Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

SNATCH RANSOMWARE

21/09/2023

CONTENIDO

INTRODUCCIÓN

Desde mediados de 2021, los actores de amenazas de Snatch han evolucionado constantemente sus tácticas para aprovechar las tendencias actuales en el espacio de los ciberdelincuentes y han aprovechado los éxitos de las operaciones de otras variantes de ransomware. Los actores de amenazas de Snatch se han dirigido a una amplia gama de sectores de infraestructura crítica, incluidos los sectores de Base Industrial de Defensa (DIB), Alimentación y Agricultura y Tecnología de la Información. Los actores de amenazas de Snatch realizan operaciones de ransomware que implican la exfiltración de datos y la doble extorsión. Después de la exfiltración de datos, que a menudo implica comunicaciones directas con las víctimas que exigen un rescate, los actores de amenazas de Snatch pueden amenazar a las víctimas con una doble extorsión, donde los datos de las víctimas se publicarán en el blog de extorsión de Snatch si el rescate no se paga.

SNATCH RANSOMWARE

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2023_09_21_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	21/09/2023
Es día cero (0 day):	No

RESUMEN

Desde mediados de 2021, los actores de amenazas de Snatch han evolucionado constantemente sus tácticas para aprovechar las tendencias actuales en el espacio de los ciberdelincuentes y han aprovechado los éxitos de las operaciones de otras variantes de ransomware. Los actores de amenazas de Snatch se han dirigido a una amplia gama de sectores de infraestructura crítica, incluidos los sectores de Base Industrial de Defensa (DIB), Alimentación y Agricultura y Tecnología de la Información. Los actores de amenazas de Snatch realizan operaciones de ransomware que implican la exfiltración de datos y la doble extorsión. Después de la exfiltración de datos, que a menudo implica comunicaciones directas con las víctimas que exigen un rescate, los actores de amenazas de Snatch pueden amenazar a las víctimas con una doble extorsión, donde los datos de las víctimas se publicarán en el blog de extorsión de Snatch si el rescate no se paga.

TÉCNICAS

Apareciendo por primera vez en 2018, Snatch opera un modelo de ransomware como servicio (RaaS) y se cobró su primera víctima con sede en los Estados Unidos en 2019. Originalmente, el grupo fue referido como Team Truniger, basado en el apodo de un miembro clave del grupo, Truniger, que anteriormente

operaba como un afiliado de GandCrab. Los actores de amenazas de Snatch utilizan una variante de ransomware personalizada notable por reiniciar los dispositivos en modo seguro [T1562.009], lo que permite que el ransomware eluda la detección por antivirus o protección de punto final, y luego cifrar archivos cuando se ejecutan pocos servicios.

Se ha observado que los actores de amenazas de Snatch compran datos previamente robados de otras variantes de ransomware en un intento de explotar aún más a las víctimas para que paguen un rescate para evitar que sus datos se publiquen en el blog de extorsión de Snatch.

Nota: Desde noviembre de 2021, un sitio de extorsión que opera bajo el nombre de Snatch sirvió como centro de intercambio de datos exfiltrados o robados de las empresas víctimas en Clearnet y TOR alojados por un servicio de alojamiento a prueba de balas. En agosto de 2023, las personas que afirmaban estar asociadas con el blog dieron una entrevista a los medios alegando que el blog no estaba asociado con el ransomware Snatch y "ninguno de nuestros objetivos ha sido atacado por Ransomware Snatch …", a pesar de que múltiples datos confirmados de víctimas de Snatch aparecen en el blog junto con víctimas asociadas con otros grupos de ransomware, especialmente Nokoyawa y Conti.

ACCESO INICIAL Y PERSISTENCIA

Los actores de amenazas emplean varios métodos diferentes para obtener acceso y mantener la persistencia en la red de una víctima. Los afiliados de Snatch se basan principalmente en explotar las debilidades en el Protocolo de Escritorio Remoto (RDP) [T1133]. En algunos casos, los afiliados de Snatch han buscado credenciales comprometidas de foros / mercados criminales [T1078].

