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

Siempre con el pueblo

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc

Lima, 30 de julio de 2022

N° 205-2022-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 Aérea del 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 las empresas 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

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 205	Fecha: 30-07-2022
		Página 04 de 07

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Mas de una docena de aplicaciones de Android en Google Play Store lanzan malware		
Tipo de ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegacion de Internet		
Código de familia	C	Código de Subfamilia	C02
Clasificación temática familia	Código Malicioso		

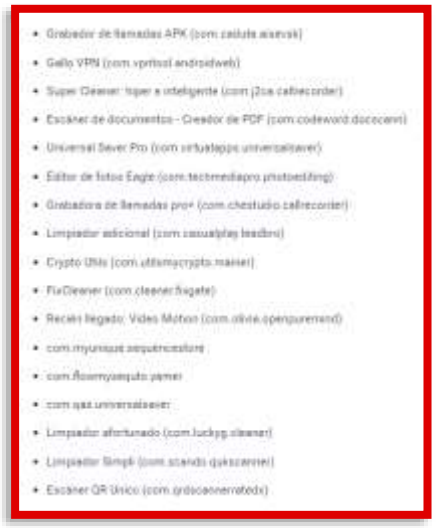
Descripción

FECHA DEL EVENTO:

A través del monitoreo y búsqueda de amenazas en el ciberespacio del día 30 de julio del 2022, se tomó conocimiento a través de la publicación realizada en la página web de **"THE HACKER NEWS"**, sobre una campaña malintencionada que aprovechó las aparentemente inocuas aplicaciones de cuentagotas de Android en Google Play Store para comprometer los dispositivos de los usuarios con malware bancario.

ANTECEDENTES:

Estas 17 aplicaciones cuentagotas, denominadas colectivamente DawDropper por Trend Micro, se hacen pasar por aplicaciones de productividad y utilidades, como escáneres de documentos, lectores de códigos QR, servicios de VPN y grabadoras de llamadas, entre otras.



DETALLES:

"DawDropper utiliza Firebase Realtime Database, un servicio en la nube de terceros, para evadir la detección y obtener dinámicamente una dirección de descarga de carga útil", dijeron los investigadores "También alberga cargas útiles maliciosas en GitHub".

Los droppers son aplicaciones diseñadas para evadir los controles de seguridad de Play Store de Google, luego de lo cual se utilizan para descargar malware más potente e intrusivo en un dispositivo, en este caso, Octo (Coper), Hydra , Ermac y TeaBot .

Las cadenas de ataque involucraron al malware DawDropper estableciendo conexiones con una base de datos en tiempo real de Firebase para recibir la URL de GitHub necesaria para descargar el archivo APK malicioso. La lista de aplicaciones maliciosas se encuentra en la imagen. Entre los cuentagotas se incluye una aplicación llamada "Unicc QR Scanner" que Zscaler marcó anteriormente a principios de este mes como distribuidora del troyano bancario Coper, una variante del malware móvil Exobot.

También se sabe que Octo deshabilita Google Play Protect y usa la computación de red virtual (VNC) para grabar la pantalla del dispositivo de la víctima, incluida información confidencial como credenciales bancarias, direcciones de correo electrónico y contraseñas, y PIN, todo lo cual se extrae posteriormente a un servidor remoto. .

Los droppers bancarios, por su parte, han evolucionado desde principios de año, pasando de las direcciones de descarga de carga útil codificadas a usar un intermediario para ocultar la dirección que aloja el malware.

"Los ciberdelincuentes encuentran constantemente formas de evadir la detección e infectar tantos dispositivos como sea posible", dijeron los investigadores. "Además, debido a que existe una gran demanda de formas novedosas de distribuir malware móvil, varios actores maliciosos afirman que sus droppers podrían ayudar a otros ciberdelincuentes a difundir su malware en Google Play Store, lo que resulta en un modelo dropper-as-a-service (DaaS). ."

RECOMENDACIONES

- Si instaló alguna de estas aplicaciones deberá desinstalarlas de su dispositivo manualmente y ejecutar un escaneo AV para limpiar cualquier remanente o restablecer a configuración de fábrica su dispositivo.
- Asegúrese de que Play Protect esté activo en su dispositivo y supervise regularmente sus datos de Internet y el consumo de batería para identificar cualquier proceso sospechoso que se ejecute en segundo plano.
- Verificar las reseñas y calificaciones de las aplicaciones antes de descargarlos y visitar el sitio web del desarrollador, leer la política de privacidad y prestar atención a los permisos solicitados durante la instalación.

Fuentes de información	▪ https://thehackernews.com/2022/07/over-dozen-android-apps-on-google-play.html

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 205	Fecha: 30-07-2022
		Página 05 de 07

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de Alerta	Phishing, suplantando la identidad de la empresa de entretenimiento y plataforma de Streaming Netflix.		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medio 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 se vienen llevando a cabo una campaña de Phishing, quienes vienen suplantando la identidad de la empresa de entretenimiento y plataforma de Streaming Netflix, el supuesto sitio web cuenta con logos característicos al oficial, el cual tiene como finalidad robar sus credenciales de acceso.

2. Detalles del proceso de estafa de Phishing.

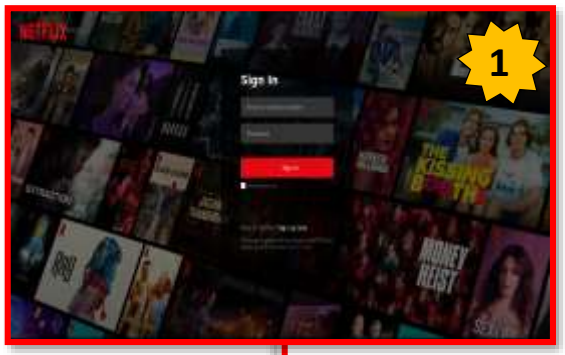


Imagen 1: Sitio web fraudulento, donde solicita acceder a la plataforma a través de las credenciales de inicio de sesión (correo electrónico y contraseña).

