Investigación

CBR-Investigación Hive

Referencia del informe:	**CBR-INV02**
Clasificación de la información:	**RESTRINGIDA**

Tabla de contenido

1 Control de versiones

N.º Versión	Fecha	Cambio	Autor
1.0	23/06/2022	Creación	Rosa García López

2 Introducción

Hive (o HiveLeaks), observado por primera vez en 2021, es una variante de ransomware basado en afiliados que usan los ciberdelincuentes para realizar ataques ransomware a centros de salud u hospitales, organizaciones sin fines de lucro, minoristas, proveedores de energía, y otros sectores. Hive está diseñado para que sea distribuido con un modelo de Ransomware-as-a-service (RaaS), esto permite a sus miembros afiliados utilizarlo de la forma que quieran.

Esta variante utiliza tácticas, técnicas y procedimientos (TTPs) comunes de los ransomware para comprometer el dispositivo de la víctima. El operador desactiva las protecciones antivirus y después extrae archivos confidenciales y encripta los archivos comerciales.

Se usan múltiples mecanismos para comprometer las redes de sus víctimas; incluyendo phishing con emails que contienen archivos maliciosos, credenciales de VPN filtradas, y explotando vulnerabilidades que pueda haber. Además, Hive deja un mensaje en el que amenaza con publicar los datos en la página de TOR “HiveLeaks” si la víctima no cumple con las condiciones.

3 Firma de Hive

MD5	7802d6315bf0d45f27bd97fb48e70f8e
SHA1	3f0b80eb4c27e8a39768099c42c242da79cfab60
SHA256	d0ceb8f5170972fe737ab9cbdd6f3ee472fbe62e244cccc46d137094d33f1afc

4 Distribución de TTPs

4.1 Initial Access

El acceso inicial consiste en técnicas que usan varios vectores de entrada para obtener su acceso inicial dentro de la red.

Las técnicas que utiliza, o ha utilizado, Hive de esta táctica son:

- **T1190 – Exploit Public-Facing Application**: Los atacantes pueden intentar acceder al sistema explotando vulnerabilidades o bugs, en cualquier aplicación que tenga sockets

abiertos y accesibles a través de internet. Algunas de las vulnerabilidades que Hive ha explotado son: CVE-2021-34473, CVE-2021-34523 y CVE-2021-31207.

- **T1133 – External Remote Services**: Los servicios remotos abiertos al exterior son el vector de entrada más común y fácil que utilizan los grupos ransomware para ganar el acceso inicial en el sistema. Servicios remotos como VPNs, Windows Remote Management y otros mecanismos de acceso, permiten a los usuarios contectarse a la red interna de la empresa desde una localización externa.
  En varios análisis se ha determinado que Hive es uno de los grupos que utiliza esta táctica.
- **T1566.001 – Phishing: Spearphishing Attachment**: Esta táctica es una variante del *phishing* en la que el malware está adjuntado en un archivo del email y normalmente depende de la ejecución del usuario. Hive ha utilizado técnicas de ingeniería social para hacer que el usuario descargue el archivo malicioso desde Telegram y lo ejecute en su máquina.
- **T1078 – Valid Accounts**: Las credenciales comprometidas pueden ser usadas para evitar los controles de acceso en los sistemas de la red e incluso pueden ser utilizados para mantener el acceso a sistemas remotos. Hive ha usado cuentas de dominio con permisos de administrador para comprometer a más equipos.

4.2 Execution

Consiste en técnicas que resultan en código controlado por el atacante que es ejecutado en un sistema local o remoto.

Las técnicas que utiliza, o ha utilizado, Hive de esta táctica son:

- **T1059.001 – Command and Scripting Interpreter: PowerShell**: PowerShell es una interfaz de línea de comandos incluida en Windows. Hive ha usado PowerShell para descargar y ejecutar scripts de malware y reconocimiento.
- **T1059.003 – Command and Scripting Interpreter: Windows Command Shell**: La interfaz de comandos de Windows (cmd) puede ser usada para controlar casi todos los aspectos del sistema. Hive ha ejecutado comandos utilizando cmd.exe.
- **T1106 – Native API**: Las API nativas proporcionan un medio controlado para llamar a los servicios del sistema operativo de bajo nivel dentro del kernel. Hive las ha utilizado para ejecutar varios comandos o rutinas.
- **T1204.002 – User Execution: Malicious File**: El atacante depende de que el usuario abra un archivo malicioso, esto conllevará la ejecución de código. Como se ha explicado previamente, Hive ha conseguido que las victimas descarguen un archivo y sea ejecutado por el usuario; por ejemplo: “C:\Users\<xxx>\Downloads\Telegram Desktop\wana_setup.zip”.
- **T1047 – Windows Management Instrumentation**: WMI es una herramienta de administración que proporciona un entorno uniforme para acceder los componentes del sistema Windows. Hive ha usado esta característica para ejecutar un archivo .bat que contenía varios comandos para copiar un ejecutable desde el directorio “\\<xxx>\share$\xxx.exe” al directorio %APPDATA% en diferentes sistemas.

4.3 Persistence

Consiste en técnicas usadas por los atacantes para mantener acceso al sistema, aunque este sea reiniciado, cambien las credenciales, o se produzcan otras interrupciones que puedan finalizar su acceso.

Las técnicas que utiliza, o ha utilizado, Hive de esta táctica son:

- **T1098 – Account Manipulation**: La manipulación de cuentas incluye cambiar las contraseñas de cuentas comprometidas, añadir cuentas a grupos con más permisos, modificar las políticas de contraseñas y cualquier acción que preserve el acceso del atacante a la cuenta. Hive ejecuta comandos para crear cuentas y añadirlas al grupo de administradores. Además, también utilizan comandos para descubrir grupos y cuentas.
- **T1197 – BITS Jobs**: Proveen un mecanismo de persistencia al ejecutar payloads. También pueden ser útiles a la hora de evitar ser detectado, pues se ejecutan en segundo plano. Las tareas de transferencia de archivos son implementadas como BITS Jobs. Hive extiende su ransomware utilizando bitsadmin y después ejecutándolo.
- **T1543.003 – Create or Modify System Process: Windows Service**: Consiste en crear o modificar servicios de Windows para ejecutar repetidamente payloads como parte de resistencia, ya que se ejecutan en segundo plano. Hive utiliza el framework CobalStrike, cuyos beacons son instalados como servicios.
- **T1053.005 – Scheduled Task/Job: Scheduled Task**: Los atacantes abusan del programador de tareas de Windows para programar tareas de ejecución inicial o recurrente de código malicioso. Hive registra y ejecuta tareas maliciosas.

