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, 01 de febrero de 2024

028-2024-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°028**	**Fecha: 01-02-2024**
		Página: 4 de 13

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Cloudflare fue pirateado usando tokens de autenticación robados en el ataque de Okta		
Tipo de Ataque	Intento de acceso con vulneración de credenciales	Abreviatura	IAVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. **ANTECEDENTES**:

   Cloudflare reveló hoy que su servidor interno Atlassian fue violado por un presunto "atacante de estado nación" que accedió a su wiki Confluence, a su base de datos de errores Jira y al sistema de gestión de código fuente Bitbucket.

2. **DETALLES:**

   El actor de amenazas obtuvo acceso por primera vez al servidor Atlassian autohospedado de Cloudflare el 14 de noviembre y luego accedió a los sistemas Confluence y Jira de la compañía luego de una etapa de reconocimiento.

   "Luego regresaron el 22 de noviembre y establecieron acceso persistente a nuestro servidor Atlassian usando ScriptRunner para Jira, obtuvieron acceso a nuestro sistema de administración de código fuente (que usa Atlassian Bitbucket) e intentaron, sin éxito, acceder a un servidor de consola que tenía acceso al centro de datos que Cloudflare aún no había puesto en producción en São Paulo, Brasil", dijeron el CEO de Cloudflare, Matthew Prince, el CTO John Graham-Cumming y el CISO Grant Bourzikas.

   Para acceder a sus sistemas, los atacantes utilizaron un token de acceso y tres credenciales de cuenta de servicio robadas durante un compromiso anterior vinculado a la violación de Okta en octubre de 2023 que Cloudflare no pudo rotar (de miles se filtraron durante el compromiso de Okta).

   Cloudflare detectó la actividad maliciosa el 23 de noviembre, cortó el acceso del hacker en la mañana del 24, y sus especialistas forenses en ciberseguridad comenzaron a investigar el incidente tres días después, el 26 de noviembre.

   Mientras abordaba el incidente, el personal de Cloudflare rotó todas las credenciales de producción (más de 5000 únicas), segmentó físicamente los sistemas de prueba y preparación, realizó una clasificación forense en 4893 sistemas, volvió a crear imágenes y reinició todos los sistemas en la red global de la empresa, incluidos todos los servidores Atlassian (Jira, Confluence y Bitbucket) y las máquinas a las que accedió el atacante.

   Los actores de amenazas también intentaron piratear el centro de datos de Cloudflare en São Paulo, que aún no se utiliza en producción, pero estos intentos fracasaron. Posteriormente, todos los equipos del centro de datos de Cloudflare en Brasil fueron devueltos a los fabricantes para garantizar que el centro de datos fuera 100% seguro.

   Los esfuerzos de remediación terminaron hace casi un mes, el 5 de enero, pero la compañía dice que su personal todavía está trabajando en el fortalecimiento del software, así como en la gestión de credenciales y vulnerabilidades.

   "Basándonos en nuestra colaboración con colegas de la industria y el gobierno, creemos que este ataque fue realizado por un atacante de un estado nación con el objetivo de obtener acceso persistente y generalizado a la red global".

   "Al analizar las páginas wiki a las que accedieron, los problemas de la base de datos de errores y los repositorios de código fuente, parece que estaban buscando información sobre la arquitectura, la seguridad y la gestión de nuestra red global; sin duda, con miras a ganar un punto de apoyo más profundo".

3. **RECOMENDACIONES:**

   - Implementar sistemas sólidos de detección de intrusiones.
   - Practicar una higiene estricta de sus contraseñas. Utilizar contraseñas únicas y complejas, y distintas para cada una de las cuentas, y cambiarlas periódicamente.
   - Habilitar la autenticación de dos factores cuando esté disponible.

Fuente de Información:	• hxxps://www.bleepingcomputer.com/news/security/cloudflare-hacked-using-auth-tokens-stolen-in-okta-attack/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°028	Fecha: 01-02-2024
		Página: 5 de 13

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades en impresora Lexmark CX331adwe		
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:

Se ha reportado múltiples vulnerabilidades de severidad **CRÍTICA** y **ALTA** de tipo falta de autenticación, falta de validación adecuada que afectan a las impresoras Lexmark CX331adwe. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar código arbitrario en instalaciones afectadas de impresoras Lexmark CX331adwe.

