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, 23 de marzo de 2024

072-2024-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°072	Fecha: 23-03-2024
		Página: 4 de 8

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Los piratas informáticos rusos utilizan el malware 'WINELOADER' para atacar a los partidos políticos alemanes		
Tipo de Ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegacion de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

Los investigadores advierten que un notorio grupo de hackers vinculado al Servicio de Inteligencia Exterior de Rusia (SVR) está atacando a partidos políticos en Alemania por primera vez.

APT29 (también conocido como Midnight Blizzard, NOBELIUM, Cozy Bear) es un grupo de piratería de espionaje ruso que se cree que forma parte del Servicio de Inteligencia Exterior de Rusia (SVR). Ha estado vinculado a muchos ataques cibernéticos, incluido el infame ataque a la cadena de suministro de SolarWinds en diciembre de 2020.

Los actores de amenazas han permanecido activos a lo largo de estos años, generalmente apuntando a gobiernos, embajadas, altos funcionarios y diversas entidades utilizando una variedad de tácticas de phishing o compromisos en la cadena de suministro.

2. DETALLES:

Los ataques de phishing están diseñados para implementar un malware de puerta trasera llamado WineLoader, que permite a los actores de amenazas obtener acceso remoto a dispositivos y redes comprometidas.

Este malware es capaz de suplantar a partidos políticos alemanes con correos electrónicos que simulaban ser de la Unión Cristianodemócrata (CDU) en torno al 26 de febrero de 2024.

Las cadenas de ataque aprovechan los correos electrónicos de phishing con contenido señuelo en alemán que pretende ser una invitación a una cena para engañar a los destinatarios para que hagan clic en un enlace falso y descarguen un archivo de aplicación HTML (HTA) fraudulento, un cuentagotas de primera etapa llamado ROOTSAW (también conocido como EnvyScout) que actúa como un conducto para entregar WINELOADER desde un servidor remoto.

"El documento señuelo en alemán contiene un enlace de phishing que dirige a las víctimas a un archivo ZIP malicioso que contiene un dropper ROOTSAW alojado en un sitio web comprometido controlado por un actor", dijeron los investigadores. "El ROOTSAW entregaba un documento señuelo de segunda etapa con un tema de la CDU y una carga útil WINELOADER de seguimiento".

WINELOADER, invocado a través de una técnica llamada carga lateral de DLL usando el sqldumper.exe legítimo, viene equipado con capacidades para contactar un servidor controlado por un actor y recuperar módulos adicionales para su ejecución en los hosts comprometidos.

3. RECOMENDACIONES:

- No hacer clic en enlaces sospechosos ni descargar archivos adjuntos de fuentes desconocidas.
- Verificar la fuente de información de tus correos entrantes.
- Mantener el software actualizado. Actualizar periódicamente los sistemas operativos, las aplicaciones y el software de seguridad para corregir las vulnerabilidades.
- Implementar soluciones de seguridad integrales que puedan detectar y bloquear malware.
- Capacitar a los usuarios sobre las mejores prácticas de ciberseguridad.

Fuente de Información:	• hxxps://thehackernews.com/2024/03/russian-hackers-use-wineloader-malware.html • hxxps://www.bleepingcomputer.com/news/security/russian-hackers-target-german-political-parties-with-wineloader-malware/#google_vignette

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°072	Fecha: 23-03-2024
		Página: 5 de 8

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:**

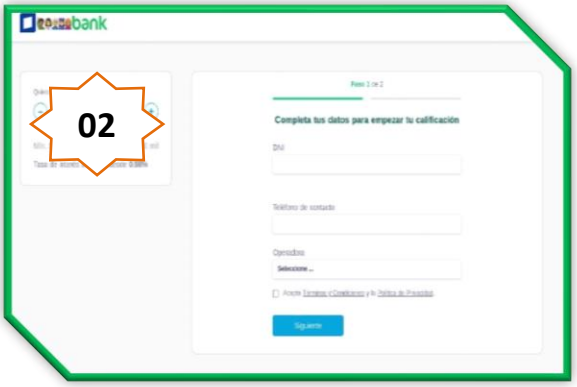
A través del monitoreo y búsqueda de amenazas en el espacio digital, se detectó que actores de amenazas vienen llevando a cabo una campaña de Phishing, suplantando el sitio web de solicitud de préstamos del Banco Interbank, con la finalidad de robar información sensible de los usuarios de la entidad financiera como números de documento de identidad, tarjetas bancarias, etc.

