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, 22 de setiembre de 2022

N° 259-2022-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° 259	Fecha: 22-09-2022
		Página 04 de 10

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Vulnerabilidad de 15 años sin parche en Python		
Tipo de ataque	Explotación de vulnerabilidades	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

En una publicación de setiembre por BleepingComputer, se reveló que una vulnerabilidad en el lenguaje de programación Python, revelado en 2007, no cuenta con un parche hasta la fecha. Este fallo probablemente esté afectando a miles de repositorios conduciendo a la ejecución de código arbitrario.

ANTECEDENTES:

- Python es un lenguaje de programación, sencillo de leer y escribir debido a su alta similitud con el lenguaje humano. Ha ganado popularidad en los últimos años debido a lo fácil que puede ser aprenderlo; sin embargo, ni siquiera los lenguajes de programación pueden estar exentos de los fallos de seguridad, como ha ocurrido con Python.
- Revelado en 2007 y etiquetado como CVE-2007-4559, el problema de seguridad nunca recibió un parche, la única mitigación proporcionada fue una actualización de la documentación que advertía a los desarrolladores sobre el riesgo.

DETALLES:

- Según BleepingComputer, la vulnerabilidad se encuentra en el paquete *tarfile* de Python, en el código que utiliza la función *tarfile.extract()* no desinfectada o en los valores predeterminados integrados de *tarfile.extractall()*. Es un error de path traversal que permite a un atacante sobrescribir archivos de forma arbitraria.

- Los detalles técnicos de CVE-2007-4559 han estado disponibles desde el informe inicial lanzado agosto de 2007. Si bien no hay informes sobre el aprovechamiento del error en los ataques, representa un riesgo en la cadena de suministro del software.
- Una semana después de su descubrimiento, en 2007, un mensaje de Python anunció que el problema estaba solucionado; sin embargo, la solución solo fue actualizar la documentación con una advertencia: “Podría ser peligroso extraer archivos de fuentes no confiables".

- Desde su descubrimiento, este fallo fue analizado por diferentes investigadores de ciberseguridad, que pese a encontrar el informe donde se anunciaba este error, no encontraron la posible solución. Por lo que se pusieron a trabajar para detectar miles de proyectos de software, de código abierto o cerrado.
- A comienzos del presente año, un investigador de "Trellix" redescubrió esta vulnerabilidad y recientemente, dicha empresa de ciberseguridad descubrió los pasos simples para explotar CVE-2007-4559 en la versión de Windows de Spyder IDE, un entorno de desarrollo integrado multiplataforma de código abierto para programación científica.
- Los investigadores demostraron que la vulnerabilidad también se puede aprovechar en Linux. Lograron escalar la escritura de archivos y la ejecución del código en el producto Polemarch.
- Además de llamar la atención sobre la vulnerabilidad y el riesgo que representa, Trellix también creó parches para 11,000 proyectos aproximadamente. Las correcciones estarán disponibles en un *branch* del repositorio afectado y se agregarán al proyecto principal a través un *pull*.
- Debido a la gran cantidad de repositorios afectados, los investigadores esperan que más de 70.000 proyectos reciban una solución en las próximas semanas.

RECOMENDACIONES:

- Contar con estrictos controles de seguridad.
- Utilizar la metodología de desarrollo seguro.
- Mantener actualizado el software.
- Concientizar sobre las vulnerabilidades que pueda tener un lenguaje de programación.

Fuentes de información	▪ hxxps://www.bleepingcomputer.com/news/security/unpatched-15-year-old-python-bug-allows-code-execution-in-350k-projects/ ▪ hxxps://www.trellix.com/en-us/about/newsroom/stories/threat-labs/tarfile-exploiting-the-world.html ▪ hxxps://blog.segu-info.com.ar/2022/09/import-tarfile-error-de-15-anos-sin.html ▪ Análisis propio de fuentes abiertas.

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 259	**Fecha: 22-09-2022**
		Página 06 de 10

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	El relleno de credenciales representa el 34% de todos los intentos de inicio de sesión		
Tipo de ataque	Ataque de fuerza Bruta	Abreviatura	AtaqFueBru
Medios de propagación	Red, Correo, Navegación de Internet		
Código de familia	A	Código de Subfamilia	A01
Clasificación temática familia	Acceso no autorizado		

Descripción

A través del monitoreo y búsqueda de amenazas en el ciberespacio del día 21 de septiembre del 2022, se tomó conocimiento sobre los ataques de relleno de credenciales se han vuelto tan frecuentes en el primer trimestre de este año que el tráfico superó el de los intentos de inicio de sesión legítimos de usuarios normales en algunos países.

