I. DATOS GENERALES:

Clase de alerta: Malware

Tipo de incidente: Troyano

Nivel de riesgo: Medio

II. ALERTA

Investigadores de ESET descubrieron en marzo de 2023 una campaña de malware denominada "Operación Guinea Pig" que apuntaba a varios países de América Latina. El objetivo de la campaña era infectar a las víctimas con el malware AgentTesla.

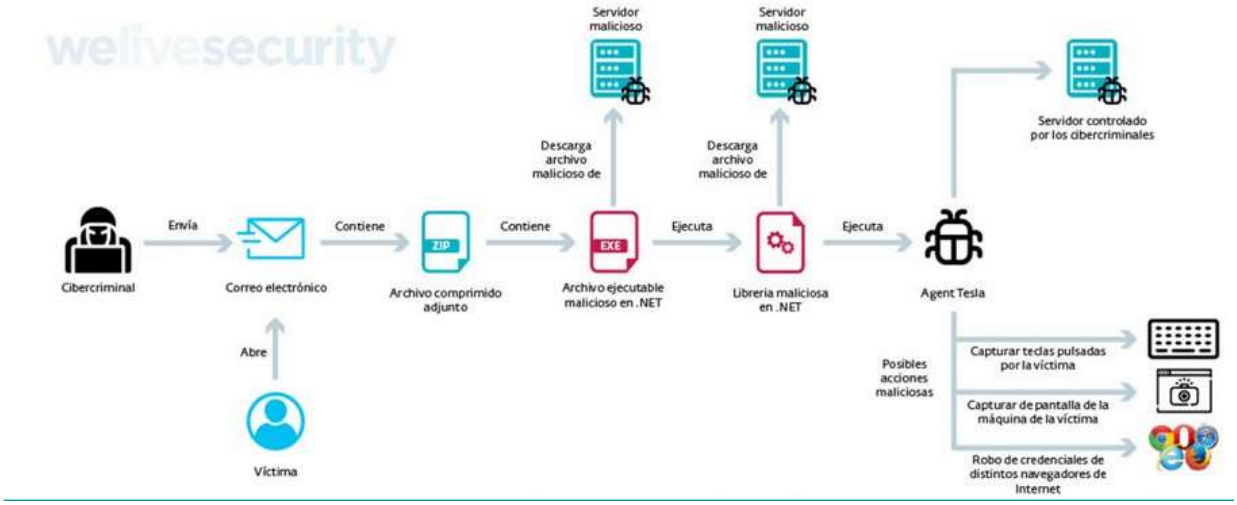

Figura 1.- Proceso de infección de Operación Guinea Pig.
Fuente: welivesecurity.com

III. INTRODUCCIÓN

El malware AgentTesla es un troyano de acceso remoto (RAT), que está activo desde 2014 y que es distribuido como un Malware-as-a-Service (MaaS) en campañas a nivel global.

Según Eset, el malware está desarrollado con el framework .NET y es utilizado para espiar y robar información como: credenciales de distintos software, obtener cookies de los navegadores, registrar las pulsaciones del teclado de la máquina (Keylogging), realizar capturas de pantalla y del clipboard (portapapeles).

Este código malicioso utiliza distintos métodos para el envío de la información recopilada desde la victima hacia el atacante.

IV. VECTOR DE ATAQUE:

Correo electrónico, phishing

V. IMPACTO:

La campaña OPERACIÓN GUINEA PIG comienza con el envío de correos de tipo phishing adjuntando un archivo ejecutable comprimido, desarrollado con el framework Microsoft .NET que contiene un código malicioso en Visual Basic ofuscado.

El archivo con código malicioso tiene doble extensión, .jpg y .exe; con el objetivo de confundir a la víctima haciendo creer que el archivo se trata de una imagen (.jpeg) y no un ejecutable (.exe).

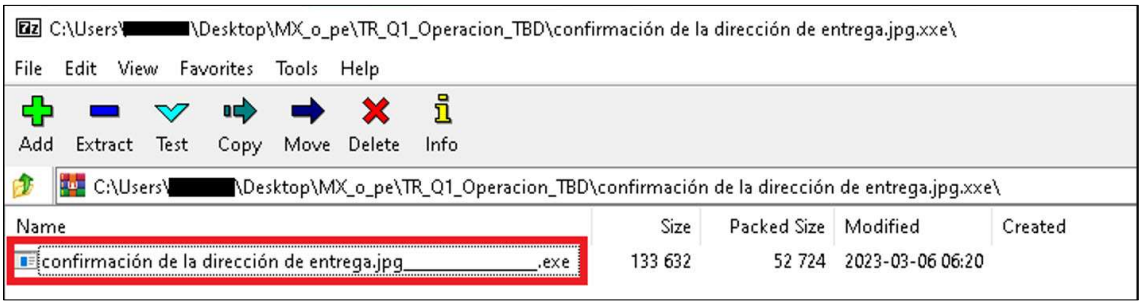

Figura 2.-*Archivo adjunto malicioso asociado a la campaña* Operación Guinea Pig
Fuente: welivesecurity.com

El principal objetivo del código malicioso que se observa en la figura 2, es invocar al intérprete de PowerShell para ejecutar otro código malicioso que se encargará de descargar una DLL maliciosa alojada en la siguiente URL:

https[:]//firebase.ngrok.io/testing/EXE_DLL.txt.