4.4 Privilege Escalation

Consiste en técnicas que usan los adversarios para ganar permisos de mayor nivel en un sistema o red.

La técnica que utiliza, o ha utilizado, Hive de esta táctica es:

- **T1068 – Exploitation for Privilege Escalation**: Los atacantes pueden obtener permisos de alto nivel al explotar servidores web de cara al público para el acceso inicial. Hive ha hecho uso de esa explotación para obtener mayores privilegios.

4.5 Defense Evasion

Consiste en técnicas usadas por los atacantes para evitar ser detectados tras comprometer a la víctima.

Las técnicas que utiliza, o ha utilizado, Hive de esta táctica son:

- **T1140 – Deobfuscate/Decode Files or Information**: Los atacantes pueden usar archivos ofuscados o información para esconder los artefactos usados en una intrusión de un análisis. Hive utiliza un truco conocido como “IPfuscation” para esconder la payload.

- **T1562.001 – Impair Defenses: Disable or Modify Tools**: El ransomware deshabilita las características de seguridad para asegurarse de que la ejecución de su muestra y la encriptación de archivos no será bloqueada. Hive ejecuta reg.exe para encargarse de las características de Microsoft Defender.
- **T1070.001 – Indicator Removal on Host: Clear Windows Event Logs**: Los atacantes limpian los logs para ocultar evidencia de su intrusión. Esto hace el trabajo del equipo de respuesta ante incidentes más difícil. Hive hace uso de una utilidad muy popular, "wevutil", para esto.
- **T1070.004 – Indicator Removal on Host: File Deletion**: Los atacantes borran los archivos que se hayan podido crear por causa de su intrusión para no dejar rastro. Hive, como muchos ransomware, se borra a sí mismo para dificultar la obtención de la muestra.
- **T1036 – Masquerading**: Los atacantes intentan manipular las características de sus herramientas para hacerlas parecer legítimas o benignas. Hive crea un servicio con un nombre determinado para parecer el binario normal de Windows "explorer.exe":

```
$windir\$system32\cmd.exe /k C:\Windows\inf\usbhub\explorer.exe -f
C:\Windows\inf\usbhub\config.log
```

- **T1055 – Process Injection**: Los atacantes inyectan código en procesos siendo ejecutados con el fin de evadir las defensas basadas en procesos, y también para elevar privilegios.
- **T1218 – System Binary Proxy Execution**: Los atacantes pueden sobrepasar las defensas basadas en procesos y/o firmas mediante la delegación de ejecución de su contenido malicioso en archivos binarios firmados o confiables.

4.6 Credential Access

Consiste en técnicas para robar credenciales como nombres de cuentas y contraseñas.

Las técnicas que utiliza, o ha utilizado, Hive de esta táctica son:

- **T1110 – Brute Force**: Los atacantes pueden usar técnicas de fuerza bruta para obtener acceso a cuentas cuando no conocen la contraseña o han obtenido los hashes de las contraseñas.
- **T1003.001 - OS Credential Dumping: LSASS Memory**: Los atacantes intentan acceder a material con credenciales guardado en el proceso de memoria del Local Security Authority Subsystem Service (LSASS). En un incidente de Hive, se ha observado como configura la Registry Key para forzar al sistema a almacenar las contraseñas, en texto plano, en memoria.

4.6.1 Discovery

Consiste en técnicas que permiten al atacante obtener conocimiento sobre nuestro sistema y red interna.

Las técnicas que utiliza, o ha utilizado, Hive de esta táctica son:

- **T1087 – Account Discovery**: Los atacantes tratan de obtener un listado de cuentas en un sistema o entorno. Un comando comúnmente usado es:

```
whoami /groups
```

- **T1083 – File and Directory Discovery**: Se trata de una técnica que implica enumerar archivos y directorios para determinar si ciertos objetos deberían ser encriptados/robados o no. Los troyanos de ransomware generalmente hacen una búsqueda automática de archivos con determinadas extensiones o nombres.
- **T1135 - Network Share Discovery**: Con el objetivo de encriptar máquinas cercanas y tener más víctimas, los atacantes buscan carpetas y discos compartidos en sistemas remotos.
- **T1057 – Process Discovery**: Hive hace uso de métodos que enumeran procesos activos para formar los siguientes pasos del ataque.
- **T1018 – Remote System Discovery**: Consiste en enumerar los dispositivos remotos que pertenecen a la red comprometida. Algunos de los comandos usados son:

```
>> net view /all
>> net view /all /domain
>> dsquery subnet -limit 0
>> nltest /domain _ trusts
>> nltest /dclist
```

- **T1049 – System Network Connections Discovery**: Para ganar acceso al sistema, los atacantes normalmente buscan conexiones activas en el sistema en las que se puedan mover y encriptar. Típicamente usan los comandos:

```
>> net sesión
>> net use
>> netstat -ano
>> query session
```

4.7 Lateral Movement

Consiste en técnicas que utilizan los atacantes para entrar y controlar sistemas remotos en una red.

Las técnicas que utiliza, o ha utilizado, Hive de esta táctica son:

- **T1570 – Lateral Tool Transfer**: Hive hace uso de RDP para propagar el ransomware o las herramientas usadas, dentro de la red. Se les ha visto utilizar bitsadmin con el comando:

```
Bitsadmin /transfer debjob /download
\\[localuser]\C$\Windows\[Hive].dll C:\Windows\[hive].dll
```

- **T1021.001 – Remote Services: Remote Desktop Protocol**: Tras acceder al sistema, el grupo puede continuar moviéndose en la red con el uso de conexiones de escritorio remoto.
- **T1021.002 – Remote Services: SMB/Windows Admin Shares**: Hive usa RDP para transferir y ejecutar las payloads del ransomware y otras herramientas. Utilizan un script, COPY.bat, que copia el troyano xxx.exe desde la carpeta share$ al directorio C:\windows\temp\ en diferentes sistemas de la red.
- **T1021.006 – Remote Services: Windows Remote Management**: Se utiliza WMI para ejecutar y desplegar scripts y payloads del ransomware.

4.8 Collection

Consiste en técnicas para recolectar información y las fuentes de las que se recoge esa información que son relevantes para que los atacantes lleven sus objetivos a cabo.

