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, 09 de noviembre de 2023

268-2023-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°268	Fecha: 09-11-2023
		Página: 4 de 14

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Deepweb: cómo funciona la compraventa de credenciales robadas		
Tipo de Ataque	Robo de información	Abreviatura	RobInfo
Medios de propagación	Red, Internet, Redes sociales		
Código de familia	K	Código de Sub familia	K01
Clasificación temática familia	Uso inapropiado de recursos		

Descripción

1. ANTECEDENTES:

Una de las tantas actividades cibercriminales por la que la Deep Web es conocida es el mercado negro de credenciales y cuentas robadas.

En la Deep web se pueden encontrar foros y mercados en línea especializados donde los delincuentes pueden comprar y vender credenciales robadas de manera relativamente segura.

Si bien la mayoría de los sitios tiene un acceso sencillo, los que contienen material de "mayor interés" cibercriminal suelen requerir invitaciones, membresías exclusivas o participar activamente como vendedor, por lo que acceden personas comprometidas con actividades delictivas.

Todo este mercado se vale principalmente del anonimato y esta anonimización se logra a través de redes de como la red. onion, que oculta las direcciones IP y hacen que sea difícil rastrear a quienes participan en ella.

2. DETALLES:

Usualmente, estos mercados comercian casi todo tipo de cuentas de productos y servicios digitales. Sin embargo, las credenciales más solicitadas y disponibilizadas son:

Cuentas de redes sociales: Para generar interacciones artificiales — como la compra de likes — o llevar a cabo algún otro tipo de cibercrimen como la ingeniería social.

Cuentas de servicios de streaming: Como Netflix, Disney+, Hulu y Spotify, vendiendo aquellas con suscripciones pagas a un precio reducido en comparación con las suscripciones legítimas.

Cuentas de juegos en línea: El foco está en aquellas que vienen con niveles avanzados, elementos valiosos o monedas virtuales. Esto ahorra tiempo y esfuerzo a los compradores.

Cuentas de correo electrónico y servicios en la nube: El comprador usualmente tiene el objetivo de utilizar estos servicios para enviar spam o almacenar datos robados.

Cuentas de servicios financieros: Como PayPal, tarjetas de crédito robadas o cuentas bancarias en línea. Éstas son especialmente lucrativas para los criminales, ya que pueden realizar transacciones financieras fraudulentas o incurrir en delitos como el lavado de dinero.

Credenciales de organizaciones: Sea para acceder a información confidencial o sistemas internos, o en formato de bases de datos robadas con accesos de clientes.

El precio varía en función de la demanda y la calidad de las credenciales, o si se trata de un lote de credenciales o una individual. En general, las más valiosas son las del rubro bancario o comercial, seguidas por aquellas que traen consigo una plataforma o producto pago como un videojuego, —pueden llegar al equivalente en criptomonedas de 50 dólares, mientras que los lotes se suelen valorar en menos de 20—. Los registros individuales que pueden valer unos pocos centavos.

Uno de los métodos más comunes es el phishing. Los atacantes envían mensajes falsos que parecen legítimos para engañar a las víctimas, usualmente suplantando la identidad de la compañía dueña del servicio cuya cuenta desean obtener. Los rubros más apuntados suelen ser compañías de redes sociales, comercio electrónico y bancarias o financieras.

Otro, son los ataques de fuerza bruta: mediante un software automatizado prueban combinaciones de nombre de usuario y contraseña comunes hasta que encuentran una coincidencia. Esto no solo ocurre con cuentas de redes sociales, sino que suelen ejecutarse en sistemas internos de organizaciones, luego de un ataque en el que el cibercriminal logró acceder a ellos.

Un modo distinto es la infección con códigos maliciosos, principalmente usando aquellos que tienen capacidades de espionaje como los keyloggers o los RATs (troyanos de acceso remoto) que pueden monitorear las pulsaciones de teclado de la víctima y su pantalla. Una gran parte de los códigos maliciosos buscan archivos con credenciales en texto plano o contraseñas guardadas en navegadores, dentro de los equipos a los que infectan.