2. DETALLES:

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-50737 podría permitir a atacantes adyacentes a la red ejecutar código arbitrario en instalaciones afectadas de impresoras Lexmark CX331adwe. No se requiere autenticación para aprovechar esta vulnerabilidad. La falla específica existe en la implementación de la autenticación dentro de la interfaz web. El problema se debe a la falta de autenticación antes de permitir el acceso a la funcionalidad. Un atacante puede aprovechar esta vulnerabilidad para ejecutar código en el sistema afectado.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-50736 podría permitir a atacantes adyacentes a la red ejecutar código arbitrario en instalaciones afectadas de impresoras Lexmark CX331adwe. No se requiere autenticación para aprovechar esta vulnerabilidad. La falla específica existe en el análisis de datos PostScript. El problema se debe a la falta de validación adecuada de los datos proporcionados por el usuario, lo que puede provocar una condición de corrupción de la memoria. Un atacante puede aprovechar esta vulnerabilidad para ejecutar código en el contexto del usuario creador de páginas.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-50735 podría permitir a atacantes remotos ejecutar código arbitrario en instalaciones afectadas de impresoras Lexmark CX331adwe. No se requiere autenticación para aprovechar esta vulnerabilidad. La falla específica existe en el análisis de archivos PDF. El problema se debe a la falta de validación adecuada de los datos proporcionados por el usuario, lo que puede provocar una condición de corrupción de la memoria. Un atacante puede aprovechar esta vulnerabilidad para ejecutar código en el contexto del usuario creador de páginas.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-50734 podría permitir a atacantes adyacentes a la red ejecutar código arbitrario en instalaciones afectadas de impresoras Lexmark CX331adwe. No se requiere autenticación para aprovechar esta vulnerabilidad. La falla específica existe dentro del método make42charstring. El problema se debe a la falta de una validación adecuada de la longitud de los datos proporcionados por el usuario antes de copiarlos en un búfer basado en pila de longitud fija. Un atacante puede aprovechar esta vulnerabilidad para ejecutar código en el contexto de la raíz.

A. Productos afectados:

- Impresora Lexmark CX331adwe;

3. RECOMENDACIÓN:

- Actualizar el producto afectado con las últimas actualizaciones de software que corrigen estas vulnerabilidades.

Fuente de Información:	• hxxps://www.zerodayinitiative.com/advisories/ZDI-24-084/ • hxxps://www.zerodayinitiative.com/advisories/ZDI-24-083/ • hxxps://www.zerodayinitiative.com/advisories/ZDI-24-082/ • hxxps://www.zerodayinitiative.com/advisories/ZDI-24-081/ • hxxps://www.lexmark.com/en_us/solutions/security/lexmark-security-advisories.html

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°028	Fecha: 01-02-2024
		Página: 6 de 13

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidades en IBM Cloud Pak para AIOps		
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:

Se ha reportado dos vulnerabilidades de severidad **ALTA** de tipo neutralización inadecuada de elementos especiales utilizados en una consulta LDAP (Protocolo ligero de acceso a directorios) y comparación utilizando factores incorrectos en IBM Cloud Pak para AIOps. La explotación exitosa de estas vulnerabilidades permite a un atacante remoto eludir el proceso de autenticación y aplicar fuerza bruta a los hashes de contraseñas.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2022-46337 de tipo neutralización inadecuada de elementos especiales utilizados en una consulta LDAP, existe debido a una validación de entrada incorrecta al procesar consultas DLAP. Un atacante remoto no autenticado puede enviar una consulta LDAP especialmente diseñada a la aplicación, eludir el proceso de autenticación y obtener acceso no autorizado a la aplicación.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2020-28052 de tipo comparación utilizando factores incorrectos, existe debido a un error de comparación en la función OpenBSDBCrypt.checkPassword() en core/src/main/java/org/bouncycastle/crypto/generators/OpenBSDBCrypt.java al hacer coincidir contraseñas con hashes. Un atacante remoto puede pasar una contraseña incorrecta que la biblioteca aceptará como válida, eludir el proceso de autenticación y obtener acceso no autorizado a la aplicación que utiliza la versión vulnerable de Bouncy Castle.

