0xfffffe08874778840:svchost.exe R--r-d \Device\Hardd 1012 0 lum 620 Window 16 \System 0 2018-11-04 14:16:04 UTC+0000
0xfffffe08874654080:svchost.exe R--r-d \Device\Device 1852 \CMP 620 fy 4 0 2018-11-04 14:16:06 UTC+0000
0xfffffe0887469a400:WaAppAgent.exe R--r-d \Device\Device 1076 \CMP 620 fy 20 0 2018-11-04 14:16:07 UTC+0000
0xfffffe0887477c840:svchost.exe R--r-d \Device\Device 964 \CMP 620 fy 28 0 2018-11-04 14:16:04 UTC+0000
0xfffffe08874744080:svchost.exe R--r-d \Device\Hardd 712 0 lum 620 Window 21 \System 0 2018-11-04 14:16:03 UTC+0000
0xfffffe08876fc7840:ShellExperienc d \Device\Hardd 4864 0 lum 712 Window 22 \System 0 2018-11-04 14:27:16 UTC+0000
0xfffffe088788d9200:ApplicationFra d \Device\Hardd 1092 0 lum 712 Window 2 \System 0 2018-11-04 15:58:27 UTC+0000
0xfffffe08878d28080:smartscreen.exe R--r-d \Device\WUDFL 1284 vice 712 ocess 7 nageme 0 2018-11-04 16:40:17 UTC+0000
0xfffffe0887663d080:WmiPrvSE.exe R--r-d \Device\Hardd 3620 0 lum 712 Window 7 \assen 0 2018-11-04 16:26:11 UTC+0000
0xfffffe08876fdb840:RuntimeBroker.ni.dll 4132 712 19 0 2018-11-04 14:27:06 UTC+0000
0xfffffe088793f91c0:mmc.exe 0 RW--r-w- \Device\Hardd 2960 0 lum 4132 \Dire 7 ory 0 2018-11-04 16:37:23 UTC+0000
0xfffffe0887933f780:WmiPrvSE.exe R--r-d \Device\Hardd 3744 0 lum 712 Window 4 \System 0 2018-11-04 16:26:53 UTC+0000
... 0xfffffe08876fc3840:SearchUI.exe 5016 712 31 0 2018-11-04 14:27:18 UTC+0000
```



¿Qué pasó hermano?



volatility -f VMDelegM.dmp --profile=Win10x64_14393 pstree