Por último, podemos nombrar las violaciones de bases de datos de organizaciones que hayan sufrido alguna intrusión, o se encuentren vulnerables, lo que exponen una gran cantidad de credenciales. En estos casos se suele comerciar, además, bases de datos confidenciales como correos electrónicos, identificadores gubernamentales, nombres completos.

3. RECOMENDACIONES:

- Tener cuidado con el phishing: Ante la recepción de un correo electrónico, mensaje o llamada inesperada que solicite información personal o financiera, debes verificar la autenticidad de la fuente antes de responder o hacer clic en enlaces.
- Evitar hacer clic en enlaces sospechosos: Se recomienda evitar hacer clic en enlaces que te lleguen en comunicaciones no solicitadas, o en links que aparezcan en resultados de búsquedas que no tengan el dominio de la compañía, u organización.
- Mantener los sistemas actualizados: Es fundamental mantener instaladas las últimas actualizaciones de seguridad en la computadora y los dispositivos móviles para prevenir posibles vulnerabilidades conocidas.
- Utilizar contraseñas seguras: Es importante emplear contraseñas robustas que combinen letras mayúsculas y minúsculas, números y caracteres especiales. También, evitar el reciclaje de contraseñas para disminuir el daño en caso de sufrir una filtración de credenciales.

Fuente de Información:	• hxxps://www.welivesecurity.com/es/cibercrimen/deepweb-como-funciona-la-compraventa-de-credenciales-robadas/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°268	Fecha: 09-11-2023
		Página: 6 de 14

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Nueva campaña de Spam utiliza el portal de noticias de Windows para distribuir malware		
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:

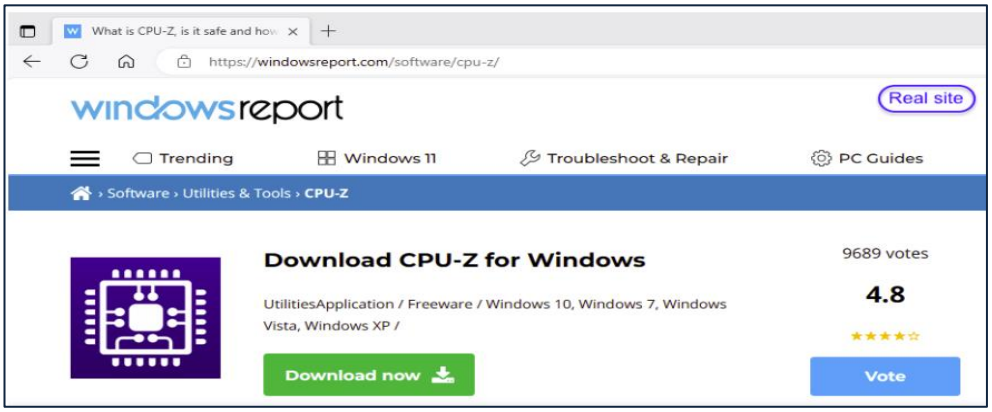
Investigadores de Inteligencia de amenazas de Malwarebytes, han informado que se ha detectado una nueva campaña de distribución de malware "RedLine Stealer", que utiliza publicidad maliciosa y se hace pasar por un portal de noticias legítimo de Windows. Un ataque exitoso podría permitir a un actor de amenazas el robo de credenciales de inicio de sesión, el robo de contraseñas, tarjetas de crédito e información confidencial, entre otros. De igual forma, un actor de amenazas también podría infectar a sus víctimas con otros tipos de malware, como ransomware, troyanos, mineros de criptomonedas y RAT.