Las técnicas que utiliza, o ha utilizado, Hive de esta táctica son:

- **T1560.001 – Archive Collected Data: Archive via Utility**: Hive utiliza una herramienta para comprimir la información robada y, posteriormente, exfiltrarla.
- **T1005 – Data from local system**: Busca en el sistema local información o archivos de interés, como bases de datos e información confidencial.

4.9 Command and Control

Consiste en técnicas que usan los atacantes para comunicarse con sistemas bajo su control dentro de la red de la víctima.

La técnica que utiliza, o ha utilizado, Hive de esta táctica son:

- **T1071.001 - Application Layer Protocol: Web Protocols**: Hive utiliza el malware RedLine Stealer para comunicarse con el servidor C2. Dependiendo de la versión de este malware puede usar HTTP+ SOAP, .NET Binary Format SOAP o JSON. Puede descargar y ejecutar archivos, ejecutar comandos con cmd.exe o abrir links en un navegador.

4.10 Exfiltration

Consiste en técnicas cuya finalidad es robar datos de tu red.

Las técnicas que utiliza, o ha utilizado, Hive de esta táctica son:

- **T1041 – Exfiltration Over C2 Channel**: Mencionado anteriormente, RedLine; usado por Hive, es capaz de buscar por datos específicos en el sistema como contraseñas, cookies, tarjetas de crédito, credenciales en plataformas de juego, etc. Tras encontrar archivos interesantes se mandan al servidor C&C a través del canal de comunicación.
- **T1567.002 – Exfiltration Over Web Service: Exfiltration to Cloud Storage**: Exfiltrar datos a un servidor en la nube puede verse como algo legítimo, por lo que es una ventaja para los atacantes. Hive utiliza MegaSync para ello.

4.11 Impact

Consiste en técnicas que alteran la disponibilidad o comprometan la integridad mediante la manipulación de los procesos comerciales y operacionales.

Las técnicas que utiliza, o ha utilizado, Hive de esta táctica son:

- **T1486 – Data encrypted for impact**: Hive encripta los archivos de su víctima con una llave generada aleatoriamente. Posteriormente, esa llave también será encriptada con RSA.
- **T1490 – Inhibit System Recovery**: En esta técnica los atacantes hacen todo lo posible para que no se pueda recuperar la información si no es negociando con ellos. Para conseguirlo, eliminan copias de seguridad, las copias shadow y desactivan las características de reparación y recuperación automáticas.
- **T1489 – Service Stop**: Hive ha sido observado parando servicios con "sc.exe". Estos comandos se pueden ver más adelante.

5 Versión 5 de Hive

5.1 Cambio del lenguaje de programación

Recientemente, Hive ha cambiado su lenguaje de programación de Go a Rust. Uno de los motivos puede haber sido la creación de una herramienta capaz de desencriptar los archivos de versiones anteriores. Con este cambio han mejorado su encriptación y se beneficia de las siguientes ventajas de Rust:

- Ofrece seguridad en la memoria, tipo de datos e hilo.
- Tiene un control profundo de los recursos de bajo nivel.
- Tiene una sintaxis amigable para el usuario.
- Consta de varios mecanismos para concurrencia y paralelismo, por lo que permite la encriptación de archivos rápida y segura.
- Tiene una buena variedad de librerías criptográficas.
- Es relativamente más difícil de hacer ingeniería inversa.

Además de mejorar la encriptación de archivos, también encripta las cadenas. Estas cadenas residen en la sección *.rdata* y son desencriptadas durante su ejecución por *XORing* con constantes. Las constantes usadas para desencriptar a veces cambian entre las muestras, por lo que no son una base fiable para la detección.

5.2 Parámetros en la línea de comando

En variantes antiguas, el usuario y la contraseña con los que acceder a su página web para pagar están insertados en la muestra. En la nueva variante, estas credenciales deben ser escritas a través de la línea de comando con el parámetro *"-u"*, lo que significa que no se podrán obtener por los analistas de la muestra.

Los parámetros encontrados en la nueva variante son los siguientes:

Parámetro	Funcionalidad
-no-local	No encriptar los archivos locales
-no-mounted	No encriptar los archivos en recursos compartidos de red montados
-no-discovery	No descubrir recursos compartidos de red
-local-only	Encriptar solo los archivos locales
-network-only	Encriptar solo archivos en recursos compartidos de red
-explicit-only	Encriptar carpeta/s específicas. Ej.: *"-explicit-only c:\mydocs c:\myphotos"*
-min-size	Tamaño mínimo del archivo, en bytes, para encriptar. Ej.: *'-min-size 102400'* encriptará archivos con un tamaño igual o mayor a 100kb
-da	[Su uso está siendo analizado]
-f	[Su uso está siendo analizado]
-force	[Su uso está siendo analizado]
-wmi	[Su uso está siendo analizado]

Por lo general, parece que versiones diferentes tienen parámetros distintos que están siendo actualizados constantemente. A diferencia de variantes previas donde había un menú de ayuda (*help*), en la nueva variante el atacante debe saber los parámetros de antemano porque no existe este menú. Esto dificulta a los investigadores encontrar los parámetros.

5.3 Encriptación

5.3.1 Enfoque único

La nueva variante utiliza un enfoque único para encriptar los archivos. En vez de incrustar una llave encriptada en cada archivo, genera dos sets de llaves en memoria, las utiliza para encriptar archivos, y después encripta y escribe los sets en el directorio raíz del disco que ha encriptado; ambas tienen la extensión *.key*.

Por ejemplo, si tenemos los siguientes archivos soltados en el directorio *C:*: "*C:\4lk56Oyf.key*" y "*C:\jFn4dO03.key*"; un archivo llamado "example.txt" sería renombrado a "C:\example.txt. jFn4dO03_ -B82BhIaGhI8".

