Nro. Alerta:	EC-2022-012	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	24-enero-2022	**Microsoft PowerPoint: Archivos maliciosos son utilizados para enviar troyanos de acceso remoto**	V 1.0

I. DATOS GENERALES:

Clase de alerta: Malware

Tipo de incidente: Troyano de acceso remoto (RAT)

Nivel de riesgo: Medio

II. ALERTA

Desde diciembre de 2021, ha surgido una tendencia creciente de campañas de envío de phishing, las cuales utilizan documentos de Microsoft PowerPoint de tipo maliciosos, para robo de información y distribución de varios tipos de malware, incluidos troyanos de acceso remoto (RAT).

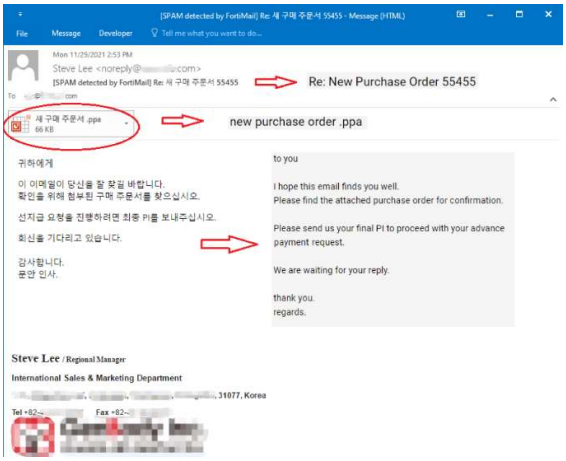

Figura 1. RAT AgentTesla desplegado a través de correo electrónico malicioso **Fuente:** Fortinet/BleepingComputer

III. INTRODUCCIÓN

Actores maliciosos, utilizan archivos de Microsoft PowerPoint, combinados con servicios legítimos en la nube, los cuales alojan cargas útiles de malware; montadas en varias plataformas legítimas, por lo que, es poco probable que generen señales de alerta con herramientas de seguridad

Nro. Alerta:	EC-2022-012	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	24-enero-2022	**Microsoft PowerPoint: Archivos maliciosos son utilizados para enviar troyanos de acceso remoto**	V 1.0

Las familias desplegadas en la campaña rastreada son: Warzone (también conocido como AveMaria) y AgentTesla, dos poderosas RAT, con el objetivo de robo de información, que se dirige a muchas aplicaciones, así como también, dirigidos al hurto de criptomonedas.

El archivo de Microsoft PowerPoint, adjunto al correo electrónico de tipo malicioso, contiene una macro ofuscada, que se ejecuta a través de una combinación de PowerShell (interfaz de consola de Windows) y MSHTA (Host de aplicación HTML de Microsoft), ambas herramientas integradas de Windows.

Posteriormente, el script VBS (Visual Basic Script) se desofusca y, agrega nuevas entradas de registro de Windows para la persistencia, lo que lleva a la ejecución de dos scripts. El primero, obtiene AgentTesla de una URL externa, y el segundo, desactiva Windows Defender.

Figura 2. Etapas de ejecución del VBS **Fuente:** Netskope/BleepingComputer

Además, el VBS, crea una tarea programada que ejecuta un script cada hora, la cual obtiene un "ladrón de criptomonedas" ejecutable de PowerShell, desde una URL del portal Web de Blogger.

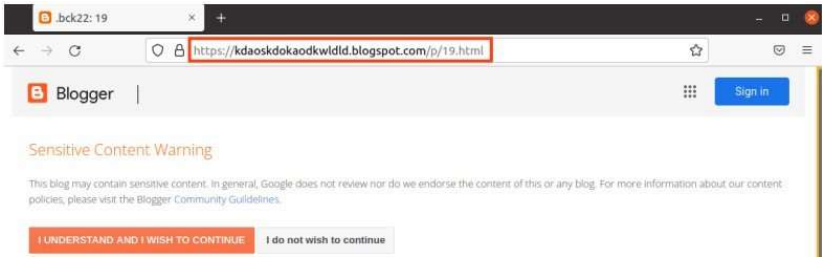

Figura 3. Portal Web de BLOGGER utilizado de forma maliciosa **Fuente:** Netskope/BleepingComputer

Nro. Alerta:	EC-2022-012	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	24-enero-2022	**Microsoft PowerPoint: Archivos maliciosos son utilizados para enviar troyanos de acceso remoto**	V 1.0

IV. VECTOR DE ATAQUE

Remoto, Phishing

V. IMPACTO:

AgentTesla, es un RAT (troyano de acceso remoto) basado en .NET (lenguaje de programación), que puede robar contraseñas del navegador, registrar pulsaciones de teclas, robar contenido del portapapeles, etc.

Se ejecuta a través de PowerShell, y, viene ligeramente ofuscado, mientras que también hay una función que inyecta la carga útil en una instancia de "aspnet_compiler.exe".

Figura 4. PowerShell que ejecuta AgentTesla **Fuente:** Netskope/BleepingComputer

La segunda carga útil entregada, es Warzone, también una RAT, de la que, aún no dan muchos detalles al respecto.

El “ladrón de criptomonedas” (admite Bitcoin, Ethereum, XMR, DOGE y más), es la tercera carga útil de esta campaña, la cual, verifica los datos del portapapeles con una expresión regular, que coincide con los patrones de la billetera de criptomonedas. Si se encuentra,

Nro. Alerta:	EC-2022-012	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	24-enero-2022	**Microsoft PowerPoint: Archivos maliciosos son utilizados para enviar troyanos de acceso remoto**	V 1.0

reemplaza la dirección del destinatario con una bajo el control del actor.

