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

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

Lima, 31 de enero de 2024

027-2024-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°027**	**Fecha: 31-01-2024**
		Página: 4 de 11

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Los mercados de Telegram impulsan los ataques de phishing con kits y malware fáciles de usar		
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 Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. **ANTECEDENTES**:

   Los investigadores de ciberseguridad están llamando la atención sobre la "democratización" del ecosistema de phishing debido al surgimiento de Telegram como epicentro del cibercrimen, que permite a los actores de amenazas montar un ataque masivo por tan solo 230 dólares.

   "Esta aplicación de mensajería se ha transformado en un centro bullicioso donde tanto los ciberdelincuentes experimentados como los recién llegados intercambian herramientas e ideas ilícitas creando una cadena de suministro oscura y bien engrasada de herramientas y datos de las víctimas", dijeron los investigadores de Guardio Labs Oleg Zaytsev y Nati Tal en un nuevo informe.

2. **DETALLES:**

   "Muestras gratuitas, tutoriales, kits e incluso piratas informáticos contratados: todo lo necesario para construir una campaña maliciosa completa de extremo a extremo". La compañía también describió a Telegram como un "paraíso de los estafadores" y un "caldo de cultivo para las operaciones modernas de phishing".

   En abril de 2023, Kaspersky reveló cómo los phishers crean canales de Telegram para educar a los novatos sobre el phishing, así como para anunciar bots que pueden automatizar el proceso de creación de páginas de phishing para recopilar información confidencial, como credenciales de inicio de sesión.

   Uno de esos robots maliciosos de Telegram es Telekopye (también conocido como Classiscam), que puede crear páginas web, correos electrónicos y mensajes SMS fraudulentos para ayudar a los actores de amenazas a realizar estafas de phishing a gran escala.

   Guardio dijo que los componentes básicos para construir una campaña de phishing se pueden comprar fácilmente en Telegram - "algunos se ofrecen a precios muy bajos y otros incluso gratis" - lo que hace posible configurar páginas fraudulentas a través de un kit de phishing, alojar la página en un sitio web de WordPress comprometido a través de un shell web y aprovechar un correo de puerta trasera para enviar los mensajes de correo electrónico.

   Los correos de puerta trasera, comercializados en varios grupos de Telegram, son scripts PHP inyectados en sitios web ya infectados pero legítimos para enviar correos electrónicos convincentes utilizando el dominio legítimo del sitio web explotado para evitar los filtros de spam.

   "Esta situación pone de relieve una doble responsabilidad de los propietarios de los sitios", dijeron los investigadores. "Deben salvaguardar no sólo sus intereses comerciales, sino también protegerse contra el uso de sus plataformas por parte de estafadores para albergar operaciones de phishing, enviar correos electrónicos engañosos y realizar otras actividades ilícitas, todo ello sin que ellos lo sepan".

   Telegram también alberga conjuntos de datos masivos que contienen direcciones de correo electrónico y números de teléfono válidos y relevantes a los que dirigirse. Conocidos como "clientes potenciales", a veces se "enriquecen" con información personal como nombres y direcciones físicas para maximizar el impacto.

3. **RECOMENDACIONES:**

   - No hacer clic en enlaces sospechosos ni descargue archivos adjuntos de fuentes desconocidas.
   - Implementar sistemas sólidos de detección de intrusiones.
   - Capacitar a los usuarios sobre las mejores prácticas de ciberseguridad.

Fuente de Información:	• hxxps://thehackernews.com/2024/01/telegram-marketplaces-fuel-phishing.html

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°027**	**Fecha: 31-01-2024**
		Página: 5 de 11

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad crítica en productos de Comunicaciones Unificadas de Cisco		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Cisco ha reportado una vulnerabilidad de severidad **CRÍTICA** de tipo ejecución remota de código en múltiples productos de soluciones de centros de contacto y comunicaciones unificadas de Cisco. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en un dispositivo afectado.

2. DETALLES:

La vulnerabilidad de severidad **crítica**, identificada por MITRE como CVE-2024-20253 en múltiples productos de soluciones de centros de contacto y comunicaciones unificadas de Cisco podría permitir que un atacante remoto no autenticado ejecute código arbitrario en un dispositivo afectado.