ANTECEDENTES:

Este tipo de ataque aprovecha el "reciclaje de contraseñas", que es la mala práctica de usar los mismos pares de credenciales (nombre de usuario y contraseña) en varios sitios. Una vez que las credenciales se filtran o se fuerzan brutamente desde un sitio, los actores de amenazas realizan un ataque de relleno de credenciales que intenta usar las mismas credenciales filtradas en otros sitios para obtener acceso a las cuentas de los usuarios.

Como advirtió recientemente el FBI, estos ataques están creciendo en volumen gracias a las listas agregadas fácilmente disponibles de credenciales filtradas y las herramientas automatizadas puestas a disposición de los ciberdelincuentes, lo que les permite probar pares contra muchos sitios.

Más de 10 mil millones de intentos de relleno de credenciales. Okta informa que la situación empeoró en 2022, ya que la empresa de administración de acceso e identidad registró más de 10 000 millones de eventos de relleno de credenciales en su plataforma en los primeros 90 días de 2022. Este número representa aproximadamente el 34 % del tráfico de autenticación general, lo que significa que un tercio de todos los intentos son maliciosos y fraudulentos.

Cuando se examina desde una perspectiva geográfica, los peores casos son el sudeste asiático y los Estados Unidos, donde el tráfico de relleno de credenciales eclipsó constantemente los intentos de inicio de sesión normales durante el primer trimestre de 2022.

En términos de qué industrias fueron más atacadas, Okta informa que la mayoría de los intentos fueron contra el comercio minorista/eCommerce. También se registraron volúmenes de ataques significativos contra la educación, la energía, los servicios financieros y el software/SaaS.

Desde la perspectiva de los usuarios, el uso de la autenticación multifactor y el establecimiento de contraseñas seguras y únicas para todas sus cuentas en línea ofrece una protección adecuada contra la mayoría de las amenazas de este tipo.

Sin embargo, como se vio en los recientes ataques MFA Fatigue (Fatiga de MFA: la nueva táctica favorita de los piratas informáticos en infracciones de alto perfil) , los actores de amenazas han encontrado formas de eludir MFA a través de la ingeniería social. Por lo tanto, es importante que las organizaciones aseguren adecuadamente MFA con umbrales de intento de autenticación y coincidencia de números.

Recomendaciones

- Tener actualizado el sistema operativo de la estación de trabajo.
- Proteger los dispositivos con antivirus y mantener su actualización.
- Hacer cambio de contraseñas mínimo 1 vez a la semana.
- Realizar periódicamente respaldos de seguridad.

Fuentes de información	▪ https://www.bleepingcomputer.com/news/security/okta-credential-stuffing-accounts-for-34-percent-of-all-login-attempts/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 259	Fecha: 22-09-2022
		Página 08 de 10

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Phishing, suplantado la identidad del sitio web de la financiera "INTERBANK".		
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 se vienen llevando a cabo una campaña de Phishing, a través de los diferentes navegadores web, suplantando el sitio oficial de la financiera "INTERBANK", con el objetivo de acceder u obtener datos personales y/o bancarios; para luego utilizarlas por los ciberdelincuentes para cumplir con sus falsos propósitos.

2. **Imagen**: Proceso del ataque Phishing:

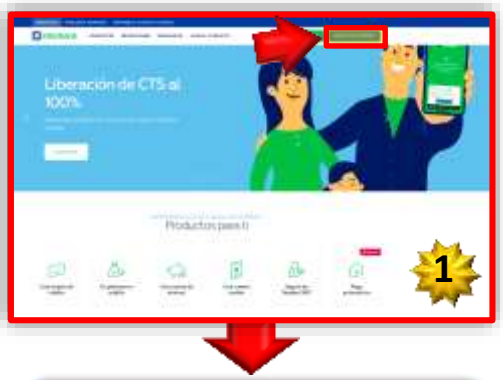


Imagen 1: Cuenta con los diferentes ítems similares que el sitio web original de la entidad financiera "Interbank" presenta.