```
.. 0xffffe08873446080:svchost.exe R--r-d \Device\Hardd 336 ptum 620 Window 16 System 0 2018-11-04 14:16:04 UTC+0000
.. 0xffffe08874695840:svchost.exe RW-rwd \Device\Hardd 1468 ptum 620 Directory 6 0 2018-11-04 14:16:07 UTC+0000
.. 0xffffe08876163080:svchost.exe RW-r-- \Device\Devi 2928 Swb 620 e 9 0 2018-11-04 15:16:35 UTC+0000
.. 0xffffe0887477e840:svchost.exe R--r-d \Device\Hardd 936 ptum 620 Window 39 System 0 2018-11-04 14:16:04 UTC+0000
... 0xffffe08876fab440:rdpclip.exe RW-r-- \Device\Termi 4104 DOX2 936 vice 11 000064 0 2018-11-04 14:27:05 UTC+0000
.. 0xffffe088774824c0:vds.exe RW-rwd \Device\Hardd 2904 ptum 620 SHFTM 16 0 2018-11-04 16:37:23 UTC+0000
.. 0xffffe088748b4080:svchost.exe RW-r-- \Device\Devi 1528 CMN 620 by 3 0 2018-11-04 14:26:44 UTC+0000
.. 0xffffe088746e8840:svchost.exe RWD-r-- \Device\Hardd 2044 ptum 620 Window 7 Softw 0 2018-11-04 14:16:07 UTC+0000
.. 0xffffe088746a66c0:svchost.exe R--r-d \Device\Hardd 2020 ptum 620 Window 14 System 0 2018-11-04 14:16:07 UTC+0000
. 0xffffe08874720080:lsass.exe RW-r-d \Device\Hardd 628 ptum 492 Window 8 System 0 2018-11-04 14:16:03 UTC+0000
0xffffe088741c1700:csrss.exe RW-r-d \Device\Hardd 408 ptum 400 Window 12 SysWO 0 2018-11-04 14:16:02 UTC+0000
0xffffe08872c98700:System RW-r-d \Device\Harddisk 4 ptum 20 Prog 111 Files 0 2018-11-04 14:15:58 UTC+0000
. 0xffffe08873577840:smss.exe RW-r-d \Device\Hardd 308 ptum 4 Volume2 4 System 0 2018-11-04 14:15:58 UTC+0000
.. 0xffffe08874c7a840:smss.exe RW-r-d \Device\Hardd 3168 ptum 308 Window 0 System 0 2018-11-04 14:26:59 UTC+0000
... 0xffffe0887672c840:csrss.exe RW-rwd \Device\Hardd 3232 ptum 3168 Secu 12 $SI 0 2018-11-04 14:26:59 UTC+0000
... 0xffffe08876e35840:winlogon.exe RW-r-d \Device\Hardd 3688 ptum 3168 Window 5 Fonts 0 2018-11-04 14:26:59 UTC+0000
.... 0xffffe0887680e080:userinit.exe RW-r-d \Device\Hardd 4548 ptum 3688 Window 0 System 0 2018-11-04 14:27:09 UTC+0000
..... 0xffffe088748e7080:explorer.exe RW-d \Device\Hardd 4572 ptum 4548 Ser 203 $SDH 0 2018-11-04 14:27:09 UTC+0000
.... 0xffffe08876e77080:dwm.exe RW-r-d \Device\Hardd 720 ptum 3688 Window 13 System 0 2018-11-04 14:27:00 UTC+0000
.. 0xffffe08874398080:smss.exe RW-r-d \Device\Hardd 484 ptum 308 Window 0 System 0 2018-11-04 14:16:02 UTC+0000
... 0xffffe08874257080:winlogon.exe RW-r-- \Device\Termi 552 DOX2 484 vice 02 000063 0 2018-11-04 14:16:02 UTC+0000
.... 0xffffe088747c8080:dwm.exe RW-r-- \Device\Hardd 884 ptum 552 Window 12 System 0 2018-11-04 14:16:04 UTC+0000
.... 0xffffe0887475c080:LogonUI.exe RW-r-- \Device\NamedP 876 552 12 0 2018-11-04 14:16:04 UTC+0000
... 0xffffe0887438f100:csrss.exe RW-r-d \Device\Hardd 500 ptum 484 Window 11 System 0 2018-11-04 14:16:02 UTC+0000
0xffffe08876152840:mspaint.exe RW-rwd \Device\Hardd 2940 ptum 3200 Users\3 urex\A 0 2018-11-04 15:16:35 UTC+0000
0xffffe08878347280:cmd.exe RW-r-d \Device\Hardd 2912 ptum 4392 Users\1 urex\V 0 2018-11-04 16:41:12 UTC+0000
. 0xffffe08878cee680:RamCapture64.e RW-r-- \Device\Devi 4780 0 0 0 2018-11-04 16:41:13 UTC+0000
. 0xffffe08876385840:conhost.exe RW-r-- \Device\Devi 4380 0 0 0 2018-11-04 16:41:12 UTC+0000
```

Parrot Terminal



¿Qué pasó hermano?



volatility -f VMDelegM.dmp --profile=Win10x64_14393 netscan > netscan.txt

Offset (P)	Proto	Local Address	Foreign Address	State	Pid	Owner	Created
0xbe8000195c50	UDPv4	0.0.0.0:5355	*:*		0	svchost.exe	2018-11-04 14:16:13
0xbe8000195c50	UDPv6	:::5355	*:*		0	svchost.exe	2018-11-04 14:16:13
0xbe80001a9ec0	TCPv4	0.0.0.0:3389	0.0.0.0:0	LISTENING	0	svchost.exe	2018-11-04 14:16:06
0xbe80001aade0	TCPv4	0.0.0.0:3389	0.0.0.0:0	LISTENING	0	svchost.exe	2018-11-04 14:16:06
0xbe80001aade0	TCPv6	:::3389	:::0	LISTENING	0	svchost.exe	2018-11-04 14:16:06
0xe08872d95c50	UDPv4	0.0.0.0:5355	*:*		0	svchost.exe	2018-11-04 14:16:13
0xe08872d95c50	UDPv6	:::5355	*:*		0	svchost.exe	2018-11-04 14:16:13
0xe0887349a980	UDPv4	127.0.0.1:1900	*:*		0	svchost.exe	2018-11-04 14:19:44
0xe088735f9b70	UDPv4	0.0.0.0:0	*:*		0	WaAppAgent.exe	2018-11-04 14:16:33
0xe088735f9b70	UDPv6	:::0	*:*		0	WaAppAgent.exe	2018-11-04 14:16:33
0xe08872da9ec0	TCPv4	0.0.0.0:3389	0.0.0.0:0	LISTENING	0	svchost.exe	2018-11-04 14:16:06
0xe08872daade0	TCPv4	0.0.0.0:3389	0.0.0.0:0	LISTENING	0	svchost.exe	2018-11-04 14:16:06
0xe08872daade0	TCPv6	:::3389	:::0	LISTENING	0	svchost.exe	2018-11-04 14:16:06
0xe088735a0b90	TCPv4	192.168.1.4:49678	52.239.143.196:443	ESTABLISHED	-1		2018-11-04 14:16:29
0xe08874263ec0	UDPv4	192.168.1.4:138	*:*		0	System	2018-11-04 14:16:06
0xe088742bdc70	UDPv4	0.0.0.0:3389	*:*		0	svchost.exe	2018-11-04 14:16:06
0xe088742cbec0	UDPv4	0.0.0.0:5355	*:*		0	svchost.exe	2018-11-04 14:16:13
0xe08874410650	UDPv4	127.0.0.1:61436	*:*		0	svchost.exe	2018-11-04 14:16:09
0xe088745312d0	UDPv4	0.0.0.0:0	*:*		0	WindowsAzureGu	2018-11-04 14:16:14
0xe08874556ca0	UDPv4	192.168.1.4:55415	*:*		0	svchost.exe	2018-11-04 14:16:13
0xe088745f0350	UDPv4	0.0.0.0:3544	*:*		0	svchost.exe	2018-11-04 14:16:13



¿Qué pasó hermano?



volatility -f VMDelegM.dmp --profile=Win10x64_14393 wintree

