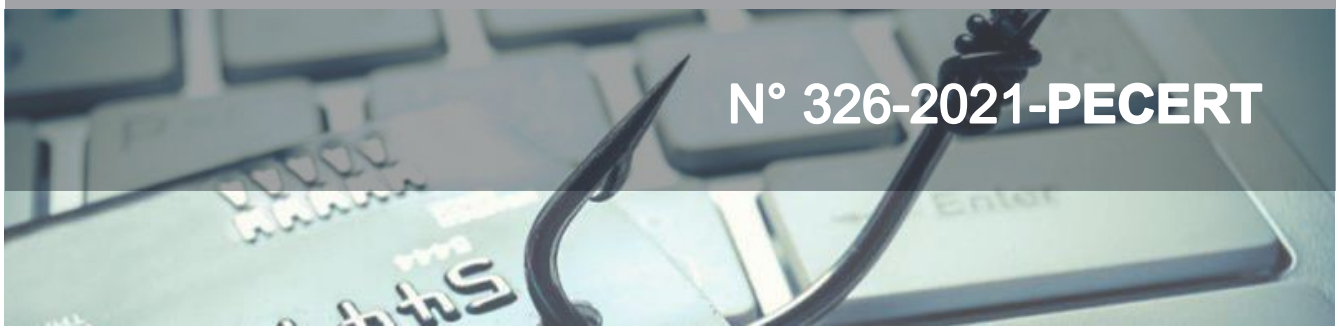
PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Lima, 13 de diciembre de 2021



N° 326-2021-PECERT

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 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

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 326	Fecha: 13-12-2021
		Página: 3 de 12

Componente que reporta	**COMANDO OPERACIONAL DE CIBERDEFENSA DEL COMANDO CONJUNTO DE LAS FUERZAS ARMADAS**		
Nombre de la alerta	Vulnerabilidad critica de biblioteca de Java Log4J – Actualiza ya		
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

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se tuvo conocimiento que una falla atroz y fácilmente explotada en la biblioteca de registro de Java, Apache Log4j, podría permitir la ejecución de código remoto no autenticado (RCE) y la adquisición completa del servidor, y está siendo explotado en la naturaleza.

2. Apache Log4j es una herramienta de registro basada en el lenguaje de programación Java, desarrollado por Apache Foundation y se utiliza ampliamente en el desarrollo de sistemas empresariales como en servicios en la nube.
3. El 24 de noviembre de 2021, el equipo de seguridad de Alibaba Cloud informo oficialmente de la vulnerabilidad. Tras la verificación por parte del equipo se ven afectados: Apache Strust2, Apache Solr, Apache Druid y Apache Flink.
4. Rastreado como CVE-2021-44228 y por los apodos Log4Shell o LogJam, el problema se refiere a un caso de ejecución de código remoto no autenticado (RCE) en cualquier aplicación que use la utilidad de código abierto y afecta a las versiones **Log4j 2.0-beta hasta 2.14.1**. El error obtuvo una puntuación perfecta de 10 sobre 10 en el sistema de clasificación CVSS, lo que indica la gravedad del problema.
5. La explotación se puede lograr mediante una sola cadena de texto, que puede hacer que una aplicación se comunique con un host externo malicioso si se registra a través de la instancia vulnerable de Log4j, lo que le otorga al adversario la capacidad de recuperar una carga útil de un servidor remoto y ejecutarlo localmente.
6. Log4j se utiliza como un paquete de registro en una variedad de software popular diferente por varios fabricantes, incluidos Amazon, Apple iCloud, Cisco, CloudFlare, ElasticSearch, Red Hat, Steam, tesla, twitter y videojuegos como Minecraft.
7. Las firmas de seguridad BitDefender, Cisco Talos, Huntress labs y Sonatype han confirmado evidencia de escaneo masivo de aplicaciones afectadas en la naturaleza en busca de servidores vulnerables y ataques registrados contra sus redes honeypot luego de la disponibilidad de un exploit de prueba de concepto (PoC).
8. El jefe de investigación de Nextron Systems, Florian Roth, ha compartido un conjunto de reglas YARA para detectar intentos de explotación de CVE-2021-44228 en “https://gist.github.com/Neo23x0/e4c8b03ff8cdf1fa63b7d15db6e3860b”.

