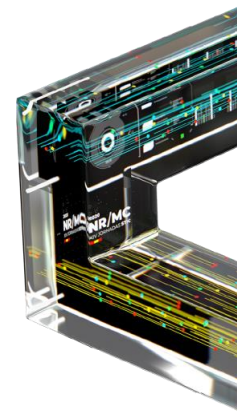


#XIVJORNADASCCNCERT

Movimientos laterales en Ransomware





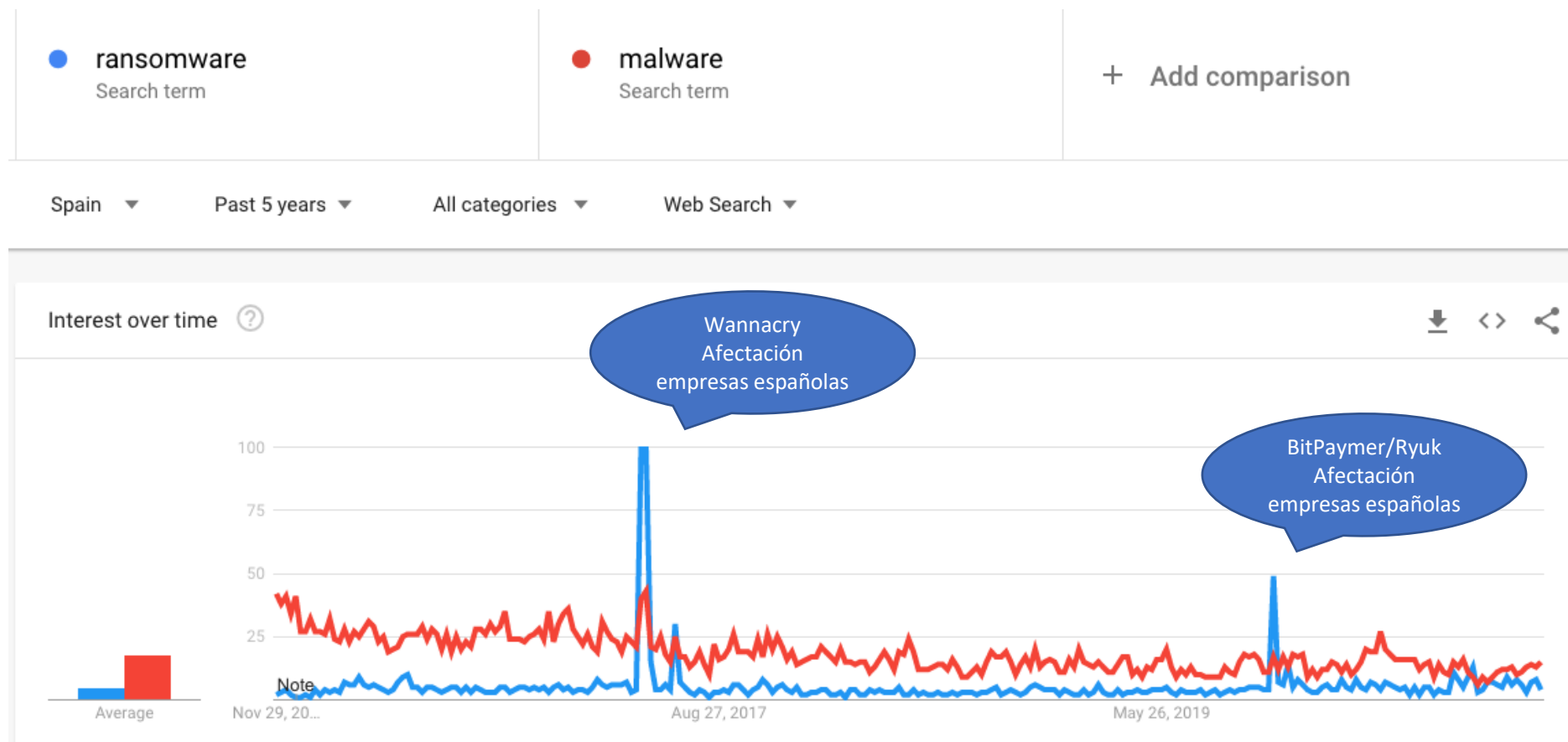
David Barroso

CounterCraft

dbarroso@countercraftsec.com
@lostinsecurity

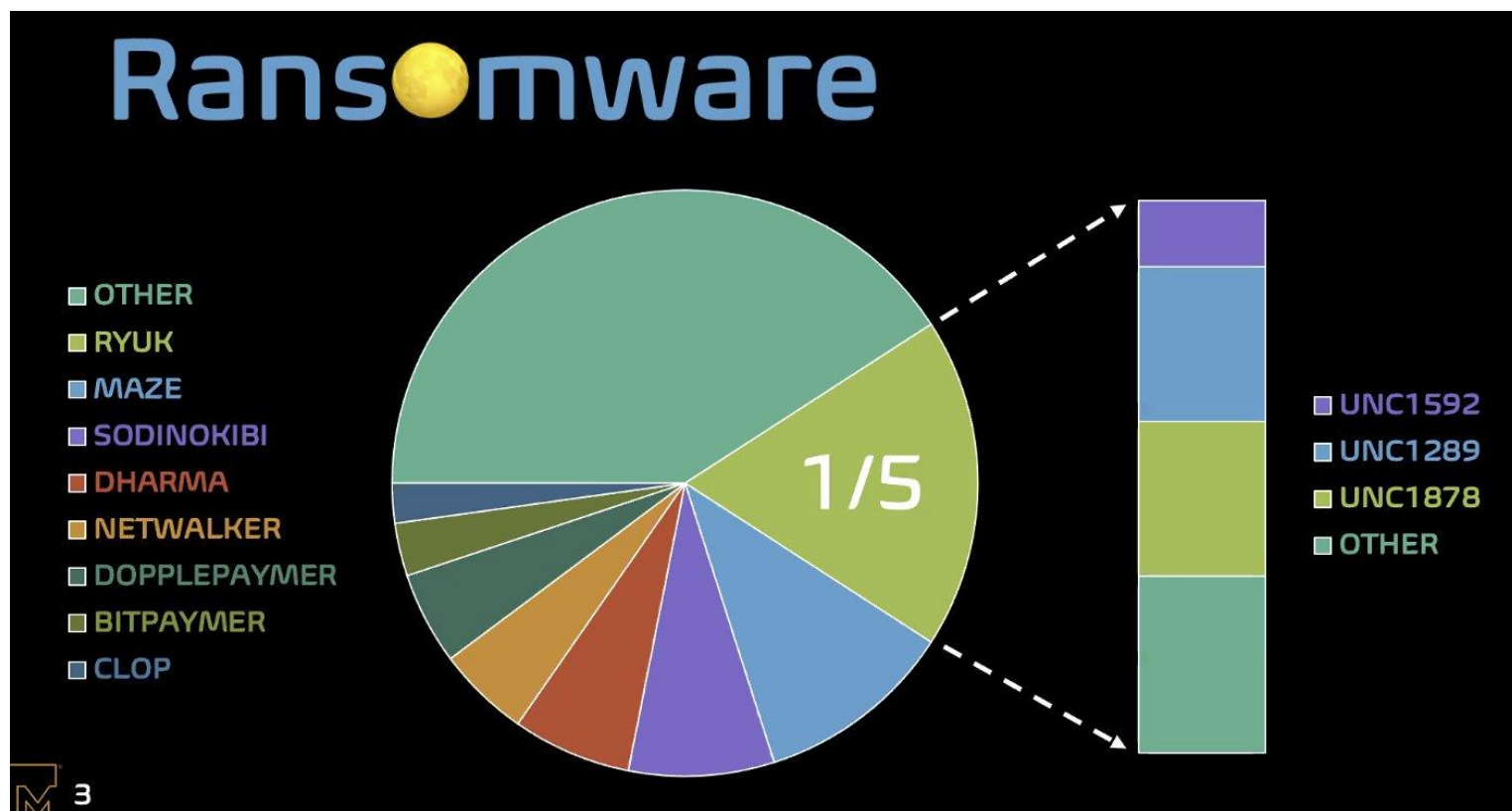
Ransomware

El malware que nos preocupa



Ransomware

El malware que nos preocupa



Fuente: Mandiant

Ransomware

El malware que nos preocupa



Fuente: Mandiant

Ransomware

Unos pasos bien definidos



Ransomware

Time to Ransomware

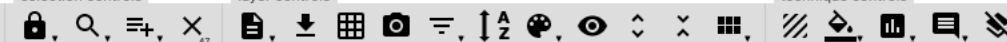


Ransomware

Unos pasos bien definidos

1. Reconocimiento
2. Compromiso inicial
3. Descubrimiento de la infraestructura
4. Movimientos laterales
5. Escalada de privilegios
6. Despliegue del ransomware
7. Detonación
8. Negociación
9. PROFIT

Un paso por delante
Asumamos que ocurre
Talón de Aquiles
Nuestro foco principal
Asumamos que ocurre
Ya es tarde
Game Over
Recuperación desastre
LOSS



Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 14 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (0/4)	Exploitation of Remote Services	Archive Collected Data (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credentials from Password Stores (0/3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Inter-Process Communication (0/2)	Boot or Logon Autostart Execution (0/12)	Boot or Logon Autostart Execution (0/12)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoded (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Clipboard Data	Data from Cloud Storage Object	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Scheduled Task/Job (0/6)	Browser Extensions	Create or Modify System Process (0/4)	Direct Volume Access	Input Capture (0/4)	Cloud Service Dashboard	Remote Services (0/6)	Data from Configuration Repository (0/2)	Data from Cloud Storage Object	Dynamic Resolution (0/3)	Defacement (0/2)
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (0/15)	Execution Guardrails (0/1)	Man-in-the-Middle (0/2)	Cloud Service Discovery	Replication Through Removable Media	Data from Information Repositories (0/2)	Data from Configuration Repository (0/2)	Encrypted Channel (0/2)	Disk Wipe (0/2)
Search Closed Sources (0/2)		Supply Chain Compromise (0/3)	Software Deployment Tools	Create Account (0/3)	Exploitation for Privilege Escalation	File and Directory Permissions Modification (0/2)	Modify Authentication Process (0/4)	Domain Trust Discovery	Software Deployment Tools	Data from Local System	Fallback Channels	Exfiltration Over Other Network Medium (0/1)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)		Trusted Relationship	System Services (0/2)	Create or Modify System Process (0/4)	Group Policy Modification	Group Policy Modification	Network Sniffing	File and Directory Discovery	Taint Shared Content	Data from Network Shared Drive	Ingress Tool Transfer	Exfiltration Over Physical Medium (0/1)	Firmware Corruption
Search Open Websites/Domains (0/2)		Valid Accounts (0/4)	Windows Management Instrumentation	Event Triggered Execution (0/15)	Hijack Execution Flow (0/11)	Hide Artifacts (0/7)	OS Credential Dumping (0/8)	Network Service Scanning	Use Alternate Authentication Material (0/4)	Data from Removable Media	Multi-Stage Channels	Exfiltration Over Web Service (0/2)	Network Denial of Service (0/2)
Search Victim-Owned Websites				External Remote Services	Process Injection (0/11)	Hijack Execution Flow (0/11)	Steal Application Access Token	Network Share Discovery		Data from Removable Media	Non-Application Layer Protocol	Scheduled Transfer	Resource Hijacking
				Hijack Execution Flow (0/11)	Scheduled Task/Job (0/6)	Impair Defenses (0/7)	Steal or Forge Kerberos Tickets (0/4)	Network Sniffing		Email Collection (0/3)	Non-Standard Port	Transfer Data to Cloud Account	Service Stop
				Implant Container Image	Valid Accounts (0/4)	Indicator Removal on Host (0/6)	Steal Web Session Cookie	Password Policy Discovery		Input Capture (0/4)	Protocol Tunneling		System Shutdown/Reboot
				Office Application Startup (0/6)	Masquerading (0/6)	Indirect Command Execution	Two-Factor Authentication Interception	Peripheral Device Discovery		Man in the Browser	Proxy (0/4)		
				Pre-OS Boot (0/5)	Modify Authentication Process (0/4)	Masquerading (0/6)	Unsecured Credentials (0/6)	Permission Groups Discovery (0/3)		Man-in-the-Middle (0/2)	Remote Access Software		
				Scheduled Task/Job (0/6)	Modify Cloud Compute Infrastructure (0/4)	Modify Authentication Process (0/4)		Process Discovery		Screen Capture	Traffic Signaling (0/1)		
				Server Software Component (0/3)	Modify Registry	Modify Cloud Compute Infrastructure (0/4)		Query Registry		Video Capture	Web Service (0/3)		
				Traffic Signaling (0/1)	Modify System Image (0/2)	Modify Registry		Remote System Discovery					
				Valid Accounts (0/4)	Network Boundary Bridging (0/1)	Modify System Image (0/2)		Software Discovery (0/1)					
						Network Boundary Bridging (0/1)		System Information Discovery					
								System Network Configuration Discovery					

Ransomware

Unos pasos bien definidos

1. Reconocimiento
2. Compromiso inicial
3. Descubrimiento de la infraestructura
4. Movimientos laterales
5. Escalada de privilegios
6. Despliegue del ransomware
7. Detonación
8. Negociación
9. PROFIT

Un paso por delante
Asumamos que ocurre
Talón de Aquiles
Nuestro foco principal
Asumamos que ocurre
Ya es tarde
Game Over
Recuperación desastre
LOSS

A tener en cuenta

Al final todo es A, B o C

Independientemente de el framework de post-explotación o herramienta utilizada, todos por debajo utilizan siempre las mismas técnicas. Esas técnicas son lo realmente importante de detectar, no si se utiliza una herramienta u otra.

Acordémonos de la pirámide del dolor de David Bianco, y pensemos en TTPS, no en hashes, direcciones IP o nombres de fichero.

Descubrimiento de la infraestructura

No todas las organizaciones son iguales

Los objetivos principales son:

- Descubrimiento de la máquina local comprometida.
- Descubrimiento del Directorio Activo: dominios, relaciones de confianza, PDCs, administradores, etc.
- Comprobación de que están online las máquinas más interesantes.

Nombre: Herramientas genéricas de Windows

Descripción: herramientas del sistema operativo

Detección: difícil puesto que son usadas por administradores y usuarios avanzados.



```
quser.exe
whoami.exe /user
net.exe group /domain
net.exe group "Domain Users" /domain
nltest.exe /dclist:
Nslookup "-q=srv_kerberos._tcp"
net view /all /domain
nltest /domain_trusts /all_trusts
net localgroup "administrator"
dsquery
arp -a
```

Nombre: PowerShell

Descripción: es necesario cargar el módulo de ActiveDirectory para consultas al AD

Detección: difícil puesto que son usadas por administradores y usuarios avanzados, aunque en teoría pocos las tendrían que utilizar.