2. DETALLES:

Los investigadores han observado una nueva campaña de publicidad maliciosa en la que los actores de amenazas copian un portal de noticias legítimo de Windows (WindowsReport.com) para distribuir un instalador malicioso de malware "RedLine Stealer", para la popular herramienta de procesador CPU-Z. Cabe señalar, que el portal de noticias de Windows nunca se vio comprometido y es legítimo, sino que los actores de amenazas copiaron su contenido para engañar a los usuarios, al suplantar el sitio oficial por otra que contiene la carga útil de malware.

"RedLine Stealer" es un programa malicioso de robo de información más destacados y utilizados en la actualidad. Según un informe de Insikt Group, es uno de los mayores proveedores de credenciales robadas para dos mercados clandestinos: Amigos Market y Russian Market. Su comercio se ha observado en mercados clandestinos a través de una serie de videos de YouTube sobre las principales tendencias globales de interés, como las NFT. Se detectó en foros de cibercriminales en febrero de 2020, como Malware-as-a-Service (MaaS).

"RedLine Stealer" es conocido por troyanizar servicios populares como Telegram (utilizando tácticas de ingeniería social como señuelos COVID-19), Signal y Discord (disfrazados de instaladores de Windows 11). También aprovecha las campañas de phishing por correo electrónico, Google Ads (para clasificar sitios web maliciosos) y experimentos con tácticas de ingeniería social dirigidas a los entusiastas de NFT.



El anuncio malicioso es para CPU-Z, una utilidad popular para usuarios de Windows que desean solucionar problemas de su procesador y otros detalles del hardware de su computadora. El anunciante aparece como Scott Cooper y probablemente sea una identidad falsa o comprometida.

Una técnica común utilizada por los actores de amenazas para evadir la detección es emplear encubrimiento. Cualquier persona que haga clic en el anuncio y que no sea la víctima prevista verá un blog estándar con varios artículos. Si la víctima que busca la aplicación CPU-Z hace clic en el anuncio, será redirigida a la página de descarga del software suplantado, donde pueden suponer erróneamente que es legítimo. Sin embargo, la URL de la barra de direcciones no coincide con la URL oficial de la aplicación.

Sin embargo, en un caso real, la víctima objetivo es redirigida a una página de descarga que contiene un instalador MSIX firmado digitalmente para evadir la detección. Una vez que el usuario hace clic en el instalador, se ejecuta en el sistema un script de PowerShell malicioso llamado "FakeBat", que descarga Redline Stealer. El script muestra el servidor de comando y control (C2) de malware, así como la carga útil remota Redline stealer. Los cargadores MSI son bastante comunes y permiten a los actores de amenazas actualizar la carga útil final simplemente intercambiando un script de PowerShell.

Según la infraestructura, los nombres de dominio y las plantillas de encubrimiento utilizadas, los investigadores creen que el incidente es parte de una campaña de publicidad maliciosa más amplia dirigida a otras utilidades como Notepad++, Citrix y VNC Viewer.

A. Indicadores de compromiso (IoC):

Dominios publicitarios:
- argenferia[.]com.
- realvnc[.]pro.
- Corporatecomf[.]online.
- cilrix-corp[.]pro.
- thecoopmodel[.]com.
- winscp-apps[.]online.
- wirehark-app[.]online.
- cilrix-corporate[.]online.
- workspace- aplicación[.]online.

URL de carga útil:
- thecoopmodel[.]com/CPU-Z-x86.msix.
- kaotickontracting[.]info/account/hdr.jpg.
- ivcgroup[.]en/temp/Citrix-x64.msix.
- robo-reclamo[.]sitio/orden/team.tar.gpg.
- argenferia[.]com/RealVNC-x64.msix.

Cargas útiles:
- 55d3ed51c3d8f56ab305a40936b446f761021abfc55e5cc8234c98a2c93e99e1.
- 9acbf1a5cd040c6dcecbe4e8e65044b380b7432f46c5fbf2ecdc97549487ca88.
- 419e06194c01ca930ed5d7484222e6827fd24520e72bfe6892cfde95573ffa16.
- cf9589665615375d1ad22d3b84e97bb686616157f2092e2047adb1a7b378cc95.