9. Recomendaciones:
   - Actualizar a la última versión que Apache ha lanzado (Log4j 2.15.0), a fin de abordar la vulnerabilidad.
   -
   - Mitigar en versiones anteriores (2.10 y posteriores) estableciendo la propiedad del sistema "log4j2.formatMsgNoLookups" en "true" o eliminando la clase JndiLookup del classpath.

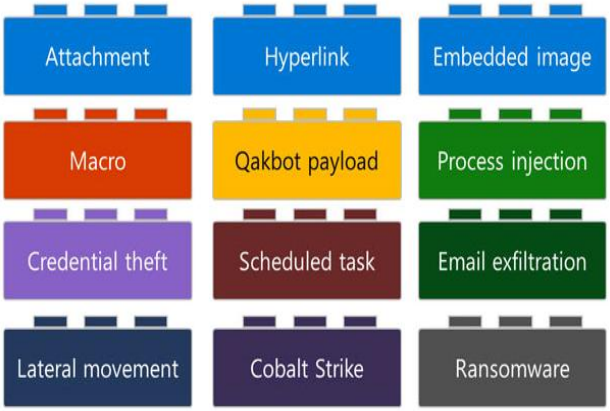
Fuentes de información	▪ https://blog.segu-info.com.ar/2021/12/log4shell-vulnerabilidad-critica-con.html ▪ https://www.bleepingcomputer.com/news/security/new-zero-day-exploit-for-log4j-java-library-is-an-enterprise-nightmare/ ▪ https://thehackernews.com/2021/12/extremely-critical-log4j-vulnerability.html

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 326	Fecha: 13-12-2021
		Página: 5 de 12

Componente que reporta	**CIBERDEFENSA Y TELEMÁTICA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Microsoft detalla los bloques de construcción del troyano bancario Qakbot ampliamente activo		
Tipo de ataque	Troyano	Abreviatura	Troyano
Medios de propagación	USB, disco, red, internet		
Código de familia	C	Código de subfamilia	C02
Clasificación temática familia	Código malicioso		

Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio del día 13 de diciembre de 2021, se tomó conocimiento de la información publicada en la página web de "The Hacker News" donde las cadenas de infección asociadas con el malware Qakbot multipropósito se han dividido en "bloques de construcción distintos", un esfuerzo que, según Microsoft, ayudará a detectar y bloquear la amenaza de manera eficaz y proactiva.
2. Se cree que Qakbot es la creación de un grupo de amenazas de ciberdelincuentes con motivaciones financieras conocido como Gold Lagoon. Es un malware de robo de información prevalente que, en los últimos años, se ha convertido en un precursor de muchos ataques de ransomware críticos y generalizados, ofreciendo una instalación de malware como servicio que permite muchas campañas.
3. Descubierto por primera vez en 2007, el malware modular, como TrickBot, ha evolucionado desde sus primeras raíces como troyano bancario hasta convertirse en una navaja suiza capaz de exfiltrar datos y actuar como un mecanismo de entrega para las cargas útiles de la segunda etapa, incluido el ransomware. También es notable su táctica de secuestrar los hilos de correo electrónico legítimos de las víctimas de los clientes de Outlook a través de un componente de recopilador de correo electrónico y usar esos hilos como señuelos de phishing para infectar otras máquinas.



4. Detalles:
   - "Poner en peligro los servicios IMAP y los proveedores de servicios de correo electrónico (ESP), o secuestrar los hilos de correo electrónico, permite a los atacantes aprovechar la confianza que una víctima potencial tiene en las personas con las que han mantenido correspondencia anteriormente, y también permite la suplantación de una organización comprometida", investigadores de Trend Micro Ian Kenefick y Vladimir Kropotov detallaron el mes pasado. "De hecho, será mucho más probable que los objetivos previstos abran correos electrónicos de un remitente reconocido".
   - La actividad de Qakbot rastreada por la firma de ciberseguridad durante un período de siete meses entre el 25 de marzo de 2021 y el 25 de octubre de 2021 muestra que EE. UU., Japón, Alemania, India, Taiwán, Italia, Corea del Sur, Turquía, España y Francia son los principales países objetivo, y las intrusiones afectaron principalmente a los sectores de telecomunicaciones, tecnología y educación.
   -
   - Más recientemente, las campañas de spam han dado como resultado el despliegue de un nuevo cargador llamado SQUIRRELWAFFLE que permite a los atacantes ganar un punto de apoyo inicial en las redes empresariales y colocar cargas útiles maliciosas, como Qakbot y Cobalt Strike, en los sistemas infectados.
   - Ahora, según Microsoft, las cadenas de ataque que involucran a Qakbot se componen de varios bloques de construcción que trazan las diversas etapas del compromiso, desde los métodos adoptados para distribuir el malware (enlaces, archivos adjuntos o imágenes incrustadas) antes de llevar a cabo una serie de post- actividades de explotación como el robo de credenciales, la exfiltración de correo electrónico, el movimiento lateral y el despliegue de balizas y ransomware de Cobalt Strike.

