Informes de APTs de ESET Threat Intelligence PREMIUM

Digital Security
Progress. Protected.

INVESTIGACIÓN DE AMENAZAS

RESUMEN DE LA ACTIVIDAD

Edición:

AS-2021-0007

1 de abril - 15 de abril de 2021

GRUPO LAZARUS

Visión general del grupo

El Grupo Lazarus, activo desde al menos 2009, es responsable de incidentes de gran repercusión como el ataque a Sony Pictures Entertainment en 2016, los ciberataques de decenas de millones de dólares en 2016, el brote de WannaCryptor (también conocido como WannaCry) en 2017 y un largo historial de ataques destructivos contra las infraestructuras públicas y críticas de Corea del Sur al menos desde 2011 hasta la actualidad. La diversidad, el número y la excentricidad en la ejecución de las campañas de Lazarus definen a este grupo, así como que realizan los tres pilares de las actividades cibercriminales: ciberespionaje, cibersabotaje y búsqueda de beneficios económicos.

Resumen de la actividad

Operación In(ter)cepción

Operación In(ter)cepción es el nombre de ESET para una serie de ataques atribuidos al grupo Lazarus. Estos ataques han estado en curso al menos desde septiembre de 2019, dirigidos a empresas aeroespaciales, militares y de defensa. La operación es notable por utilizar spearphishing basado en LinkedIn y emplear trucos efectivos para permanecer bajo el radar. Su principal objetivo parece ser el espionaje corporativo.

A principios de abril de 2021 apareció en VirusTotal una nueva versión del descargador de la fase 1. La funcionalidad principal y la estructura del malware siguen siendo las mismas, sin embargo, los autores introdujeron el cifrado XOR de 1 byte de las cadenas importantes, como las URLs, el agente de usuario y las cabeceras HTTP, para que no puedan leerse fácilmente durante el análisis estático.

Victimología / Verticales empresariales

Empresas aeroespaciales, militares y de defensa.

Vector de infección

No disponible

Actividad posterior al acuerdo

No disponible

IoCs

Operación In(ter)cepción

Fecha	**07-04-2021 00:08:38**
MD5	2CBE0BEA035DB9240CEB338CF9EA7FE6
SHA-1	9A8B7F11104156F0DF4F07827EC12E5C2300C4EE
SHA-256	40B6CBCC594D3696952E90FA15CCD733EBC2777554092E8C15694334274E5B90
Nombre del archivo	c.exe
Descripción	Stage 1 loader.
C&C	*https://kehot.com[.]ar/Pubs/menus.jpg* https://www.meisami[.]net/css/search.css https://www.sfaonweb[.]com/pdf/{A76E7D01-6BAF-4FE4-98E0-.pdf *https://amon-werbeartikel[.]de/Media/Uploaded/chrisen.png*
Detección	Win64/Interception.G
Sello de compilación PE	04-02-2020 18:01:33 (Duración)

Informes de APTs de ESET Threat Intelligence PREMIUM

Digital Security
Progress. Protected.

INVESTIGACIÓN DE AMENAZAS

ANÁLISIS TÉCNICO NETVULTURE & TURLACHOPPER

Edición:

TA-2021-0002

12 de marzo de 2021

RESUMEN GENERAL

Turla es un infame grupo de ciberespionaje activo desde hace más de una década. Se centra principalmente en objetivos de alto perfil, como gobiernos y entidades diplomáticas, en Europa, Asia Central y Oriente Medio. Es conocido por haber vulnerado importantes instituciones como el Departamento de Defensa de Estados Unidos en 2008 y la empresa de defensa suiza RUAG en 2014. Durante los últimos años, *hemos documentado gran parte* del *arsenal del grupo* para dar a conocer sus actividades.

En enero de 2021, detectamos actividad sospechosa en un servidor de Microsoft Exchange perteneciente a un Ministerio de Asuntos Exteriores de Europa del Este. Descubrimos dos nuevas familias de malware que atribuimos a Turla: TurlaChopper y NETVulture.

Puntos clave de este informe:

- El servidor de Microsoft Exchange Outlook Web Access fue comprometido probablemente usando CVE-2020-0688.
- En este servidor, los atacantes implementaron un webshell personalizado, que denominamos TurlaChopper.
- Dos meses más tarde, los atacantes implementaron un backdoor previamente desconocido, que hemos denominado NETVulture, en otro servidor Windows de la misma compañía. Probablemente se instaló utilizando TurlaChopper.
- NETVulture es un backdoor desarrollado en .NET y que utiliza Microsoft OneDrive como servidor de C&C.
- Las variantes NETVulture y TurlaChopper se han utilizado activamente con fines maliciosos desde principios de 2020 hasta principios de enero de 2021.

PERFIL DE TURLA

Turla, también conocido como Snake, es un conocido grupo de ciberespionaje activo desde hace al menos una década. El grupo es conocido por sus avanzadas herramientas personalizadas y su capacidad para realizar operaciones muy específicas.

Durante más de una década, Turla ha sido responsable de numerosas vulneraciones de alto nivel. Los objetivos incluyen el *Mando Central de Estados Unidos en 2008*, el *Ministerio de Asuntos Exteriores de Finlandia en 2013*, la empresa militar suiza RUAG en 2014 y el *Ministerio de Asuntos Exteriores de Alemania en 2017*. Más recientemente, al parecer comprometió a las *Fuerzas Armadas francesas en 2018* y al *Ministerio de Asuntos Exteriores de Austria en 2019*. La línea de tiempo de la figura 1 presenta algunos de los principales ataques atribuidos públicamente a Turla.