5.3.2 Generación del set de llaves

La siguiente ilustración muestra el esquema de encriptación:

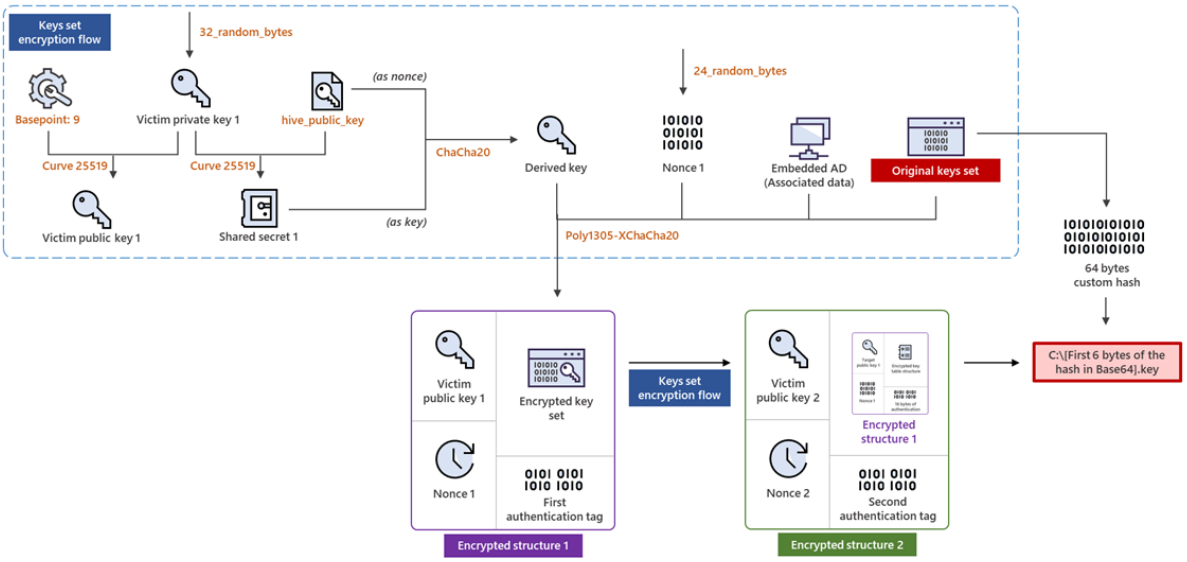

Ilustración 1 - Diagrama de encriptación del set de llaves

Como se puede observar en el diagrama, el "Keys set encryption Flow" se ejecuta dos veces. En la primera ejecución se realiza con el set de llaves originales como entrada. En la segunda, se ejecuta con la "encrypted estructure 1" como entrada. En su segunda ejecución, todos los demás valores introducidos son diferentes exceptuando los AD (datos asociados) y el Basepoint 9.

5.3.3 Encriptación de archivos

Después de que las dos llaves sean escritas en el disco, la encriptación de archivos multihilo comienza. Antes de encriptar cada archivo, Hive comprueba su nombre y extensión contra una lista de strings. Si hay una coincidencia, ese archivo no será encriptado. Esta lista de strings (como todas las demás strings) es encriptada y desencriptada cada vez que ocurre este proceso.

El método de encriptación para los archivos es el mismo que el que usan versiones anteriores del malware: dos números aleatorios son generados y usados como offset para el set de llaves.

Una vez terminado este proceso, el ransomware muestra un documento con nombre "_HOW_TO_DECRYPT.txt" para informar al usuario de que ha sido infectado.

6 Herramientas y exploits usados

En esta tabla se recogen las herramientas, métodos o exploits utilizados, clasificados en base a la táctica de la matriz del MITRE, que Hive ha usado.

Initial Access	Execution	Discovery	Lateral Movement	Defense Evasion	Exfiltration
Phishing emails with malicious attachments	• PsExec • WMI • Cobalt Strike	• TrojanSpy.DATASPY • SoftPerfect	• PSExec • RDP • BitsAdmin • WMI	• PCHunter • GMER • KillAV	• 7-Zip • MEGASync • uFile.io • SendSpace • AnonFiles

7 Desencriptación y limpieza

Puesto que este grupo ransomware no presenta técnicas de persistencia, podríamos utilizar herramientas que nos den la posibilidad de recuperar nuestros datos. En este informe se describen dos versiones de Hive: la versión 5, que es la más reciente y programada en Rust, y la versión 4, última versión de Hive escrita en Go.

Para la versión 5 se ha publicado recientemente una herramienta que posibilita la desencriptación de set de llaves generado por Hive, y consecuentemente la recuperación de los datos. Esta herramienta tendrá que ser adaptada por cada usuario para que funcione, se explica qué hacer en el enlace que lleva al repositorio oficial.

En la versión 4, nos encontramos con una herramienta desarrollada por investigadores de Corea del Sur que funciona desde la versión 1 hasta la 4 de Hive. Tras las pruebas realizadas se concluyó que llegan a desencriptar el 98% de los archivos.

Para asegurarnos de que no hay rastro de ransomware en el sistema, se recomienda utilizar un escáner o antivirus que se considere fiable. Algunos ejemplos son: Avast Free Antivirus, Avast Premium Tech Support, Kaspersky Anti-Ransomware, etc. También existe una página que es capaz de identificar el ransomware al aportar archivos cifrados y la nota que dejan los atacantes; Crypto Sheriff.

8 Mitigación

La mejor forma de responder ante el ataque del ransomware es aislar el dispositivo infectado de la red/VLAN existente en la entidad atacada, así se evita la expansión hacia otros dispositivos y se limita el impacto causado.

Esto podría causar una interrupción en los servicios que ofrece la entidad al tener que apagar o reiniciar los dispositivos infectados; sin embargo, nos permite contener el ataque y con ello facilitar la recuperación.

9 IOC's

9.1 Servicios que para

windefend, msmpsvc, kavsvc, antivirservice, zhudongfungyu, vmm, vmwp, sql, sap, oracle, mepocs, veeam, backup, vss, msexchange, mysql, sophos, pdfservice, backupexec, gxblr, gxvss, gxclmgrs, gxvcd, gxcimgr, gxmmm, gxvsshwprov, gxfwd, sap, qbcfmonitorservice, qbidpservice, acronisagent, mvarmor, acrsch2svc.

9.2 Procesos que para

dbsnmp, dbeng50, bedbh, excel, encsvc, visios, firefox, isqlplussvc, mspub, mydesktopqos, notepad, ocautoupds, ocomm, ocssd, onenote, outlook, sqbcoreservice, sql, steam, tbirdconfig, thunderbird, winword, wordpad, xfssvccon, vxmon, benetns, bengien, pvlsvr, raw_agent_svc, cagservice, sap, qbidpservice, qbcfmonitorservice, teamviewer_service, teamviewer, tv_w32, tv_x64, cvd, saphostexec, sapstartsrv, avscc, dellsystemdetect, enterpriseclient, veeam, thebat, cvfwd, cvods, vsnapvss, msaccess, vaultsvc, beserver, appinfo, qbdmgrn, avagent, spooler, powerpnt, cvmountd, synctime, oracle, wscsvc, winmgmt, sql.