Los actores de amenazas de Snatch ganan persistencia en la red de una víctima al comprometer una cuenta de administrador [T1078.002] a un servidor de comando y control (C2) ubicado en un servicio de alojamiento a prueba de balas ruso [T1583.003]. Por tráfico IP de los registros de eventos proporcionados por víctimas recientes, los actores de amenazas de Snatch iniciaron conexiones RDP desde un servicio de alojamiento a prueba de balas ruso y a través de otros servicios de red privada virtual (VPN) [T1133].

DESCUBRIMIENTO DE DATOS Y MOVIMIENTO LATERAL

Se observó que los actores de amenazas usaban diferentes TTP para descubrir datos, moverse lateralmente y buscar datos para filtrar. Los actores de amenazas de Snatch usan para configurar, consultar, detener, iniciar, eliminar y agregar servicios del sistema mediante la línea de comandos de Windows. Además de, los actores de amenazas de Snatch también usan herramientas como Metasploit y Cobalt Strike [S0154].

Antes de implementar el ransomware, se observó que los actores de amenazas de Snatch pasaban hasta tres meses en el sistema de una víctima. Dentro de este período de tiempo, los actores de amenazas de Snatch explotaron la red de la víctima [T1590] para la mayor implementación posible de ransomware y la búsqueda de archivos y carpetas [T1005] seguido de cifrado de archivos [T1486].

EVASIÓN Y EJECUCIÓN DE LA DEFENSA

Durante las primeras etapas de la implementación de ransomware, los actores de amenazas de Snatch intentan deshabilitar el software antivirus [T1562.001] y ejecutar un ejecutable como un archivo llamado o alguna variación del mismo. En víctimas recientes, el nombre del ejecutable del ransomware consistía en una cadena de caracteres hexadecimales que coinciden con el hash del archivo en un esfuerzo por vencer la detección basada en reglas [T1036]. Tras el inicio, el ransomware Snatch consulta la carga útil y modifica las claves de registro [T1012 (enlace es externo)][T1112]. En algunos casos, el programa intenta eliminar todas las instantáneas de volumen de un sistema [T1490]. Después de la ejecución de los archivos por lotes, el ejecutable elimina los archivos por lotes del sistema de archivos de la víctima [T1070.004].safe.exeSHA-256.bat

El ejecutable del ransomware Snatch agrega una serie de caracteres hexadecimales a cada nombre de archivo y carpeta que cifra, único para cada infección, y deja un archivo de texto titulado en cada carpeta. Los actores de amenazas Snatch se comunican con sus víctimas a través del correo electrónico y la plataforma de comunicación Tox basada en identificadores dejados en notas de rescate o a través de su blog de extorsión. Desde noviembre de 2021, algunas víctimas informaron haber recibido una llamada falsa de una mujer desconocida que afirmaba estar asociada con Snatch y las dirigió al sitio de extorsión del grupo. En algunos casos, las víctimas de Snatch tenían una variante de ransomware diferente implementada en sus sistemas, pero recibieron una nota de rescate de los actores de amenazas de Snatch. Como resultado, los datos de las víctimas se publican en el blog de ransomware que involucra las diferentes variantes de ransomware y en el blog de extorsión de los actores de amenazas Snatch.HOW TO RESTORE YOUR FILES.TXT

INDICADORES DE COMPROMISO (IOC)

Los IOC de Snatch detallados en esta sección se obtuvieron a través de investigaciones del FBI desde septiembre de 2022 hasta junio de 2023.

Desde 2019, los actores de amenazas de Snatch han utilizado numerosas direcciones de correo electrónico para enviar correos electrónicos a las víctimas. Las direcciones de correo electrónico utilizadas por los actores de amenazas de Snatch son aleatorias, pero generalmente se originan en uno de los siguientes dominios enumerados en las Tablas 1 y 2:

Dominios de correo electrónico
sezname[.]cz
cock[.]li
airmail[.]cc

La Tabla 2 muestra una lista de dominios de correo electrónico legítimos que ofrecen servicios de correo electrónico cifrados que han sido utilizados por los actores de amenazas d Snatch. Estos dominios de correo electrónico están disponibles públicamente y son legales. El uso de estos dominios de correo electrónico por parte de un actor de amenazas no debe atribuirse a los dominios de correo electrónico, en ausencia de hechos articulables específicos que tiendan a mostrar que se utilizan bajo la dirección o bajo el control de un actor de amenazas.

