



PERÚ

Presidencia
del Consejo de Ministros

Secretaría de Gobierno
y Transformación Digital



Siempre
con el pueblo



ALERTA INTEGRADA DE SEGURIDAD DIGITAL



Lima, 17 de octubre de 2022

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

N° 282-2022-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

Troyano bancario “Zanubis” activo en aplicaciones de usuarios en Perú.....	4
Vulnerabilidad de elevación de privilegios de servicios de certificados de Active Directory	7
Microsoft lanzó una actualización que corrige fallas en el protocolo de enlace TLS en Windows Server 2019.....	9
Phishing suplantando la identidad del Banco de Crédito del Perú - BCP	11
Índice alfabético	13

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 282			Fecha: 17-10-2022
				Página 04 de 13
Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL			
Nombre de la alerta	Troyano bancario "Zanubis" activo en aplicaciones de usuarios en Perú			
Tipo de ataque	Malware	Abreviatura	Malware	
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet			
Código de familia	C	Código de subfamilia	C02	
Clasificación temática familia	Código Malicioso			
Descripción				
<p>En las últimas semanas se ha observado el regreso del troyano bancario "Zanubis" en aplicaciones Android de usuarios en Perú, cuyo objetivo es robar credenciales bancarias de las víctimas.</p> <p>ANTECEDENTES:</p> <ul style="list-style-type: none"> Zanubis es una pieza de malware clasificada como troyano bancario, dirigido a los sistemas operativos Android. La función principal de este programa es obtener sigilosamente credenciales de cuentas bancarias en línea y obtener acceso a los fondos almacenados en ellas. Zanubis apunta a bancos latinoamericanos, particularmente aquellos con sede en Perú. <p>DETALLES:</p> <ul style="list-style-type: none"> Una conocida variante de malware en dispositivos Android llamado "Zanubis" dirigido aplicaciones móviles en el Perú, se encuentra activo y está siendo utilizado por actores de amenaza según los últimos reportes de incidentes en estas semanas. Investigadores de Cyble Research realizaron un informe en donde analizaron una muestra del troyano identificándolo como una nueva variante de "Android Banking Trojan", dirigida a más de 40 aplicaciones del Perú. Según los investigadores, el actor de amenazas usa la cadena "Zanubis" como clave para descifrar las respuestas recibidas del servidor C&C (comando y control), por lo que utilizaron ese nombre para denominar al malware. <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <pre> this.KEY_STR = "zanubis"; this.URL_INICIAL = "http://sakomountain.com/blog/3/"; this.ALARMA_NOMBRE = "startAlarm"; this.TEXTO_TOAST_PERMISO_BATERIA = "Habilite los permisos de bateria para "; this.TEXTO_TOAST_PERMISO_ACCESIBILIDAD = "Active el permiso de accesibilidad para "; this.SPLIT_PREFERENCE = "#"; this.FALSE_STR = "false"; this.TRUE_STR = "true"; this.NO = "no"; this.SI = "si"; this.EMPTY_STR = ""; this.PREF_TOKE_PEDIR = "pref_toke_pedir"; this.APP_NOMBRE = "personal.pdf"; this.APP_PACKAGE = BuildConfig.APPLICATION_ID; this.PREF_LLAVE = "cc638784cf213986ec75983a4aa08cda"; </pre> </div> <ul style="list-style-type: none"> El objetivo de este malware es robar credenciales de cuentas bancarias para acceder a ellas. Para ello, este pretende ser un documento PDF (formato utilizado en oficinas bancos, organizaciones gubernamentales e instituciones educativas). Los archivos con inyección de malware analizados se dirigían a bancos en Perú y a dos aplicaciones de redes sociales: WhatsApp y Gmail. El equipo de investigación decodificó algunas de las muestras del malware, incluido un archivo llamado "Personal[.pdf]" que contenía un paquete llamado "com[.]personal[.]pdf" y un código hash SHA256 alfanumérico de 64 dígitos. 				