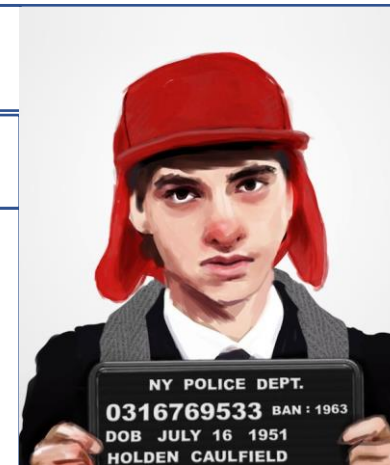
Get-ADComputer –Filter {enabled –eq \$true} –properties * | select Name, DNSHostName, OperatingSystem, LastLogonData | Export-CSV C:\Users\AllWindows.csv –NoTypeInfoInformation –Encoding UTF8

Get-ADUser

Nombre: AdFind.exe

Descripción: <http://www.joeware.net/freetools/tools/adfind/>

Detección: debería ser sencilla, pero cualquiera podría cambiar el nombre y el hash

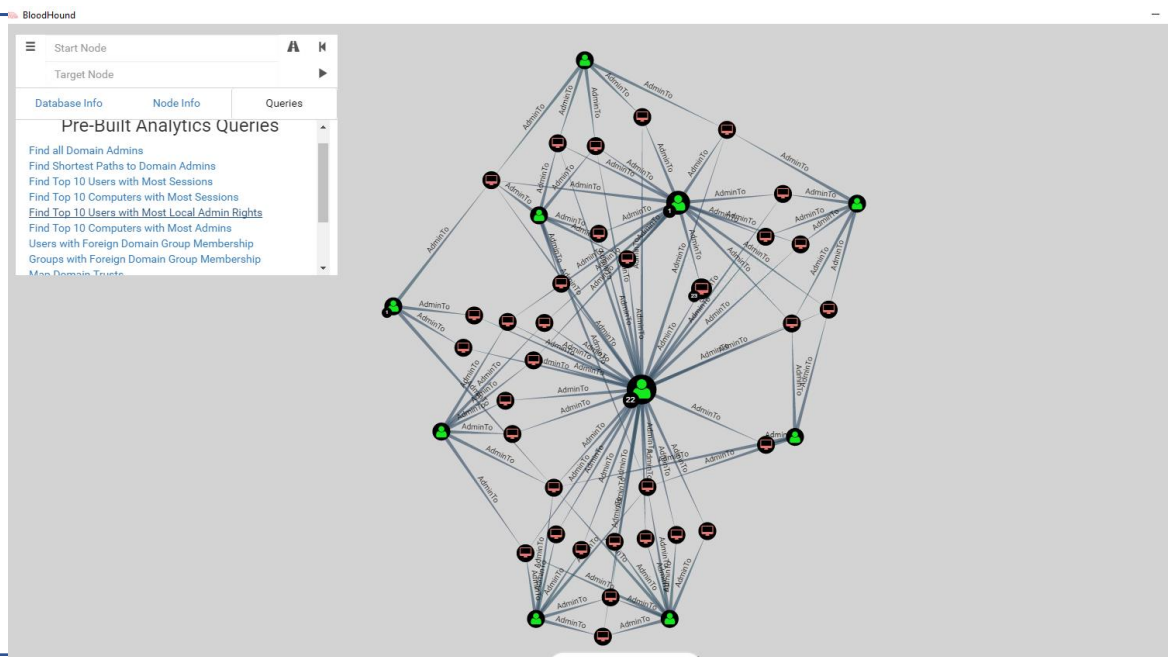
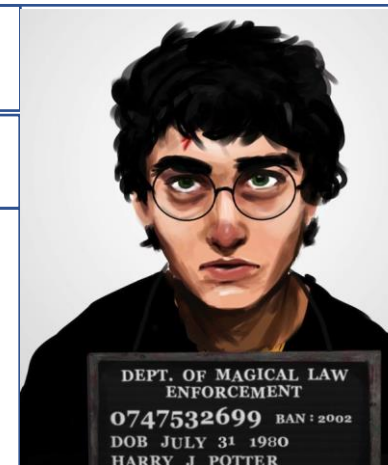


```
adfind.exe -f (objectcategory=person) > <user_list>.txt
adfind.exe -f objectcategory=computer > <computer_list>.txt
adfind.exe -f (objectcategory=organizationalUnit) > <ou_list>.txt
adfind.exe -subnets -f (objectCategory=subnet) > <subnet_list>.txt
adfind.exe -f "(objectcategory=group)" > <group_list>.txt
adfind.exe -gcb -sc trustdmp > <trustdmp>.txt
adfind -f objectcategory=computer -csv name cn OperatingSystem dNSHostName > some.csv
```

Nombre: BloodHound

Descripción: <https://github.com/BloodHoundAD/BloodHound>

Detección: Alto volúmen de peticiones LDAP al AD. Peticiones más largas. Utilización masiva de las pipes srvsvc y lsass



Nombre: Frameworks clásicos de PowerShell (Empire, PowerSploit, etc.)