Dominios de correo electrónico
tutanota[.]com / tutamail[.]com / tuta[.]io
mail[.]fr
keemail[.]me
protonmail[.]com / proton[.] me
swisscows[.]email

Tabla 3: Direcciones de correo electrónico de Snatch reportadas por víctimas recientes

Direcciones de correo electrónico
sn.tchnews.top@protonmail[.]me
funny385@swisscows[.]email
funny385@proton[.]me
russellrspeck@seznam[.]cz
russellrspeck@protonmail[.]com
Mailz13MoraleS@proton[.]me
datasto100@tutanota[.]com
snatch.vip@protonmail[.]com

ID de mensajería TOX
CAB3D74D1DADE95B52928E4D9DFC003FF5ADB2E082F59377D049A91952E8BB3B419DB2FA9D3F
7229828E766B9058D329B2B4BC0EDDD11612CBCCFA4811532CABC76ACF703074E0D1501F8418
83E6E3CFEC0E4C8E7F7B6E01F6E86CF70AE8D4E75A59126A2C52FE9F568B4072CA78EF2B3C97
0FF26770BFAEAD95194506E6970CC1C395B04159038D785DE316F05CE6DE67324C6038727A58
NOTA: Según las notas de rescate, este es un TOX de "servicio al cliente" para comunicarse si la identificación original de TOX no responde.

Creación de carpetas
C:\$SysReset

Comandos
wmiadap.exe /F /T /R
%windir%\System32\svchost.eve –k WerSvcGroup
conhost.exe 0xFFFFFFFF -ForceV1
vssadmin delete shadows /all /quiet
bcdedit.exe /set {current} safeboot minimal
REG ADD HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\VSS /VE /T REG_SZ /F /D Service
REG ADD HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\mXoRpcSsx /VE /T REG_SZ /F /D Service
REG QUERY HKLM\SYSTEM\CurrentControlSet\Control /v SystemStartOptions
%CONHOST% "1088015358-1778111623-1306428145949291561678876491840500802412316031-33820320
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --flag-switches-begin --flag-switches-end --no-startup-window /prefetch:5
cmd /d /c cmd /d /c cmd /d /c start " " C:\Users\grade1\AppData\Local\PRETTYOCEANluvApplication\PRETTYOCEANApplicationidf.bi.

Claves del Registro
HKLM\SOFTWARE\Microsoft\Windows Media Player NSS\3.0\Servers\D8B548F0-E306-4B2B-BD82-25DAC3208786\FriendlyName
HKU\S-1-5-21-4270068108-2931534202-3907561125-1001\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{ED50FC29-B964-48A9-AFB3-15EBB9B97F36} {ADD8BA80-002B-11D0-8F0F-00C04FD7D062} 0xFFFF

Mutexes creados
\Sessions\1\BaseNamedObjects\gcc-shmem-tdm2-fc_key
\Sessions\1\BaseNamedObjects\gcc-shmem-tdm2-sjlj_once
\Sessions\1\BaseNamedObjects\gcc-shmem-tdm2-use_fc_key
gcc-shmem-tdm2-fc_key
gcc-hmem-tdm2-sjlj_once
gcc-shmem-tdm2-use_fc_key