2. **DETALLES:**

El proceso del Phishing es el siguiente:

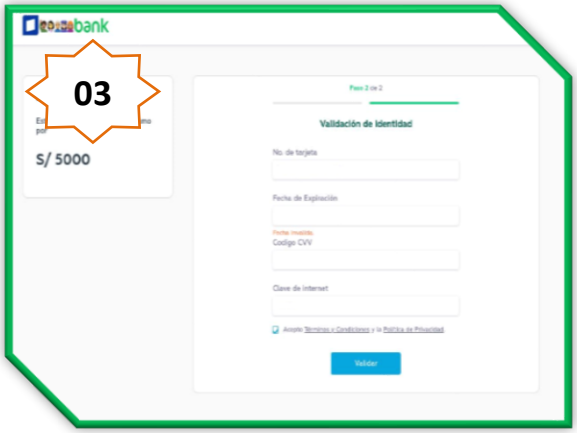
Paso Nº01

Sitio web fraudulento del Banco de Interbank, solicita a la víctima registrar el monto del préstamo solicitado, para luego dar clic en <Calificar ahora>.



Paso Nº02

Al ingresar el monto solicitado y darle clic <Calificar ahora>, solicita a la víctima completar los datos para empezar la calificación como el número del Documento Nacional de Identidad (DNI), número de celular y operador telefónico, para luego dar clic en <Siguiente>.



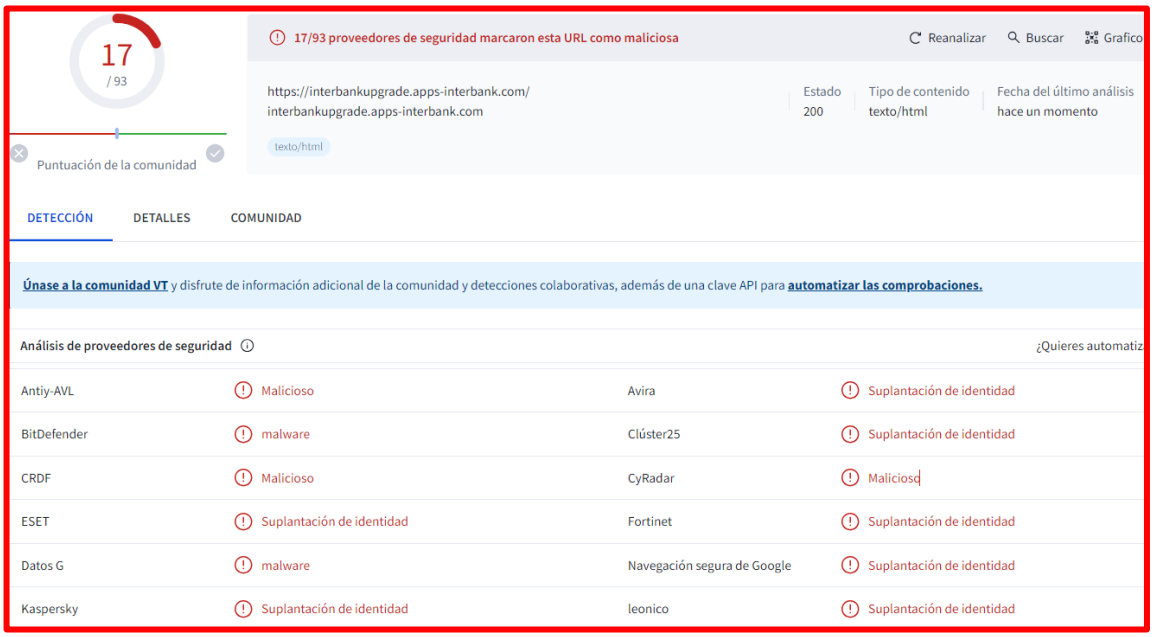
Paso Nº03

Una vez brindado los datos solicitados en el paso N.º 02, aparece una pantalla requiriendo información como el numero de la tarjeta bancaria, la fecha de expiración, el código de seguridad (CVV) y la clave de seis dígitos del intranet, para luego dar clic en <Validar>. Pero, pasado unos segundos, redirige 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.

