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, 26 de setiembre de 2022

N° 263-2022-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

Centro Nacional de Seguridad Digital	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 263**	**Fecha: 26-09-2022**
		Página 04 de 10

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Grupo Guacamaya filtra miles de documentos confidenciales de las Fuerzas Armadas en Latinoamérica		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red no Indexada (Dark/Deep web)		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Filtración y Exposición de Datos Sensibles de institución pública		

Descripción

El grupo hacktivista "Guacamaya" es considerado responsable de filtrar alrededor de 10 TB de correos electrónicos de instituciones de la fuerza del orden en distintos países de Latinoamérica. Hasta el momento solo se han publicado los correos electrónicos de las Fuerzas Armadas de Chile; sin embargo, el grupo indicó que próximamente estarán filtrando la información del resto de países objetivo.

ANTECEDENTES:

- En marzo del presente año, el grupo Guacamaya publicó 4.2 TB de información (archivos y correos electrónicos) de subsidiarias mineras de un grupo de inversión suizo, que detalla la aparente contaminación por parte de las empresas mineras a Guatemala.
- En agosto también publicaron más de 2 TB de correos electrónicos y archivos de una gran cantidad de empresas mineras y petroleras de Latinoamérica, aparentemente con la intención de resaltar el daño ambiental en la región. Los documentos filtrados procedían de la Empresa Nacional de Minería (ENAMI) en Ecuador, Agencia Nacional de Hidrocarburos (ANH) en Colombia, Corporación de Energía Nueva Granada en Colombia, empresa minera Quiborax en Chile, empresa petrolera Orix en Venezuela, empresa minera Tezucana en Brasil, y el Ministerio de Medio Ambiente y Recursos Naturales de Guatemala.

DETALLES:

- El pasado 19 de setiembre, el grupo Guacamaya filtró 366 GB de información (400 mil correos electrónicos aproximadamente) del Estado Mayor Conjunto de las Fuerza Armadas de Chile (EMCO). La operación denominada "Fuerzas Represivas" corresponde a una serie de ataques a fuerzas policiales y militares en Latinoamérica.
- Según CyberScope, esta filtración de datos es la última acción de Guacamaya, un grupo enfocado en infiltrarse en empresas mineras y petroleras, fuerzas del orden y diversas agencias reguladoras latinoamericanas desde marzo del 2022. Guacamaya sigue un patrón de apuntar a instituciones que, según el grupo hacktivista, son responsables de la degradación ambiental del área y la supresión de las poblaciones nativas.

- En el comunicado oficial del grupo Guacamaya, mencionan también a Perú como parte de la filtración masiva de información de las Fuerzas Militares. “Filtramos sistemas militares y policiales de México, Perú, Salvador, Chile, Colombia y entregamos esto a quienes legítimamente hagan lo que puedan con estas informaciones”.
-

Otros

- Policía Nacional Civil de El Salvador (4 TB, @pnc.gob.sv)
- Comando General de las Fuerzas Militares de Colombia (275 GB, @cgfm.mil.co)
- Fuerza Armada de El Salvador (50 GB, @faes.gob.sv)
- Comando Conjunto de las Fuerzas Armadas de Peru (35 GB, @ccffaa.mil.pe)
- Ejercito del Peru (70 GB, @ejercito.mil.pe)

- La raíz de esta filtración de información fue la explotación de la vulnerabilidad “ProxyShell”, cuyo objetivo es acceder a los servidores Microsoft Exchange de las organizaciones. Los atacantes crean “Webshells” (backdoors) en los servidores no parchados para el acceso.
- En agosto, Microsoft Exchange lanzó un anuncio con los detalles de las vulnerabilidades asociadas a ProxyShell. ProxyShell es el nombre que se le ha dado a la ejecución de una serie de vulnerabilidades en la plataforma Microsoft Exchange, que, al ser encadenadas, permiten la ejecución remota de código en el servidor. Las vulnerabilidades fueron asignadas como:

