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, 8 de febrero de 2022

N° 039-2022-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.

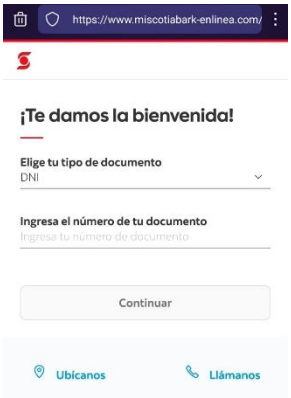
Contenido

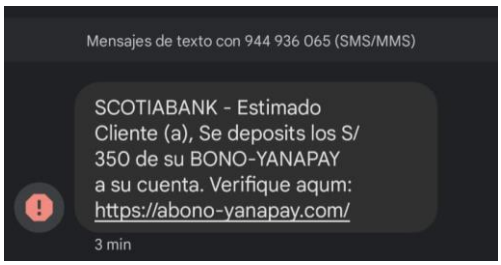
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 039	Fecha: 08-02-2022
		Página: 3 de 12

Componente que reporta	**COMANDO OPERACIONAL DE CIBERDEFENSA DEL COMANDO CONJUNTO DE LAS FUERZAS ARMADAS**			
Nombre de la alerta	Campaña phishing "Bono YANAPAY - Scotiabank"			
Tipo de ataque	Explotación de vulnerabilidades		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. El 08 de febrero de 2022, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se tuvo conocimiento de una campaña Phishing con el nombre "Bono YANAPAY - Scotiabank" viene circulando en los principales medios de mensajería instantánea SMS, WhatsApp, Telegram entre otras. Los ciberdelincuentes suplantaron la identidad del Banco Scotiabank, y a través del engaño intentan que los usuarios les faciliten información en una página Web fraudulenta.
2. Los ataques de phishing son cada vez más avanzados en su utilización de técnicas de ingeniería social. En la mayoría de los casos, los estafadores tratan de asustar a los usuarios empleando una razón aparentemente importante para que el destinatario confiera sus datos personales.
3. El robo de identidad no es la única amenaza presentada por un enlace de phishing. Muchas veces, los enlaces falsos pueden conducir a spywares, keyloggers o troyanos. Por lo que, aun cuando un usuario no tenga una cuenta de interés para los estafadores, eso no quiere decir que estén a salvo de estas amenazas.
4. Un truco típico del phishing es utilizar enlaces muy similares a las direcciones URL de los sitios originales. Este truco está diseñado para atrapar a los usuarios menos experimentados. Un usuario cuidadoso probablemente notará que un enlace es diferente al del sitio legítimo. Estos enlaces pueden comenzar con una dirección IP, y las grandes empresas jamás utilizan links como éstos.





5. Se recomienda:
   - Instalar y mantener actualizados los sistemas de antivirus en los dispositivos móviles y equipos del usuario.
   - Mantener el software actualizado en los equipos, incluyendo los últimos parches de seguridad.
   - Verificar que la dirección sea la correcta, siendo esta de la fuente oficial.
   - Y lo más importante, conocer y elevar la conciencia de seguridad sobre la naturaleza de los ciberataques de este tipo, evitar las cadenas de spam pueden contener códigos maliciosos. Recuerda un click hace la diferencia, abriendo puertas para q los ciberatacantes logren su cometido.

Fuentes de información	Equipo CSIRT Comando Operacional de Ciberdefensa

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 039	Fecha: 08-02-2022
		Página: 4 de 12