9.3 Procesos lanzados

Como parte de su actividad ransomware, Hive normalmente ejecuta procesos que borran copias de seguridad y previenen su recuperación. Existen diferencias entre las versiones, y algunas muestras no tienen por que ejecutar todos estos procesos, pero una muestra que lanza la mayoría de los procesos es:

SHA-256: 481dc99903aa270d286f559b17194b1a25deca8a64a5ec4f13a066637900221e

Los procesos son los siguientes:

- *“vssadmin.exe delete shadows /all /quiet”*
- *“wmic.exe shadowcopy delete”*
- *“wbadmin.exe delete systemstatebackup”*
- *“wbadmin.exe delete catalog -quiet”*
- *“bcdedit.exe /set {default} recoveryenabled No”*
- *“bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures”*

- *“wbadmin.exe delete systemstatebackup -keepVersions:3”*

9.4 IP's maliciosas

- 139.60.161.228
- 139.60.161.56
- 91.208.52.149
- 185.70.184.8
- 176.123.8.228
- 41.184.8.181
- 46.166.161.93
- 93.115.27.71
- 192.53.123.202
- 23.215.176.152
- 13.107.4.50

9.5 Comandos ejecutados

Comando
vssadmin.exe delete shadows /all /quiet
wevtutil.exe cl security
wevtutil.exe cl system
wevtutil.exe cl application
wmic.exe SHADOWCOPY /nointeractive
wmic.exe shadowcopy delete
bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
bcdedit.exe /set {default} recoveryenabled no
net.exe stop "NetMsmqActivator" /y
C:\Windows\system32\net1 stop "NetMsmqActivator" /y
net.exe stop "SamSs" /y
C:\Windows\system32\net1 stop "SamSs" /y

net.exe stop "SDRSVC" /y
C:\Windows\system32\net1 stop "SDRSVC" /y
net.exe stop "SstpSvc" /y
C:\Windows\system32\net1 stop "SstpSvc" /y
net.exe stop "UI0Detect" /y
C:\Windows\system32\net1 stop "UI0Detect" /y
net.exe stop "VSS" /y
C:\Windows\system32\net1 stop "VSS" /y
net.exe stop "wbengine" /y
C:\Windows\system32\net1 stop "wbengine" /y
net.exe stop "WebClient" /y
C:\Windows\system32\net1 stop "WebClient" /y
sc.exe config "NetMsmqActivator" start= disabled
sc.exe config "SamSs" start= disabled
sc.exe config "SDRSVC" start= disabled
sc.exe config "SstpSvc" start= disabled
sc.exe config "UI0Detect" start= disabled
sc.exe config "VSS" start= disabled

sc.exe config "wbengine" start= disabled
sc.exe config "WebClient" start= disabled
reg.exe add "HKLM\System\CurrentControlSet\Services\SecurityHealthService" /v "Start" /t REG_DWORD /d "4" /f
reg.exe delete "HKLM\Software\Policies\Microsoft\Windows Defender" /f
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender" /v "DisableAntiSpyware" /t REG_DWORD /d "1" /f
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender" /v "DisableAntiVirus" /t REG_DWORD /d "1" /f
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\MpEngine" /v "MpEnablePus" /t REG_DWORD /d "0" /f
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableBehaviorMonitoring" /t REG_DWORD /d "1" /f
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableIOAVProtection" /t REG_DWORD /d "1" /f
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableOnAccessProtection" /t REG_DWORD /d "1" /f
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableRealtimeMonitoring" /t REG_DWORD /d "1" /f
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableScanOnRealtimeEnable" /t REG_DWORD /d "1" /f
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Reporting" /v "DisableEnhancedNotifications" /t REG_DWORD /d "1" /f
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v "DisableBlockAtFirstSeen" /t REG_DWORD /d "1" /f
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v "SpynetReporting" /t REG_DWORD /d "0" /f

reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v "SubmitSamplesConsent" /t REG_DWORD /d "0" /f
reg.exe add "HKLM\System\CurrentControlSet\Control\WMI\Autologger\DefenderApiLogger" /v "Start" /t REG_DWORD /d "0" /f
reg.exe add "HKLM\System\CurrentControlSet\Control\WMI\Autologger\DefenderAuditLogger" /v "Start" /t REG_DWORD /d "0" /f
schtasks.exe /Change /TN "Microsoft\Windows\ExploitGuard\ExploitGuard MDM policy Refresh" /Disable
schtasks.exe /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Cache Maintenance" /Disable
schtasks.exe /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Cleanup" /Disable
schtasks.exe /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Scheduled Scan" /Disable
schtasks.exe /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Verification" /Disable
reg.exe delete "HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run" /v "Windows Defender" /f
reg.exe delete "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v "Windows Defender" /f
reg.exe delete "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /v "WindowsDefender" /f
reg.exe delete "HKCR*\shellex\ContextMenuHandlers\EPP" /f
reg.exe delete "HKCR\Directory\shellex\ContextMenuHandlers\EPP" /f
reg.exe delete "HKCR\Drive\shellex\ContextMenuHandlers\EPP" /f

reg.exe add "HKLM\System\CurrentControlSet\Services\WdBoot" /v "Start" /t REG_DWORD /d "4" /f
reg.exe add "HKLM\System\CurrentControlSet\Services\WdFilter" /v "Start" /t REG_DWORD /d "4" /f
reg.exe add "HKLM\System\CurrentControlSet\Services\WdNisDrv" /v "Start" /t REG_DWORD /d "4" /f
reg.exe add "HKLM\System\CurrentControlSet\Services\WdNisSvc" /v "Start" /t REG_DWORD /d "4" /f
reg.exe add "HKLM\System\CurrentControlSet\Services\WinDefend" /v "Start" /t REG_DWORD /d "4" /f
reg.exe add "HKLM\System\CurrentControlSet\Services\SecurityHealthService" /v "Start" /t REG_DWORD /d "4" /f
cmd.exe /c "C:\Program Files\Windows Defender\MpCmdRun.exe" -RemoveDefinitions -All
"C:\Program Files\Windows Defender\MpCmdRun.exe" -RemoveDefinitions -All
cmd.exe /c powershell Set-MpPreference -DisableIOAVProtection $true
powershell Set-MpPreference -DisableIOAVProtection $true
cmd.exe /c powershell Set-MpPreference -DisableRealtimeMonitoring $true
powershell Set-MpPreference -DisableRealtimeMonitoring $true