Descripción: Framework de post-explotación

Detección: difícil puesto que utiliza herramientas de PowerShell del sistema
<https://github.com/PowerShellMafia/PowerSploit/tree/master/Recon>



Get-NetLocalGroup	- enumerates the local groups on the local (or remote) machine
Get-NetLocalGroupMember	- enumerates members of a specific local group on the local (or remote) machine
Get-NetShare	- returns open shares on the local (or a remote) machine
Get-NetLoggedon	- returns users logged on the local (or a remote) machine
Get-NetSession	- returns session information for the local (or a remote) machine
Get-RegLoggedOn	- returns who is logged onto the local (or a remote) machine through enumeration of
Get-NetRDPSession	- returns remote desktop/session information for the local (or a remote) machine
Test-AdminAccess	- tests if the current user has administrative access to the local (or a remote) machine
Get-NetComputerSiteName	- returns the AD site where the local (or a remote) machine resides
Get-WMIRegProxy	- enumerates the proxy server and WPAD contents for the current user
Get-WMIRegLastLoggedOn	- returns the last user who logged onto the local (or a remote) machine
Get-WMIRegCachedRDPConnection	- returns information about RDP connections outgoing from the local (or remote) machine
Get-WMIRegMountedDrive	- returns information about saved network mounted drives for the local (or remote) machine
Get-WMIProcess	- returns a list of processes and their owners on the local or remote machine
Find-InterestingFile	- searches for files on the given path that match a series of specified criteria

Get-DomainGPO	- returns all GPOs or specific GPO objects in AD
Get-DomainGPOLocalGroup	- returns all GPOs in a domain that modify local group memberships through 'Rest
Get-DomainGPOUserLocalGroupMapping	- enumerates the machines where a specific domain user/group is a member of a sp
Get-DomainGPOComputerLocalGroupMapping	- takes a computer (or GPO) object and determines what users/groups are in the s
Get-DomainPolicy	- returns the default domain policy or the domain controller policy for the curr

Nombre: Cobalt Strike

Descripción: Framework de post-explotación favorito del ransomware

Detección: difícil puesto que utiliza herramientas de sistema

<https://github.com/killswitch-GUI/CobaltStrike-ToolKit/blob/master/Invoke-DACheck.ps1>

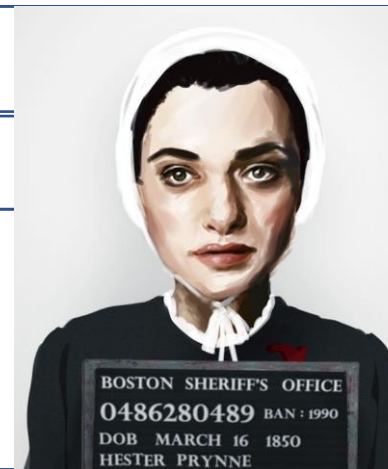


```
$groupname = 'Domain Admins'
$DAUsers = (New-Object System.DirectoryServices.DirectoryEntry((New-Object
System.DirectoryServices.DirectorySearcher("&(objectCategory=Group)(name= $($groupname))").FindOne()
.GetDirectoryEntry().Path)).member | % { (New-Object
System.DirectoryServices.DirectoryEntry("LDAP://"+$_)) } | foreach {$_ .sAMAccountName}
return $DAUsers
```

Nombre: Ping y network scan

Descripción: Una vez localizados los servidores que nos interesan. ¿Están online?

Detección: difícil detectar un ping o un network scan sin tener miles de falsos positivos



ping DOMAINCONTROLLER

Network Scanner <https://www.softperfect.com/products/networkscanner/>

Descubrimiento de la infraestructura

No todas las organizaciones son iguales



Descubrimiento de la infraestructura

No todas las organizaciones son iguales

Sí, el compromiso inicial es en un ordenador de la organización, pero al final cualquier herramienta que utilicen utilizará el Directorio Activo. ¡Es nuestra ventaja conocer que lo tienen que utilizar!

¿Qué podemos hacer para detectarlos?

Si nos fijamos, todas ellas tienen un punto en común: el Directorio Activo.

Nuestra estrategia de detección tiene que ser intentar detectar quién está haciendo este descubrimiento del Directorio Activo. Formas de conseguirlo:

- Detección de herramientas de inventariado de Directorio Activo en los ordenadores (complejidad media)
- Monitorización de la red buscando patrones contra el Directorio Activo (complejidad alta)
- Monitorización del Directorio Activo (complejidad alta)
- Utilización de HoneyTokens en el Directorio Activo. (complejidad baja)
- Creación de otros Forests ficticios y monitorización de peticiones a los mismos (complejidad baja)

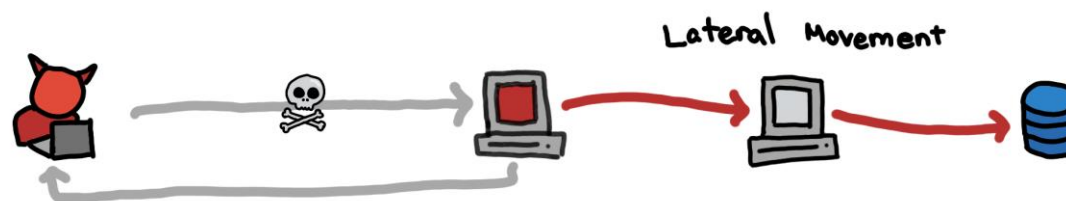
Movimientos laterales

Maximizando el impacto

Existen multitud de formas de escalar privilegios y de obtener credenciales. En esta presentación, asumimos que lo han conseguido y nos centramos en detectar cómo se mueven lateralmente.