APP ICON

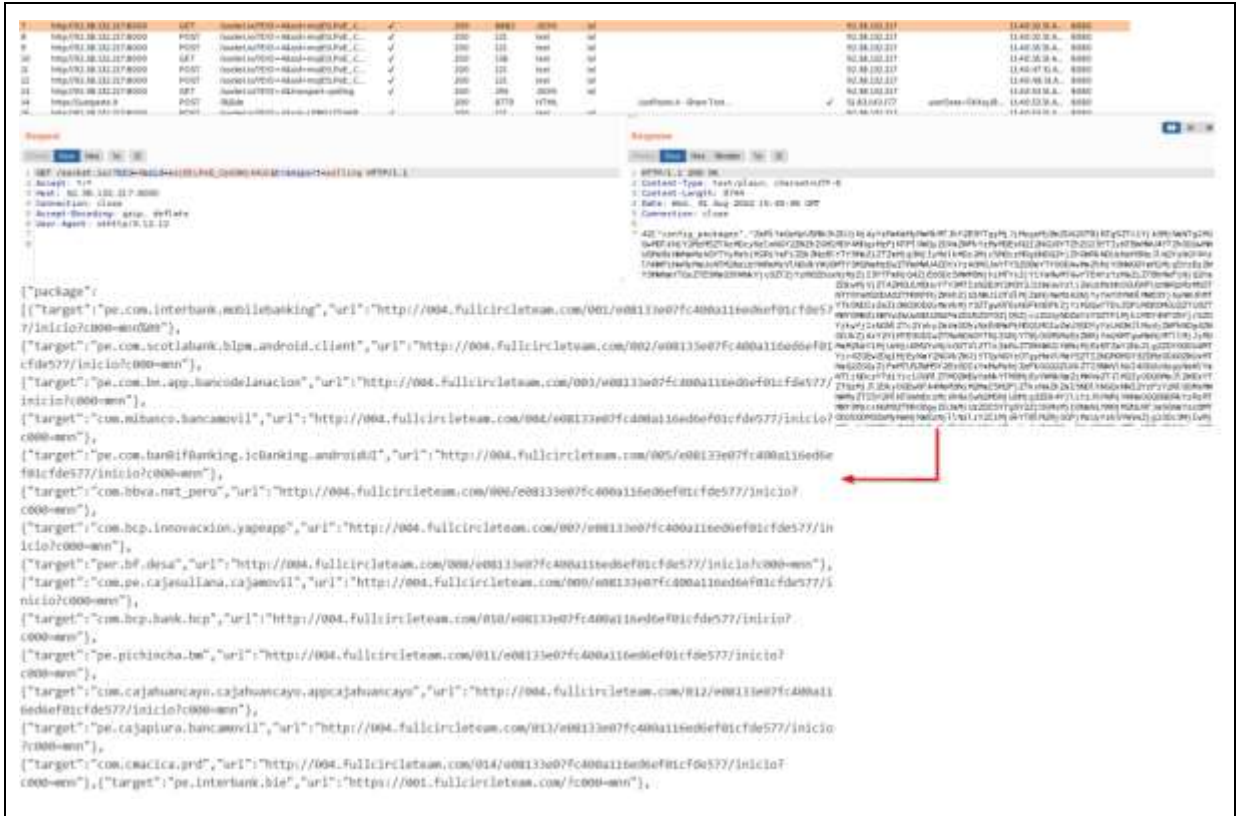


FILE INFORMATION

File Name: documento_2a3d3dd.pdf.apk
 Size: 4.04MB
 MD5: 8f78d9b128eb2b0fb576269bba6a9fb
 SHA1: 2128c991887a80152ca36689be503eaa6afc1bf
 SHA256: 33adbff1a79da4a3fde49cececac5a6b99bf217b0c6db6cd85a46bf2087e57

