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

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Lima, 19 de abril de 2021

N° 092-2021-PECERT

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 Aérea del Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros, en el marco del Centro Nacional de Seguridad Digital.

El objetivo de esta Alerta **es informar a los responsables de la Seguridad de la Información de las entidades públicas y las empresas privadas sobre las amenazas en el ciberespacio** 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. **Esta información no ha sido preparada ni dirigida a ciudadanos.**

Contenido

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 092**	**Fecha: 19-04-2021**
		Página: 3 de 8

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**			
Nombre de la alerta	Nueva campaña de malware introduce código malicioso en los chips M1 de Apple			
Tipo de ataque	Malware		Abreviatura	Malware
Medios de propagación	USB, disco, red, correo, navegación de internet			
Código de familia	C	Código de subfamilia	C03	
Clasificación temática familia	Código malicioso			

Descripción

1. Resumen:

   Los Investigadores de la compañía de ciberseguridad de Trend micro y Kaspersky han identificado una nueva campaña de malware dirigida a los desarrolladores de "Xcode" para agregar código en los chips M1 de Apple y expandir sus funciones, con la finalidad de extraer información confidencial de aplicaciones. Una muestra que XCSSET continúa abusando de la versión de desarrollo del navegador Safari para instalar puertas traseras de JavaScript en sitios web a través de ataques de Universal Cross-site Scripting (UXSS). La campaña se encuentra activa y también los atacantes están adaptando activamente sus ejecutables y transfiriéndolos para que se ejecuten en los nuevos Apple Silicon Macs de forma nativa.

2. Detalles:

   XCSSET se convirtió en el centro de atención en agosto de 2020 después de que se descubrió que se propagaba a través de proyectos IDE de Xcode modificados que se configuraron para ejecutar la carga útil. El malware vuelve a empaquetar los módulos de carga útil para imitar las aplicaciones legítimas de Mac, que son en última instancia responsables de infectar los proyectos locales de Xcode e inyectar la carga útil principal para que se ejecute cuando se compile el proyecto comprometido.

   Los módulos XCSSET vienen con la capacidad de robar credenciales, capturas de pantalla, inyectar JavaScript malicioso en sitios web, saquear datos de usuarios de diferentes aplicaciones e incluso cifrar archivos para obtener un rescate.

   Luego, los investigadores de Kaspersky descubrieron muestras XCSSET compiladas para los nuevos chips Apple M1, lo que sugiere que la campaña de malware no solo estaba en curso, sino que también los adversarios están adaptando activamente sus ejecutables y transfiriéndolos para que se ejecuten en los nuevos Apple Silicon Macs de forma nativa.

   La última investigación de Trend Micro muestra que XCSSET continúa abusando de la versión de desarrollo del navegador Safari para instalar puertas traseras de JavaScript en sitios web a través de ataques de Universal Cross-site Scripting (UXSS).

   Los investigadores de Trend Micro en un análisis publicado indica que "Aloja los paquetes de actualización de Safari en el servidor [de comando y control], luego descarga e instala los paquetes para la versión del sistema operativo del usuario", También, indica que Para adaptarse al recién lanzado Big Sur, se agregaron nuevos paquetes para 'Safari 14'.

   Además de troyanizar Safari para extraer datos, el malware también es conocido por explotar el modo de depuración remota en otros navegadores como Google Chrome, Brave, Microsoft Edge, Mozilla Firefox, Opera, Qihoo 360 Browser y Yandex Browser para llevar a cabo ataques UXSS.

   Asimismo, el malware ahora intenta robar información de la cuenta de varios sitios web, incluidas las plataformas de comercio de criptomonedas Huobi, Binance, NNCall.net, Envato y 163.com, con capacidades para reemplazar la dirección en la billetera de criptomonedas de un usuario con las que están bajo el control del atacante.

   El modo de distribución de XCSSET a través de proyectos Xcode manipulados representa una seria amenaza, ya que los desarrolladores afectados que comparten sin saberlo su trabajo en GitHub podrían transmitir el malware a sus usuarios en forma de proyectos Xcode comprometidos, lo que lleva a "un ataque similar a una cadena de suministro para los usuarios que confían en estos repositorios como dependencias en sus propios proyectos "

3. Indicadores de compromiso (IoC):

   Ver IoC aquí: [hxxps://www.trendmicro.com/en_us/research/21/d/xcsset-quickly-adapts-to-macos-11-and-m1-based-macs.html]

4. Solución:
   - No descargar ningún archivo adjunto y analizarlo previamente con el antivirus.
   - Revisar que el enlace coincide con la dirección a la que apunta.
   - Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.
   - Bloquear los indicadores de compromisos (IOC) mostrados, en los dispositivos de seguridad de su infraestructura.