Independientemente de que se use un framework de post-explotación o no, las técnicas son muy parecidas, aunque podemos agruparlas en dos tipos de estrategias diferentes:

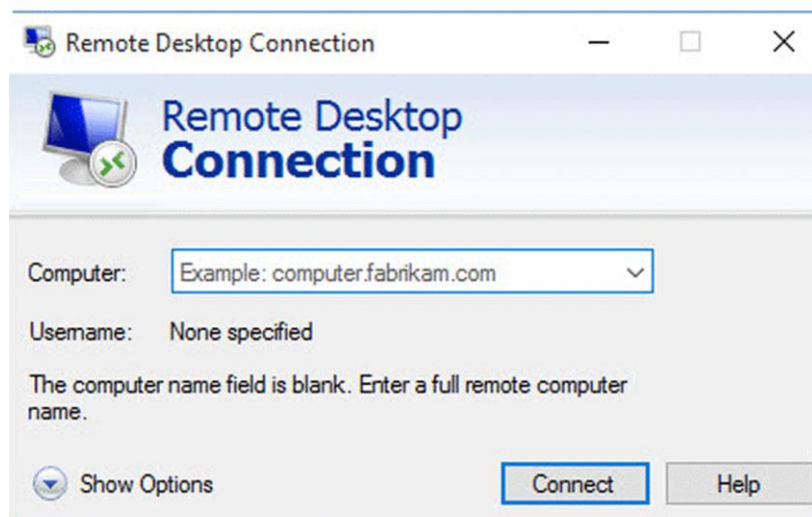
- **Movimiento lateral esporádico:** donde existe un movimiento lateral pero no se deja nada residente.
- **Movimiento lateral con implante (con o sin persistencia):** se deja algo residente (un proceso, tarea programada, suscripción a WMI, inyección en proceso, etc.) con o sin persistencia (la persistencia da para otra presentación, aunque en la mayoría de casos de Ransomware se utilizan mucho las tareas programadas).



Nombre: RDP

Descripción: Acceso remoto

Detección: difícil puesto que son usadas por administradores y usuarios. Es casi imposible revisar todos los eventos 4776, 4624 y 4625 (logon type 10) de nuestros sistemas Microsoft Windows.



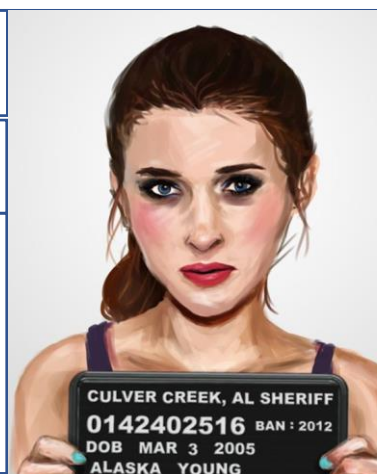
Nombre: acceso a unidades compartidas

Descripción: clásico acceso a unidades compartidas o a toda la unidad (C\$)

Detección: de nuevo la ejecución es sencilla: autenticación válida (4624) y acceso a un objeto compartido (5140). Pero la detección es complicada puesto que es normal encontrar cientos o miles de estos eventos al día.



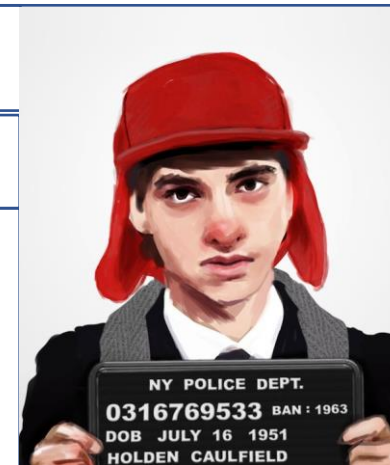
C:\Windows\system32\cmd.exe /C dir \\Server\c\$

Nombre: PsExec	
Descripción: ejecución remota usando un servicio remoto (requiere tener privilegios admin)	
Detección: tanto la herramienta de SysInternals como las implementaciones de todos los frameworks de explotación funcionan igual: acceso remoto a IPC\$ y ADMIN\$ (5140) + autenticación (4624) + Creación de servicio (7045) + creación del proceso a través de ese servicio + (opcional) borrado del servicio	
En este caso, la creación de un servicio es un evento menos común, que habría que monitorizar con calma. Casi todos los frameworks ofrecen un psexec_psh (en powershell y fileless). PsExec.exe -d \\HOST -u "DOMAIN\USER" -p "PASSWORD" -accepteula -s cmd /c "powershell.exe -ExecutionPolicy Bypass -file \\DOMAINCONTROLLER\share\$\p.ps1" C:\psexec.exe @ip-list.txt -d cmd /c "(net use q: /delete /y &; net use q: \\DomainController\DomainName /user:DomainName\administrator ThisWasThePassword &; powershell -ExecutionPolicy ByPass -NoLogo -NoProfile -windowstyle hidden -NoExit -File q:\P100119.ps1" Cobalt Strike: jump->psexec / remote-exec	

Nombre: WMI

Descripción: ejecución remota por WMI

Detección: siempre también es el mismo comportamiento: autenticación (4624) + creación del proceso por parte de 'C:\Windows\System32\wbem\WmiPrvSE.exe'



Importante monitorizar todos los procesos creados por ese proceso padre.