Nombres	SHA-256
qesbdksdvnotrjnexutx.bat	0965cb8ee38adedd9ba06bdad9220a35890c2df0e4c78d0559cd6da653bf740f
eqbglqcngblqnl.bat	1fbdb97893d09d59575c3ef95df3c929fe6b6ddf1b273283e4efadf94cdc802d
safe.exe	5950b4e27554585123d7fca44e83169375c6001201e3bf26e57d079437e70bcd
safe.exe	7018240d67fd11847c7f9737eaaae45794b37a5c27ffd02beaacaf6ae13352b3
safe.exe	28e82f28d0b9eb6a53d22983e21a9505ada925ebb61382fabebd76b8c4acff7c
safe.exe	fc31043b5f079ce88385883668eeebba76a62f77954a960fb03bf46f47dbb066
DefenderControl.exe	a201f7f81277e28c0bdd680427b979aee70e42e8a98c67f11e7c83d02f8fe7ae
PRETTYOCEANApplicationdrs.bi	6992aaad3c47b938309fc1e6f37179eb51f028536f8afc02e4986312e29220c0
Setup.exe	510e9fa38a08d446189c34fe6125295f410b36f00aceb65e7b4508e9d7c4e1d1
WRSA.exe	ed0fd61bf82660a69f5bfe0e66457cfe56d66dd2b310e9e97657c37779aef65d
ghnhfglwaplf.bat	2155a029a024a2ffa4eff9108ac15c7db527ca1c8f89ccfd94cc3a70b77cfc57
nllraq.bat	251427c578eaa814f07037fbe6e388b3bc86ed3800d7887c9d24e7b94176e30d
ygariiwfenmqteiwcr.bat	3295f5029f9c9549a584fa13bc6c25520b4ff9a4b2feb1d9e935cc9e4e0f0924
bsfyqgqeauegwyfvtp.bat	6c9d8c577dddf9cc480f330617e263a6ee4461651b4dec1f7215bda77df911e7
rgibdcghzwpk.bat	84e1476c6b21531de62bbac67e52ab2ac14aa7a30f504ecf33e6b62aa33d1fe5
pxyicmajjlqrtgcnhi.bat	a80c7fe1f88cf24ad4c55910a9f2189f1eedad25d7d0fd53dbfe6bdd68912a84
evhgpp.bat	b998a8c15cc19c8c31c89b30f692a40b14d7a6c09233eb976c07f19a84eccb40
eqbglqcngblqnl.bat	1fbdb97893d09d59575c3ef95df3c929fe6b6ddf1b273283e4efadf94cdc802d
qesbdksdvnotrjnexutx.bat	0965cb8ee38adedd9ba06bdad9220a35890c2df0e4c78d0559cd6da653bf740f
HOW TO RESTORE YOUR FILES.TXT	
safe.exe	c8a0060290715f266c89a21480fed08133ea2614

Direcciones IP
193.188.22.29
193.188.22.26
193.188.22.25
67.211.209.151
37.59.146.180
45.147.228.91
185.61.149.242
94.140.125.150
5.142.75.75
45.238.25.2
118.70.116.154
163.25.24.44

RECOMENDACIONES

- Implemente un plan de recuperación que mantenga y conserve múltiples copias de datos confidenciales o de propiedad y servidores en una ubicación segura, segmentada y separada físicamente (es decir, disco duro, dispositivo de almacenamiento o la nube).
- Implemente la segmentación de la red y mantenga copias de seguridad fuera de línea de los datos para garantizar una interrupción limitada de la organización.
- Realice copias de seguridad de los datos con regularidad y proteja con contraseña las copias de seguridad almacenadas sin conexión. Asegúrese de que las copias de los datos críticos no sean accesibles para su modificación o eliminación desde el sistema donde residen los datos.
- Mantenga actualizado todos los sistemas operativos, y software.
- Instale, actualice periódicamente y habilite la detección en tiempo real del software antivirus en todos los hosts.
- Audite las cuentas de usuarios con privilegios administrativos y configure los controles de acceso, con el principio de privilegios mínimos.
- Desactive los puertos no utilizados.
- Deshabilite las actividades y permisos de línea de comandos y scripting.
- Asegúrese de que todos los datos de copia de seguridad estén encriptados, sean inmutables
- Examine el tráfico de red entrante y saliente, en busca de actividad sospechosa dentro de su red.

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/main/20230921_01_SnatchRansomware

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente