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
ASOCIACIÓN DE BANCOS DEL PERÚ

Lima, 22 de noviembre de 2022

317-2022-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° 317	Fecha: 22-11-2022
		Página 4 de 13

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Malware instala extensiones de navegador maliciosas para robar credenciales		
Tipo de ataque	Malware	Abreviatura	Malware
Medios de propagación	Red, Internet, Redes Sociales		
Código de familia	C	Código de subfamilia	C03
Clasificación temática familia	Código malicioso		

Descripción

Se ha observado que una extensión maliciosa para los navegadores web basados en Chromium se distribuye a través de un antiguo ladrón de información de Windows llamado ViperSoftX.

La empresa de seguridad cibernética con sede en República Checa apodó el complemento de navegador no autorizado VenomSoftX debido a sus características independientes que le permiten acceder a visitas a sitios web, robar credenciales y datos del portapapeles, e incluso intercambiar direcciones de criptomonedas a través de un ataque adversary-in-the-middle (AiTM).

ANTECEDENTES:

- ViperSoftX, que salió a la luz por primera vez en febrero de 2020, fue caracterizado por Fortinet como un troyano de acceso remoto basado en JavaScript y un ladrón de criptomonedas. El analista de amenazas de Sophos, Colin Cowie, documentó a principios de este año el uso que hace el malware de una extensión del navegador para avanzar en sus objetivos de recopilación de información.

DETALLES:

- Este malware tiene múltiples etapas que exhibe interesantes técnicas de ocultación, escondido como pequeños scripts de PowerShell en una sola línea en medio de grandes archivos de registro que de otro modo parecen inocentes, entre otros", dijo el investigador de Avast, Jan Rubín, en un artículo técnico.
- ViperSoftX se centra en el robo de criptomonedas, el intercambio de portapapeles, la toma de huellas dactilares de la máquina infectada, así como la descarga y ejecución de cargas útiles adicionales arbitrarias, o la ejecución de comandos."
- El vector de distribución utilizado para propagar ViperSoftX se consigue normalmente a través de software crackeado para Adobe Illustrator y Microsoft Office que se alojan en sitios de intercambio de archivos.
- El archivo ejecutable descargado viene con una versión limpia del software descifrado junto con archivos adicionales que configuran la persistencia en el host y albergan el script ViperSoftX PowerShell.
- Las variantes más nuevas del malware también pueden cargar el complemento VenomSoftX, que se recupera de un servidor remoto, en navegadores basados en Chromium como Google Chrome, Microsoft Edge, Opera, Brave y Vivaldi.
- Esto se logra buscando archivos LNK para las aplicaciones del navegador y modificando los accesos directos con un interruptor de línea de comando " --load-extension " que apunta a la ruta donde se almacena la extensión desempaquetada.
- "La extensión intenta disfrazarse de extensiones de navegador conocidas y comunes como Google Sheets", explicó Rubín. "En realidad, VenomSoftX es otro ladrón de información implementado en la víctima desprevenida con permisos de acceso completo a cada sitio web que el usuario visita desde el navegador infectado".

Fuente: Avast

- VenomSoftX, como ViperSoftX, también está orquestado para robar criptomonedas de sus víctimas. Pero a diferencia de este último, que funciona como un recortador para redirigir las transferencias de fondos a una billetera controlada por un atacante, VenomSoftX manipula las solicitudes de API a los intercambios de cifrado para drenar los activos digitales.
- Los servicios a los que se dirige la extensión incluyen Blockchain.com, Binance, Coinbase, Gate.io y Kucoin.
- El desarrollo marca un nuevo nivel de escalada al intercambio de portapapeles tradicional, al mismo tiempo que no levanta ninguna sospecha inmediata ya que la dirección de la billetera se reemplaza a un nivel mucho más fundamental.
- Avast dijo que ha detectado y bloqueado más de 93.000 infecciones desde principios de 2022, con la mayoría de los usuarios afectados ubicados en India, EE. UU., Italia, Brasil, Reino Unido, Canadá, Francia, Pakistán y Sudáfrica.

RECOMENDACIONES:

- Evitar añadir extensiones de dudosa procedencia a los navegadores.
- Evite revelar información personal, guardar contraseñas en los navegadores.
- Mantenga sus programas, antivirus y sistema operativo actualizados.