A. Productos afectados:

- IBM Cloud Pak para Watson AIOps: anterior a 4.4.0.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda estas vulnerabilidades.

Fuente de Información:	• hxxps://www.aveva.com/content/dam/aveva/documents/support/cyber-security-updates/Security_Bulletin_AVEVA-2024-002.pdf

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°028	Fecha: 01-02-2024
		Página: 7 de 13

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Actualización de SUSE para Webkit2gtk3		
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:

Se ha reportado una vulnerabilidad de severidad **CRÍTICA** de tipo acceso a recursos mediante tipos incompatibles (confusión de tipos) en el software SUSE para Webkit2gtk3. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino.

2. DETALLES:

La vulnerabilidad de severidad **crítica**, identificada por MITRE como CVE-2024-23222 de tipo acceso a recursos mediante tipos incompatibles, existe debido a un error de confusión de tipos al procesar contenido HTML. Un atacante remoto puede engañar a la víctima para que abra un sitio web especialmente diseñado, provocar un error de confusión de tipos y ejecutar código arbitrario en el sistema de destino.

Esta vulnerabilidad, asigna o inicializa un recurso como un puntero, objeto o variable usando un tipo, pero luego accede a ese recurso usando un tipo que es incompatible con el tipo original.

A. Productos afectados:

- SUSE Linux Enterprise Server para aplicaciones SAP 15: SP2 - SP3.
- SUSE Linux Enterprise Server 15 SP3 LTSS: 15-SP3.
- SUSE Linux Enterprise Server 15: SP2 - SP3.
- SUSE Linux Enterprise Server 15 SP2 LTSS: 15-SP2.
- SUSE Linux Enterprise Computación de alto rendimiento LTSS 15: SP3.
- SUSE Linux Enterprise Computación de alto rendimiento 15: SP2 - SP3.
- SUSE Linux Enterprise Computación de alto rendimiento 15 SP2 LTSS: 15-SP2.
- Almacenamiento empresarial SUSE: 7.1.
- libwebkit2gtk3-lang: anterior a 2.42.4-150200.100.1.
- libwebkit2gtk-4_0-37: antes de 2.42.4-150200.100.1.
- libjavascriptcoregtk-4_0-18: antes de 2.42.4-150200.100.1.
- typelib-1_0-WebKit2-4_0: antes de 2.42.4-150200.100.1.
- webkit2gtk3-debugsource: anterior a 2.42.4-150200.100.1.
- libjavascriptcoregtk-4_0-18-debuginfo: antes de 2.42.4-150200.100.1.
- webkit2gtk-4_0-injected-bundles-debuginfo: antes de 2.42.4-150200.100.1.
- typelib-1_0-JavaScriptCore-4_0: antes de 2.42.4-150200.100.1.
- webkit2gtk-4_0-paquetes-inyectados: antes de 2.42.4-150200.100.1.
- webkit2gtk3-devel: anterior a 2.42.4-150200.100.1.
- libwebkit2gtk-4_0-37-debuginfo: antes de 2.42.4-150200.100.1.
- typelib-1_0-WebKit2WebExtension-4_0: antes de 2.42.4-150200.100.1.

3. RECOMENDACIÓN:

- Actualizar el paquete afectado webkit2gtk3 a la última versión de software disponible que aborde esta vulnerabilidad.

Fuente de Información:	• hxxp://www.suse.com/support/update/announcement/2024/suse-su-20240301-1/

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°028**	**Fecha: 01-02-2024**
		Página: 8 de 13

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad en el software Appwrite		
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:

Se ha reportado una vulnerabilidad de severidad **MEDIA** de tipo falsificación de solicitudes del lado del servidor (SSRF) en el software Appwrite. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto obtener acceso a datos confidenciales ubicados en la red local o enviar solicitudes maliciosas a otros servidores desde el sistema vulnerable.

2. DETALLES:

Appwrite es una plataforma de backend de código abierto que proporciona herramientas y servicios para desarrolladores de aplicaciones web y móviles.