- La compañía con sede en Redmond señaló que los correos electrónicos relacionados con Qakbot enviados por los atacantes pueden, en ocasiones, venir con un archivo ZIP adjunto que incluye una hoja de cálculo que contiene macros de Excel 4.0 , un vector de acceso inicial que se abusa ampliamente en los ataques de phishing. Independientemente del mecanismo empleado para distribuir el malware, las campañas tienen en común el uso de macros maliciosas de Excel 4.0.
- Si bien las macros están desactivadas de forma predeterminada en Microsoft Office, se solicita a los destinatarios de los mensajes de correo electrónico que habiliten la macro para ver el contenido real del documento. Esto desencadena la siguiente fase del ataque para descargar las cargas útiles maliciosas de uno o más dominios controlados por atacantes.
- La mayoría de las veces, Qakbot es solo el primer paso en lo que es parte de un ataque más grande, con los actores de amenazas utilizando el punto de apoyo inicial facilitado por el malware para instalar cargas útiles adicionales o vender el acceso al mejor postor en foros clandestinos que luego pueden aprovechar para sus propios fines. En junio de 2021, la empresa de seguridad empresarial Proofpoint reveló cómo los actores de ransomware están pasando cada vez más del uso de mensajes de correo electrónico como una ruta de intrusión a la compra de acceso a empresas ciberdelincuentes que ya se han infiltrado en entidades importantes.
- "El modularidad y la flexibilidad de Qakbot podrían representar un desafío para los analistas de seguridad y los defensores porque las campañas simultáneas de Qakbot podrían verse sorprendentemente diferentes en cada dispositivo afectado, lo que afectaría significativamente la forma en que estos defensores responden a tales ataques", dijeron los investigadores. "Por lo tanto, una comprensión más profunda de Qakbot es fundamental para construir una estrategia de defensa integral y coordinada contra él".

5. Recomendación:
   - Evitar abrir correos desconocidos.
   - Instalar y mantener actualizado el antivirus en el dispositivo móvil.
   - Implementar herramientas de seguridad en el dispositivo móvil.

Fuentes de información	https://thehackernews.com/2021/12/microsoft-details-building-blocks-of.html

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 326**	**Fecha: 13-12-2021**
		Página: 7 de 12

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**			
Nombre de la alerta	Vulnerabilidad crítica en la biblioteca Apache Log4j afecta a múltiples productos de Cisco			
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

1. Resumen:

   El 9 de diciembre de 2021, se reveló una vulnerabilidad de severidad CRÍTICA de tipo validación de entrada incorrecta en la biblioteca de registro de Java de Apache Log4j que afecta a todas las versiones de Log4j2 anteriores a la versión 2.15.0. Por consiguiente, Cisco está investigando su línea de productos para determinar qué productos pueden verse afectados por esta vulnerabilidad y a medida que avanza la investigación, Cisco actualizará la información sobre los productos que se verían afectados.

2. Detalles:
   - La vulnerabilidad crítica identificada como CVE-2021-44228 de validación de entrada incorrecta se debe a que las funciones de Apache Log4j2 JNDI no protegen contra LDAP controlado por atacantes y otros puntos finales relacionados con JNDI. El producto recibe entrada o datos, pero no valida o valida incorrectamente que la entrada tiene las propiedades que se requieren para procesar los datos de forma segura y correcta.
   - Las funciones JNDI utilizadas en la configuración, los mensajes de registro y los parámetros no protegen contra LDAP controlado por atacantes y otros puntos finales relacionados con JNDI. Un atacante que puede controlar mensajes de registro o parámetros de mensajes de registro puede ejecutar código arbitrario cargado desde servidores LDAP cuando la sustitución de búsqueda de mensajes está habilitada. Desde log4j 2.15.0, este comportamiento se ha desactivado de forma predeterminada.
   - Para ayudar a detectar la explotación de esta vulnerabilidad en sus múltiples productos, Cisco ha publicado reglas de Snort en la siguiente ubicación: Reglas de Talos 2021-12-11.
   - SNORT es un software NIDS de código abierto o, dicho en otras palabras, es un sistema para detectar la existencia de intrusos en una Red. Las reglas SNORT por lo tanto son una guía para conocer cómo funcionan y cómo podemos aplicarlas.