```
new 47 x new 49 x new 48 x netscan.txt psxview.txt wintree.txt explorer.txt mspaint.txt new 48.txt
223 ● .#403ee explorer.exe:4572 -
224 .Default IME rdpclip.exe:4104 TaskbarDPI_Deskband
225 .#e0388 rdpclip.exe:4104 -
226 ● .wall.jpg - Paint (visible) mspaint.exe:2940 -
227 ..#30290 (visible) mspaint.exe:2940 -
228 ..#30286 (visible) mspaint.exe:2940 -
229 ..#30284 (visible) mspaint.exe:2940 -
230 ..#30288 (visible) mspaint.exe:2940 -
231 ..#3027e (visible) mspaint.exe:2940 -
232 ...#40278 (visible) mspaint.exe:2940 -
233 ....+ (visible) mspaint.exe:2940 -
234 ....#40094 (visible) mspaint.exe:2940 -
235 ....- (visible) mspaint.exe:2940 -
236 ....100% (visible) mspaint.exe:2940 ImmersiveContextMenuArray_182748816-31006
237 ....Zoo&m mspaint.exe:2940 ImmersiveContextMenuArray_182748816-31006
238 ..UIRibbonWorkPane mspaint.exe:2940 -
239 ..#50140 (visible) mspaint.exe:2940 -
240 ..#40208 (visible) mspaint.exe:2940 -
241 ...#50294 mspaint.exe:2940 -
242 ...#7029c mspaint.exe:2940 -
243 ...#e01f4 mspaint.exe:2940 -
244 ...#302a2 (visible) mspaint.exe:2940 -
245 ..UIRibbonDockBottom mspaint.exe:2940 -
```



¿Qué pasó hermano?



volatility -f VMDelegM.dmp --profile=Win10x64_14393 memdump -p 2940 --dump-dir /extracted #mspaint y lo pasamos a formato texto con strings