La vulnerabilidad de severidad **media**, identificada por MITRE como CVE-2024-1063 de tipo falsificación de solicitudes del lado del servidor (SSRF), existe debido a una validación insuficiente de la entrada proporcionada por el usuario en el punto final "/v1/avatars/favicon". Un atacante remoto puede enviar una solicitud HTTP especialmente diseñada y engañar a la aplicación para que inicie solicitudes a sistemas arbitrarios.

Esta vulnerabilidad, señala que el servidor web recibe una URL o una solicitud similar de un componente ascendente y recupera el contenido de esta URL, pero no garantiza suficientemente que la solicitud se envíe al destino esperado.

A. Productos afectados:

- Software Appwrite: 1.4.0 - 1.4.13.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxp://www.tenable.com/security/research/tra-2024-03

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°028	Fecha: 01-02-2024
		Página: 9 de 13

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad en el software Aveva Edge		
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:

Se ha reportado una vulnerabilidad de severidad **ALTA** de tipo elemento de ruta de búsqueda no controlada en Aveva Edge. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante ejecutar código arbitrario y escalar privilegios.

2. DETALLES:

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-6132 de tipo elemento de ruta de búsqueda no controlada, podría permitir a un atacante con acceso al sistema de archivos lograr la ejecución de código arbitrario y escalada de privilegios mediante la manipulación de Aveva Edge para cargar un DLL inseguro.

Esta vulnerabilidad, utiliza una ruta de búsqueda fija o controlada para encontrar recursos, pero una o más ubicaciones en esa ruta pueden estar bajo el control de actores no deseados.

A. Productos afectados:

- Aveva Edge 2020 R2 SP2 y versiones anteriores.

3. RECOMENDACIÓN:

- Actualizar a AvevaEdge 2023 o AvevaEdge 2020 R2 SP2 P01. Los clientes que utilizan AvevaEdge 2020 R2 SP2 y todas las versiones anteriores (anteriormente conocido como InduSoft Web Studio) están afectados.

Fuente de Información:	• hxxps://www.aveva.com/content/dam/aveva/documents/support/cyber-security-updates/Security_Bulletin_AVEVA-2024-002.pdf

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°028	Fecha: 01-02-2024
		Página: 10 de 13

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Detección de sitio web fraudulento del Banco 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 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 Interbank (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:**

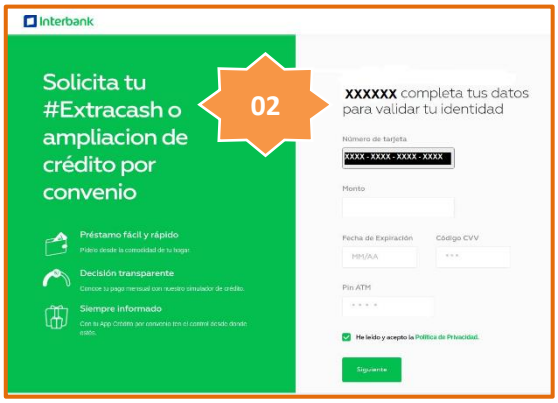
El proceso del Phishing es el siguiente:

Paso N.º 01

Solicitan a la víctima registrar lo siguiente:

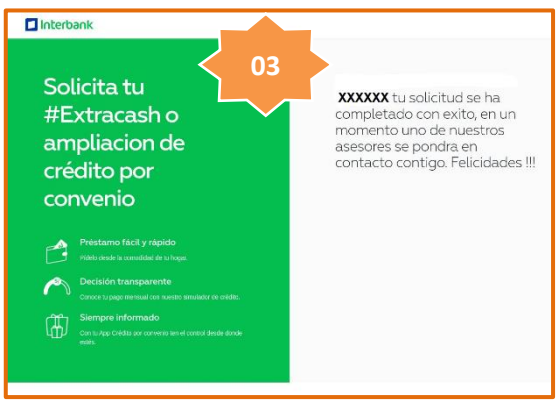
- El Documento Nacional de Identidad (DNI).
- Tarjeta de débito o crédito de la entidad financiera.
- Clave Intranet de seis dígitos.
- Operador y número telefónico.

