Nro. Alerta:	EC-2022-003	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	04-enero-2022	**Telegram: Instaladores maliciosos contienen malware "Purple Fox"**	V 1.0

I. DATOS GENERALES:

Clase de alerta: Malware

Tipo de incidente: RootKit / escalamiento de privilegios

Nivel de riesgo: Medio

II. ALERTA

Instalador malicioso de "Telegram for Desktop" distribuye malware Purple Fox para instalar cargas útiles maliciosas en dispositivos infectados.

Figura 1. Purple Fox a través de Telegram **Fuente:** Minerva

III. INTRODUCCIÓN

El instalador de Telegram detectado como malicioso, es un script compilado de AutoIt (un lenguaje de scripting gratuito similar al BASIC diseñado para automatizar la GUI de Windows y el scripting general) llamado "Telegram Desktop.exe". Archivo que, al ser ejecutado, libera dos archivos, un instalador de Telegram real y un descargador malicioso.

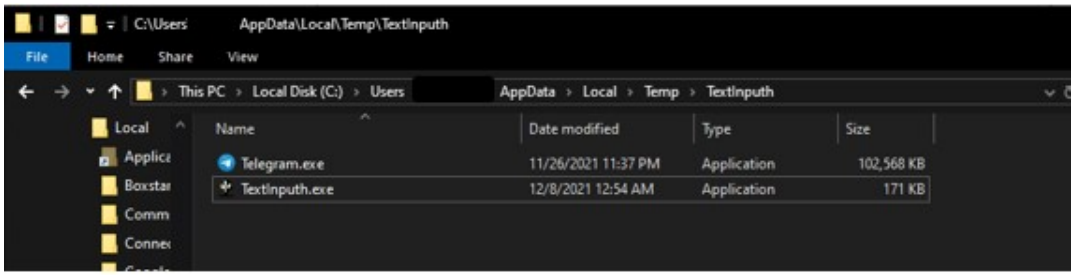

Figura 2. Archivos liberados en computador infectado **Fuente:** Minerva

Nro. Alerta:	EC-2022-003	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	04-enero-2022	**Telegram: Instaladores maliciosos contienen malware "Purple Fox"**	V 1.0

Cuando se ejecuta, TextInputh.exe crea una nueva carpeta llamada "1640618495" en el directorio C: \ Users \ Public \ Videos \. El archivo TextInputh.exe se utiliza como descargador para la siguiente etapa del ataque. Se pone en contacto con un servidor C&C y descarga dos archivos en la carpeta recién creada:

- 1.rar - que contiene los archivos para la siguiente etapa. 7zz.exe: un archivador 7z legítimo.
- El 7zz.exe se usa para desarchivar 1.rar, que contiene los siguientes archivos:

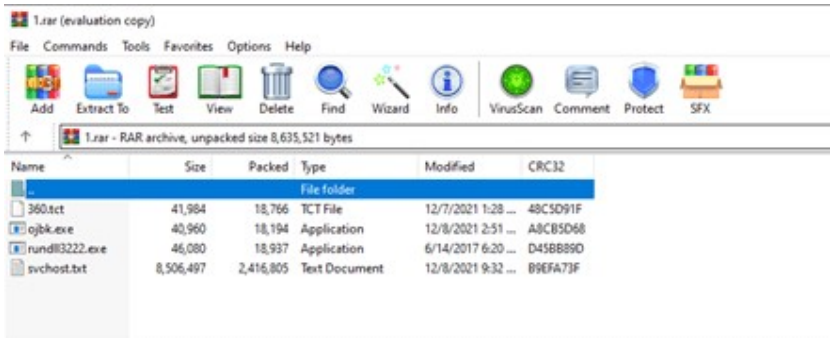

Figura 3. Contenido de archivo 1.rar en computador infectado **Fuente:** Minerva

A continuación, TextInputh.exe realiza las siguientes acciones:

- Copia 360.tct con el nombre "360.dll", rundll3222.exe y svchost.txt en la carpeta ProgramData
- Ejecuta ojbk.exe con la línea de comando "ojbk.exe -a"
- Elimina 1.rar y 7zz.exe y sale del proceso

IV. VECTOR DE ATAQUE

Hasta la fecha de publicación de la presente alerta, el vector de ataque es desconocido, sin embargo, malware similar, que se hace pasar por software legítimo, se distribuyeron anteriormente a través de videos de YouTube, foros de spam y sitios de software sospechosos.