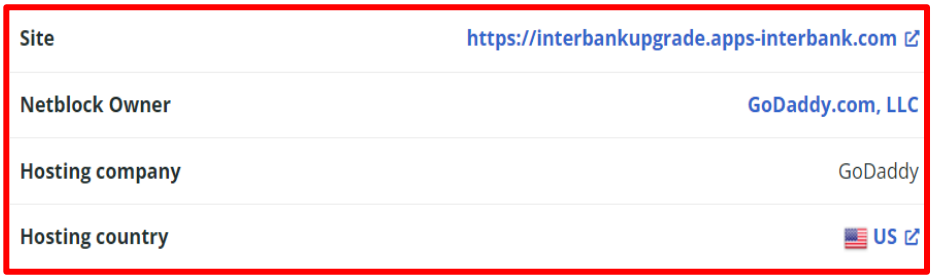
- Existe una diferencia entre la URL original y la URL fraudulenta.
- La URL del sitio web fraudulento posee protocolo de seguridad de red (https)
- Existe una similitud entre ambas páginas en imagen, fondo y color.

B. Proveedor de seguridad informática no alerta como SUPLANTACIÓN DE IDENTIDAD - PHISHING.

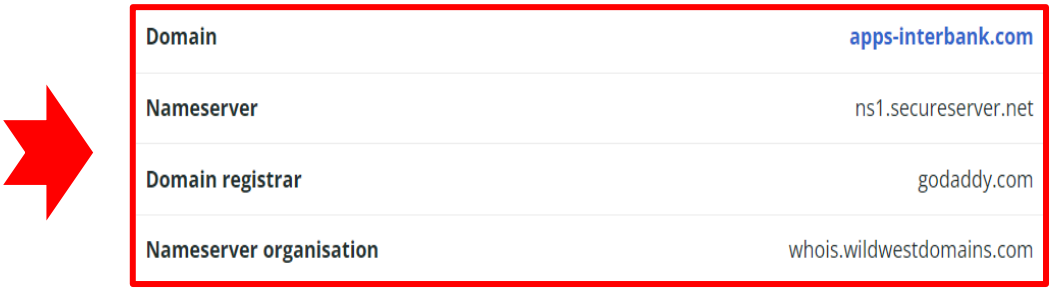


C. Indicadores de compromiso (IoC)

- Url : hxxps[:]//interbankupgrade[.]apps-interbank[.]com/



- Dominio : apps-interbank[.]com



Domain	apps-interbank.com
Nameserver	ns1.secureserver.net
Domain registrar	godaddy.com
Nameserver organisation	whois.wildwestdomains.com

- IP : 166[.]62[.]85[.]139

IPv4 address (166.62.85.139)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ 166.0.0.0-166.255.255.255	United States	NET166	Various Registries (Maintained by ARIN)
↳ 166.62.0.0-166.62.127.255	United States	GO-DADDY-COM-LLC	GoDaddy.com, LLC
↳ 166.62.85.139	United States	GO-DADDY-COM-LLC	GoDaddy.com, LLC

- SHA-256 : e9bfea87b7dd52e96fc57cc17621276966a9b03828948e639042e919f016d866
- Servidor : APACHE
- Tipo Contenido : Texto/Html

D. Apreciación de la información:

- La presente campaña de Phishing permite a los actores de amenazas obtener información bancaria de los usuarios del Banco Interbank.
- 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 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).
- Comunicar a la entidad financiera si ha realizado un registro de acceso en un sitio web sospechoso.

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

Índice alfabético