CVE-ID	Nombre	Parche
CVE-2021-34473	Pre-auth Path Confusion leads to ACL Bypass	KB5001779 – Abril 2021
CVE-2021-34523	Elevation of Privilege on Exchange PowerShell Backend	KB5001779 – Abril 2021
CVE-2021-31207	Post-auth Arbitrary-File-Write leads to RCE	KB5003435 – Mayo 2021
CVE-2021-31206	Microsoft Exchange Server Remote Code Execution Vulnerability	KB5004780 – Julio 2021

- Las versiones vulnerables son:
    - Microsoft Exchange Server 2019
    - Microsoft Exchange Server 2016
    - Microsoft Exchange Server 2013
- Distintos investigadores indican que ProxyShell podría ser el sucesor de "ProxyLogon", otra vulnerabilidad crítica que terminó siendo ampliamente explotada tanto por ciberdelincuentes con fines de lucro (como grupos de ransomware, malware y ciberespionaje, entre otros) como por actores de amenaza patrocinados por un estado.
- Asimismo, se tiene una vulnerabilidad de ProxyLogon, asignada como:

CVE-ID	Nombre	Parche
CVE-2021-26855	Microsoft Exchange Server Remote Code Execution Vulnerability	KB500871 – Marzo 2021

- Según CronUp, Latinoamérica cuenta con más de 4,400 servidores Microsoft Exchange expuestos a Internet, siendo Perú el sexto en la lista con 214 servidores.

- En dicho anuncio, Microsoft dio una serie de recomendaciones, entre ellas, instalar los parches de seguridad para cada vulnerabilidad asociada a ProxyShell.
    - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34473
    - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34523
    - https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-31207
    - https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-31206

- A continuación, se brinda el parche de seguridad para la vulnerabilidad asociada a ProxyLogon.
    - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855

RECOMENDACIONES:

- Instalar los parches de seguridad de Microsoft Exchange Server.
- Mantener actualizado el software de su infraestructura.
- Contar con un SIEM para poder monitorear los servicios de su infraestructura en tiempo real.
- Realizar un análisis de malware y un análisis de seguridad para determinar si los servidores de Exchange ya se han visto comprometidos.

Fuentes de información	▪ hxxps://enlacehacktivista.org/index.php?title=Fuerzas_Represivas ▪ hxxps://nationworldnews.com/who-is-behind-guacamaya-the-group-of-hackers-who-claimed-to-have-attacked-the-joint-chiefs-of-staff-nation-world-news/ ▪ hxxps://www.cronup.com/proxyshell-el-nuevo-rce-en-microsoft-exchange-version-latam/ ▪ hxxps://techcommunity.microsoft.com/t5/exchange-team-blog/proxyshell-vulnerabilities-and-your-exchange-server/ba-p/2684705 ▪ Análisis propio de fuentes abiertas.

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 263	Fecha: 26-09-2022
		Página 08 de 10

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Nueva campaña de phishing suplantando la identidad de la red social Instagram		
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 suplantando la identidad de la red social Instagram, con el objetivo robar credenciales de acceso de inicio de sesión.

2. Proceso del ataque phishing.

<u>Imagen 1:</u> Solicita ingresar las credenciales de inicio de sesión, como número de teléfono o dirección de correo electrónico y contraseña de la cuenta.

<u>Imagen 2:</u> Al hacer clic en iniciar sesión es redirigido automáticamente a un supuesto perfil de Instagram; sin embargo, los ciberdelincuentes capturaron las credenciales de acceso.

<u>Imagen 3</u>: Al cabo de 10 segundos, muestra el sitio web oficial de Instagram, solicitando nuevamente ingresar las credenciales de inicio de sesión.