C:\Windows\system32\cmd.exe /C WMIC/node:"DC.DOMAIN.local" process call create "cmd /c

C:\PerfLogs\servisess.exe\"

WMIC /node:\"DC.example.domain\" process call create \"rundll32 C:\\PerfLogs\\arti64.dll, StartW\"

Cobalt Strike: jump->wmi / remote-exec

Koadic: implant/pivot/exec_wmi

Nombre: tarea programada remota

Descripción: creación de una tarea programada remota

Detección: de nuevo la ejecución es sencilla: autenticación válida (4624) y creación de una tarea programada (4698)



Como hemos ido comentado, las tareas programadas se utilizan tanto para movimientos laterales como para persistencia, con lo que es importante monitorizar la creación de las mismas (evento 4698 de windows)

Nombre: WinRM

Descripción: acceso a WinRM (sólo en Windows Server)

Detección: aunque menos utilizadas en casos de ransomware, es también una técnica válida. La detección es parecida a la de WMI puesto que hay una autenticación válida (4624) + creación del proceso cuyo padre es 'C:\Windows\System32\wsmprovhost.exe'



Nombre: Uso de exploits (MS17-010,

Descripción: uso de exploits remotos

Detección: aunque no es muy frecuente, es posible ver la utilización de exploits remotos para movimientos laterales: como MS17-010 (EternalBlue) contra SMBv1 o CVE-2020-1472 (ZeroLogon) como los controladores de dominio



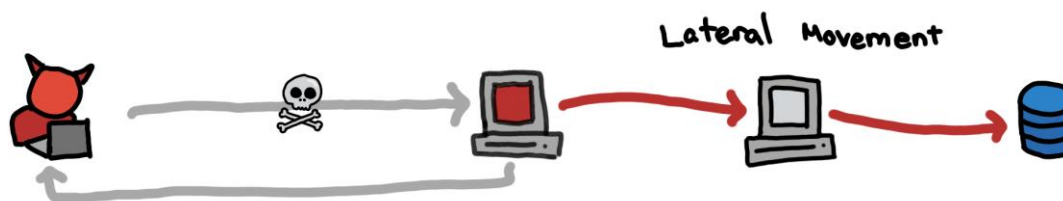
En este caso, estos exploits son bastante ‘ruidosos’ con lo que sería relativamente fácil poder detectar el uso de los mismo, tanto analizando el tráfico de red con un IDS, como revisando los logs de los sistemas afectados (4742 con ANONYMOUS LOGON). Aunque es posible que salgan muchos falsos positivos.

Movimientos laterales

Maximizando el impacto

Identificar movimientos laterales algunas veces es buscar una aguja en un pajar. Pero tenemos algunas opciones muy interesantes para poder identificar conexiones anómalas que pudieran detectar esta fase de movimientos laterales.

- Identificar la creación de nuevos servicios (7045) (complejidad baja/media)
- Identificar la creación de tareas programadas (4698) (complejidad baja/media)
- Identificar la creación de procesos cuyos padres sea WMI o WinRM (complejidad baja – aunque depende del EDR/Sysmon)
- Utilizar herramientas de engaño (deception) para atraer a los atacantes e identificar los eventos más complicados de detectar por pasar desapercibidos (autenticaciones válidas, acceso a recursos compartidos, acceso a RDP, etc...)



Cobalt Strike

¿Por qué hablamos tanto de él?



COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

DOWNLOAD!

FEATURES **SCREENSHOTS** **TRAINING** **SUPPORT**

Cobalt Strike

Cobalt Strike View attacks: Exporting info

Event Log X Screenshots X Beacon 10.10.10.4@1009 X Script Console X

User	Computer	pid	when
SYSTEM	DC	4016	09/11 14:18:50
SYSTEM	DC	4016	09/11 13:54:00
SYSTEM	FILESERVER	1008	09/11 13:54:00
whatta.hogg	WS2	3952	09/11 13:54:00
SYSTEM	DC	4016	09/11 13:53:21
SYSTEM	FILESERVER	1008	09/11 13:53:21
whatta.hogg	WS2	3952	09/11 13:53:21

Cobalt Strike

¿Por qué hablamos tanto de él?

Aunque existen otros frameworks de post-explotación, Cobalt Strike es el que más activamente desarrollado está. Incluye nuevas técnicas de persistencia, movimiento lateral, volcado de credenciales, escalada de privilegios etc. tan pronto como son descubiertas. Permite también personalizar todo para hacer más difícil su detección.