Imagen 2: Al hacer clic en la opción **"BANCA POR INTERNET"**, solicita ingresar el número de la tarjeta, DNI y la clave web.

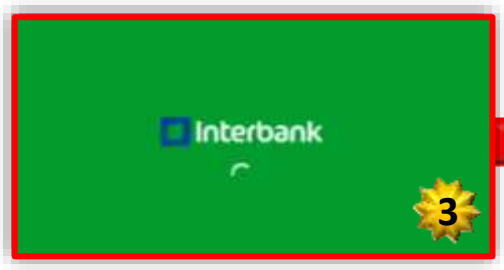


Imagen 3: Se muestra una ventana aparentemente de la entidad financiera "INTERBANK", aludiendo como si estuviese cargando dicha página.

3. **Comparación del sitio web oficial del Banco Interbank, con el fraudulento:**

SITIO WEB OFICIAL	SITIO WEB FRAUDULENTO
URL: https://bancaporintenet.interbank.pe/login 	URL: hxxps[:]//empresa[.]netinterbank[.]com[.]ru/1663856077/pe/banc4porinternet/login 

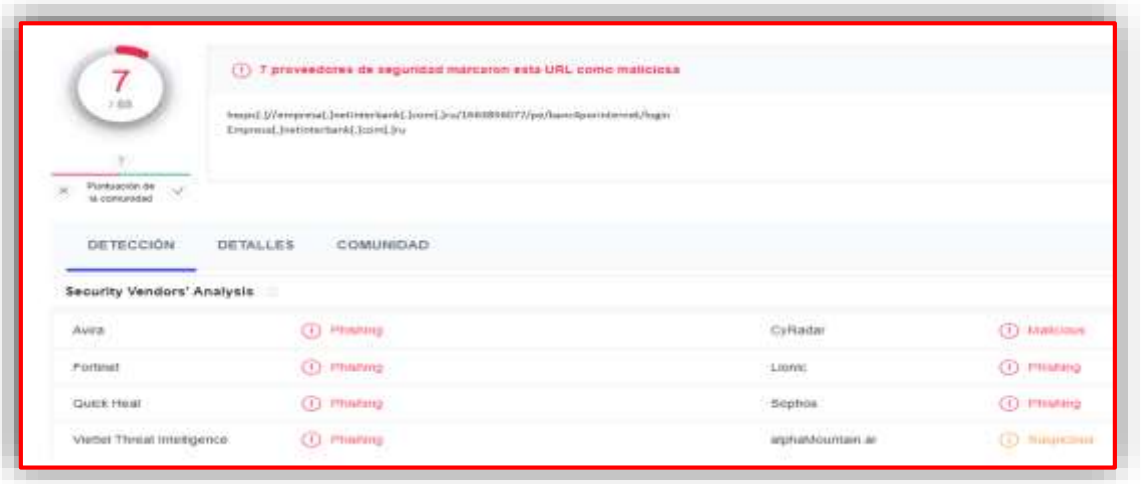
- Existe similitud entre ambas páginas, en imagen, fondo y escritura la diferencia se encuentra en la URL.
- La URL falsa utiliza protocolo HTTPS, no significa que la web sea segura.

- El dominio (empresa.netinterbank.com.ru) 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 - PHISHING:**

- **INDICADORES DE COMPROMISO:**

  - ✓ **URL:** hxxps[:]//empresa[.]netinterbank[.]com[.]ru/1663856077/pe/banc4porinternet/login
  - ✓ **Dominio:** empresa[.]netinterbank[.]com[.]ru
  - ✓ **IP:** 172[.]64[.]80[.]1
  - ✓ **Código:** 404
  - ✓ **Longitud:** 6.69KB



- **OTRAS DETECCIONES:**

5. ALGUNAS RECOMENDACIONES:

- Verificar la información en la entidad correspondiente.
- Acceder al sitio web a través de fuentes oficiales.
- No abrir enlaces de dudosa procedencia.
- No seguir indicaciones de sitios web fraudulentos.
- No compartir la información con terceras personas, amigos o familiares.
- Mantener instalado un servicio de antivirus en el dispositivo.

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

Índice alfabético