```
~Lsp}Ls
~Ls@}Ls`{Ls0|Ls
{Ls@
JshE9u
Ls`9Ks
9Ks@LKs
"C:\Windows\system32\mspaint.exe" "C:\Windows\system32\wall.jpg"
Is 5Isp Is
sti.dll
```

PROCESS	PID	PRIO	PATH
mspaint.exe	2940	Normal	C:\Windows\SysWOW64\mspaint.exe "C:\Windows\system32\mspaint.exe" "C:\Windows\system32\wall.jpg"
cmd.exe	4004	Normal	C:\Windows\SysWOW64\cmd.exe C:\Windows\system32\cmd.exe /c ""E:\LiveResponseCollection-Bambiraptor\I
pv.exe	1656	Normal	E:\LiveResponseCollection-Bambiraptor\LiveResponseCollection-Bambiraptor\Windows_Live_Response\Tools
FILE0			



¿Qué pasó hermano?



```
volatility -f VMDelegM.dmp --profile=Win10x64_14393 memdump -p 4572 --dump-dir /extracted #explorer
```

```
new 49 x new 48 x netscan.txt x psxview.txt x wintree.txt x explorer.txt x mspaint.txt x new 48.txt x new 50 x shell.txt x
7 Muta
8 Ntfs
9 AfdBzS
0 GET / HTTP/1.1
1 Host: 52.136.239.150:5000
2 Connection: keep-alive
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
5 DNT: 1
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
7 Accept-Encoding: gzip, deflate
8 Accept-Language: es-ES,es;q=0.9,en;q=0.8
9 46cfa"}, {"ObservationName": "[Context]ResourceGroup", "IsHealthy": true, "Description": "[Context]", "Value": "Recursos"}, {"ObservationName": "[Co
0 </body>
1 </html>
2 Free
3 File
4 MmLd
5
```



¿Qué pasó hermano?



Búsqueda en los programas de inicio

The screenshot shows a Notepad++ window with a script containing several 'File not found' errors and a File Explorer window showing a directory listing.

```
885 vidc.uvyv
886 msyuv.dll
887 File not found: msyuv.dll
888
889 vidc.yuy2
890 msyuv.dll
891 File not found: msyuv.dll
892
893 vidc.yvu9
894 tsbyuv.dll
895 File not found: tsbyuv.dll
896
897 vidc.yvyu
898 msyuv.dll
899 File not found: msyuv.dll
900
901 wavemapper
902 msacm32.drv
903 File not found: msacm32.drv
904
905
906 C:\Users\azure\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
907 Invoke-SocksProxy.psml
908 C:\Users\azure\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Invoke-SocksProxy.psml
909 c:\users\azure\appdata\roaming\microsoft\windows\start menu\programs\startup\invoke-socksproxy.psml
910 11/4/2018 3:16 PM
911 MD5: 4CA59AB0F4DE4913D37234E58A90856B
912 SHA1: B2BED2C4617903CB9A1E800E5F38B34209793D48
913 PESHAl: B2BED2C4617903CB9A1E800E5F38B34209793D48
914 SHA256: 0D27CDCC556F29108D22842C16DBC5EF4C63E5AB72D525843259D7097FE43C6E
915 PESHAS256: 0D27CDCC556F29108D22842C16DBC5EF4C63E5AB72D525843259D7097FE43C6E
916
```

The File Explorer window shows the following directory listing:

Nombre	Fecha de modifica...	Tipo	Tamaño
autorunsc.csv	04/11/2018 17:26	Archivo de valores...	82 KB
autorunsc.txt	04/11/2018 17:26	Documento de tex	81 KB
Driver_group_load_order_wmic.txt	04/11/2018 17:26	Documento de tex	11 KB
Loaded_dlls.txt	04/11/2018 17:26	Documento de tex	113 KB
scheduled_tasks.txt	04/11/2018 17:24	Documento de tex	247 KB



¿Qué pasó hermano?



Nos fijamos en: Invoke-SocksProxy.psm1