APP INFORMATION

App Name: Personal.pdf
 Package Name: com.personal.pdf
 Main Activity: com.personal.pdf.vistas.MainActivity
 Target SDK: 31 Min SDK: 23 Max SDK:
 Android Version Name: 1.0 Android Version Code: 1



```

["package":
  [{"target": "pe.com.interbank.mobilebanking", "url": "http://004.fullircircleteam.com/001/e08133e07fc400a116ed6ef01cfde577/inicio?c000=mn"},
  [{"target": "pe.com.totolabank.bipa.android.client", "url": "http://004.fullircircleteam.com/002/e08133e07fc400a116ed6ef01cfde577/inicio?c000=mn"},
  [{"target": "pe.com.bt.app.bancodelaunion", "url": "http://004.fullircircleteam.com/003/e08133e07fc400a116ed6ef01cfde577/inicio?c000=mn"},
  [{"target": "com.mibanco.bancamovil", "url": "http://004.fullircircleteam.com/004/e08133e07fc400a116ed6ef01cfde577/inicio?c000=mn"},
  [{"target": "pe.com.banifibanking.icBanking.android", "url": "http://004.fullircircleteam.com/005/e08133e07fc400a116ed6ef01cfde577/inicio?c000=mn"},
  [{"target": "com.bbva.net_peru", "url": "http://004.fullircircleteam.com/006/e08133e07fc400a116ed6ef01cfde577/inicio?c000=mn"},
  [{"target": "com.bcp.innovaciones.yapeapp", "url": "http://004.fullircircleteam.com/007/e08133e07fc400a116ed6ef01cfde577/inicio?c000=mn"},
  [{"target": "per.bf.desa", "url": "http://004.fullircircleteam.com/008/e08133e07fc400a116ed6ef01cfde577/inicio?c000=mn"},
  [{"target": "com.pe.cajesallana.cajamovil", "url": "http://004.fullircircleteam.com/009/e08133e07fc400a116ed6ef01cfde577/inicio?c000=mn"},
  [{"target": "com.bcp.bank.bcp", "url": "http://004.fullircircleteam.com/010/e08133e07fc400a116ed6ef01cfde577/inicio?c000=mn"},
  [{"target": "pe.pichincha.bs", "url": "http://004.fullircircleteam.com/011/e08133e07fc400a116ed6ef01cfde577/inicio?c000=mn"},
  [{"target": "com.cajahuancayo.cajahuancayo.appcajahuancayo", "url": "http://004.fullircircleteam.com/012/e08133e07fc400a116ed6ef01cfde577/inicio?c000=mn"},
  [{"target": "pe.cajapiura.bancamovil", "url": "http://004.fullircircleteam.com/013/e08133e07fc400a116ed6ef01cfde577/inicio?c000=mn"},
  [{"target": "com.enacica.pdf", "url": "http://004.fullircircleteam.com/014/e08133e07fc400a116ed6ef01cfde577/inicio?c000=mn"}, {"target": "pe.interbank.bis", "url": "https://001.fullircircleteam.com/c000=mn"}],
  
```

- Se encontró que la aplicación tenía 30 permisos, de los cuales, Zanubis explota 10. Estos son los diez permisos que explotó el actor de amenaza:

Permiso	Descripción
READ_CONTACTS	Acceder a contactos telefónicos
RECEIVE_SMS	Permite que una aplicación reciba mensajes SMS
READ_SMS	Acceder a mensajes telefónicos
CAMERA	Acceder al dispositivo de la cámara.
READ_EXTERNAL_STORAGE	Permite que la aplicación lea el contenido del almacenamiento externo del dispositivo.
RECORD_AUDIO	Permite que la aplicación grabe audio con el micrófono.
WRITE_EXTERNAL_STORAGE	Permite que la aplicación escriba o elimine archivos en el almacenamiento externo del dispositivo.
CALL_PHONE	Permite que la aplicación inicie una llamada telefónica sin pasar por la interfaz de usuario del marcador para que el usuario confirme la llamada.
SEND_SMS	Permite que una aplicación envíe mensajes SMS
SYSTEM_ALERT_WINDOW	Permite que una aplicación cree ventanas encima de todas las demás aplicaciones

- Estos permisos incluyeron parte de la funcionalidad básica de los dispositivos, algo que no debe verse comprometido, ya que permite que el actor de amenaza acceda a archivos internos del usuario víctima, los manipule, los elimine, e incluso espíe información confidencial de los dispositivos de destino.