Fuentes de información	▪ hxxps://thehackernews.com/2022/11/this-malware-installs-malicious-browser.html

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 317**	**Fecha: 22-11-2022**
		Página 6 de 13

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad crítica en varios productos de MOXA		
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:**

MOXA ha reportado una vulnerabilidad de severidad CRÍTICA de tipo gestión de privilegios inadecuada en varios de sus **productos**. La explotación exitosa de esta vulnerabilidad podría permitir a un usuario local con privilegios bajos cambiar su configuración para tener privilegios de root en los dispositivos afectados.

2. **Detalles:**

- La vulnerabilidad de severidad **crítica** identificada como CVE-2022-3088 de gestión de privilegios inadecuada de la computadora basada en Arm, podría permitir que un usuario local con privilegios normales cambie su configuración para tener privilegios de root en los dispositivos afectados.

  La vulnerabilidad de tipo gestión de privilegios inadecuada se debe a que el software no asigna, modifica, rastrea o verifica correctamente los privilegios de un actor, lo que crea una esfera de control no deseada para ese actor.

3. **Productos afectados:**

- Serie UC-8100A-ME-T versiones v1.0 a v1.6 sin paquete moxa-version_1.3.3+deb9_armhf.deb;
- Versiones de la serie UC-2100 v1.0 a v1.12 sin el paquete moxa-version_1.3.3+deb9_armhf.deb;
- Serie UC-2100-W versiones v1.0 a v1.12 sin paquete moxa-version_1.3.3+deb9_armhf.deb;
- Versiones de la serie UC-3100 v1.0 a v1.6 sin el paquete moxa-version_1.3.3+deb9_armhf.deb;
- Versiones de la serie UC-5100 v1.0 a v1.4 sin el paquete moxa-version_1.3.3+deb9_armhf.deb;
- Versiones de la serie UC-8100 v3.0 a v3.5 sin el paquete moxa-version_1.3.3+deb9_armhf.deb;
- UC-8100-ME-T Series versiones v3.0 y v3.1 sin paquete moxa-version_1.3.3+deb9_armhf.deb;
- Serie UC-8100A-ME-T versiones v1.0 a v1.6 sin paquete moxa-version_1.3.3+deb9_armhf.deb;
- Versiones de la serie UC-8200 v1.0 a v1.5 sin el paquete moxa-version_1.3.3+deb9_armhf.deb;
- AIG-300 Series versiones v1.0 a v1.4 sin la última versión de ThingsPro Proxy;
- Serie UC-8410A (con Debian 9) versiones v4.0.2 y v4.1.2 sin paquete moxa-version_1.3.3+deb9_armhf.deb;
- Serie UC-8580 (con Debian 9) versiones v2.0 y v2.1 sin paquete moxa-version_1.3.3+deb9_armhf.deb;
- Serie UC-8540 (con Debian 9) versiones v2.0 y v2.1 sin paquete moxa-version_1.3.3+deb9_armhf.deb;
- DA-662C-16-LX Series (GLB) versiones v1.0.2 a 1.1.2 sin paquete moxa-version_1.3.3+deb9_armhf.deb.

4. **Solución:**

- MOXA ha lanzado actualizaciones de software que abordan esta vulnerabilidad.

Fuentes de información	▪ hxxps://www.moxa.com/en/support/product-support/security-advisory/arm-based-computer-improper-privilege-management-vulnerability

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 317	Fecha: 22-11-2022
		Página 7 de 13

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Microsoft lanzó una actualización fuera de banda sobre un parche de seguridad reciente de Windows Server		
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:**

Microsoft lanzó una actualización fuera de banda después de tomar conocimiento de que un parche de seguridad reciente de Windows comenzó a generar problemas con la autenticación Kerberos. La explotación exitosa de esta vulnerabilidad de tipo elevación de privilegios requiere que un atacante recopile información específica del entorno del componente objetivo para obtener privilegios de administrador.