C2:
- 11234jkhfkujhs[.]site.
- 11234jkhfkujhs[.]top.
- 94.131.111[.]240.
- 81.177.136[.]179.

3. RECOMENDACIONES:

- Verificar la suma de comprobación de un archivo para asegurarse de que no haya sido manipulado comparando su suma hash SHA256 con lo que se publica en el sitio web del proveedor.
- Mantener su sistema operativo y software actualizados con los últimos parches y actualizaciones de seguridad.
- Utilizar un programa antivirus y mantenerlo siempre actualizado.
- Tener cuidado al abrir archivos adjuntos de correo electrónico o al hacer clic en enlaces de fuentes desconocidas.
- Evitar descargar software de fuentes no confiables y de sitios no oficiales.
- Utilizar contraseñas seguras y únicas para todas sus cuentas y evite guardar contraseñas en su navegador.
- Hacer una copia de seguridad periódica de sus datos importantes en un disco duro externo o en un servicio de almacenamiento en la nube.

Fuente de Información:	• hxxps://www.malwarebytes.com/blog/threat-intelligence/2023/11/malvertiser-copies-pc-news-site-to-deliver-infostealer • hxxps://cyware.com/news/threat-actors-impersonate-windows-news-portal-to-distribute-redline-stealer-7b320bfd • hxxps://cyware.com/resources/research-and-analysis/all-about-high-in-demand-information-theft-tool-redline-stealer-0df1

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°268**	**Fecha: 09-11-2023**
		Página: 8 de 14

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades en PostgreSQL		
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 **ALTA** de tipo desbordamiento de enteros, divulgación de información y permisos, privilegios y controles de acceso en PostgreSQL. La explotación exitosa de estas vulnerabilidades podría permitir a un usuario remoto ejecutar código arbitrario en el sistema de destino, realizar un ataque denegación de servicio (DoS) y obtener acceso a información confidencial.

2. DETALLES:

PostgreSQL, también llamado Postgres, es un sistema de gestión de bases de datos relacional orientado a objetos y de código abierto, publicado bajo la licencia PostgreSQL, similar a la BSD o la MIT.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-5869 de tipo desbordamiento de enteros, existe debido al desbordamiento de enteros en la modificación de la matriz. Un usuario remoto puede pasar datos especialmente diseñados a la aplicación, provocar un desbordamiento de enteros y ejecutar código arbitrario en el sistema de destino.

Esta vulnerabilidad realiza un cálculo que puede producir un desbordamiento o envoltura de enteros, cuando la lógica supone que el valor resultante siempre será mayor que el valor original. Esto puede introducir otras debilidades cuando el cálculo se utiliza para la gestión de recursos o el control de ejecución.

Se han asignado los siguientes identificadores para las vulnerabilidades de severidad baja: CVE-2023-5868 y CVE-2023-5870.

A. Productos afectados:

- PostgreSQL: 11.0 - 16.0

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxp://www.postgresql.org/about/news/postgresql-161-155-1410-1313-1217-and-1122-released-2749/

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°268**	**Fecha: 09-11-2023** **Página: 9 de 14**

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad crítica en la herramienta SysAid		
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 recorrido de ruta (Path Traversal) en la herramienta SysAid. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino y comprometer el sistema.

2. DETALLES:

La vulnerabilidad de severidad **crítica**, identificada por MITRE como CVE-2023-47246 de tipo recorrido de ruta (Path Traversal), existe debido a un error de validación de entrada al procesar secuencias de recorrido de directorio. Un atacante remoto puede cargar y ejecutar código arbitrario en el sistema. Tenga en cuenta que el actor Lace Tempest (DEV-0950) está explotando activamente la vulnerabilidad en la naturaleza.