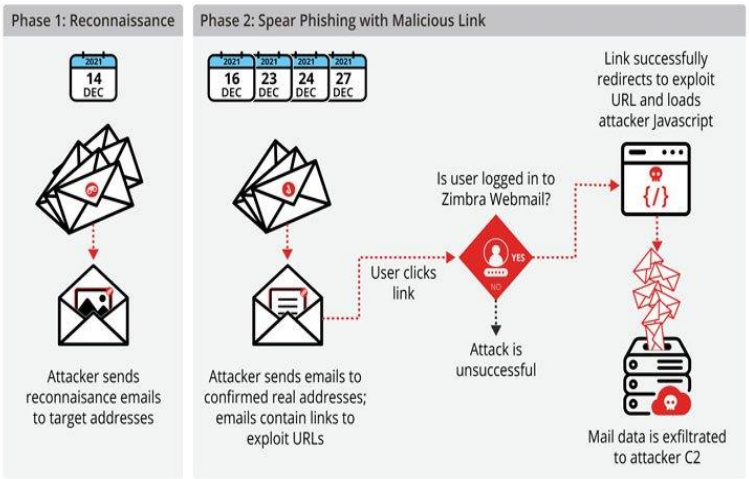
Componente que reporta	**COMANDO OPERACIONAL DE CIBERDEFENSA DEL COMANDO CONJUNTO DE LAS FUERZAS ARMADAS**			
Nombre de la alerta	Vulnerabilidad Critica Zimbra Zero Days			
Tipo de ataque	Explotación de vulnerabilidades		Abreviatura	Ransomware
Medios de propagación	Correo electrónico, redes sociales, entre otros			
Código de familia	C	Código de subfamilia	C09	
Clasificación temática familia	Código malicioso			

Descripción

1. El 08 de febrero de 2022, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se tuvo conocimiento que está intentando activamente explotar una vulnerabilidad de día cero en la plataforma de correo electrónico de código abierto Zimbra como parte de las campañas de phishing que comenzaron en diciembre de 2021.

2. La operación de espionaje, cuyo nombre en código es " EmailThief ", fue detallada por la empresa de ciberseguridad Volexity en un informe técnico, señalando que la explotación exitosa de la vulnerabilidad de secuencias de comandos entre sitios (XSS) podría resultar en la ejecución de código JavaScript arbitrario en el contexto de la sesión Zimbra del usuario.

3. Según los investigadores, para que el ataque tenga éxito, el objetivo tendría que visitar el enlace del atacante mientras estaba conectado al cliente de correo web de Zimbra desde un navegador web. Sin embargo, el enlace en sí podría iniciarse desde una aplicación para incluir un cliente pesado, como Thunderbird o Outlook.



4. Se recomienda:
   - Instalar y mantener actualizados los sistemas de antivirus en los dispositivos móviles y equipos del usuario.
   - Mantener el software actualizado en los equipos, incluyendo los últimos parches de seguridad.

Fuentes de información	hxxps://thehackernews.com/2022/02/hackers-exploited-0-day-vulnerability.html

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 039	Fecha: 08-02-2022
		Página: 5 de 12

Componente que reporta	**COMANDO OPERACIONAL DE CIBERDEFENSA DEL COMANDO CONJUNTO DE LAS FUERZAS ARMADAS**			
Nombre de la alerta	Vulnerabilidad Critica Serie RV Cisco Small Business			
Tipo de ataque	Explotación de vulnerabilidades		Abreviatura	Ransomware
Medios de propagación	Correo electrónico, redes sociales, entre otros			
Código de familia	C	Código de subfamilia	C09	
Clasificación temática familia	Código malicioso			

Descripción

1. El 08 de febrero de 2022, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se tuvo conocimiento que La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) está instando a las agencias federales a proteger sus sistemas contra una vulnerabilidad de seguridad explotada activamente en Windows que podría ser objeto de abuso para obtener permisos elevados en los hosts afectados.

2. Registrada como CVE-2022-21882 en el catálogo de vulnerabilidades explotadas conocidas, lo que requiere que las agencias de la Rama Ejecutiva Civil Federal (FCEB) corrijan todos los sistemas contra esta vulnerabilidad antes del 18 de febrero de 2022.

3. CVE-2022-21882, que ha sido etiquetado con una evaluación de explotación más probable, se refiere a un caso de vulnerabilidad de elevación de privilegios que afecta al componente Win32k. Estos tipos de vulnerabilidades son un vector de ataque frecuente para los actores cibernéticos maliciosos de todo tipo y representan un riesgo significativo para la empresa federal

4. Un atacante local autenticado podría obtener un sistema local elevado o privilegios de administrador a través de una vulnerabilidad en el controlador Win32k.sys. La falla afecta a Windows 10, Windows 11, Windows Server 2019 y Windows Server 2022.

5. Se recomienda:
   - Instalar y mantener actualizados los sistemas de antivirus en los dispositivos móviles y equipos del usuario.
   - Mantener el software actualizado en los equipos, incluyendo los últimos parches de seguridad

Fuentes de información	hxxps://thehackernews.com/2022/02/cisa-orders-federal-agencies-to-patch.html

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 039	Fecha: 08-02-2022
		Página: 6 de 12

Componente que reporta	**COMANDO OPERACIONAL DE CIBERDEFENSA DEL COMANDO CONJUNTO DE LAS FUERZAS ARMADAS**			
Nombre de la alerta	Vulnerabilidad Critica Serie RV Cisco Small Business			
Tipo de ataque	Explotación de vulnerabilidades		Abreviatura	Ransomware
Medios de propagación	Correo electrónico, redes sociales, entre otros			
Código de familia	C	Código de subfamilia	C09	
Clasificación temática familia	Código malicioso			

Descripción

1. El 08 de febrero de 2022, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se tuvo conocimiento que Cisco ha parcheado múltiples vulnerabilidades de seguridad críticas que afectan a sus enrutadores de la serie RV que podrían armarse para elevar los privilegios y ejecutar código arbitrario en los sistemas afectados, al tiempo que advierte sobre la existencia de un código de explotación de prueba de concepto (PoC) que apunta a algunos de estos errores.

2. Registrada como CVE-2022-20699, CVE-2022-20700 y CVE-2022-20707, tienen la calificación CVSS más alta de 10.0 y afectan a sus enrutadores de las series Small Business RV160, RV260, RV340 y RV345. Además, las fallas podrían explotarse para eludir las protecciones de autenticación y autorización, recuperar y ejecutar software sin firmar e incluso causar condiciones de denegación de servicio (DoS).

3. CVE-2022-20699 se refiere a un caso de ejecución remota de código que podría ser explotado por un atacante mediante el envío de solicitudes HTTP especialmente diseñadas a un dispositivo que funciona como una puerta de enlace SSL VPN, lo que conduce efectivamente a la ejecución de código malicioso con privilegios de raíz.

4. CVE-2022-20708, la tercera falla que recibe una puntuación de 10.0 en la escala CVSS, se debe a una validación insuficiente de la entrada proporcionada por el usuario, lo que permite al adversario inyectar comandos maliciosos y obtenerlos en el sistema operativo Linux subyacente.

5. Se recomienda:
   - Instalar y mantener actualizados los sistemas de antivirus en los dispositivos móviles y equipos del usuario.
   - Mantener el software actualizado en los equipos, incluyendo los últimos parches de seguridad.

Fuentes de información	hxxps://thehackernews.com/2022/02/critical-flaws-discovered-in-cisco.html

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 039	Fecha: 08-02-2022
		Página: 7 de 12

Componente que reporta	**COMANDO OPERACIONAL DE CIBERDEFENSA DEL COMANDO CONJUNTO DE LAS FUERZAS ARMADAS**			
Nombre de la alerta	Troyano FluBot y Medusa			
Tipo de ataque	Explotación de vulnerabilidades		Abreviatura	Malware
Medios de propagación	Correo electrónico, redes sociales, entre otros			
Código de familia	C	Código de subfamilia	C09	
Clasificación temática familia	Código malicioso			

Descripción

1. El 08 de febrero de 2022, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se tuvo conocimiento de dos troyanos bancarios para Android diferentes, FluBot y Medusa, dependen del mismo vehículo de entrega como parte de una campaña de ataque simultáneo, según una nueva investigación publicada por ThreatFabric.

2. Medusa, descubierta por primera vez dirigida a organizaciones financieras turcas en julio de 2020, ha sufrido varias iteraciones, la principal de las cuales es la capacidad de abusar de los permisos de accesibilidad en Android para desviar fondos de aplicaciones bancarias a una cuenta controlada por el atacante.

3. Las aplicaciones plagadas de malware que se usan junto con FluBot se hacen pasar por aplicaciones de DHL y Flash Player para infectar los dispositivos. Además, los ataques recientes que involucran a Medusa han ampliado su enfoque más allá de Turquía para incluir a Canadá y los EE. UU., y los operadores mantienen múltiples botnets para cada una de sus campañas.