9.6 Archivos maliciosos

Nombre del archivo	MD5	SHA1
Windows.exe		
Mimikatz.exe	6c9ad4e67032301a61a9897377d9cff8	655979d56e874fbe7561bb1b6e512316c25cbb19
advanced_port_scanner_2.5.3869.exe	6a58b52b184715583cda792b56a0a1ed	3477a173e2c1005a81d042802ab0f22cc12a4d55

advanced port scanner.exe	4fdabe571b66ceec3448939bfb3ffcd1	763499b37aacd317e7d2f512872f9ed719aacae1
scan.exe	bb7c575e798ff5243b5014777253635d	2146f04728fe93c393a74331b76799ea8fe0269f
p.bat	5e1575c221f8826ce55ac2696cf1cf0b	ecf794599c5a813f31f0468aecd5662c5029b5c4
shadow.bat	3f14de33882f80fa59622f5c3320bfa2	c00395a13f501e784a3eb73ae684ce2417a95712
hive.bat		
Webshell #1	d46104947d8478030e8bcfcc74f2aef7	d1ef9f484f10d12345c41d6b9fca8ee0efa29b60
Webshell #2	2401f681b4722965f82a3d8199a134ed	2aee699780f06857bb0fb9c0f73e33d1ac87a385
main_template.docx		33094acd614825a916b77df6c5141c088fc3768b
vspub1.dll	edbe98468cd888bf029bc8e297a310b3	bf0f7abda2228059bb00ec9658ee447fbe84d277
vspub2.dll	994104c30d57141a99e0e414ef2d8837	d40510da42a478d72e649993208710668a7f6c27
xrjkrobuy.dll		14f52ae68344e1643b3066c10f7044fdd819db4e
upywloeza.dll	ab9103c8fd35ec7b5a99e463a2f8fc59	0cc7cca16afd632857e3883c06b2f55c057b563e
dtzvlbtxn.dll	61b94dfc9bea1a876b140a72c450e4bb	d36e983886a084887f887c6d562d3bc0664587c4
lvgoywrnxwy.dll	cd1096991867bb5ad72b983441bfe04b	fea7d944e317c7b2ef1aba57600a8c5310368085
qcuqqgxmy.dll	e14d7460f62a122d85a2ce1b69080497	35423e04e58ab1f2267e19c47e1c69ea5b7041cc
pdxqzmftr.dll	0fdb43fc559a35afcc422b786f45a997	fd9620c0c295caaee3096423532bb1dbfb7064c5
lowpro3.13.exe	bc59fa5dbb11f5d286fc41e8f25c6cc0	cb0b39534d99057b02b090c3650fb1de43d19a02

wsus.exe	888fa9c56b06cf6255142e2c592b2437	caff1d315a5d87014e5fa62346f58407755d971e
FakeL.exe	945fff5b2d903ccc0787f41a9ba6df98	45c43ec18d15ba7850e6ad2e2e54671636f4d926

Nombre del archivo	Sha256	Nombre de detección
psexec	fd3e7d0f6a31b821604707ef99da281e4fd7d11c7804e46eeed11f66b200a391	
7zip.exe	321d0c4f1bbb44c53cd02186107a18b7a44c840a9a5f0a78bdac06868136b72c	Ransom.Win64.GOHIVE.YEBIF
ac.exe	be1565961e123f52e54e350e0ca2666f8ffa42fdc46df18dca6f7c0ac2b43d23	Ransom.Win64.HIVE.YMBJG
%SYSTEMROOT%\winlo.exe	3ec89b737c5b91eb9da0a2d9c6c1f0e637087b4552e26806d959c11f8f06e96f	Ransom.Win64.HIVE.A
	1e21c8e27a97de1796ca47a9613477cf7aec335a783469c5ca3a09d4f07db0ff	Ransom.Win64.GOHIVE.SMJMA
	c04509c1b80c129a7486119436c9ada5b0505358e97c1508b2cfb5c2a177ed11	Ransom.Win64.GOHIVE.SMJMA
	88f7544a29a2ceb175a135d9fa221cbfd3e8c71f32dd6b09399717f85ea9afd1	Ransom.Win64.GOHIVE.SMJMA
	a0b4e3d7e4cd20d25ad2f92be954b95eea44f8f1944118a3194295c5677db749	Ransom.Win64.GOHIVE.SMJMA
	77a398c870ad4904d06d455c9249e7864ac92dda877e288e5718b3c8d9fc6618	Ransom.Win32.HIVE.THFCOBA
	612e5ffd09ca30ca9488d802594efb5d41c360f7a439df4ae09b14bce45575ec	Ransom.Win64.GOHIVE.SMJMA
	a290ce75c6c6b37af077b72dc9c2c347a2eede4fafa6551387fa8469539409c7	TrojanSpy.PS1.DATASPY.B
	977b2ce598bd6518913fe216d1139c041e159a6510cd71a6a14a49570c1019be	TrojanSpy.PS1.DATASPY.A
gmer.exe	e8a3e804a96c716a3e9b69195db6ffb0d33e2433af871e4d4e1eab3097237173	PUA.Win32.GMER.YABBI

Bk74AE.tmp/PCHunter64.exe	d1aa0ceb01cca76a88f9ee0c5817d24e7a15ad40768430373ae3009a619e2691	PUA.Win64.PCHunter.B
c:\Users\Public\Music\lapress_32.exe	8f3c5f9cd657e3785d751305023cf83a7f27780d5441817614d442e28dbe3ac4	Ransom.Win64.HIVE.A
%SYSTEMROOT%\Temp\xxx.exe	c367ab50c1f103963da0f0404eeda46c9e768711797d638afa1c4cf740575613	Ransom.Win64.HIVE.YABIW
791251-1632642588.exe	fdbc66ebe7af710e15946e1541e2e81ddfd62aa3b35339288a9a244fb56a74cf	Ransom.Win64.GOHIVE.SMJMA
	ed614cba30f26f90815c28e189340843fab0fe7ebe71bb9b4a3cb7c78ff8e3d2	Ransom.Win64.GOHIVE.SMJMA
	5954558d43884da2c7902ddf89c0cf7cd5bf162d6feefe5ce7d15b16767a27e5	Ransom.Win64.GOHIVE.SMJMA
	e514be3e997895c7e3ece03549c8cb6b5700fe8f814948ed201ca59daa8733fb	Ransom.Linux.HIVE.C
C:\ProgramData\nds.dll/nds.dll	7b7f13ab85bc78849e04a5589c84f0ec1847460106c03ca3db84703c7af054f3	Ransom.Win32.HIVE.YXBJR
	bdf3d5f4f1b7c90dfc526340e917da9e188f04238e772049b2a97b4f88f711e3	Ransom.Linux.HIVE.A
	6983ef6e484c0c70356d6f868ac03bc90a1055560642706743511f76aa6f28ad	Ransom.Linux.HIVE.B
linux	6a0449a0b92dc1b17da219492487de824e86a25284f21e6e3af056fe3f4c4ec0	Ransom.Linux.HIVE.A
xxx.000	5d95bf2518918422a6cac03f90548f02a5848dbc43836868636b61d0a87ed968	Ransom.Win64.HIVE.YXBKC
windows.exe	47006ed84afb1f1fd761b81f3ae7b6547c0cb4845538301035e1388693fc6f7f	Ransom.Win64.HIVE.YABLG
mmm.exe"	25793a0764a51b38806b7dcf5f5d8df9620f090f72362aa03187c8813e054482	Ransom.Win64.HIVE.VSNW01L21
	7b7f13ab85bc78849e04a5589c84f0ec1847460106c03ca3db84703c7af054f3	Ransom.Win32.HIVE.SMYXBJR.hp
xxx.000	d64f9742539436acba5ff9c4f1c8ca501cad86dfa823828b65418b493c8109ac	Ransom.Win64.HIVE.YXCACZ
	bd6d8f7c9e016dd7395ee7f0f8485de622a9b034b7c5d2e1af25cb762dd8d8c9	Ransom.Win64.HIVE.YXBKFZ