Nro. Alerta:	EC-2022-003	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	04-enero-2022	**Telegram: Instaladores maliciosos contienen malware "Purple Fox"**	V 1.0

V. IMPACTO:

Una vez terminado el proceso de carga de Purple Fox en el computador infectado, se crea una clave de registro para la persistencia, una DLL (rundll3222.dll) deshabilita UAC (Utilidad de Windows que evita instalación no autorizada de aplicaciones o el cambio de la configuración del sistema), se ejecuta la carga útil (scvhost.txt) y los siguientes cinco archivos adicionales se colocan en el sistema infectado:

- Calldriver.exe
- Driver.sys
- dll.dll
- matar murciélago
- speedmem2.hg

El propósito de estos archivos adicionales es bloquear colectivamente el inicio de procesos 360 AV y evitar la detección de Purple Fox en la máquina comprometida.

El siguiente paso para el malware es recopilar información básica del sistema, verificar si se está ejecutando alguna herramienta de seguridad y, finalmente, enviar todo eso a una dirección C2 codificada.

Una vez que se completa este proceso de reconocimiento, Purple Fox se descarga del C2 en forma de un archivo .msi que contiene shellcode cifrado para sistemas de 32 y 64 bits.

Tras la ejecución de Purple Fox, la máquina infectada se reiniciará para que surta efecto la nueva configuración del registro, y lo más importante, el Control de cuentas de usuario (UAC) deshabilitado.

Deshabilitar la omisión de UAC es vital porque otorga privilegios de administrador a cualquier programa que se ejecute en el sistema infectado, incluidos virus y malware, es decir, permite a Purple Fox realizar funciones maliciosas como búsqueda y exfiltración de archivos, eliminación de procesos, eliminación de datos, descarga y ejecución de código e incluso infección a otros sistemas Windows.

Nro. Alerta:	EC-2022-003	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	04-enero-2022	**Telegram: Instaladores maliciosos contienen malware "Purple Fox"**	V 1.0

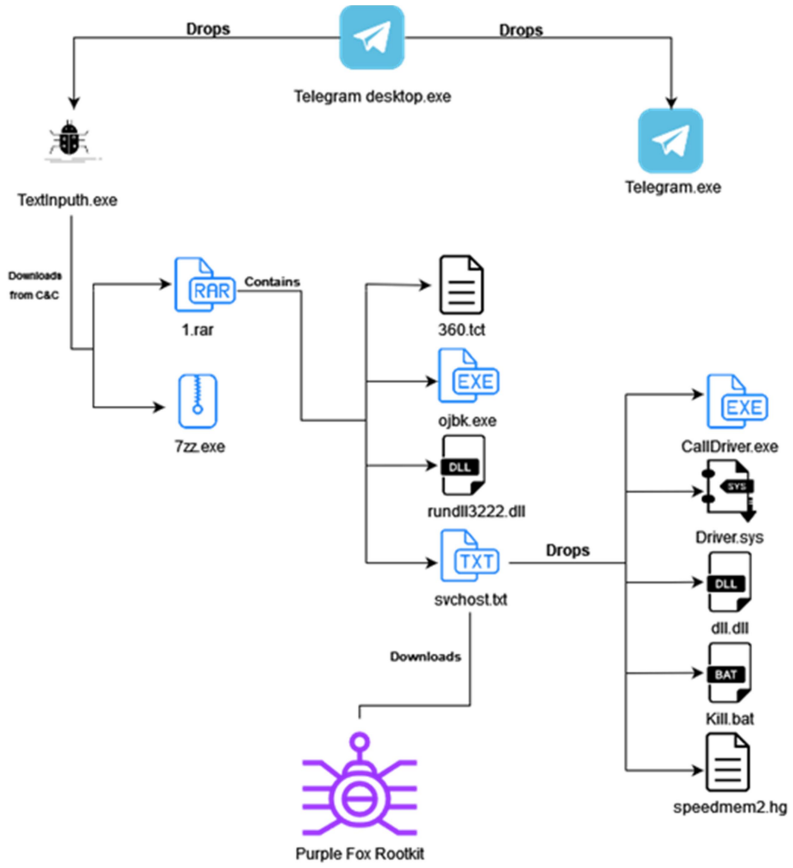

Figura 4. Ciclo de vida de Purple Fox en computador infectado **Fuente:** Minerva