4. Esta no es la primera vez que se descubre que el malware de Android se propaga creando respuestas automáticas a los mensajes en WhatsApp. El año pasado, ESET y Check Point Research descubrieron aplicaciones no autorizadas que se hacían pasar por Huawei Mobile y Netflix que empleaban el mismo modus operandi para realizar los ataques de gusanos.

5. Se recomienda:
   - Instalar y mantener actualizados los sistemas de antivirus en los dispositivos móviles y equipos del usuario.
   - Mantener el software actualizado en los equipos, incluyendo los últimos parches de seguridad.

Fuentes de información	hxxps://thehackernews.com/2022/02/medusa-android-banking-trojan-spreading.html

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 039	**Fecha: 08-02-2022**
		Página: 8 de 12

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**			
Nombre de la alerta	El nuevo malware CapraRAT para Android se dirige al gobierno y al personal militar de la India			
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

1. Fecha del evento:

   A través del monitoreo y búsqueda de amenazas en el ciberespacio del día 08 de febrero de 2022, se tomó conocimiento de la publicación realizada en la página web de "THE HACKER NEWS", un grupo de amenazas persistentes avanzadas (APT) políticamente motivado ha ampliado su arsenal de malware para incluir un nuevo troyano de acceso remoto (RAT) en sus ataques de espionaje dirigidos a entidades militares y diplomáticas indias.

2. Antecedentes:

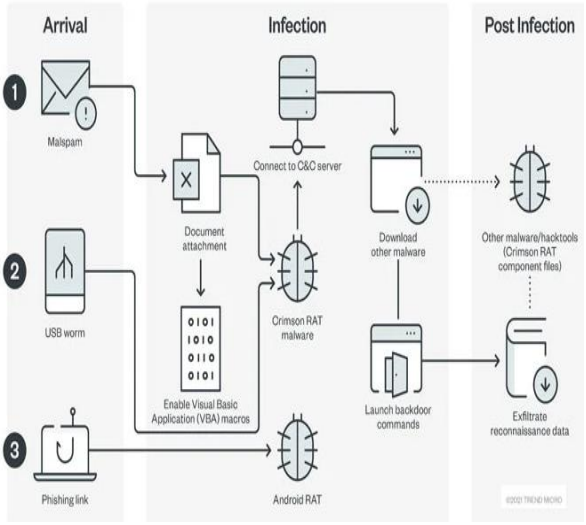
   Los primeros signos concretos de la existencia de APT36 aparecieron en 2016 cuando el grupo comenzó a distribuir malware de robo de información a través de correos electrónicos de phishing con archivos adjuntos PDF maliciosos dirigidos al personal militar y gubernamental indio. Se cree que el grupo es de origen Paquistaní y está operativo.

   También se sabe que el actor de amenazas es consistente en su modus operandi, con los ataques predominantemente apostando por la ingeniería social y un gusano basado en USB como puntos de entrada. Entre los elementos comunes en el arsenal del grupo se encuentra una puerta trasera de Windows llamada CrimsonRAT que permite a los atacantes un amplio acceso a los sistemas comprometidos, aunque las campañas recientes han evolucionado para ofrecer ObliqueRAT.

3. Detalles:

   CrimsonRAT se configura como un binario .NET cuyo propósito principal es obtener y exfiltrar información de los sistemas Windows de destino, incluidas capturas de pantalla, pulsaciones de teclas y archivos de unidades extraíbles, y cargarlos en el servidor de comando y control del atacante.

   La nueva adición a su conjunto de herramientas es otra RAT personalizada de Android que se implementa mediante enlaces de phishing. Se dice que CapraRAT, se disfraza como una aplicación de YouTube, es una versión modificada de una RAT de código abierto llamada AndroRAT y viene con una variedad de funciones de exfiltración de datos, incluida la capacidad de recopilar las ubicaciones de las víctimas, los registros telefónicos y la información de contacto.



4. Recomendaciones:
   - Se recomienda a los usuarios que tengan cuidado con los correos electrónicos no solicitados.
   - Evitar hacer clic en enlaces o descargar archivos adjuntos de correo electrónico de remitentes desconocidos.
   - Instalar aplicaciones solo de fuentes confiables y tener cuidado cuando se trata de otorgar permisos solicitados por las aplicaciones.

Fuentes de información	hxxps://thehackernews.com/2022/02/new-caprarat-android-malware-targets.html

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 039	Fecha: 08-02-2022
		Página: 9 de 12

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**			
Nombre de la alerta	Shuckworm Group utiliza un documento de Word armado para infectar la computadora de las víctimas			
Tipo de ataque	Virus Informático		Abreviatura	Virus
Medios de propagación	USB, disco, red, correo, navegación de 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 04 de febrero de 2022, se tomó conocimiento por medido de la publicación realizada en la página web de **"GB HACKERS"** que el equipo Threat Hunter de Symantec ha descubierto recientemente un grupo de piratería que se denomina Shuckworm que tiene sus vínculos raíz con Rusia utilizando documentos de Word armados para infectar las computadoras de sus objetivos, de acuerdo con el siguiente detalle:

2. Antecedentes:

Este grupo de piratería vinculado a Rusia, Shuckworm, ha estado activo desde 2013, y está especializado principalmente en operar campañas de ciberespionaje contra las entidades en Ucrania. Este grupo es conocido también como Gamaredon y Armagedón

Se cree que el grupo de piratería Shuckworm opera directamente desde el FSB (Servicio Federal de Seguridad) ruso. Los operadores de Shuckworm utilizan correos electrónicos de phishing para distribuir Sistema de manipulador remoto (RMS), UltraVNC y Pterodo/Pteranodon (malware personalizado).

Sin embargo, en los últimos tiempos este grupo ha desarrollado sofisticadamente todos sus TTP y los ha utilizado para robar las credenciales de sus víctimas e infectar la red para moverse lateralmente.

Se detectaron el uso de los siguientes archivos binarios autoextraíbles SFX en los ataques realizados recientemente: (descender.exe, hundido profundamente.exe, z4z05jn4.egf.exe, desafiante.exe, verde profundo.exe).

En la máquina comprometida, se abrieron varios documentos desde varias ubicaciones antes de la instalación del cliente VNC para crear confusión y aumentar la complejidad.

Al hacerlo, ayuda a los actores de amenazas a recopilar y exfiltrar información confidencial del sistema comprometido de su objetivo. Además, los documentos a los que acceden los actores de amenazas van desde descripciones de trabajo hasta información confidencial.

3. Recomendaciones:
   - Mantener actualizados los sistemas operativos, así como todo el software de uso.
   - No usar software ilegal en nuestros ordenadores, debido que suelen ir acompañados de malware en los parches de activación.
   - Tener cuidado con el correo electrónico, sobre todo el de procedencias desconocidas.

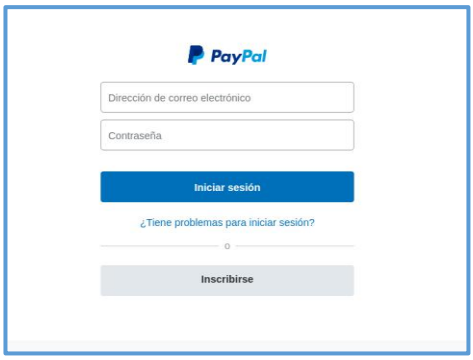
Fuentes de información	hxxps://gbhackers.com/shuckworm-campaign/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 039	Fecha: 08-02-2022
		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 empresa de pagos en línea PayPal			
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 vienen suplantando la identidad de la empresa de pagos en línea "PayPal", el supuesto sitio web cuenta con colores y logos característicos idénticos al original, el cual tiene como finalidad robar información confidencial de las posibles víctimas, como dirección de correo electrónico, contraseña, datos bancarios (nombre, número, fecha de expiración de la tarjeta).
2. Imagen: detalles del proceso de phishing.

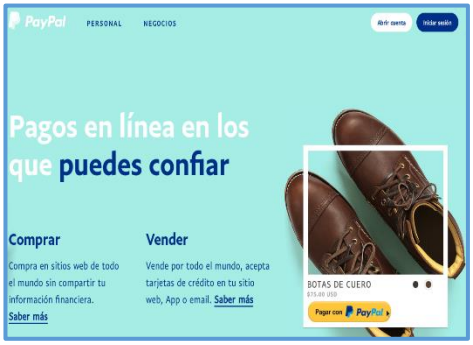


Paso Nº 01

Solicitan las credenciales de acceso (correo electrónico y contraseña) del servicio de pago en línea.