2. **Detalles:**

- Microsoft indicó que las actualizaciones y parches publicadas el 8 de noviembre de 2022 abordaron la vulnerabilidad de escalada de privilegios registrada como CVE-2022-37966 que afecta a Windows Server. La vulnerabilidad de severidad crítica, podría permitir a un atacante no autenticado recopilar información sobre el sistema objetivo y obtener privilegios de administrador.
- La explotación exitosa de esta vulnerabilidad podría permitir a un atacante no autenticado realizar un ataque y explotar las vulnerabilidades del protocolo criptográfico en RFC 4757 (tipo de cifrado Kerberos RC4-HMAC-MD5) y MS-PAC (especificación de estructura de datos de certificado de atributo privilegiado) para eludir las funciones de seguridad en un entorno de Windows AD (Active Directory o Directorio Activo).
- La explotación exitosa de esta vulnerabilidad requiere que un atacante recopile información específica del entorno del componente objetivo. Un atacante que aprovechara con éxito esta vulnerabilidad podría obtener privilegios de administrador.
- Sin embargo, unos días después del lanzamiento del parche, los usuarios comenzaron a reportar problemas relacionados con la autenticación Kerberos. Es por ello, que Microsoft actuó rápidamente y unos días después proporcionó mitigaciones.
- El 17 de noviembre de 2022, Microsoft lanzó una actualización fuera de banda que soluciona esta vulnerabilidad.

3. **Productos afectados:**

- Múltiples versiones de Windows Server.

4. Solución:

- Microsoft señala que los usuarios que aún no hayan instalado las actualizaciones de seguridad lanzadas el 8 de noviembre de 2022 deben instalar las actualizaciones fuera de banda publicadas en Microsoft Update Catalog a partir del 17 de noviembre de 2022 en su lugar. Los clientes que ya instalaron las actualizaciones de seguridad de Windows del 8 de noviembre de 2022 y que tienen problemas, deben instalar las actualizaciones fuera de banda.

Fuentes de información	▪ hxxps://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37966

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 317**	**Fecha: 22-11-2022**
		Página 9 de 13

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades en Zimbra Collaboration		
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:**

Se ha reportado múltiples vulnerabilidades de severidad MEDIA de tipo secuencias de comandos entre sitios (XSS), carga de archivos arbitrarios, interpretación inconsistente de solicitudes HTTP y bucle infinito que afecta a Zimbra Collaboration. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto realizar ataques XSS, de phishing, de denegación de servicio (DoS) y comprometer un sistema vulnerable.

2. **Detalles:**

- La vulnerabilidad de severidad **media** de tipo secuencias de comandos entre sitios podría permitir a un atacante remoto realizar ataques XSS. La vulnerabilidad existe debido a la desinfección insuficiente de los datos proporcionados por el usuario en la página de inicio de sesión de la IU clásica y pasados a través de uno de los atributos en las direcciones URL de correo web. Un atacante remoto puede engañar a la víctima para que siga un enlace especialmente diseñado por correo electrónico y ejecute código HTML y script arbitrario en el navegador del usuario en el contexto de un sitio web vulnerable. La explotación exitosa de esta vulnerabilidad puede permitir a un atacante remoto robar información potencialmente confidencial, cambiar la apariencia de la página web, realizar ataques de phishing y de descarga oculta.
- La vulnerabilidad de severidad **media** de tipo carga de archivos arbitrarios podría permitir a un usuario remoto comprometer un sistema vulnerable. La vulnerabilidad existe debido a una validación insuficiente del archivo durante la carga del archivo dentro de la función ***ClientUploader***. Un administrador remoto puede cargar un archivo malicioso y ejecutarlo en el servidor.
- La vulnerabilidad de severidad **media** registrada como CVE-2022-26377 podría permitir a un atacante remoto realice ataques de contrabando de solicitudes HTTP. La vulnerabilidad existe debido a una validación incorrecta de las solicitudes HTTP en ***mod_proxy_ajp***. Un atacante remoto puede enviar una solicitud HTTP especialmente diseñada al servidor y contrabandear solicitudes al servidor AJP al que reenvía las solicitudes. La explotación exitosa de la vulnerabilidad puede permitir que un atacante envenene la memoria caché HTTP y realice ataques de phishing.
- Las vulnerabilidades de severidad **media** registradas como CVE-2022-20770 y CVE-2022-20771 de bucle infinito podría permitir a un atacante remoto realizar un ataque de denegación de servicio. Las vulnerabilidades existen debido a un bucle infinito en el analizador de archivos CHM / TIFF. Un atacante remoto puede consumir todos los recursos disponibles del sistema y provocar una condición de denegación de servicio.