```
w 47 x | new 49 x | new 48 x | netscan.bt x | wintree.bt x | explorer.txt x |
94 Startup
95 Invoke-SocksProxy.psm1
96 @c\t4
97 ^c\t4
98 C\PY
99 /I&@i/
```

```
GitHub, Inc. [US] | https://github.com/p3nt4/Invoke-SocksProxy/blob/master/Invoke-SocksProxy.psm1
9 .DESCRIPTION
10
11 Creates a Socks proxy using powershell.
12
13 Supports both Socks4 and Socks5 connections.
14
15 This is only a subset of the Socks 4 and 5 protocols: It does not support authentication,
16
```

<https://github.com/p3nt4/Invoke-SocksProxy/blob/master/Invoke-SocksProxy.psm1>



¿Qué pasó hermano?



Vemos las variables del sistema

```
w 47 x new 49 x new 48 x netscan.txt wintree.txt explorer.txt mspaint.txt new 48.txt new 50 x sh
kc\ (Q
ure\AppData\NC\
PROFILE=OC\
=C:\Windows
LOCALAPPDATA=C:\Users\azure\AppData\Local
NUMBER_OF_PROCESSORS=2
OS=Windows_NT
Path=C:\Python27\;C:\Python27\Scripts;C:\Windows\system32;C:\Windows;C:\Windows\S
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=4f01
ProgramFiles(x86)=C:\Program Files (x86)
PSModulePath=C:\Program Files\WindowsPowerShell\Modules;C:\Windows\system32\Windc
PUBLIC=C:\Users\Public
SESSIONNAME=RDP-Tcp#1
CT@Q
SystemDrive=C:
windir=C:\Windows
SystemRoot=C:\Windows
USERNAME=azure
TEMP=C:\Users\azure\AppData\Local\Temp\2
KR\ w
```

```
47 x new 49 x new 48 x netscan.txt wintree.txt explorer.txt x
47 ASYC
1 Users
2 Documents
3 \MNT
4 server.py
5 ,Rt></
6 0\M&
7 0\M&
8 0\M&
9 LMEM
0 sersd
1 0\M&
2 eLMEM
3 nLMEM
4 0\M&$
5 \MNT
6
```