Fuentes de información	▪ hxxps://www.trendmicro.com/en_us/research/21/d/xcsset-quickly-adapts-to-macos-11-and-m1-based-macs.html ▪ hxxps://thehackernews.com/2021/04/malware-spreads-via-xcode-projects-now.html

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 092**	**Fecha: 19-04-2021**
		Página: 5 de 8

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**			
Nombre de la alerta	Vulnerabilidad de escalamiento de privilegios en VMWare NSX-T			
Tipo de ataque	Explotación de vulnerabilidades conocidas		Abreviatura	EVC
Medios de propagación	Red, internet			
Código de familia	H	Código de subfamilia	H01	
Clasificación temática familia	Intento de intrusión			

Descripción

1. Resumen:

   Los investigadores de la compañía de software de virtualización de VMWare ha reportado una vulnerabilidad de severidad ALTA de tipo escalamiento de privilegios afecta a los productos de VMWare NSX-T. La explotación exitosa de estas vulnerabilidades podría permitir a los atacantes con una cuenta de usuario invitado local asignar privilegios superiores a su propio nivel de permiso.

2. Detalles:

   La vulnerabilidad (CVE-2021-21981) existe debido a un problema con la asignación de roles de RBAC (control de acceso basado en roles). La explotación exitosa de este problema puede permitir a los atacantes con una cuenta de usuario invitado local asignar privilegios superiores a su propio nivel de permiso. Además, para que el atacante pueda aprovechar esta vulnerabilidad, el administrador de NSX Enterprise debe activar la cuenta de usuario invitado local. No está activado por defecto.

3. Productos afectados:

   VMWare NSX-T versión 3.1.1

4. Solución:

   VMWare recomienda actualizar su producto VMWare NSX-T a la versión 3.1.2

Fuentes de información	hxxps://www.vmware.com/security/advisories/VMSA-2021-0006.html

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 092	Fecha: 19-04-2021
		Página: 6 de 8

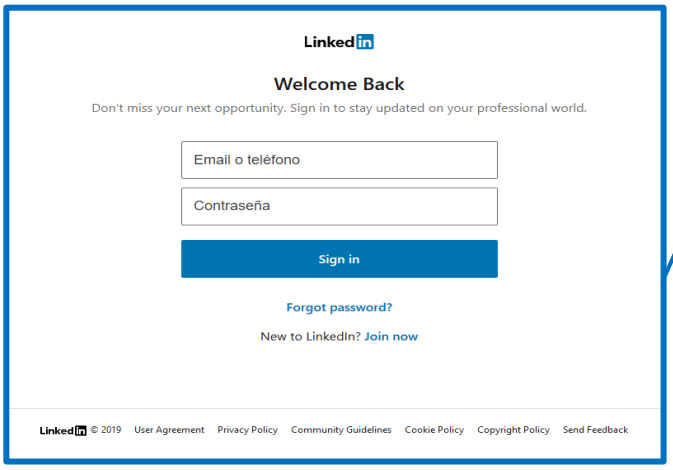
Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**			
Nombre de la alerta	Phishing, suplantando la identidad de la red social Linkedin			
Tipo de ataque	Phishing		Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros			
Código de familia	G	Código de subfamilia	G02	
Clasificación temática familia	Fraude			

Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo una campaña de phishing, a través de los diferentes navegadores web, el cual vienen suplantando la identidad de la red social Linkedin, con la finalidad obtener información de email y contraseña de las posibles víctimas.

2. Detalles del proceso de estafa de phishing.

1



Sitio web fraudulento donde suplanta la identidad de la red social Linkedin, el cual solicita a la posible víctima ingresar la dirección de su correo electrónico y contraseña.

2

Una vez ingresado un correo electrónico y contraseña, direcciona a una ventana indicando **"PÁGINA NO ENCONTRADA".** Dando por terminada la estafa.

3. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo la siguiente información:
   - Dominio: temperoalternativo.com.br
   - Talla: 57B
   - Dirección IP De Servicio: 104.21.6.123
   - Puntuación de amenaza: 85/100
   - URL: hXXp://temperoalternativo[.]com[.]br/of/linkedin_/

- Sitio Web catalogado como PELIGROSO.

4. Cómo funciona el phishing:
   - Los correos electrónicos incluyen enlaces a sitios web preparados por los ciberdelincuentes en los que solicitan información personal.
   - Medios de propagación del phishing: WhatsApp, telegram, redes sociales, SMS entre otros.
   - Los ciberdelincuentes intentan suplantar a una entidad legitima (organismo público, entidad financiera, servicio técnico, etc.).
5. Referencia:

   Phishing o suplantación de identidad: Es un método que los ciberdelincuentes utilizan para engañar a los usuarios y conseguir que se revele información personal, como contraseñas, datos de tarjetas de crédito o de la seguridad social y números de cuentas bancarias, entre otros.
6. Recomendaciones
   - Verifica la información en los sitios web oficiales.
   - No introduzcas datos personales en páginas sospechosas.
   - Siempre ten presente que los ciberdelincuentes, quieren obtener siempre tus datos personales.

Fuentes de información	Análisis propio de redes sociales y fuente abierta

Índice alfabético