- Por otro lado, los investigadores descubrieron que el malware se conecta a un servidor C&C “hxxp[:]//92[.]38[.]132 [.] 217[:] 8000” y recibe la lista de aplicaciones y su URL de superposición. Luego hace uso de todos los permisos en el dispositivo de destino. Una vez que el usuario activa el “servicio de accesibilidad”, el malware evita que el sistema se desactive y activa todos los permisos en el dispositivo de destino.
- Después de recibir todos los detalles requeridos, el malware comienza a descifrar la respuesta y guarda los archivos con el nombre “cc638784cf213986ec75983a4aa08cda[.]xml”. Después, escanea a través de la información en el dispositivo de destino y envía la lista de aplicaciones de instalación, contactos, estado del permiso SMS y otra información al ciberdelincuente a través del servidor C&C.
- A continuación, se incluyen los indicadores de compromiso asociados al troyano “Zanubis”:

Indicador	Tipo de indicador	Descripción
0198b8fa11bf9e8442defa00befa2ab224ada5ebb4a60256f2bf5fc491cca0a1	SHA256	Hash del archivo APK analizado
93be818f6087423909594f5630b67cf0ddcf71b6	SHA1	Hash del archivo APK analizado
0b3248698651c68aa79c128c26df6f5c	MD5	Hash del archivo APK analizado
33adbff1a79da4a3fde49cececac5a6b99bf217be0c6db6cdf85a46bf2087e57	SHA256	Hash del archivo APK analizado
2128c991887a80152ca36689be503eaa6afc1b1f	SHA1	Hash del archivo APK analizado
8f78df9b128eb2b0fb576269bba6a9fb	MD5	Hash del archivo APK analizado
95242e1d105de9c33b2c9d8a9514f58327ca32d7d24af9af19ff3f0d075ea451	SHA256	Hash del archivo APK analizado
74c03b47d0449e08ef9e645e79aaada5e0aedc9d	SHA1	Hash del archivo APK analizado
e7495ddd6f4e5c686c2ee68b3db91f9b	MD5	Hash del archivo APK analizado
hxxp://92.38.132[.]217:8000	URL	Servidor C&C

RECOMENDACIONES:

- Descargar aplicaciones solo en tiendas oficiales como Google Play Store o iOS App Store.
- Hacer uso de contraseñas seguras.
- Aplicar la autenticación multifactor siempre que sea posible.
- Realizar una copia de seguridad de los archivos personales.
- En caso de una transacción fraudulenta, informar inmediatamente al banco en cuestión.

Fuentes de información	<ul style="list-style-type: none"> ▪ hxxps://blog.cyble.com/2022/09/02/zanubis-new-android-banking-trojan/ ▪ hxxps://theyberexpress.com/cyble-new-android-banking-trojan-zanubis/ ▪ Análisis propio de fuentes abiertas.
------------------------	--

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 282			Fecha: 17-10-2022
	Página 07 de 13			
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA			
Nombre de la alerta	Vulnerabilidad de elevación de privilegios de servicios de certificados de Active Directory			
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				
<p>1. Resumen:</p> <p>Microsoft ha reportado una vulnerabilidad de severidad CRÍTICA de tipo gestión inadecuada de privilegios que afecta a al Servicio de certificados de Active Directory (ADCS) en múltiples versiones de Windows Server. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante obtener privilegios de administrador de dominio.</p> <p>2. Detalles:</p> <ul style="list-style-type: none"> La vulnerabilidad de severidad crítica rastreada como CVE 2022 37976 de elevación de privilegios afecta a los servicios de certificados de Active Directory en varias versiones de Windows Server que podría permitir a un atacante elevar privilegios y obtener privilegio de administrador de dominio. Un cliente DCOM (Modelo de Objetos de Componentes Distribuidos) malicioso podría forzar a un servidor DCOM a autenticarse a través del Servicio de certificados de Active Directory y usar la credencial para lanzar un ataque entre protocolos. La explotación exitosa de esta vulnerabilidad podría afectar la confidencialidad, integridad y disponibilidad del sistema afectado. La vulnerabilidad de tipo gestión inadecuada de privilegios se debe a que el software no asigna, modifica, rastrea o comprueba adecuadamente los privilegios de un actor, creando una esfera de control no deseada para dicho actor. Cabe señalar que un sistema es vulnerable solo si tanto el rol de Servicios de certificados de Active Directory como el rol de Servicios de dominio de Active Directory están instalados en un servidor de la red. Tenga en cuenta que no necesariamente tendrían que estar en el mismo servidor. <p>3. Productos afectados:</p> <ul style="list-style-type: none"> Windows Server 2016; Windows Server 2022 (Server Core installation); Windows Server 2022; Windows Server 2019 (Server Core installation); Windows Server 2019; Windows Server 2012 R2 (Server Core installation); Windows Server 2008 for 32-bit Systems Service Pack 2; Windows Server 2016 (Server Core installation); Windows Server 2012 R2; Windows Server 2012 (Server Core installation); Windows Server 2012; Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation); Windows Server 2008 R2 for x64-based Systems Service Pack 1; Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation); Windows Server 2008 for x64-based Systems Service Pack 2; Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation). 				