Figura 1. Cronología de los ataques atribuidos públicamente a Turla

Los sectores a los que se dirige el grupo han sido bastante consistentes en los últimos años:

- Ministerios de Asuntos Exteriores y representaciones diplomáticas (embajadas, consulados, etc.)
- Organizaciones militares
- Organizaciones políticas regionales
- Entidades de defensa

El grupo maneja un gran repertorio de familias de malware: desde Skipper, que suele verse en campañas de watering hole, hasta sofisticados backdoors como *ComRAT v4*, un backdoor que utiliza Gmail para las comunicaciones de C&C, *LightNeuron*, un implante especialmente diseñado para los servidores de correo electrónico de Microsoft Exchange, y Crutch, un backdoor que utiliza Dropbox como servidor de C&C.

27-02-2020
Se instalaron dos webshells en el servidor de Microsoft Exchange. Estaban instaladas en el servidor web de Outlook Web Access (OWA) y, por tanto, eran accesibles desde Internet.

16-03-2020
Los responsables de Turla crearon la cuenta de OneDrive que posteriormente utilizó NETVulture.

23-04-2020
La primera versión de NETVulture se instaló en otro servidor local.

04-05-2020
Otro webshell fue instalado en el servidor web de OWA.

05-06-2020
Se implementó una segunda versión de NETVulture (en el mismo servidor que la primera).

06-01-2021
NETVulture ya no puede autenticarse en Microsoft Graph (por una razón desconocida). El backdoor está inactivo de por sí.

06-01-2021
Los atacantes intentaron instalar un webshell en el servidor WSUS local.

Figura 2. Cronología de los acontecimientos importantes relacionados con el incidente de NETVulture

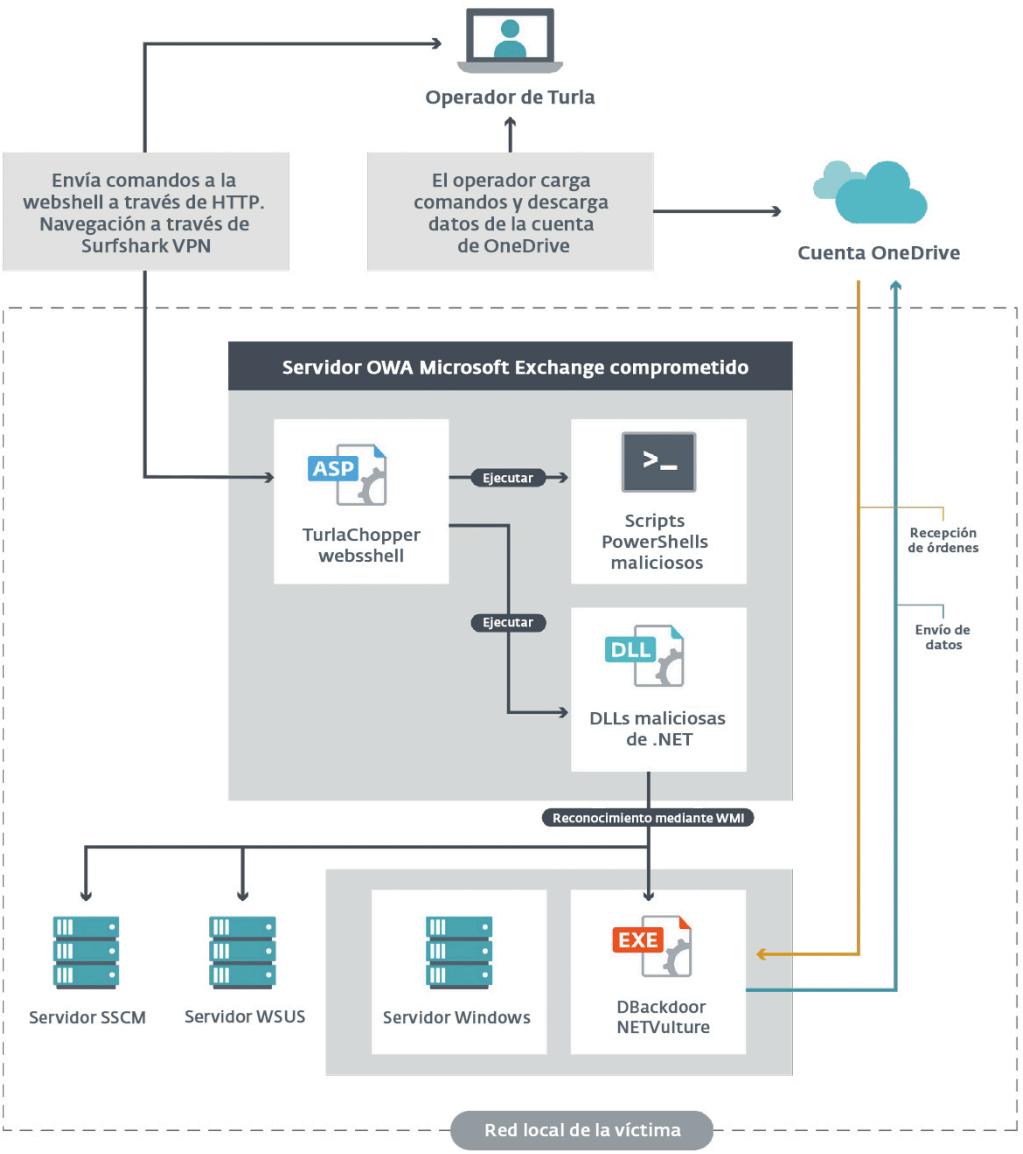

Figura 3. Resumen del uso de TurlaChopper y NETVulture