3. Productos afectados:
   - Cisco publico una sección de productos vulnerables que incluye los ***ID de error de Cisco*** para cada producto afectado. Se puede acceder a los errores a través de la herramienta de búsqueda de errores de Cisco que contienen información adicional específica de la plataforma, incluidas soluciones alternativas (si están disponibles) y versiones de software corregidas.
   - Asimismo, Cisco está investigando sus ofertas en la nube para determinar qué productos pueden verse afectados por esta vulnerabilidad.

4. Solución:
   - Cisco recomienda actualizar los productos afectados a la última versión fija disponible que corrige esta vulnerabilidad. Asimismo, Cisco indicó que cualquier solución alternativa se documenta en los errores de Cisco específicos del producto, que se identifican en la sección Productos vulnerables.

Fuentes de información	hxxps://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 326**	**Fecha: 13-12-2021**
		Página: 8 de 12

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**			
Nombre de la alerta	Nueva campaña de phishing utiliza códigos QR para robar credenciales bancarias			
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 financiero			

Descripción

1. Resumen:

   Investigadores de Cofense han descubierto una nueva campaña de phishing dirigida a los usuarios de banca electrónica, que incluye códigos QR en el proceso de robo de credenciales. Los actores de amenaza están utilizando una variedad de tácticas para evadir las soluciones de seguridad y engañar a sus víctimas para que abran los mensajes y sigan las instrucciones de engaño. Los actores registran sus propios dominios personalizados que se utilizan para estas redirecciones, así como para los propios sitios de phishing. En esta campaña, los actores de amenazas utilizan códigos QR en lugar de botones para redireccionar a sus víctimas a los sitios web de phishing y robarles sus credenciales bancarias.

2. Detalles:
   - Los ciberdelincuentes están utilizando una variedad de trucos para eludir las soluciones de seguridad y convencer a sus objetivos de que abran los mensajes y sigan las instrucciones. Se ha descubierto que los correos electrónicos de phishing están cuidadosamente elaborados, con logotipos bancarios, contenido bien estructurado y un estilo generalmente coherente.
   - Los temas varían, desde pedirle al usuario su consentimiento a los cambios en la política de datos implementados por el banco o solicitarle que revise nuevos procedimientos de seguridad. Si se hace clic en el botón incrustado, la víctima llega al sitio de phishing después de pasar por el servicio de proxy de alimentación de Google "FeedBurner". Los dominios phishing normalmente son sitios recién registrados en el registrador ruso REG.RU y siguen una estructura de URL estándar según el banco de destino.
   - En estas campañas de phishing, los ciberdelincuentes utilizan códigos QR en lugar de botones para llevar a las víctimas a sitios de phishing. Estos correos electrónicos no contienen URL de texto sin cifrar y, en cambio, se ocultan a través de los códigos QR, lo que dificulta que el software de seguridad los detecte. Una vez que la víctima llega al sitio de phishing, se le solicita que ingrese su ubicación bancaria, código, nombre de usuario y PIN. Si estos detalles se ingresan en la página de phishing, el usuario espera la validación y luego se le solicita que ingrese sus credenciales nuevamente debido a que son incorrectas.

3. Indicadores de compromiso (IoC):

   URL
   - hxxps://spk-kundenumstellung[.]com/5RFANYAORO; hxxps://spk-sicherungssysteme[.]com/AK8SI4TVYD;
   - hxxps://spk-angleichung[.]com/7D2ZJAT8MK; hxxp://vr-neuerungszenter[.]com;
   - hxxps://djbetosom[.]designja[.]com[.]br/wp-admin/volksbanken/vr[.]de; hxxps://spk-kundenumstellung[.]com/;
   - hxxps://spk-sicherungssysteme[.]com/; hxxps://spk-angleichung[.]com/; hxxps://djbetosom[.]designja[.]com[.]br/.

   Dominio
   - djbetosom[.]designja[.]com[.]br; spk-kundenumstellung[.]com; spk-angleichung[.]com; vr-neuerungszenter[.]com;
   - spk-sicherungssysteme[.]com.