```
x new 49 x new 48 x netscan.txt wintree.txt explorer.txt mspaint.txt new 48.txt new 50 x sh
36 tgru
37 q$>&
38 Content-Type: text/html; charset=utf-8
39 Content-Length: 1343
40 Server: Werkzeug/0.10.4 Python/2.7.15
41 Date: Sun, 04 Nov 2018 15:00:18 GMT
42 'RTSP/1.0').
43 <p>Error code explanation: 400 = Bad request syntax or unsupported method.
44 </body>
```



¿Qué pasó hermano?



¿Qué es Werkzeug???

Werkzeug

The Python WSGI Utility Library

[overview](#) | [documentation](#) | [community](#)



Welcome

Werkzeug is a WSGI utility library for Python. It's widely used and BSD licensed.

Vulnerability Details : [CVE-2016-10516](#)

Cross-site scripting (XSS) vulnerability in the render_full function in debug/tbtools.py in the debugger in Pallets Werkzeug before 0.11.11 (as used in Pallets Flask and other products) allows remote attackers to inject arbitrary web script or HTML via a field that contains an exception message.

Publish Date : 2017-10-23 Last Update Date : 2018-02-03

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#) [▼ Scroll To](#) [▼ Comments](#) [▼ External Links](#)

[Search Twitter](#) [Search YouTube](#) [Search Google](#)

- CVSS Scores & Vulnerability Types

CVSS Score	4.3
Confidentiality Impact	None (There is no impact to the confidentiality of the system.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	None (There is no impact to the availability of the system.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Cross Site Scripting
CWE ID	79



Hora de inicio de la intrusión:

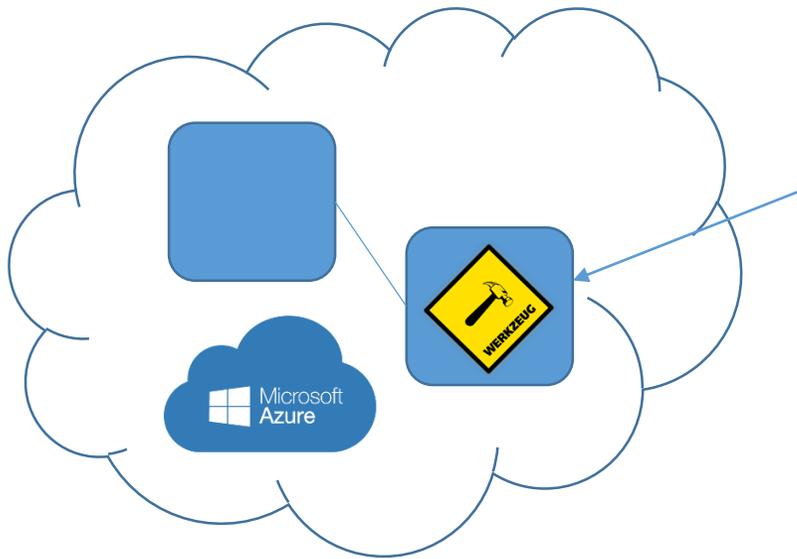
✓ 04/11/2018 a las 14:16

Hechos constatados:

- Descarga e instalación de Python 2.7
- Creación y configuración para cuando se inicie el sistema de un sock proxy que usa powershell
- Creación de un servicio web expuesto en internet
- Vulneración de este servicio web mediante un XSS



Escenario



Servidor WSGI werkzeug 0.10.4 expuesto en el puerto 5000



Home Exploits Shellcode Papers Google Hacking Database Submit Search

Werkzeug - 'Default' Remote Command Execution

EDB-ID: 43905	Author: Ali BawazeEer	Pub
CVE: N/A	Type: Remote	Plat
E-DB Verified:	Exploit: Download / View Raw	Vuln

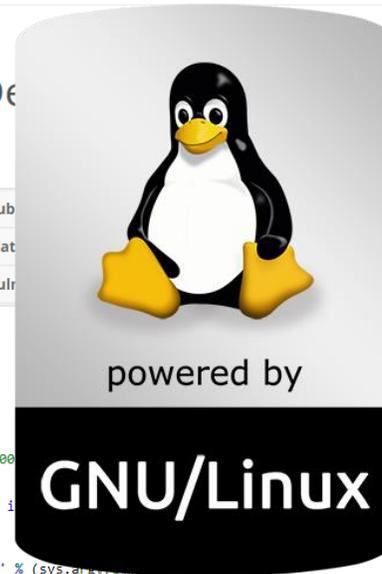
« Previous Exploit

Next Exploit »