VI. INDICADORES DE COMPROMISO

SHA256 (Phishing Email):
be453dcadd408fae5227f8b58f539f3f68aad081c9bf4f2c3dc0ff35c601ef5e

SHA256 (Infected PPAM File):
eff2feb50bebb797db7d881a44c549234315a84c861d2bb675899f7165db3ce7

SHA256 (Downloaded Script + VBS):
4674f942f3b1841744d81c6bb740879540a6514f57c54ecc443a2ea250a0c459
7a0da7d7bc7e60548bbac036b675c2a8df0869d37bdaf337d16dc93d5bd39da3

SHA256 (PowerShell files):
37bbddb8e25859349f18c619f863f151660d1ed688c05e0f4a06da942fa154ec
271028308b8a45535b865b0818f39c098e78506a36de57ffee0087c810a65cdb

SHA256 (Agent Tesla + .NET Injector):
38207b0af1ad9d0ce047ae8d3b3535921106609c1b4d640a83d1592bb06cf1e2
8915469cb570b038f78d1fcf97d4f132df89e08086a07231cd43da3c443a8016

Registry Keys:
HKCU\Microsoft\Windows\CurrentVersion\cjjhutyyaggw
HKCU\Microsoft\Windows\CurrentVersion\pilodkis

URLs:
hxxps://hahahahhasd@j[.]mp/kdwocqwqwqerheurfje
hxxps://download1507.mediafire[.]com/af0tbthsvewg/od8k8i5brx9cpof/19.doc
hxxps://8db3b91a-ea93-419b-b51b-0a69902759c5.usrfiles[.]com/ugd/8db3b9_e926d447972f4d23b3c2af4abee9467e.txt?dn=rendomtext
hxxps://8db3b91a-ea93-419b-b51b-0a69902759c5.usrfiles[.]com/ugd/8db3b9_92ec48660f134f3bb502662383ca4ffb.txt?dn=rendomtext
hxxps://kukadunikkk@kdaoskdokaodkwldld.blogspot[.]com/p/19.html
hxxp://www.starinxxxgkular.duckdns[.]org/s1/19.txt
hxxps://raw.githubusercontent[.]com/swagkarna/Bypass-Tamper-Protection/main/NSudo.exe
hxxps://www.mediafire[.]com/file/qh5j3uy8qo8cpu7/FINAL+MAIN+vbs+-+Copy.vbs/file

Nro. Alerta:	EC-2022-012	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	24-enero-2022	**Microsoft PowerPoint: Archivos maliciosos son utilizados para enviar troyanos de acceso remoto**	V 1.0

AgentTesla HTTP Request:
hxxp://103.147.185[.]68/j/p19xw/mawa/48608c2b91739edc3959.php

"Ladrón de criptomonedas" – Direcciones de billeteras electrónicas:

BTC:
3CghDNiD2J5xsS9i1wzwbvwdTJxokqGCmC

ETH:
0x8af86e2c7126d08387e71ec6699bc69f957cdee6

XMR:
83JYuoz9uBv1ny1iioYuK5GQDtyY3M5BL5Hi6NRovkLPMwiWs5QxmAREgsBpBAPDXND
EcJkfLewgLXEGHL8fKpyv7BdKmD8

XLM:
GDX6FFZUVSYTOV23NP2PUUGQIORTWQHUXXPXYOUIOY6CDQXG4NP6OEQ7

XRP:
rGT84ryubURwFMmiJChRbWUg9iQY18VGuQ

LTC:
LZApZozcKmD1JynSvXqSN8m115ZefbnYMK

DOGE:
DK4Bt1wDYMfqhbqo7jMMqFuEtfFXfvKFTa

VII. RECOMENDACIONES

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

- Evitar descargar y ejecutar archivos de tipo PPT, PPTX de Microsoft PowerPoint, que se adjunten en correos electrónicos no solicitados.
- 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 sean personales o Institucionales.

Nro. Alerta:	EC-2022-012	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	24-enero-2022	**Microsoft PowerPoint: Archivos maliciosos son utilizados para enviar troyanos de acceso remoto**	V 1.0

- Instalar y utilizar software antivirus de confianza.
- Escanear archivos de tipo PPT, PPTX de Microsoft PowerPoint, en un software antivirus, y, en el caso de necesitar ejecutarlos, mantener desactivada la ejecución de macros en su paquete informático de Microsoft Office.
- Mantener actualizado la suite de ofimática de Microsoft Office, aplicando las últimas actualizaciones y parches de seguridad disponibles.
- Mantener actualizado el sistema operativo de Microsoft Windows, aplicando las últimas actualizaciones y parches de seguridad disponibles.
- En el caso de sufrir un ataque de proporciones mayores, contacte a las Autoridades competentes en base a la Normativa a nivel Nacional.

VIII. REFERENCIAS:

Bill Toulas. (24 de enero de 2022). BleepingComputer. Obtenido de https://www.bleepingcomputer.com/news/security/malicious-powerpoint-files-used-to-push-remote-access-trojans/

NetskopeThreatLabs. (19 de enero de 2022). NetskopeThreatLabs. Obtenido de https://github.com/netskopeoss/NetskopeThreatLabsIOCs/tree/main/AgentTesla