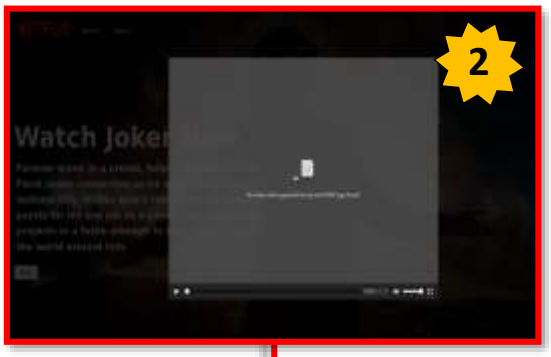


Imagen 2: Una vez ingresado las credenciales de acceso redirige a una ventana en donde los botones se encuentran inoperativos.

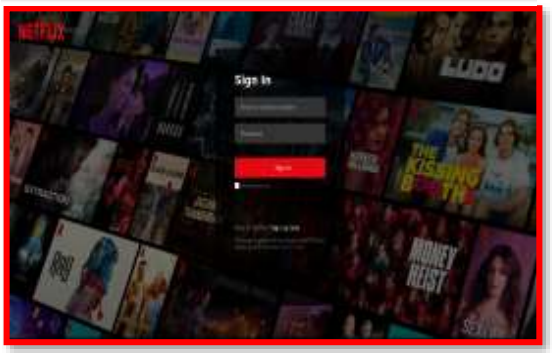
3. Comparación del sitio web oficial de la plataforma de Streaming Netflix con el fraudulento:

SITIO WEB OFICIAL

URL: https://www.netflix.com/pe/Login

SITIO WEB FRAUDULENTO

URL: hxxps://dhanushr24[.]github[.]io/clone-Netflix/SignIn[.]html

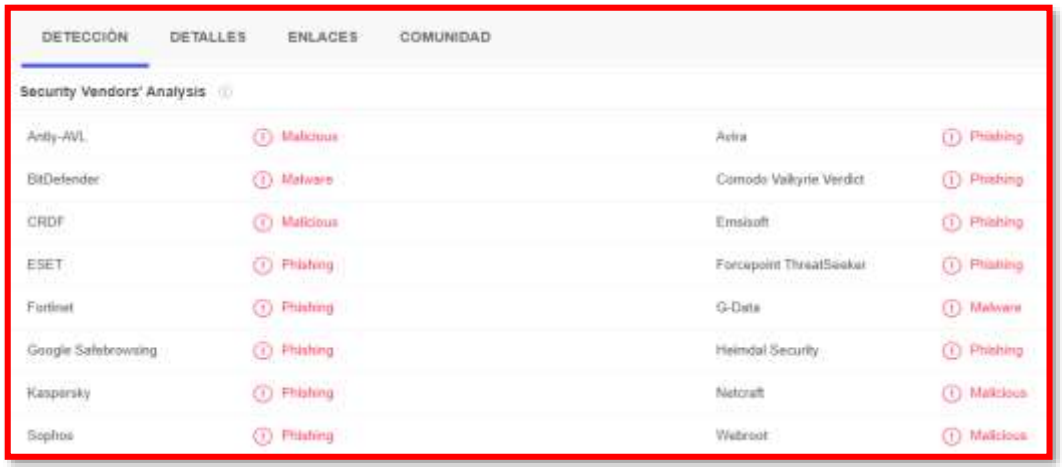


- Existe similitud entre ambas páginas, en imagen, fondo y escritura la diferencia se encuentra en la URL.
- La URL falsa utiliza protocolo HTTPS, no significa que la web sea segura.
- El dominio (dhanushr24.github.io) del sitio web fraudulento se encuentra reportado como **PHISHING.**
- La URL falsa está mal escrita y los caracteres ambiguos.

4. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD:**

- **INDICADORES DE COMPROMISO:**

  - ✓ **URL:** hxxps://dhanushr24[.]github[.]io/clone-Netflix/SignIn[.]html
  - ✓ **Dominio:** dhanushr24[.]github[.]io
  - ✓ **IP:** 185.199.110.153
  - ✓ **Código:** 404
  - ✓ **Longitud:** 9.12 KB
  - ✓ **SHA-256**: 8128383991e20e0e30d70995434cad51e6b59d013c5f91b9475eeebd75442eb5



- **OTRAS DETECCIONES:**

5. **Apreciación de la información**

- Netflix es un servicio de Streaming 'transmisión' de vídeo a través de Internet que permite ver una amplia variedad de series, películas, documentales y películas en cualquier dispositivo con acceso a internet; mediante el pago de una tarifa fija mensual.

6. **Algunas Recomendaciones**

- No abrir correos ni mensajes de dudosa procedencia.
- Ser escépticos (desconfiado) frente ofertas, promociones o premios increíbles que se ofrecen por internet.
- Prestar atención en los detalles de los mensajes o redes sociales.
- No introducir datos confidenciales en sitios web sospechosas o de dudosa procedencia.
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
- Visualizar los sitios web que se ingresen sean los oficiales.

Fuentes de información	▪ Análisis propio de redes sociales y fuente abierta

Índice alfabético