Esta vulnerabilidad, utiliza entradas externas para construir un nombre de ruta destinado a identificar un archivo o directorio ubicado debajo de un directorio principal restringido, pero el producto no neutraliza adecuadamente los elementos especiales dentro del nombre de ruta que pueden hacer que el nombre de ruta se resuelva en una ubicación que está fuera del directorio restringido.

A. Productos afectados:

- SysAid: 21.4.45 - 23.3.35

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxp://www.sysaid.com/blog/service-desk/on-premise-software-security-vulnerability-notification

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°268	Fecha: 09-11-2023
		Página: 10 de 14

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad en 4D y 4D server Windows		
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:

Alexander Huamán Jaimes (@zanganox) ha reportado una vulnerabilidad de severidad **MEDIA** de tipo elemento de ruta de búsqueda no controlado en 4D y 4D server Windows. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto la ejecución de código arbitrario.

2. DETALLES:

La vulnerabilidad de severidad **media,** identificada por MITRE como CVE-2023-4770 de tipo elemento de ruta de búsqueda no controlado, consiste en un secuestro de DLL, sustituyendo x64 shfolder.dll en la ruta de instalación y provocando una ejecución de código arbitrario.

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:

- Los ejecutables 4D.exe y 4D Server.exe, en sus versiones 19 R8 100218.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que el proveedor lance para abordar esta vulnerabilidad.

Fuente de Información:	• hxxps://es.4d.com/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°268	Fecha: 09-11-2023
		Página: 11 de 14

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Nueva campaña de Phishing que suplanta la entidad bancaria de BBVA		
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, los ciberdelincuentes vienen llevando a cabo avanzados ataques cibernéticos, por medio de envíos de correos electrónicos fraudulentos, o también conocidos como Phishing, simulado ser la entidad bancaria BBVA, en cual tiene el objetivo de robar credenciales de acceso, datos personales y/o bancarios.

2. **DETALLES:**

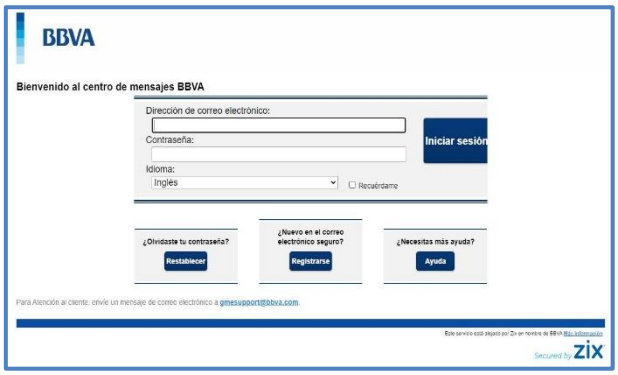


Imagen 1.
Sitio web fraudulenta del Banco BBVA, solicita a las víctimas registrar la dirección del correo electrónico, la contraseña y el idioma para iniciar sesión.

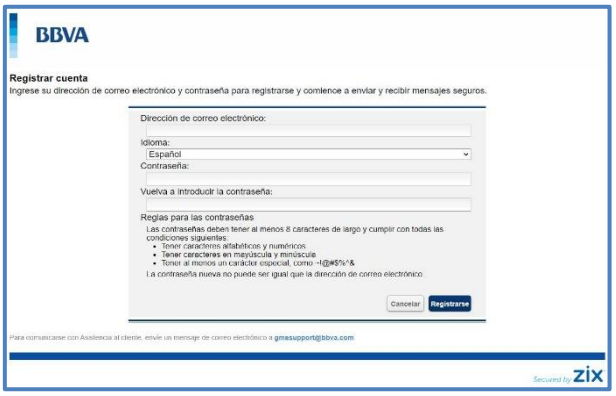


Imagen 2.
Luego de no poder iniciar sesión y darle click en “olvidaste la contraseña” requiere registrar la dirección del correo electrónico, el tipo de idioma y volver a introducir la contraseña para continuar.