Esta vulnerabilidad se debe al procesamiento inadecuado de los datos proporcionados por el usuario que se leen en la memoria. Un atacante podría aprovechar esta vulnerabilidad enviando un mensaje manipulado a un puerto de escucha de un dispositivo afectado. Un exploit exitoso podría permitir al atacante ejecutar comandos arbitrarios en el sistema operativo subyacente con los privilegios del usuario de servicios web. Con acceso al sistema operativo subyacente, el atacante también podría establecer acceso root en el dispositivo afectado.

A. Productos afectados:

Esta vulnerabilidad afecta a los siguientes productos de Cisco en la configuración predeterminada:

- Unified Communications Manager (Unified CM).
- Unified Communications Manager IM & Presence Service (Unified CM IM&P).
- Unified Communications Manager Session Management Edition (Unified CM SME).
- Unified Contact Center Express (UCCX).
- Unity Connection.
- Virtualized Voice Browser (VVB).

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que el proveedor Cisco ha lanzado para abordar estas vulnerabilidades. No existen soluciones alternativas.

Fuente de Información:	• hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-rce-bWNzQcUm

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°027**	**Fecha: 31-01-2024**
		Página: 6 de 11

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad crítica en la conexión Cisco Unity		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Cisco ha reportado una vulnerabilidad de severidad **CRÍTICA** de tipo carga de archivos arbitrarios no autenticados en la interfaz de administración basada en web de Cisco Unity Connection. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado cargar archivos arbitrarios en un sistema afectado y ejecutar comandos en el sistema operativo subyacente.

2. DETALLES:

La vulnerabilidad de severidad **crítica**, identificada por MITRE como CVE-2024-20272 en la interfaz de administración basada en web de Cisco Unity Connection podría permitir que un atacante remoto no autenticado cargue archivos arbitrarios en un sistema afectado y ejecute comandos en el sistema operativo subyacente.

Esta vulnerabilidad se debe a una falta de autenticación en una API específica y a una validación inadecuada de los datos proporcionados por el usuario. Un atacante podría aprovechar esta vulnerabilidad cargando archivos arbitrarios en un sistema afectado. Un exploit exitoso podría permitir al atacante almacenar archivos maliciosos en el sistema, ejecutar comandos arbitrarios en el sistema operativo y elevar privilegios a root.

A. Productos afectados:

- Cisco Unity Connection, versión 12.5 y anteriores, y 14.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que el proveedor Cisco ha lanzado para abordar estas vulnerabilidades. No existen soluciones alternativas.

Fuente de Información:	• hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuc-unauth-afu-FROYsCsD

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°027**	**Fecha: 31-01-2024**
		Página: 7 de 11

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad en el software Resource Hacker		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

El investigador Rafael Pedrero ha reportado una vulnerabilidad de severidad **ALTA** de tipo desbordamiento de búfer en el software Resource Hacker. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino.

2. DETALLES:

Resource Hacker es una aplicación freeware de extracción de recursos desarrollada por Angus Johnson para Windows. Se usa para modificar elementos de programas o del sistema operativo, como iconos, extrayendo recursos de programas ejecutables, bibliotecas de enlace dinámico, y ficheros de recursos.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2024-1112 de tipo desbordamiento de búfer, podría permitir a un atacante ejecutar código arbitrario a través de un argumento de nombre de archivo largo. Esta vulnerabilidad, realiza operaciones en un búfer de memoria, pero puede leer o escribir en una ubicación de memoria que esté fuera del límite previsto del búfer.

A. Productos afectados:

- Resource Hacker, versión 3.6.0.92.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.

Fuente de Información:	• hxxps://www.angusj.com/resourcehacker/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°027	Fecha: 31-01-2024
		Página: 8 de 11

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Detección de sitio web fraudulento del Banco Crédito del Perú		
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 Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. **ANTECEDENTES:**

A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que actores de amenazas vienen realizando una campaña de Phishing, suplantando el sitio web del Banco de Crédito del Perú (servicio online de préstamo personal), con la finalidad de robar información bancaria de los usuarios de la entidad financiera como números de tarjetas bancarias, clave intranet de seis dígitos, documento de identidad, etc.

2. **DETALLES:**

El proceso del Phishing es el siguiente:

Paso N.º 01

Solicitan a la víctima registrar lo siguiente:

- El monto solicitado del préstamo.
- Cuotas por pagar
- Documento Nacional de identidad (DNI).
- Número de Celular.