VI. INDICADORES DE COMPROMISO:

Hashes:

- 41769d751fa735f253e96a02d0cccadfec8c7298666a4caa5c9f90aaa826ecd1 - Telegram Desktop.exe
- BAE1270981C0A2D595677A7A1FEFE8087B07FFEA061571D97B5CD4C0E3EDB

6E0 - TextInputh.exe

- af8eef9df6c1f5645c95d0e991d8f526fbfb9a368eee9ba0b931c0c3df247e41 - instalador legítimo de telegram
- 797a8063ff952a6445c7a32b72bd7cd6837a3a942bbef01fc81ff955e32e7d0c - 1.rar
- 07ad4b984f288304003b080dd013784685181de4353a0b70a0247f96e535bd56 - 7zz.exe
- 26487eff7cb8858d1b76308e76dfe4f5d250724bbc7e18e69a524375cee11fe4 - 360.tct
- b5128b709e21c2a4197fcd80b072e7341ccb335a5decbb52ef4cee2b63ad0b3e - ojbk.exe
- 405f03534be8b45185695f68deb47d4daf04dcd6df9d351ca6831d3721b1efc4 - rundll3222.exe - rundll32.exe legítimo
- 0937955FD23589B0E2124AFEEC54E916 - svchost.txt
- e2c463ac2d147e52b5a53c9c4dea35060783c85260eaac98d0aaeed2d5f5c838 - Calldriver.exe
- 638fa26aea7fe6ebefe398818b09277d01c4521a966ff39b77035b04c058df60 - Driver.sys
- 4bdfa7aa1142deba5c6be1d71c3bc91da10c24e4a50296ee87bf2b96c731b7fa - dll.dll
- 24BCBB228662B91C6A7BBBCB7D959E56 - kill.bat
- 599DBAFA6ABFAF0D51E15AEB79E93336 - speedmem2.hg

IPs:

- 193.164.223 [.] 77 - Servidor C&C de segunda etapa.
- 144.48.243 [.] 79 - servidor C&C de última etapa.

URLs

- hxxp: //193.164.223 [.] 77: 7456 / h? = 1640618495 - contiene el archivo 1.rar
- hxxp: //193.164.223 [.] 77: 7456/77 - contiene el archivo 7zz.exe
- hxxp: //144.48.243 [.] 79: 17674 / C558B828.Png - Purple Fox Rootkit

Nro. Alerta:	EC-2022-003	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	04-enero-2022	**Telegram: Instaladores maliciosos contienen malware "Purple Fox"**	V 1.0

VII. RECOMENDACIONES

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- Descargar aplicaciones, documentos, y en sí, archivos de cualquier naturaleza, solo desde fuentes oficiales y legítimas.
- No abrir, manipular, o interactuar con correos electrónicos altamente sospechosos recibidos en las respectivas bandejas de correo ya sea personales o Institucionales.
- No abrir, manipular, o interactuar con archivos de cualquier naturaleza, accesibles a través de unidades de almacenamiento externas a la Organización/Institución, o que no sean de uso personal
- Identificar y suspender el acceso de usuarios que exhiban una actividad inusual.
- En el caso de necesitar descargar, copiar, o manipular, archivos de cualquier naturaleza, someterlos a escaneos rigurosos en sistemas antivirus antes de abrirlos o ejecutarlos
- Implementar un plan de respuesta a emergencias de la Organización/Institución, considerar la gama completa de impactos potenciales que los ciberataques plantean a las operaciones, incluida la pérdida o manipulación de la información, la pérdida o manipulación del control y, las amenazas a la seguridad.
- En el caso de sufrir un ataque de proporciones mayores, contacte a las Autoridades competentes en base a la Normativa Legal Vigente a nivel Nacional.

VIII. REFERENCIAS:

Bill Toulas. (3 de enero de 2022). Bleeping Computer. Obtenido de https://www.bleepingcomputer.com/news/security/purple-fox-malware-distributed-via-malicious-telegram-installers/

Natalie Zargarov. (3 de enero de 2022). Minerva. Obtenido de https://blog.minerva-labs.com/malicious-telegram-installer-drops-purple-fox-rootkit