	0e8e6fc94e6eb17cfd8993b3dcfd9acd11ee32f1b4e956df3097ae3259be4f9c	Ransom.Win64.HIVE.YXBKFZ
	875708f911752bef7e2ef0658d395ebeccef774d5fdb74f6e9ee60b52d86cbf0	Ransom.Win64.HIVE.YXBKFZ
"zzz.exe	5b32ac4754bd5728cc7a68f341bf64cec4a737eb584814bb2099a5f2ff69e584	Ransom.Win32.HIVE.YXBKV
	baa7a6e5a093ee6be47eca86e5acbcba196c7d1d35662eecad23ec870702116a	Ransom.Win32.HIVE.YXBKV
xxx.exe	a2ad0442cebe3e6abb86069a3b66b471b4a7c9d00286da4b8114d17a849128d6	Ransom.Win64.HIVE.YEBJM
xxx.exe	5d1db413bbb7540633fef0e40a0a8fbb2e1c309623d80503b07eec0f5b5d5a57	
main.py	6bd3adc7e43e20ede1a82ad1469cc7ecd085b324621edbd4ec23db4e4473895f	Trojan.Python.KILLAV.YPCBO
	50ad0e6e9dc72d10579c20bb436f09eeaa7bfdbcb5747a2590af667823e85609	
	cf80ffac9ddb379e041834b06c07fc99f8885948fbc6d5c0c5ee79680e2bbe0e	
	e1a7ddbf735d5c1cb9097d7614840c00e5c4d5107fa687c0ab2a2ec8948ef84e	
	b1bfc90de9dcea999dedf285c3d3d7e1901847d84ec297224a0d82720d0ed501	
	67ab2abe18b060275763e1d0c73d27c1e61b69097232ed9d048d41760a4533ef	
	d158f9d53e7c37eadd3b5cc1b82d095f61484e47eda2c36d9d35f31c0b4d3ff8	
	d2c217e9f3bc93d5f428524e80d0ef89a0b5b1f84add890ff7dc287ea460950b	

10 Matriz del MITRE ATT&CK pintada

about

Hive

Capa con las tácticas y técnicas que usa el ransomware Hive.