3. **Productos afectados:**

- Zimbra Collaboration: 8.8.15 - 9.0.0 Parche 27;
- Zimbra Collaboration: 9.0.0 - 9.0.0 Patch 27.

4. Solución:

- Se recomienda actualizar el producto afectado con las últimas versiones de software disponibles que abordan estas vulnerabilidades.

Fuentes de información	▪ hxxp://wiki.zimbra.com/wiki/Security_Center#ZCS_9.0.0_Patch_28_Released ▪ hxxp://wiki.zimbra.com/wiki/Security_Center#ZCS_8.8.15_Patch_35_Released

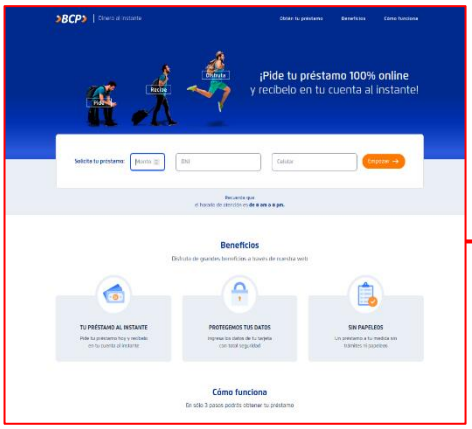
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 317	Fecha: 22-11-2022
		Página 11 de 13

Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ		
Nombre de la alerta	Campaña de Phishing suplantando la identidad del Banco de Crédito del Perú - BCP		
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

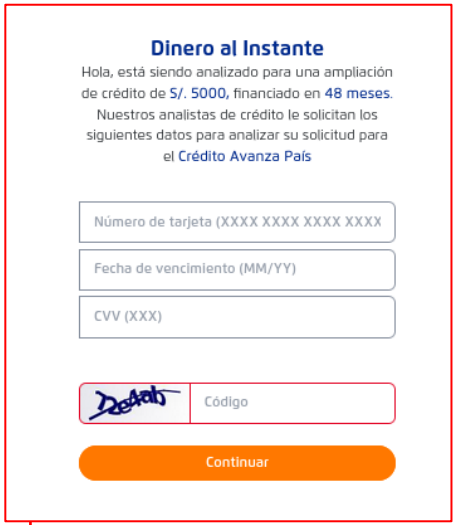
1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo una campaña de Phishing, a través de los diferentes navegadores web, quienes vienen suplantando la identidad del sitio web del "Banco de Crédito del Perú - BCP", el cual tiene como finalidad robar información confidencial y bancaria de las posibles víctimas como número de tarjeta, clave de internet, DNI, numero de celular, fecha de vencimiento, código de seguridad y clave de cajero.

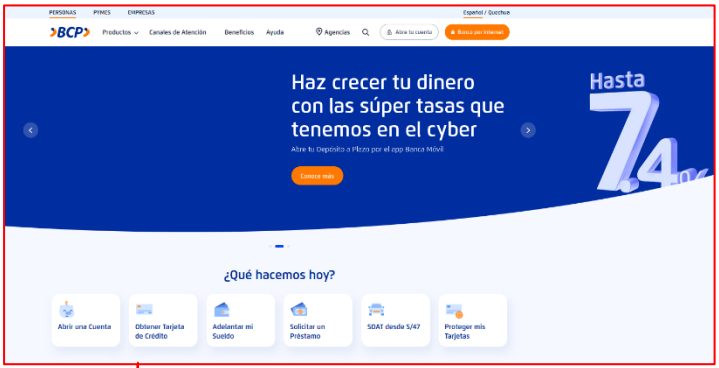
   - Detalles del proceso de phishing.