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



Paso N.º 02

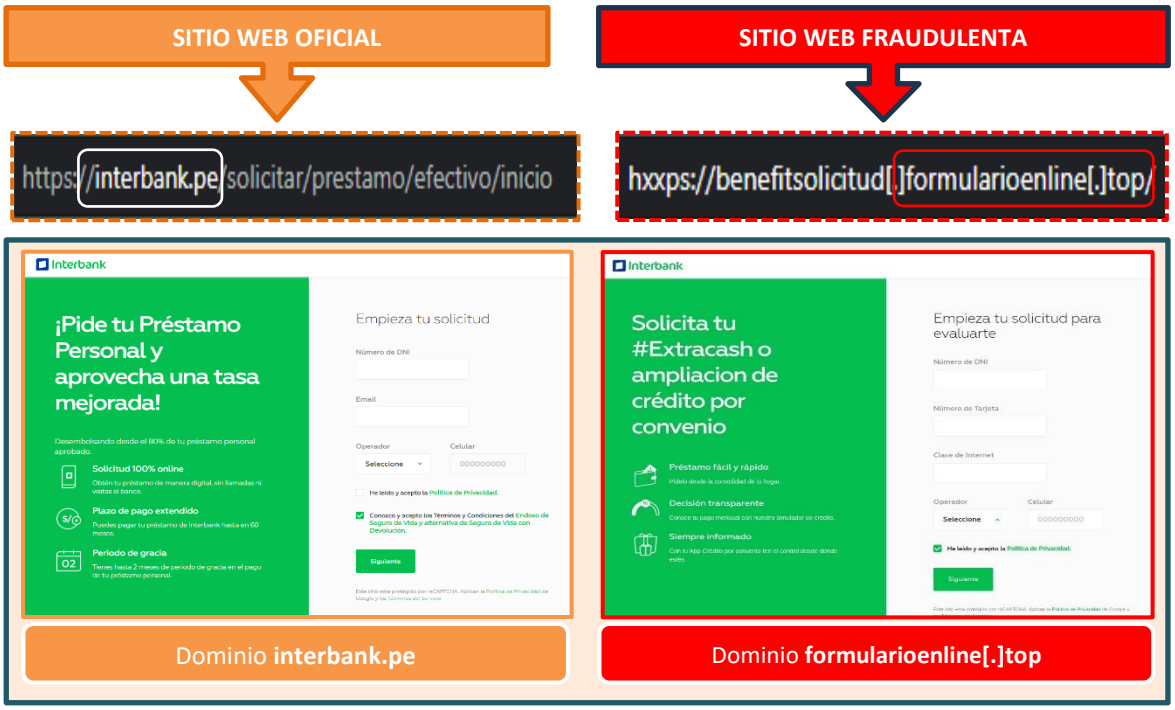
Una vez brindado los datos solicitados en el paso N.º 01, aparece una pantalla requiriendo el monto del préstamo deseado e información de la tarjeta bancaria como la fecha de expiración, el código de seguridad (CVV) y la clave de cuatro dígitos utilizado en el cajero automático, para luego dar clic en <**Siguiente**>.