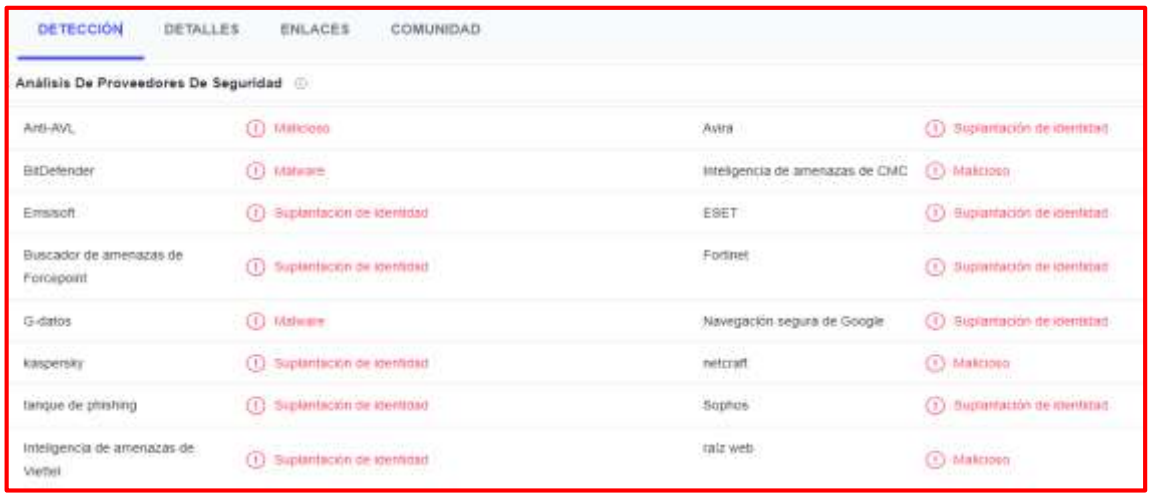
3. Comparación del sitio web oficial de Instagram y sitio web fraudulento:

SITIO WEB OFICIAL	**SITIO WEB FRAUDULENTO**
https://www.instagram.com	hxxps://yairix[.]github[.]io/Login-Instagram

- Existe una similitud entre el fondo y la forma de cada sitio web.
- Ambas URL´s utilizan el protocolo https, lo que hace más convincente a que las víctimas accedan al sitio web.
- La diferencia está en la URL, toda vez que el dominio del sitio web es fraudulento, no coincide con el oficial.

4. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo la siguiente información:

- **URL** : hxxps://yairix[.]github[.]io/Login-Instagram
- **Dominio :** yairix[.]github[.]io
- **IP** : 185[.]199[.]111[.]153
- **Tamaño** : 6.23 KB
- **SHA-256 :** bed3e83da2db4effa6e022893ab99732c88f8cc3d4b36fbc4d726320c3be3d0a



DETECCIÓN | DETALLES | ENLACES | COMUNIDAD

Análisis De Proveedores De Seguridad

Anti-AVL	Malicioso	Avira	Suplantación de identidad
BitDefender	Malware	Inteligencia de amenazas de CMC	Malicioso
Emsisoft	Suplantación de identidad	ESET	Suplantación de identidad
Buscador de amenazas de Forcepoint	Suplantación de identidad	Fortinet	Suplantación de identidad
G-datos	Malware	Navegación segura de Google	Suplantación de identidad
kaspersky	Suplantación de identidad	netcraft	Malicioso
tanque de phishing	Suplantación de identidad	Sophos	Suplantación de identidad
Inteligencia de amenazas de Viettel	Suplantación de identidad	raiz web	Malicioso

5. Algunas Recomendaciones:

- Acceder al sitio web a través de fuentes oficiales.
- Evitar responder a mensajes enviados desde (correo electrónico, Whatsapp, SMS y otros), que contengan enlaces de dudosa procedencia.
- Verificar detenidamente la redacción y ortografía de la dirección URL, que coincidan con el sitio web oficial.
- Evitar compartir la información con terceras personas, amigos o familiares.
- Utilizar una firma de antivirus actualizado, ya que es la primera barrera ante posibles ataques cibernéticos.

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

Índice alfabético