Además, aun siendo de pago (\$3.500 por usuario/año), existen versiones pirateadas fáciles de acceder.

```

~/Documents/src/cobaltstrike-cracked
> ls -alrt
total 319072
drwx----- 48 tomac staff      1536 Nov 11 23:23 ..
-rw-r--r--  1 tomac staff        964 Nov 11 23:24 README.en.md
-rw-r--r--  1 tomac staff         24 Nov 11 23:24 README.md
-rw-r--r--  1 tomac staff 63768645 Nov 11 23:24 cobaltstrike3.12_cracked-master.zip
-rw-r--r--  1 tomac staff 21217322 Nov 11 23:24 cobaltstrike3.14_cracked.7z
-rw-r--r--  1 tomac staff 25662048 Nov 11 23:24 cobaltstrike4.0-cracked.zip
-rw-r--r--  1 tomac staff 27091306 Nov 11 23:24 cobaltstrike4.0-macOS app.zip
drwxr-xr-x 10 tomac staff       320 Nov 11 23:24 .
-rw-r--r--  1 tomac staff 25603513 Nov 11 23:24 cobaltstrike4.0-original.zip

```

Cobalt Strike

¿Por qué hablamos tanto de él?

Pero como comentamos, todas las herramientas utilizan al final las mismas técnicas. Ejemplo de cómo Cobalt Strike usa la ejecución por WMI:

```

1 package beacon.methods;      Allen, a month ago • first commit
2
3 import aggressor.AggressorClient;
4 import aggressor.DataUtils;
5 import beacon.BeaconRemoteExecMethods;
6 import beacon.TaskBeacon;
7
8 public class WMI implements BeaconRemoteExecMethods.RemoteExecMethod {
9     protected AggressorClient client;
10
11     public WMI(AggressorClient aggressorClient) {
12         this.client = aggressorClient;
13         DataUtils.getBeaconRemoteExecMethods(aggressorClient.getData()).register("wmi", "Remote execute via WMI (PowerShell)", this);
14     }
15
16     public void remoteexec(String string1, String string2, String string3) {
17         TaskBeacon taskBeacon = new TaskBeacon(this.client, new String[]{string1});
18         taskBeacon.log_task(string1, "Tasked beacon to run '" + string3 + "' on " + string2 + " via WMI", "T1047");
19         taskBeacon.silent();
20         taskBeacon.PowerShellNoImport("Invoke-WMIMethod win32_process -name create -argumentlist '" + string3 + "' -ComputerName " + string2);
21     }
22 }
23
  
```

Conclusiones

Busquemos formas ágiles y sin fricción

Existen amenazas en las que tenemos que asumir perder ciertas batallas para poder ganar la guerra. El ransomware es un claro ejemplo de esas amenazas.

Debemos asumir que el compromiso inicial siempre va a ocurrir, y que una vez que consigan escalar privilegios va a ser difícil pararles.

Pero podemos hacer más daño en su talón de Aquiles: el descubrimiento y los movimientos laterales.

Si implementamos una política de detección ágil, podemos conseguir detectar estas fases de forma muy sencilla.

Utilicemos nuestros ejercicios de Red Team para simular las actividades de actores de ransomware, y así sabremos dónde podemos infligir más dolor.

Lectura recomendada

Queremos saber más

The DFIR Report: <https://thedfirreport.com/>

Navigating the MAZE: <https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html>

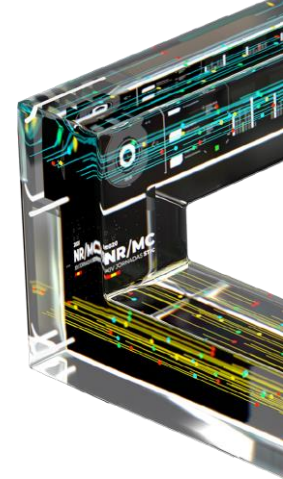
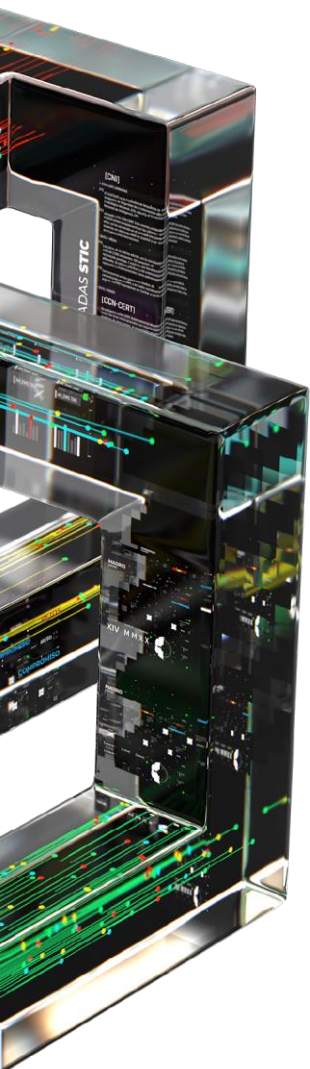
Double Trouble: Ransomware with data leak extortion: <https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/>

Mandiant webcast: <https://twitter.com/likethecoins/status/1321473634330923008>

A Bazar start: how one hospital thwarted a Ryuk ransomware outbreak: <https://redcanary.com/blog/how-one-hospital-thwarted-a-ryuk-ransomware-outbreak/>

A Bazar of Tricks: Following Team9's development cycles: <https://www.cybereason.com/blog/a-bazar-of-tricks-following-team9s-development-cycles>

WastedLocker goes big-game hunting in 2020: <https://blog.talosintelligence.com/2020/07/wastedlocker-emerges.html>



MUCHAS GRACIAS

#XIVJORNADASCCNCERT