PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Asociación de Bancos del Perú

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

241-2024-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aéreadel Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y lasempresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°241	Fecha: 18-10-2024 Página: 4 de 6

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Ataque ClickFix: alertas falsas de Google Meet instalan malware en Windows y macOS		
Tipo de Ataque	Malware		Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

Una nueva campaña de ClickFix está atrayendo a los usuarios a páginas de conferencias fraudulentas de Google Meet que muestran errores de conectividad falsos que envían malware que roba información para los sistemas operativos Windows y macOS.

ClickFix es una táctica de ingeniería social que surgió en mayo, reportada por primera vez por la empresa de ciberseguridad Proofpoint, por un actor de amenazas (TA571) que usaba mensajes que se hacían pasar por errores de Google Chrome, Microsoft Word y OneDrive.

2. DETALLES:

Los investigadores de Sekoia han detectado un aumento de los ciberataques dirigidos contra los usuarios de la popular plataforma de videoconferencias Google Meet, que emplean una táctica conocida como "ClickFix".

Los atacantes muestran mensajes de error falsos que imitan alertas legítimas de Google Meet y piden a los usuarios que hagan clic en el botón "Resolver" o que realicen otras acciones. Sin embargo, estas acciones ejecutan sin saberlo código malicioso que instala malware en el dispositivo de la víctima.

Para los usuarios de Windows, el mensaje de error falso afirmaba que había problemas con el micrófono o los auriculares.

Si hacen clic en "Probar solución", se inicia un proceso de infección estándar de ClickFix en el que el código de PowerShell copiado por el sitio web y pegado en el indicador de Windows infecta su computadora con malware, obteniendo la carga útil del dominio 'googiedrivers[.]com'. De esta manera se descargaba los robadores de información Stealc y Rhadamanthys.

Los usuarios de macOS fueron engañados para que descargaran el malware AMOS Stealer como un archivo .DMG (imagen de disco de Apple) llamado 'Launcher_v194'.

También incluyen programas maliciosos como DarkGate, Matanbuchus, NetSupport, Amadey Loader, XMRig, etc.

Algunas de las campañas más recientes están a cargo de dos grupos de amenazas, Slavic Nation Empire (SNE) y Scamquerteo, considerados subequipos de las bandas de estafadores de criptomonedas Marko Polo y CryptoLove.

El malware distribuido a través de estos ataques incluye ladrones de información, botnets y herramientas de acceso remoto. Estos programas maliciosos pueden robar datos confidenciales, comprometer sistemas y permitir nuevos ataques.

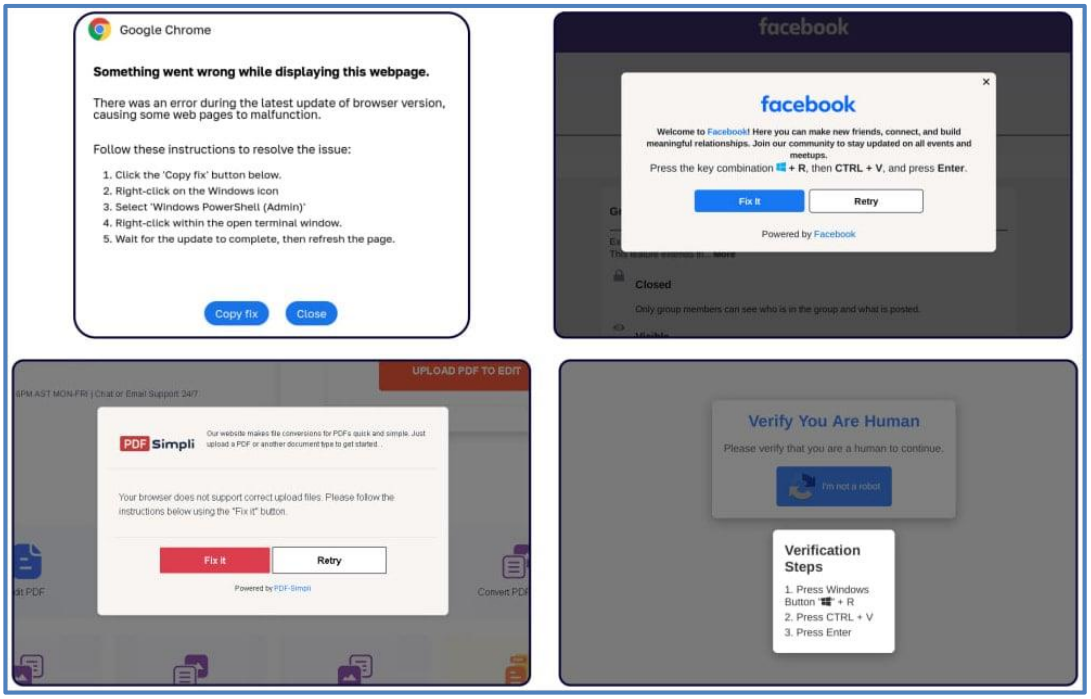
La táctica de ClickFix es particularmente peligrosa porque elude las medidas de seguridad tradicionales. Al no requerir que los usuarios descarguen un archivo directamente, evita que las funciones de seguridad del navegador web lo detecten, lo que aumenta la probabilidad de atrapar a víctimas desprevenidas.

Las URLs falsas se parecen mucho a los enlaces reales de Google Meet:

- 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

Sekoia ha identificado varios otros clústeres de distribución de malware además de Google Meet, incluidos Zoom, lectores de PDF, videojuegos falsos (Lunacy, Calipso, Battleforge, Ragon), navegadores y proyectos web3 (NGT Studio) y aplicaciones de mensajería (Nortex).



3. RECOMENDACIONES:

- Evitar abrir archivos adjuntos o enlaces sospechosos en correos electrónicos no solicitados o mensajes de redes sociales. Igualmente, verificar los scripts antes de copiarlos y pegarlos desde fuentes oficiales.
- Utilizar un software antimalware confiable en sus dispositivos y mantenerlos actualizados. Estos programas pueden detectar y eliminar ransomware y otro software malicioso antes de que puedan cifrar sus archivos.
- Mantener su sistema operativo, software antimalware y de seguridad, y todas las aplicaciones actualizadas con los últimos parches y actualizaciones de seguridad.
- Habilitar la autenticación de dos factores cuando esté disponible.
- Implementar el principio del privilegio mínimo para minimizar el impacto potencial de las infecciones
- Educar a los usuarios sobre las amenazas de ransomware y cómo reconocer los intentos de phishing.

Fuente de Información:	• hxxps://hackread.com/clickfix-fake-google-meet-alerts-windows-macos-malware/ • hxxps://thehackernews.com/2024/10/beware-fake-google-meet-pages-deliver.html • hxxps://www.bleepingcomputer.com/news/security/fake-google-meet-conference-errors-push-infostealing-malware/

Índice alfabético