4. Solución:

- Microsoft recomienda actualizar los productos afectados con las últimas actualizaciones y parches de seguridad emitidas que corrigen esta vulnerabilidad. Asimismo, recomienda aplicar las mitigaciones necesarias para reducir la explotación de esta vulnerabilidad.

La mitigación se refiere a una configuración, configuración común o mejor práctica general, existente en un estado predeterminado, que podría reducir la gravedad de la explotación de una vulnerabilidad.

Fuentes de información

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37976>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37976>

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 282			Fecha: 17-10-2022
				Página 09 de 13
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA			
Nombre de la alerta	Microsoft lanzó una actualización que corrige fallas en el protocolo de enlace TLS en Windows Server 2019			
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				
<p>1. Resumen:</p> <p>Microsoft ha publicado una actualización no relacionada con la seguridad fuera de banda (OOB) para abordar un problema crítico que desencadena fallas en el protocolo de enlace de seguridad de la capa de transporte (TLS) en los sistemas Windows Server 2019. Esta falla puede provocar problemas de instalación de actualizaciones de seguridad en algunos entornos administrados.</p> <p>2. Detalles:</p> <ul style="list-style-type: none"> Microsoft indicó que, en los dispositivos afectados, los usuarios ven errores SEC_E_ILLEGAL_MESSAGE en las aplicaciones cuando las conexiones a los servidores experimentan problemas. Estos podrían afectar algunos tipos de conexiones de Capa de sockets seguros (SSL) y TLS. Estas conexiones pueden tener fallas en el protocolo de enlace. Para los desarrolladores, es probable que las conexiones afectadas reciban uno o más registros seguidos de un registro parcial con un tamaño de menos de 5 bytes dentro de un solo búfer de entrada. La vulnerabilidad que se corrigió en esta actualización OOB (KB5020438) afecta a las plataformas de servidores, incluidas Windows Server 2019, Windows 10 Enterprise 2019 LTSC, Windows 10 IoT Enterprise 2019 LTSC y Windows 10 IoT Core 2019 LTSC. KB5020438 no está disponible para la instalación a través de Windows Update, Windows Update for Business o Windows Server Update Services (WSUS). Microsoft indicó que antes de instalar esta actualización acumulativa (KB5020438) en su dispositivo, primero debe instalar la actualización de la pila de servicio (SSU) del 10 de agosto de 2021 (KB5005112) y luego instalar esta actualización acumulativa OOB descargando el paquete independiente para su sistema desde el Catálogo de actualizaciones de Microsoft. Asimismo, dijo que después de implementar la actualización, es posible que el servicio de clúster no se inicie porque no se encuentra un controlador de red de clúster debido a una actualización de los controladores de clase PnP utilizados por el servicio. Si experimenta problemas después de instalar KB5020438, puede eliminarlo seleccionando "Ver actualizaciones instaladas" en el Panel de control de Programas y características. Microsoft dijo que accidentalmente incluyó la actualización de vista previa de Windows de septiembre en Windows Server Update Services. <p>3. Productos afectados:</p> <ul style="list-style-type: none"> Windows Server 2019; Windows 10 Enterprise 2019 LTSC; Windows 10 IoT Enterprise 2019 LTSC; Windows 10 IoT Core 2019 LTSC. 				