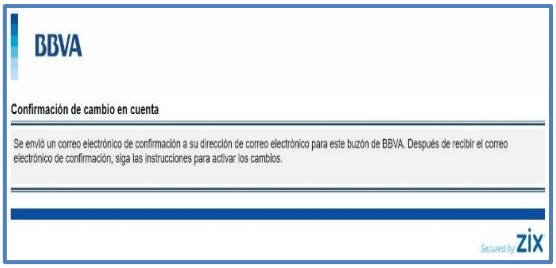
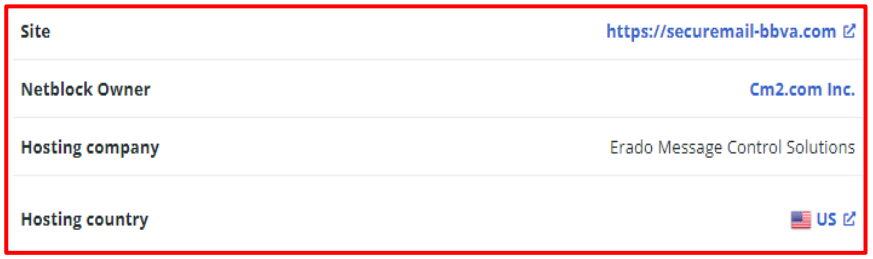


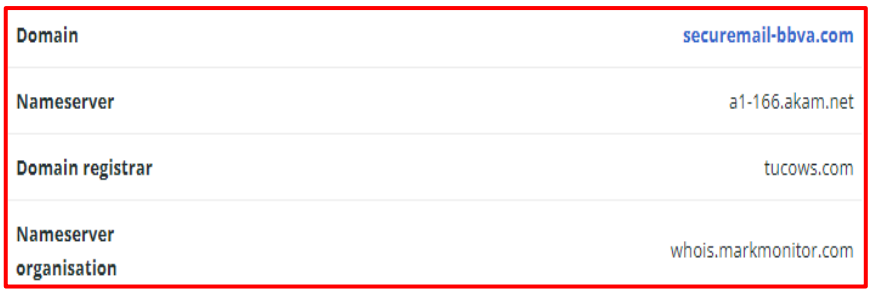
Imagen 3.
Por último, solicita a la víctima confirmar la cuenta, lo cual tendría que ingresar al correo electrónico y completar lo requerido por los atacantes, para luego informar a la víctima que ha ocurrido un error de autenticación; sin embargo, los datos fueron capturados por los cibercriminales.

A. Proveedores de seguridad informática alertan como **SUPLANTACIÓN DE IDENTIDAD – PHISHING**:

- Indicadores de compromiso:
  - **URL**: hxxps://securemail-bbva[.]com/s/e?m=ABBieQGLzTrqW02evV9TpPMp&em=3mail@b[.]c/



  - **Dominio**: securemail-bbva[.]com



  - **IP**: 207[.]195[.]182[.]15

  - **Server:** Apache
  - **SHA-256**: cca705a84a83d7a858b8435aff11da900e3a6c133c21f5efe9dfa723338d477d
  - **Tipo de Contexto:** Text/Html

- **Otros resultados del análisis**:

B. Apreciación de la información:

La presente campaña de Phishing, permite a los actores de amenazas obtener las credenciales de acceso a la banca por internet de los usuarios del Banco BBVA.

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.

C. Que es un Phishing:

Es un término informático que distingue a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza, para manipularla y hacer que realice acciones que no debería realizar.

3. RECOMENDACIONES:

- Verificar detalladamente la URL, que corresponda al sitio web oficial del banco BBVA.
- Evitar seguir las instrucciones de sitio web sospechoso o de dudosa procedencia.
- Mantener el antivirus actualizado, ya que es la primera barrera ante posibles ataques cibernéticos.
- Evitar compartir la URL con amigos y/o familiares.
- Ingresar desde fuentes oficiales (www.bbva.pe).

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

Índice alfabético