Una vez descargada la DLL, el código malicioso en PowerShell procede a ejecutarla pasándole como argumento una cadena de caracteres ofuscada; ésta DLL va a manipular la cadena de caracteres recibida para obtener así una nueva URL.

Con lo descrito, la DLL se encarga de descargar AgentTesla de la nueva URL e inyectar el malware sobre el proceso legítimo RegSvcs.exe por medio de la técnica Process Hollowing, en el que un atacante elimina código en un archivo ejecutable y lo reemplaza con código malicioso.

AgentTesla también utiliza distintos métodos a la hora de enviar la información de la víctima a los cibercriminales. Por ejemplo:

- HTTP: envía la información hacia un servidor controlado por el atacante
- SMTP: envía la información hacia una cuenta de correo electrónico controlada por el atacante
- FTP: envía la información hacia un servidor FTP controlado por el atacante
- Telegram: envía la información hacia un chat privado de Telegram.
- De acuerdo a un análisis, los cibercriminales exfiltran la información de la víctima por medio del protocolo FTP hacia el dominio ftp.sisoempresarialsas.com.
- Por otro lado, si bien este malware tiene capacidad para generar persistencia en la máquina de la víctima sobre la siguiente ruta: C:\Users\USERNAME\AppData\Roaming\eXCXES\eXCXES.exe; los investigadores no encontraron indicadores en esta campaña que demuestre que se está generando persistencia en la máquina de la víctima.

VI. INDICADORES DE COMPROMISO

A continuación, se listan las rutas que podrían ser utilizadas por los distintos códigos maliciosos propagados en esta campaña:

- C:\Users\USERNAME\AppData\Roaming\eXCXES\eXCXES.exe

Hashes de muestras analizadas:

- PowerShell/TrojanDownloader.Agent.GNZ:

80F43EA09F4918F80D4F7D84FDB6973CCAADDE05
75ADD0E232AB4164285E7804EC5379BFA84C0714
64F199EDAC6B3A8B1D994B63723555B162563B32
1652619B5095EEA2AFEC3A03B920BF63230C8C8A
D86960DD7B093DD0F3EF1DC3BC956D57217BD4EC

- MSIL/TrojanDownloader.Agent.NEN

9754596E9E8B0A6E053A4988CF85099C2617A98B

- MSIL/Spy.AgentTesla.F

1ECA09DC9001A0B6D146C01F5B549DD96A0BFE5D

Dominios e IPs detectados en las muestras analizadas:

- https[:]//firebase[.]ngrok[.]io
- ftp[.]sisoempresarialsas.com
- 195[.]178.120.24
- 3[.]22.30.40
- 51[.]161.116.202

VII. RECOMENDACIONES:

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

- Mantener todos los programas de antivirus, antimalware, firewall del sistema operativo y cualquier otro software de seguridad debidamente actualizados y parchados.
- No descargar archivos sospechosos; fijarse en la extensión del archivo a descargar.
- Hacer caso omiso a correos, links o mensajes de dudosa procedencia y marcarlos como spam o bloquearlos y comunicar a su departamento técnico.
- Ante cualquier duda contactarse directamente con la persona o empresa suplantada para su comprobación y/o denuncia.
- Bloquear los sitios web o direcciones de correo electrónicos indicados en la sección indicadores de compromisos.

- Informarse continuamente sobre tipos de amenazas en el internet
- Hacer campañas de concientización sobre pishing y demás amenazas asociadas al correo electrónico.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

Mitre. (29 de noviembre de 2021). *MITRE*. Obtenido de https://attack.mitre.org/techniques/T1055/012/

Tavella, F. (28 de abril de 2021). *Welivesecurity*. Obtenido de Agent Tesla: principales características de este malware: • https://www.welivesecurity.com/la-es/2021/04/28/agent-tesla-principales-caracteristicas-este-malware/

Tavella, F. (20 de abril de 2023). *welivesecurity*. Obtenido de https://www.welivesecurity.com/la-es/2023/04/20/operacion-guinea-pig-correos-phishing-malware-agenttesla-mexico-america-latina/