```

1  #!/usr/bin/env python
2  import requests
3  import sys
4  import re
5  import urllib
6
7  # usage : python exploit.py 192.168.56.101 5000
8
9  if len(sys.argv) != 5:
10     print "USAGE: python %s <ip> <port> <your ip> <command>"
11     sys.exit(-1)
12
13
14 response = requests.get('http://%s:%s/console' % (sys.argv[1], sys.argv[2]))
15
16 if "Werkzeug" not in response.text:

```





METAS ATACANTE

- Modificar el exploit para que sirva para Windows.
- Encontrar un puerto "Closed".
- Subir Server Proxy SOCKS5.
- Escaneo interno.





- ATAQUE:

1 - Ejecutar comandos (Whoami, ARP etc..)



2 - Descargar Ficheros



3 - Subir Server Proxy Socks



<https://github.com/p3nt4/Invoke-SocksProxy>



Terminal window header with menu items: Terminal, Sessions, View, X server, Tools, Games, Settings, Macros, Help. Quick connect... field and tabs for sessions 5, 6, and 7.

root@4nonimizer-repo:~#

Browser window header: Werkzeug - 'Debug Shell' Comm. x | +. Address bar: No es seguro | 52.136.239.150:5000.

Browser navigation and bookmark bar. Bookmarks include: Aplicaciones, Amiga, Exploits, Honeypot, Musica, Pentest, Reversing - R2, Blockchain, Exploiting, Plantas, Python, bettercap, CEH, Dominio Windows, Malware, Server, and Otros marcadores.

PROSEGUR CIBERSEGURIDAD



Acceso al servicio

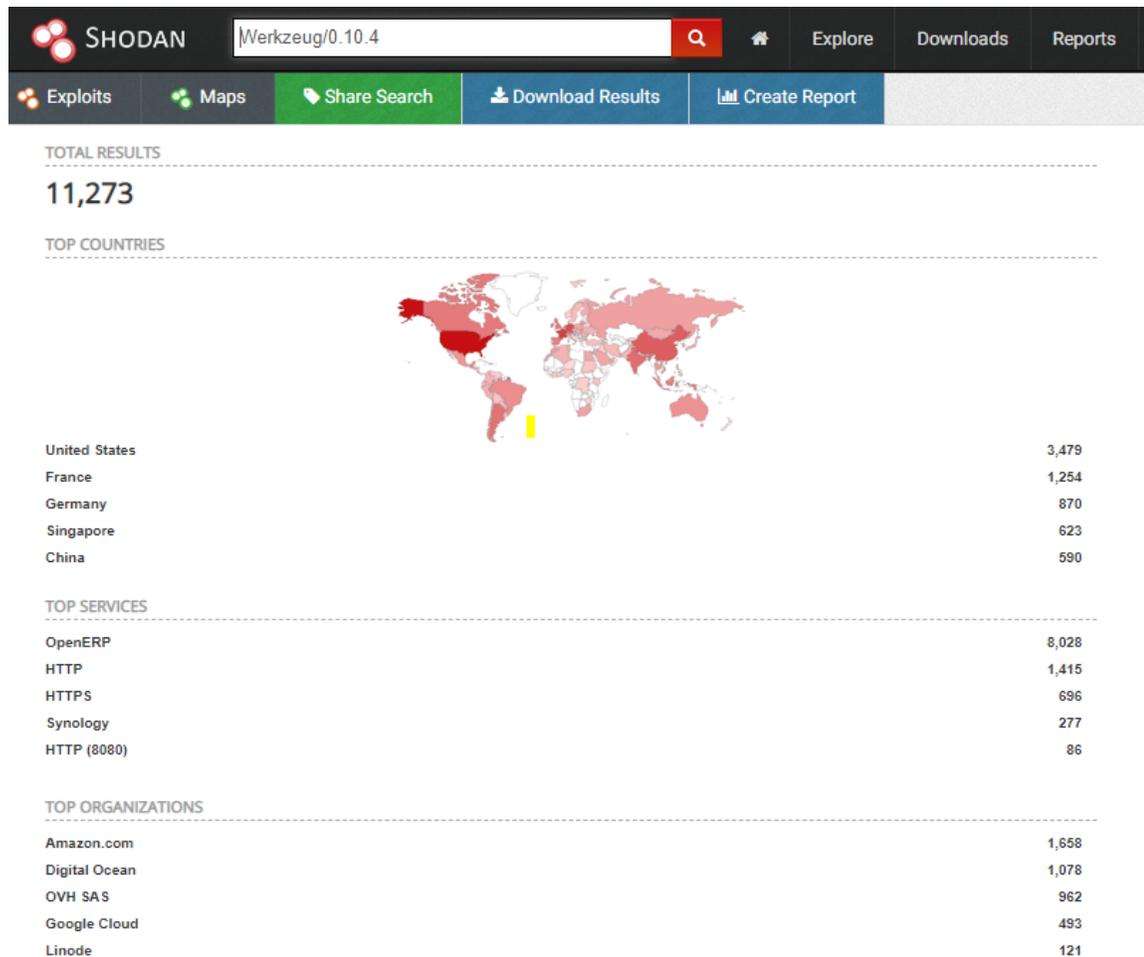
Username:

Password:

ACEPTAR



- Es un ejemplo pero....:



RED TEAM o BLUE TEAM



THANK YOU



```
Sending SIGKILL to all processes.  
Please stand by while rebooting the system.  
[64857.521348] sd 0:0:0:0: [sda] Synchronizing SCSI cache  
[64857.522838] Restarting system.
```