4. Recomendaciones:
   - Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad;
   - Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y aplicaciones;
   - Concientizar constantemente a los usuarios en temas relacionados a seguridad informática;
   - Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización;
   - Bloquear los indicadores de compromisos (IoC), en los dispositivos de seguridad de su infraestructura.

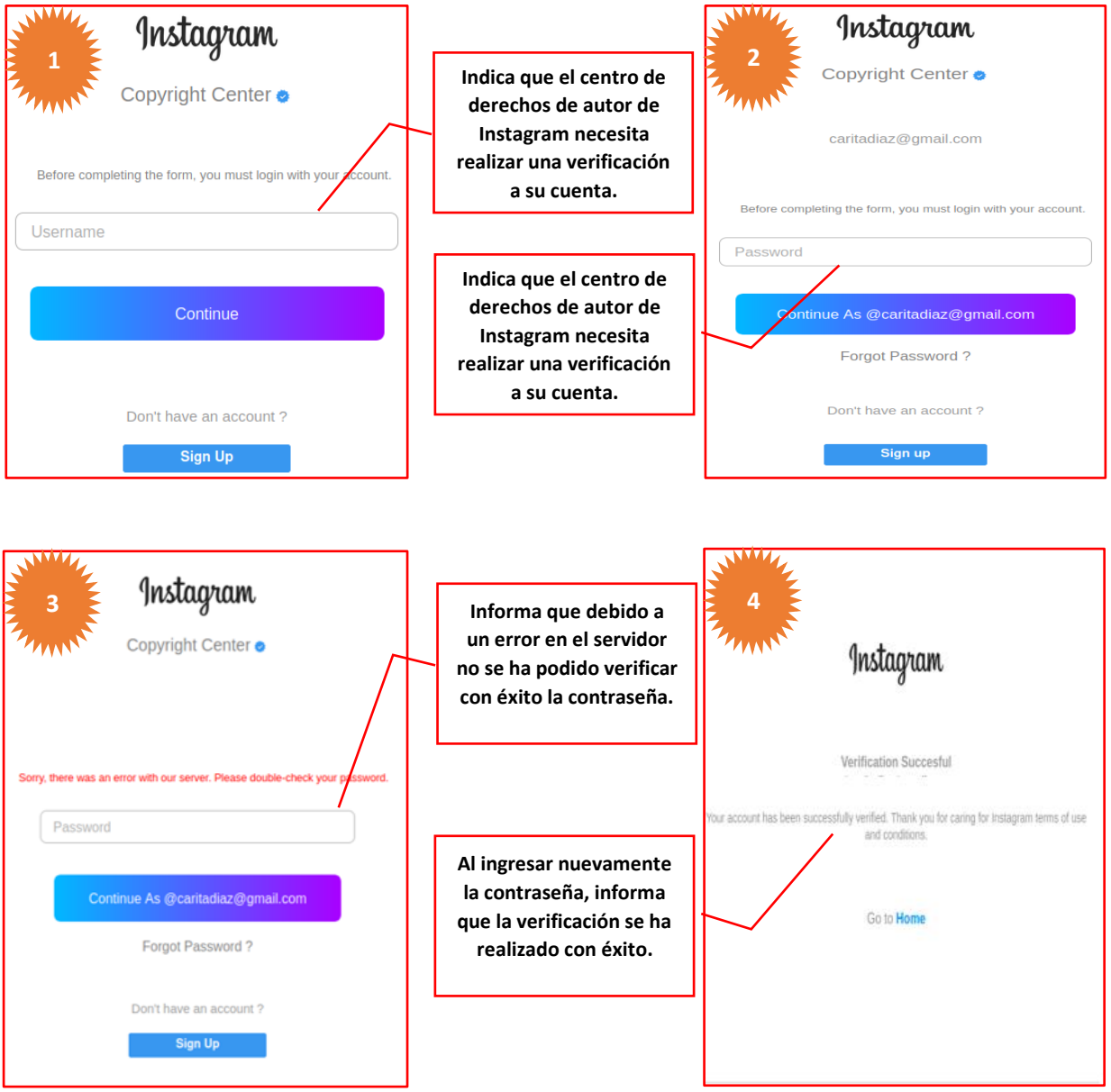
Fuentes de información	▪ hxxps://cofense.com/blog/german-users-targeted-in-digital-bank-heist-phishing-campaigns/ ▪ hxxps://www.bleepingcomputer.com/news/security/phishing-attacks-use-qr-codes-to-steal-banking-credentials/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 326	Fecha: 13-12-2021
		Página: 10 de 12

