Nro. Alerta:	AL-2024-033	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR ALERTAS DE SEGURIDAD	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	12-dic-2024	**CLICKFIX**	Pág.: **1** of **4**

I. DATOS GENERALES:

Clase de alerta: Incidente

Tipo de incidente: Malware

Nivel de riesgo: Medio

II. ALERTA

Se ha identificado una nueva amenaza llamada **ClickFix**, que utiliza tácticas avanzadas de ingeniería social para distribuir malware a través de páginas falsas de **Google Meet** y **Zoom**. Engaña a los usuarios simulando errores de dispositivos y los incita a ejecutar comandos maliciosos que descargan malware tipo **infostealer**, diseñado para robar información sensible. Esta técnica, vinculada a grupos avanzados como **APT28**, destaca por su capacidad de evadir defensas tradicionales, subrayando la necesidad de reforzar las estrategias de seguridad y detección en las organizaciones.

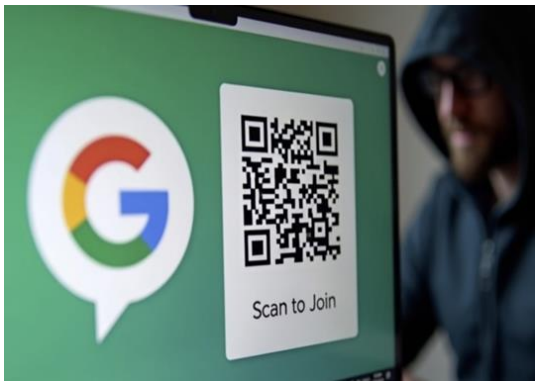

Figura 1.- *Ilustración asociada a ClickFix* ***Fuente: NDA***

III. INTRODUCCIÓN.

ClickFix es una táctica de ingeniería social que apareció por primera vez en mayo y que fue identificada por la firma de ciberseguridad Proofpoint.

Se trataría una acción de un actor de amenazas (TA571) que usaba mensajes que se hacían pasar por errores para Google Chrome, Microsoft Word y OneDrive.

Esta táctica consiste en mostrar mensajes de error falsos en los navegadores web para engañar a los usuarios para que copien y ejecuten un código PowerShell malicioso determinado, infectando finalmente los sistemas operativos.

IV. VECTOR DE ATAQUE.

En los últimos meses se ha informado ampliamente de variaciones de la campaña **ClickFix** (también conocida como **ClearFake y OneDrive Pastejacking**), en la que los actores de amenazas emplean diferentes señuelos para redirigir a los usuarios a **páginas falsas** que pretenden desplegar **malware** instando a los visitantes del sitio a ejecutar un código **PowerShell** codificado para solucionar un supuesto problema de visualización de contenidos en el navegador web.

V. INDICADORES DE COMPROMISO

Estas páginas son conocidas por hacerse pasar por servicios en línea populares, incluyendo Facebook, Google Chrome, PDFSimpli, y reCAPTCHA, y ahora Google Meet, así como potencialmente Zoom:

- meet.google.us-join[.]com
- meet.googie.com-join[.]us
- meet.google.com-join[.]us
- meet.google.web-join[.]com
- meet.google.webjoining[.]com
- meet.google.cdm-join[.]us
- meet.google.us07host[.]com
- googiedrivers[.]com
- us01web-zoom[.]us
- us002webzoom[.]us
- web05-zoom[.]us
- webroom-zoom[.]us

Más IoC se encuentran disponibles en el siguiente enlace:

https://github.com/SEKOIA-IO/Community/blob/main/IOCs/clickfix_fake_google_meet/clickfix_fake_google_meet_iocs_20241017.csv

VI. IMPACTO:

En **Windows**, la cadena de ataque culmina con el despliegue de los robos **StealC y Rhadamanthys**, mientras que los usuarios de **macOS** de Apple reciben un archivo de imagen de disco trampa (**"Launcher_v1.94.dmg"**) que deja caer otro robo conocido como **Atomic**.

Esta táctica de **ingeniería social** emergente destaca por el hecho de que elude hábilmente la detección por parte de las herramientas de seguridad, ya que implica que los usuarios ejecuten manualmente el comando **PowerShell malicioso** directamente en el terminal, en lugar de ser invocado automáticamente por un **payload** descargado y ejecutado por ellos.

Sekoia ha atribuido el clúster que suplanta la identidad de **Google Meet** a dos grupos de traficantes, a saber, **Slavic Nation Empire** (también conocido como Slavice Nation Land) y **Scamquerteo**, que son subequipos de markopolo y CryptoLove, respectivamente.

Esto, a su vez, ha planteado la posibilidad de que ambos grupos de amenazas estén haciendo uso del mismo servicio de ciberdelincuencia, aún desconocido, con un tercero probablemente gestionando su infraestructura.

La noticia se produce en medio de la aparición de campañas de **malware** que distribuyen el ladrón de código abierto **ThunderKitty**, que comparte similitudes con Skuld y Kematian Stealer, así como nuevas familias de ladrones denominadas Divulge, DedSec (también conocido como Doenerium), Duck, Vilsa y Yunit.

Los fallos provocan que la víctima copie en el portapapeles un fragmento de código de PowerShell que solventaría los problemas ejecutándolo en el símbolo del sistema de Windows.

Todo esto derivaría en que las víctimas infectan los sistemas con varios programas maliciosos, como pueden ser DarkGate, Matanbuchus, NetSupport, Amadey Loader, XMRig, un secuestrador de portapapeles y Lumma Stealer.

VII. RECOMENDACIONES:

- Evitar abrir enlaces sin autenticación para reuniones virtuales, ya que podrían estar cargadas con tácticas emergentes de ingeniería social que pueden ser utilizadas para distribuir ampliamente malware a través de campañas de phishing por correo electrónico, sitios web comprometidos e infraestructuras de distribución.
- La táctica de ClickFix engaña a los usuarios para que descarguen y ejecuten malware en sus máquinas sin necesidad de utilizar un navegador web para la descarga ni requerir la ejecución manual del archivo.
- Verificar campañas dirigidas a organizaciones que utilizan Google Workspace, especialmente Google Meet.
- Aplicar lo antes posible las actualizaciones mencionadas para mitigar los riesgos potenciales.
- Monitorear los sistemas para detectar cualquier actividad sospechosa posterior a la actualización.

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:

- https://a3sec.com/alertas/clickfix-aprovecha-las-paginas-de-gmeet-y-zoom-para-distribuir-malware-de-robo-de-informacion
- https://www.escudodigital.com/ciberseguridad/paginas-falsas-conferencias-google-meet-entregar-malware_60887_102.html
- https://enhacke.com/blog/falsas-paginas-de-google-meet-distribuyen-malware-en-campana-de-clickfix-6712701bee86e
- https://blog.sekoia.io/clickfix-tactic-the-phantom-meet/
- https://github.com/SEKOIA-IO/Community/blob/main/IOCs/clickfix_fake_google_meet/clickfix_fake_google_meet_iocs_20241017.csv