Paso Nº 02

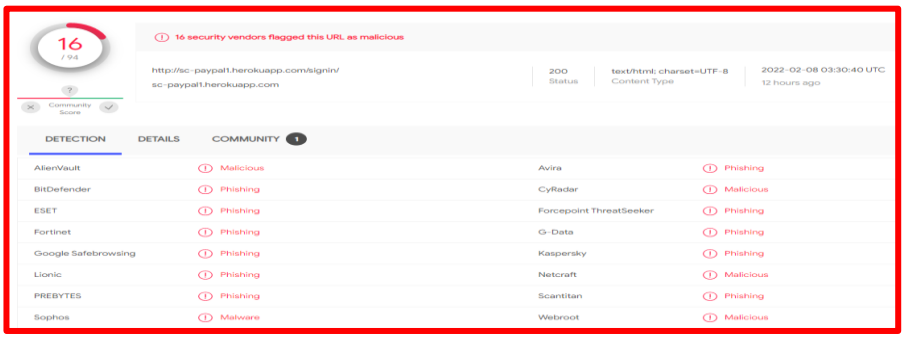
Requieren información personal y tarjeta de crédito.



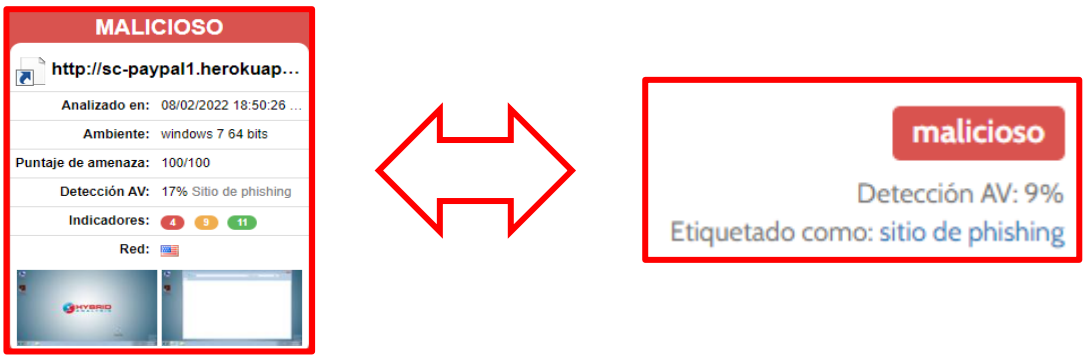
Paso Nº 03

Luego, te direcciona a la pantalla principal falsa.

3. Proveedores de seguridad informática alertan como SUPLANTACIÓN DE IDENTIDAD - PHISHING.



4. Indicadores de compromiso (IoC)
   - URL : hxxp://sc-paypal1[.]herokuapp[.]com/signin/
   - DOMINIO : sc-paypal1[.]herokuapp[.]com/signin/
   - SHA-256 : 8fe7547a29c1226b2921ec9b125b57365f5f9df7c8c15a531039ff4cbe5c9244
   - IP : 107[.]22[.]57[.]98
5. Otras detecciones:



6. Apreciación de la información:
   - La presente campaña de phishing permite a los actores de amenazas obtener información bancaria de los usuarios de la empresa de pagos en línea PayPal.
   - La propagación del sitio web fraudulento se realiza mediante envió masivos de email (SPAM), con la finalidad de obtener información sensible de las víctimas; asimismo, a través de las aplicaciones de mensajería instantánea entre ellos WhatsApp, Telegram, Messenger y mensajes de textos (SMS).
7. 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.
8. Recomendaciones:
   - Verificar detalladamente las URL de los sitios web
   - No abrir o descargar archivos sospechosos.
   - No seguir las instrucciones de sitio web sospechoso.
   - Mantener el antivirus actualizado.

Fuentes de información	Análisis propio de redes sociales y fuente abierta

Índice alfabético