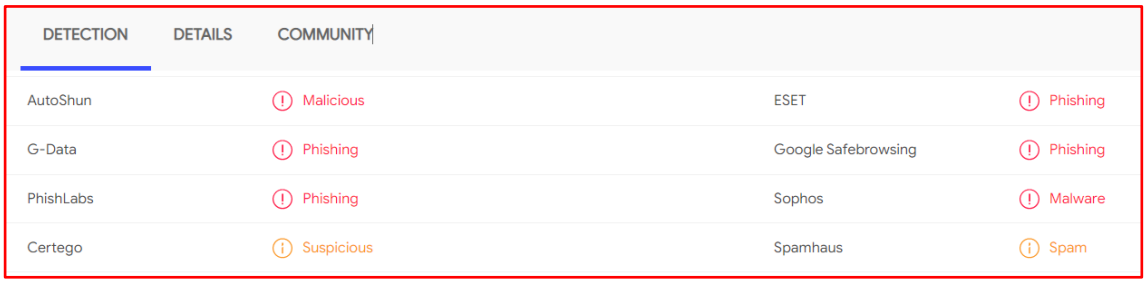
Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**			
Nombre de la alerta	Phishing, suplantando la identidad de la red social Instagram			
Tipo de ataque	Phishing		Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros			
Código de familia	G	Código de subfamilia	G02	
Clasificación temática familia	Fraude			

Descripción

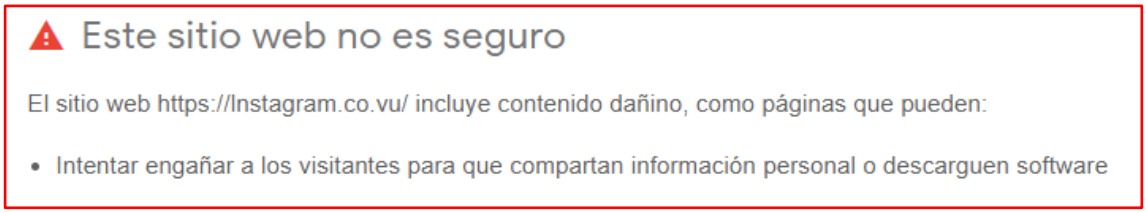
1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo una campaña de phishing, a través de los diferentes navegadores web, quienes suplantan la identidad de la red social Instagram, indicando que el centro de derechos de autor de la aplicación necesita realizar una verificación a su cuenta, para ello la víctima debe iniciar sesión a través de la dirección de correo electrónico y contraseña, que al seguir los pasos requeridos, informa que debido a un error en el serviciador no se pudo verificar con éxito la contraseña, solicitando intentar nuevamente.
2. Imagen: Detalles del proceso de estafa del phishing.



3. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo la siguiente información:
   - URL Malicioso: hxxps[:]//Instagram[.]co[.]vu/
   - Dominio: Instagram[.]co[.]vu
   - IP: 185[.]146.88[.]112
   - Tamaño: 5.50 KB
   - SHA-256: 715db6e912e3c25d28f6caf3abe7ef0ba211a34e7a5d6410c7ebec5d24399369



   - Navegación segura de Google también cataloga como sitio web dañino o malicioso.



4. Cómo funciona el Phishing:
   - Los correos electrónicos incluyen enlaces a sitios web preparados por los ciberdelincuentes en los que solicitan información personal.
   - Medios de propagación del Phishing: WhatsApp, telegram, redes sociales, SMS entre otros.
   - Los ciberdelincuentes intentan suplantar a una entidad legitima (organismo público o privado, entidad financiera, servicio técnico, etc.)
5. Referencia:
   - Phishing o suplantación de identidad: Es un método que los ciberdelincuentes, utilizan para engañar a los usuarios para conseguir que revele información personal, como contraseñas, datos de tarjetas de créditos, números de cuentas bancarias, entre otros.
6. Recomendaciones:
   - Verificar la información en el sitio web oficial.
   - No abrir o hacer clic enlaces de dudosa procedencia.
   - No seguir indicaciones de sitios web fraudulentos.
   - No brindar información personal, a sitios web sospechosos.
   - Mantener actualizado el software de sus equipos informáticos.

Fuentes de información	Análisis propio de redes sociales y fuente abierta

Índice alfabético