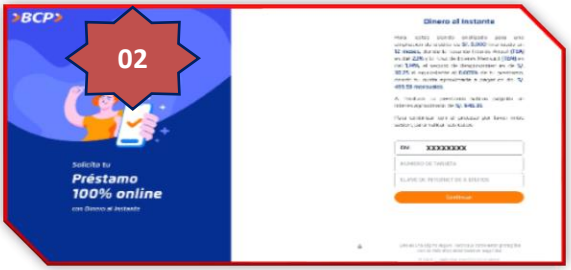
Para luego dar clic en <**Empezar**>.

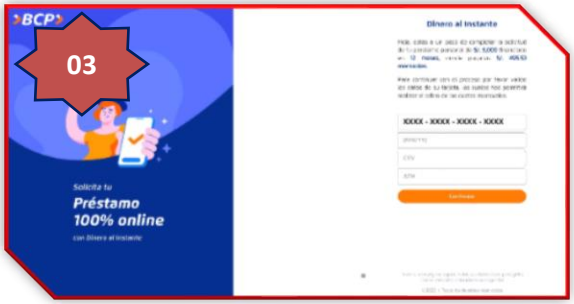
Paso N.º 02

Instan a la víctima que registre datos como:

- El número de la tarjeta bancaria.
- Clave de seis dígitos del intranet.

Para luego dar clic en <**Continuar**>.



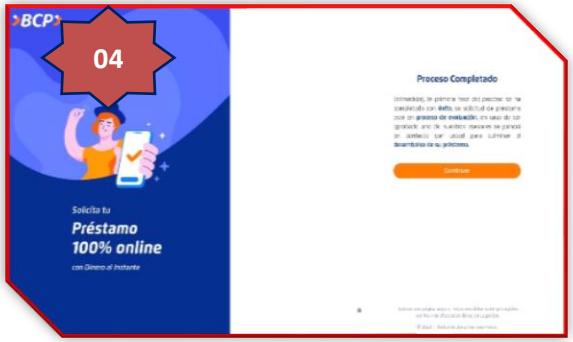


Paso N.º 03

Una vez brindado los datos solicitados en el paso N.º 02, aparece una pantalla requiriendo información de la tarjeta bancaria como la fecha de expedición, el código de seguridad (CVV) y la clave de cuatro dígitos utilizado en el cajero automático, para luego dar clic en <**Continuar**>.

Paso N.º 04

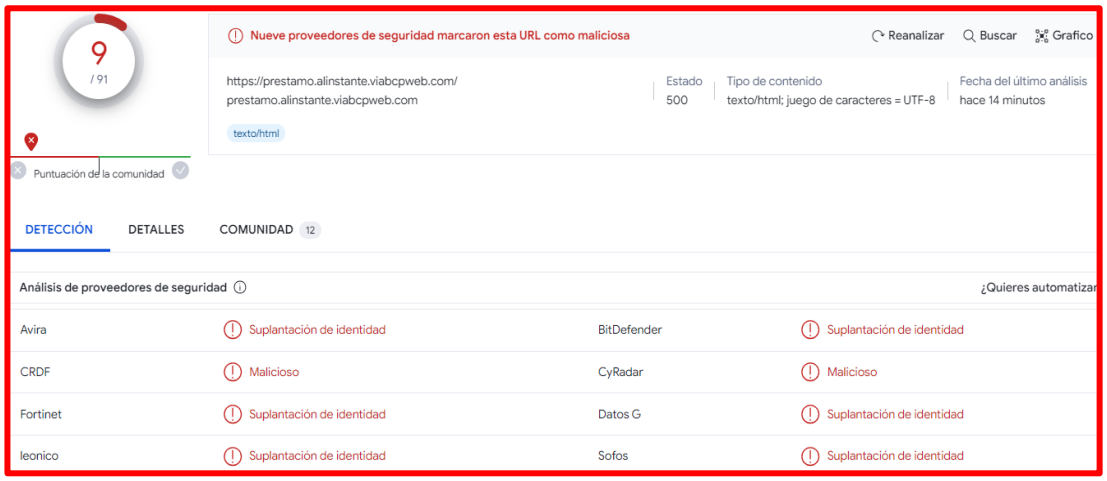
Luego, aparece una pantalla indicando se ha completado con éxito el registro de datos y de ser aprobados el crédito, asesores de la entidad bancaria se pondrán en contacto con la víctima, para luego dar clic en <**Continuar**>. Redirigiendo al sitio web oficial de la entidad bancaria; sin embargo, los ciberdelincuentes obtuvieron los datos proporcionados por la víctima.