Requiere realizar un prestamos 100% online y al instante

Da una descripción del tipo de préstamo y pide ingresar número de DNI y clave web



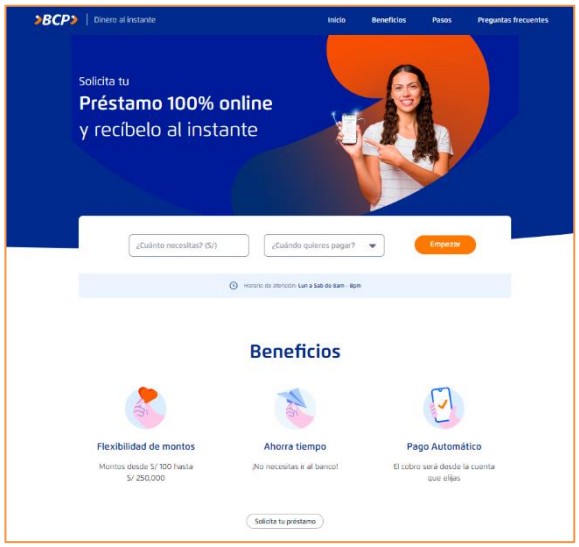


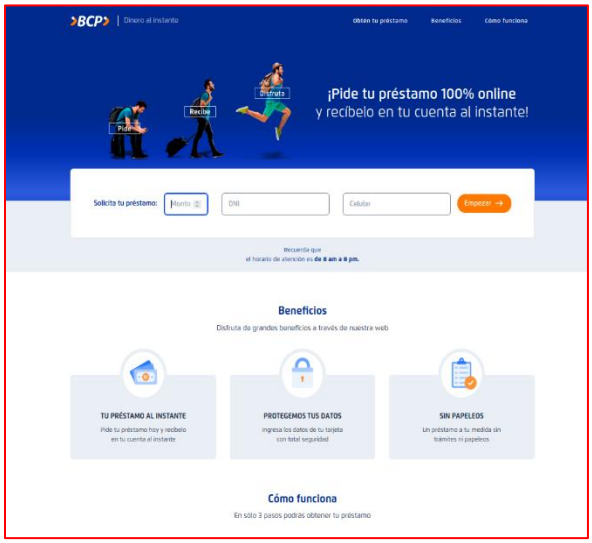
Solicita validar datos bancarios como número de tarjeta, fecha de vencimiento

Luego, redirige de manera automática al sitio web oficial del Banco de Crédito del Perú (BCP), toda vez que los datos ingresados ya fueron captados por los ciberdelincuentes

2. Comparación de la URL del sitio oficial y fraudulento:

URL OFICIAL	URL FRAUDULENTA
https://www.dineroalinstante.viabcp.com	hxxps://reactiva-benficianavidad.top

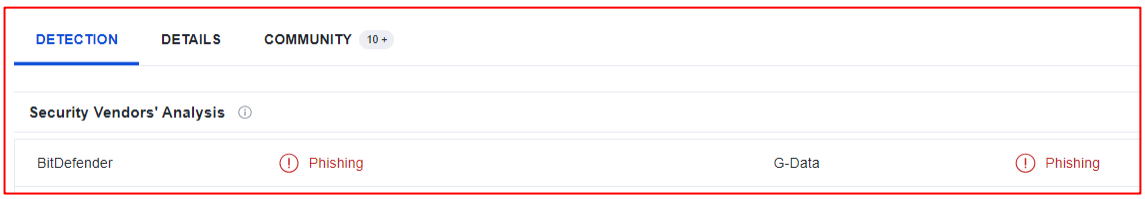




- Ambas URL utilizando el protocolo https, lo que hace mas convincente a que las víctimas ingresen a dicho sitio web.
- La diferencia está en el dominio de cada sitio web.
- Existe una similitud entre el fondo y forma de cada sitio web.

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

- Indicadores de compromisos:
  - **URL:** hxxps://reactiva-benficianavidad[.]top
  - **Dominio:** reactiva-benficianavidad[.]top
  - **IP:** 104[.]21[.]64[.]222
  - **Tamaño:** 846 KB
  - **SHA-256**: 636df912c8dad81fce6964c6221a8a13e5f0972ad23280c59c26e296406b9ac8



4. Recomendaciones:

- Acceder al sitio web a través de fuentes oficiales.
- Evitar responder a mensajes enviados (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.
- No compartir la información con terceras personas, amigos o familiares.
- Utilizar un antivirus actualizado ya que es la primera barrera ante un ataque cibernético.

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

Índice alfabético