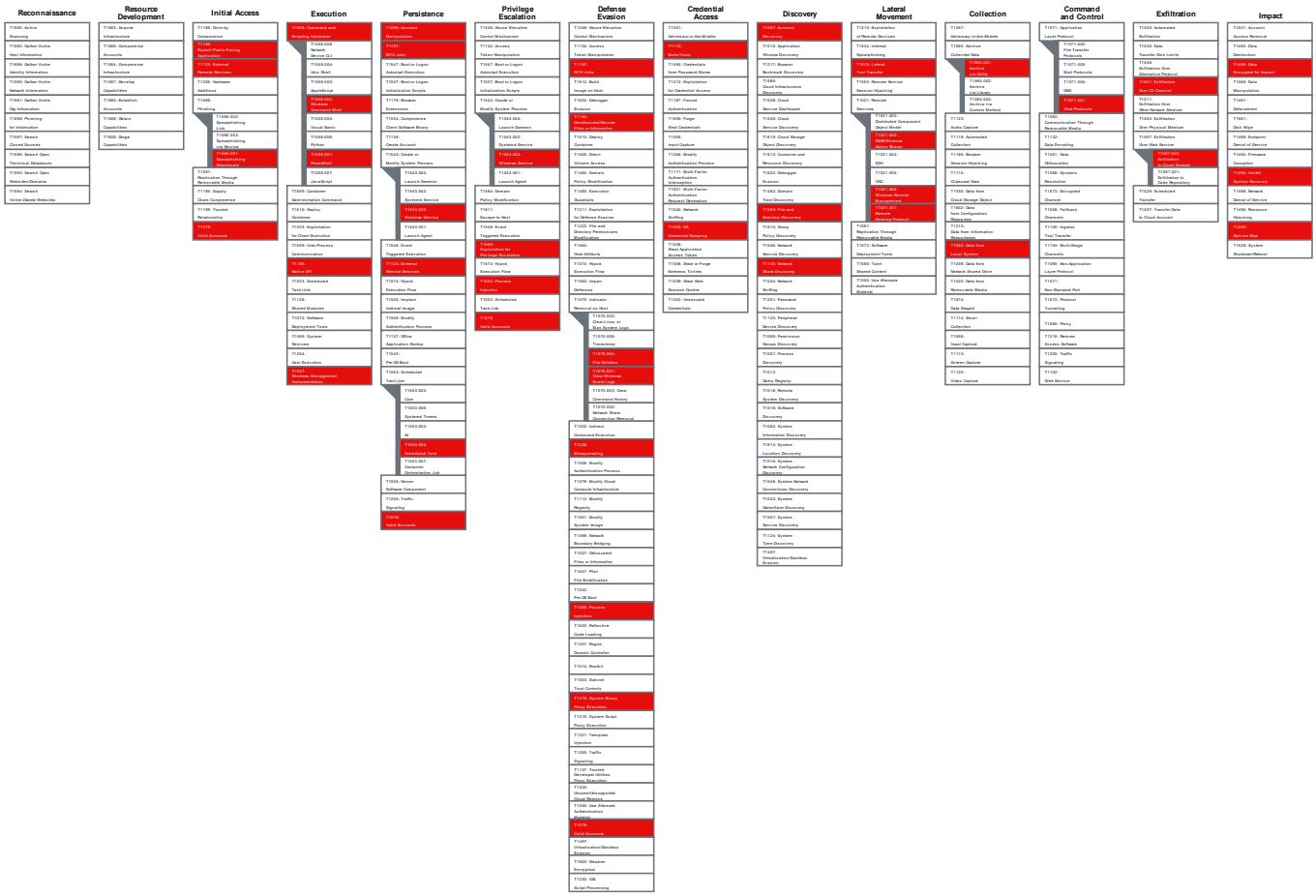

Ilustración 2 - Matriz pintada con los TTPs de Hive

11 Reglas YARA

```
import "pe"
rule Mal_Ransom_Hive_2021_unpacked
{
meta:
description = "Detects unpacked Hive ransomware"
author = "Blackberry Threat Research team"
```

```
date = "2021-06-07"

strings:

//google.com/encryptor.(*App).KillProcesses

$h =
{676f6f676c652e636f6d2f656e63727970746f722e282a417070292e4b696c6c50726f
636573736573}

//google.com/encryptor.(*App).StopServices

$h1 =
{676f6f676c652e636f6d2f656e63727970746f722e282a417070292e53746f70536572
7669636573}

//google.com/encryptor.(*App).RemoveShadowCopies

$h2 =
{676f6f676c652e636f6d2f656e63727970746f722e282a417070292e52656d6f766553
6861646f77436f70696573}

//google.com/encryptor.(*App).EncryptFiles

$h3 =
{676f6f676c652e636f6d2f656e63727970746f722e282a417070292e456e6372797074
46696c6573}

//google.com/encryptor.(*App).encryptFilesGroup

$h4 =
{676f6f676c652e636f6d2f656e63727970746f722e282a417070292e656e6372797074
46696c657347726f7570}

//google.com/encryptor.(*App).ScanFiles

$h5 =
{676f6f676c652e636f6d2f656e63727970746f722e282a417070292e5363616e46696c
6573}

//google.com/encryptor.(*App).EraseKey

$h6 =
{676f6f676c652e636f6d2f656e63727970746f722e282a417070292e45726173654b65
79}

//google.com/encryptor.(*App).RemoveItself

$h7 =
{676f6f676c652e636f6d2f656e63727970746f722e282a417070292e52656d6f766549
7473656c66}

//http://hivecust6vhekztbqgdnkks64ucehqacge3dij3gyrrpdp57zoq3ooqd.onion
/

$h8 =
{687474703a2f2f686976656375737436766865 6b7a74627167646e6b6b733634756365
687161636765336469 6a336779727270647035377a6f71336f6f71642e6f6e696f6e2f}
```

```
//http://hiveleakdbtnp76ulyhi52eag6c6tyc3xw7ez7iqy6wc34gd2nekazyd.onion
/
$h9 =
{687474703a2f2f686976656c65616b6462746e703736756c7968693532656167366336
747963337873765 7a3769717936776333346764326e656b617a79642e6f6e696f6e2f}
condition:
uint  16(0) == 0x5a4d and
all of ($h*)
}
```

```
rule Win32_Ransomware_Hive
{
meta:
description = "Detects unpacked 32-bit Hive Ransomware"
author = "Netskope Threat Labs"
strings:
$go = "GO build" nocase
$str00 = "EncryptFile"
$str01 = "EncryptFiles"
$str02 = "EraseKey"
$str03 = "ExportKey"
$str04 = "KillProcess"
$str05 = "Notify"
$str06 = "PreNotify"
$str07 = "RemoveItself"
$str08 = "RemoveShadowCopies"
$str09 = "ScanFiles"
$str10 = "StopServices"
condition:
uint16(0) == 0x5a4d
and $go and 8 of ($str*)
}
```

```
rule HiveRansomware
{
meta:
description = "Hive Ransomware code pattern"
strings:
$str_80 = {49 3B 66 10}
$str_8a = {48 83 EC 30 48 89 6C 24 28 48 8D 6C 24 28 44 0F 11 7C 24 18
66 90 48 85 C9}
$str_a9 = {48 83 F9 01}
$str_af = {48 89 5C 24 40 48 85 C0}
$str_b9 = {48 83 F9 20}
$str_bf = {48 89 4C 24 48 48 89 C8 31 DB 31 C9 ?? ?? ?? ?? ?? 48 8B 4C
24 48 48 8B 5C 24 40}
$str_da = {48 89 44 24 18 48 89 4C 24 20 ?? ?? ?? ?? ?? 48 8B 5C 24 20
48 8B 44 24 18 48 8B 6C 24 28 48 83 C4 30 C3}
$str_fd = {0F B6 0B 48 8D 15 39 0C 31 00 48 8D 0C CA 48 89 4C 24 18 48
C7 44 24 20 01 00 00 00 48 8B 44 24 18 BB 01 00 00 00 48 8B 6C 24 28 48
83 C4 30 C3}
$str_2d = {44 0F 11 7C 24 18 31 C0 31 DB 48 8B 6C 24 28 48 83 C4 30 C3}
$str_41 = {48 89 44 24 08 48 89 5C 24 10 48 89 4C 24 18 ?? ?? ?? ?? ??}
condition:
all of them
}
```

12 Referencias

https://mitre-attack.github.io/attack-navigator/

https://attack.mitre.org

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

https://www.microsoft.com/security/blog/2022/07/05/hive-ransomware-gets-upgrades-in-rust/

https://www.varonis.com/blog/hive-ransomware-analysis

https://www.connectwise.com/resources/hive-profile

https://www.ccn-cert.cni.es/seguridad-al-dia/novedades-ccn-cert/11438-analisis-del-ransomware-hive-o-hiveleaks.html

https://securityintelligence.com/posts/ta505-continues-to-infect-networks-with-sdbbot-rat/

https://www.incibe-cert.es/sites/default/files/contenidos/estudios/doc/incibe-cert_estudio_analisis_hive_2021_v1.pdf

https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6326-ccn-cert-id-15-21-hive-ransomware-1/file.html

https://www.techtarget.com/searchsecurity/news/252522715/Researcher-develops-Hive-ransomware-decryption-tool