A. *Comparación del sitio web oficial y fraudulento*.

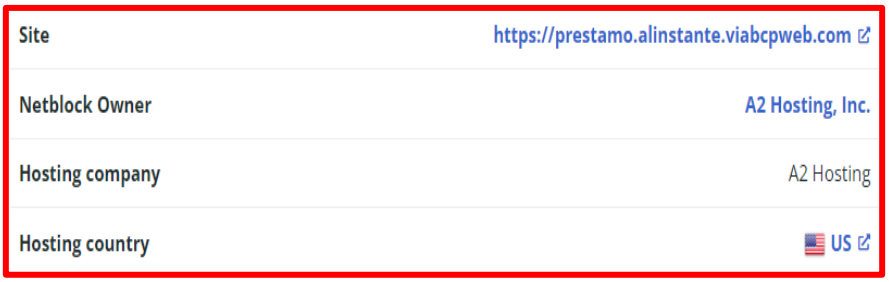
- Existe una diferencia entre la URL original y la URL fraudulenta.
- La URL del sitio web fraudulento posee protocolo de seguridad de red (https)
- Existe una similitud entre ambas páginas en imagen, fondo y colores de ambos sitios web.

B. *Proveedores de seguridad informática ALERTAN COMO SUPLANTACIÓN DE IDENTIDAD - PHISHING*.

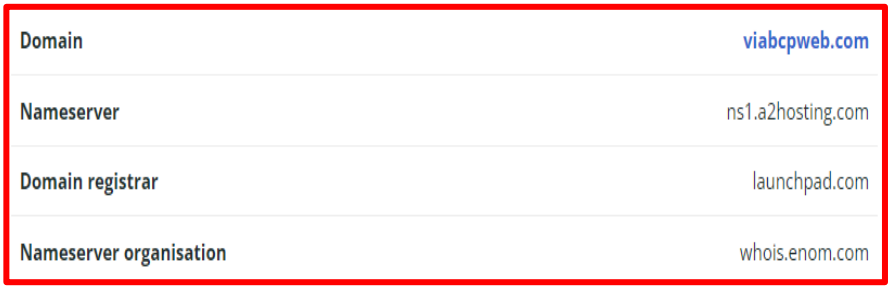


C. *Indicadores de compromiso (IoC)*

- Servidor : Apache



- Dominio : viabcpweb[.]com



Domain	viabcpweb.com
Nameserver	ns1.a2hosting.com
Domain registrar	launchpad.com
Nameserver organisation	whois.enom.com

- IP : 85[.]187[.]142[.]69

IPv4 address (85.187.142.69)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ 85.0.0.0-85.255.255.255	Netherlands	85-RIPE	RIPE Network Coordination Centre
↳ 85.187.128.0-85.187.159.255	United States	US-A2HOS-20041126	A2 Hosting, Inc.
↳ 85.187.142.69	United States	US-A2HOS-20041126	A2 Hosting, Inc.

- Servidor : Apache
- Tipo de tex. : Text/Html

1. **Apreciación de la información:**

- La presente campaña de Phishing permite a los actores de amenazas obtener información bancaria de los usuarios del Banco de Crédito del Perú.

- La propagación del sitio web fraudulento se realiza mediante envió masivos de email, adjuntando enlaces de sitios web fraudulentos con la finalidad de obtener información sensible de las víctimas; asimismo, a través de las aplicaciones de mensajería instantánea entre ellos WhatsApp, Telegram, Messenger, etc. y mensajes de textos SMS.

3. RECOMENDACIONES:

- Verificar detalladamente las URL de los sitios web.
- No abrir o descargar archivos sospechosos.
- No seguir las instrucciones de sitio web sospechoso.
- No aceptar permisos de instalación de archivos desconocidos o dudosa procedencia.
- Mantener actualizado el sistema operativo y aplicaciones del equipo de cómputo.
- Mantener actualizado el sistema antivirus (el antivirus debe ser licenciado).

Fuente de Información:	Análisis propio de redes sociales y fuente abierta.

Índice alfabético