Paso N.º 03

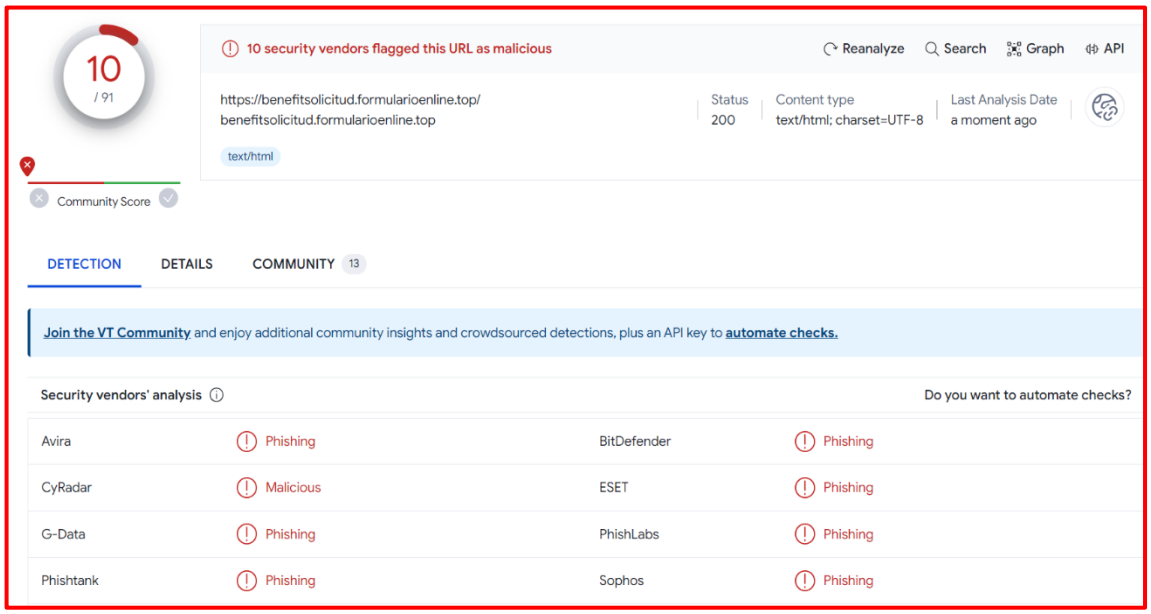
Luego, aparece una pantalla indicando que la solicitud del préstamo se ha completado con éxito y que un representante de la entidad financiera se pondrá en contacto con la víctima, para luego dar clic en <**Continuar**>. Redirigiendo al sitio web oficial de la entidad bancaria; sin embargo, los ciberdelincuentes 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.

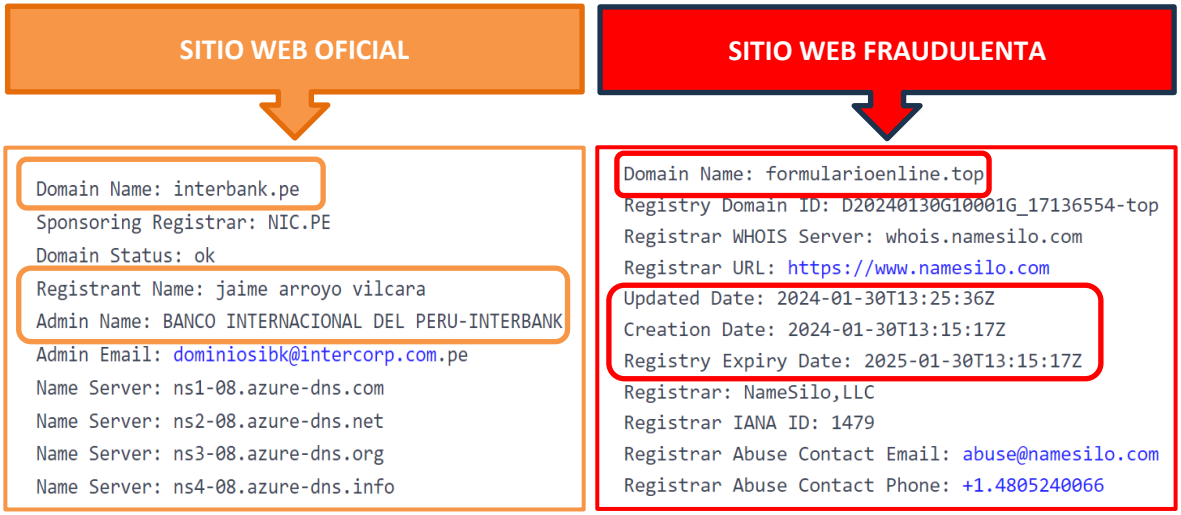
B. Proveedores de seguridad informática ALERTAN COMO SUPLANTACIÓN DE IDENTIDAD - PHISHING.



C. Indicadores de compromiso (IoC)

- Dominio : formularioenline[.]top
- SHA-256 : 796488041770d4b4eb7a6b83415f2b29506c51b350ac9f8d3a6c52fb625b4421
- IP : 104[.]21[.]2[.]111
- Servidor : Cloudflare

D. Comparación de Dominio



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