4. Solución:

Microsoft recomienda actualizar los productos afectados con la última actualización no relacionada con la seguridad fuera de banda que corrige esta vulnerabilidad.

Fuentes de información

- <https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-tls-handshake-failures-in-windows-server-2019/>
- <https://support.microsoft.com/en-us/topic/october-17-2022-kb5020438-os-build-17763-3534-out-of-band-cd499c1a-6d60-49a1-9a40-fad42c1d393a>
- <https://support.microsoft.com/en-us/topic/kb5005112-servicing-stack-update-for-windows-10-version-1809-august-10-2021-df6a9e0d-8012-41f4-ae74-b79f1c1940b2>
- <https://www.bleepingcomputer.com/news/microsoft/microsoft-windows-kb5017383-preview-update-added-to-wsus-by-mistake/>

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 282		Fecha: 17-10-2022
			Página 11 de 13
Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ		
Nombre de la alerta	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, por medio de los diferentes navegadores web, dirigido a los clientes y/o usuarios del Banco de Crédito del Perú (BCP); el cual, mediante la creación de un sitio web similar al original, solicitan a las posibles víctimas a realizar una solicitud de préstamo online, ingresando datos personas y bancarios como N° de tarjeta bancaria, clave web, fecha de vencimiento, clave de seguridad, número de contacto, entre otros.

2. Proceso del ataque phishing:



Requiere realizar una solicitud de préstamo online al instante ingresando datos personales



Para continuar con la solicitud pide ingresar la contraseña web



Luego, pide validar datos bancarios del solicitante



Por último, redirige al sitio web oficial del Banco de Crédito del Perú

3. Comparación del sitio web oficial y sitio web fraudulento:



- Ambas URL's utilizan el protocolo https, lo que hace más convincente a que las víctimas accedan al sitio web.
- La diferencia está en la URL, toda vez que el dominio del sitio web fraudulento, no coincide con el oficial.

4. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo la siguiente información:

- **URL:** hxxps://reactivabeneficioprimavera[.]top
- **Dominio:** reactivabeneficioprimavera[.]top
- **Direcciones IP:** 104[.]21[.]62[.]151
- **Tamaño:** 194B
- **SHA-256:** afca372f9959cb6c46bde573d25172c1b223dac52cba20ffad3c8fc2ea09cc8e



Antly-AVL	Ⓜ Malicious	Avira	Ⓜ Phishing
BitDefender	Ⓜ Phishing	Certego	Ⓜ Phishing
Comodo Valkyrie Verdict	Ⓜ Phishing	Emsisoft	Ⓜ Phishing
ESET	Ⓜ Phishing	Forcepoint ThreatSeeker	Ⓜ Phishing
Fortinet	Ⓜ Phishing	G-Data	Ⓜ Phishing
Kaspersky	Ⓜ Phishing	Lionic	Ⓜ Phishing
Netcraft	Ⓜ Malicious	Phishing Database	Ⓜ Phishing
Phishtank	Ⓜ Phishing	Sophos	Ⓜ Phishing
Viettel Threat Intelligence	Ⓜ Phishing	Webroot	Ⓜ Malicious

5. Recomendaciones:

- No abrir correos ni mensajes de dudosa procedencia
- Desconfiar de los enlaces y archivos enviados a través de mensajes o correos electrónicos
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Prestar atención en los detalles de los mensajes o redes sociales
- Evaluar el bloqueo preventivo de los indicadores de compromisos
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar los sitios web que se ingresen sean los oficiales.

Fuentes de información

- Análisis propio de redes sociales y fuente abierta

Índice alfabético

amenazas.....	11
ciberdelincuente.....	6
ciberdelincuentes.....	11
ciberespacio.....	11
digital.....	12
monitoreo.....	11
parches.....	8
Phishing.....	11
seguridad.....	9, 12
troyano.....	4
víctimas.....	12
vulnerabilidad.....	7, 9
Zanubis.....	4