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, 05 de mayo de 2022

N° 123-2022-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° 123	Fecha: 05-05-2022
		Página 4 de 10

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Vulnerabilidades de RCE en plataformas dotCMS		
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

I. DATOS GENERALES:

CVE-2022-26352: Ejecución remota de código.

Investigadores: Compañía Assetnote.

Se ha revelado una vulnerabilidad de ejecución remota de código autenticado previamente en dotCMS, un sistema de gestión de contenido (CMS) de código abierto escrito en Java.

II. EVIDENCIA:

- La falla crítica, rastreada como CVE-2022-26352, se deriva de un ataque transversal de directorio al realizar cargas de archivos, lo que permite que un adversario ejecute comandos arbitrarios en el sistema subyacente.
- "Un atacante puede cargar archivos arbitrarios en el sistema", dijo Shubham Shah de Assetnote en un informe. "Al cargar un archivo JSP en el directorio raíz de Tomcat, es posible lograr la ejecución del código, lo que lleva a la ejecución del comando".

III. TEMA:

- En otras palabras, se puede abusar de la falla de carga de archivos arbitrarios para reemplazar los archivos ya existentes en el sistema con un shell web, que luego se puede usar para obtener acceso remoto persistente.
- Aunque el exploit hizo posible escribir en archivos JavaScript arbitrarios servidos por la aplicación, los investigadores dijeron que la naturaleza del error era tal que podría convertirse en un arma para obtener la ejecución del comando.
- AssetNote dijo que descubrió e informó la falla el 21 de febrero de 2022, luego de lo cual se lanzaron parches en las versiones 22.03, 5.3.8.10 y 21.06.7.
- La vulnerabilidad considerada crítica, no cuenta con puntuación en las listas de CVE-Mitre hasta el 04/05/2022.

IV. CONCLUSIÓN:

- "Cuando los archivos se cargan en dotCMS a través de la API de contenido, pero antes de que se conviertan en contenido, dotCMS escribe el archivo en un directorio temporal", dijo la compañía.
- "En el caso de esta vulnerabilidad, dotCMS no desinfecta el nombre del archivo pasado a través del encabezado de solicitud de varias partes y, por lo tanto, no desinfecta el nombre del archivo temporal".
- "En el caso de este exploit, un atacante puede cargar un archivo .jsp especial en el directorio webapp/ROOT de dotCMS que puede permitir la ejecución remota de código", señaló.

V. RECOMENDACIÓN:

- Actualizar las versiones dotCMS que contienen correcciones de código para el problema. Incluidas las versiones 22.03, 5.3.8.10_lts y/o 21.06.7_lts. Si no es posible realizar una actualización, el proveedor ha desarrollado complementos basados en OSGI que pueden implementarse en los entornos dotCMS.
- Revisar y contar con directrices WAF para el desarrollo seguro de aplicaciones Web.
- Deshabilitar el envío de contenido anónimo de la plataforma.
- Se sugiere contar con directrices de desarrollo seguro de software, según sea el caso: S-SCLD, DevOpsSec.

Fuentes de información	▪ hxxps://thehackernews.com/2022/05/critical-rce-bug-reported-in-dotcms.html ▪ hxxps://blog.assetnote.io/2022/05/03/hacking-a-bank-using-dotcms-rce/ ▪ hxxps://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26352

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 123	Fecha: 05-05-2022
		Página 5 de 10

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Descubren dos grandes vulnerabilidades en Avast y AVG		
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

I. DATOS GENERALES:

Vulnerabilidades: CVE-2022-26522, CVE-2022-26523.

Investigadores: SentinelOne.

Se han descubierto dos vulnerabilidades de seguridad de alta gravedad, que pasaron desapercibidas durante varios años, en un controlador legítimo que forma parte de las soluciones antivirus de Avast y AVG.

II. EVIDENCIA:

- Rastreadas como CVE-2022-26522 y CVE-2022-26523, las fallas residen en un controlador de kernel anti-rootkit legítimo llamado aswArPot.sys y se dice que se introdujeron en la versión 12.1 de Avast, que se lanzó en junio de 2016.
- El investigador de SentinelOne, Kasif Dekel, dijo lo siguiente en un informe compartido y publicado en internet:

"Estas vulnerabilidades permiten a los atacantes escalar privilegios que les permiten deshabilitar productos de seguridad, sobrescribir componentes del sistema, corromper el sistema operativo o realizar operaciones maliciosas sin obstáculos".

- Específicamente, las deficiencias tienen su origen en un controlador de conexión de socket en el controlador del kernel que podría conducir a una escalada de privilegios al ejecutar código en el kernel de un usuario que no sea administrador, lo que podría causar que el sistema operativo se bloquee y muestre una pantalla azul de muerte (BSoD) error.
- Si bien no hay evidencia de que se haya abusado de estas vulnerabilidades a gran escala, la revelación se produce pocos días después de que Trend Micro detallara un ataque de ransomware AvosLocker, que aprovechó otro problema en el mismo controlador para finalizar las soluciones antivirus en el sistema comprometido.

III. TEMA:

- De manera preocupante, las fallas también podrían explotarse como parte de un ataque de navegador de segunda etapa o para realizar un escape de sandbox, lo que tendría consecuencias de largo alcance.
- Dichas fallas se pusieron en conocimiento de Avast en diciembre de 2021 y la compañía, que también es la propietaria de AVG tras su compra en 2016, ha lanzado actualizaciones de seguridad para abordar estas vulnerabilidades.

IV. CONCLUSIÓN:

- La mayoría de los usuarios de Avast y AVG recibirán el parche (versión 22.1) automáticamente, ya que está disponible desde el mes de febrero 2022. Por el momento los investigadores no tienen constancia de evidencias de abuso de este exploit a gran escala.
- Los usuarios de Avast y AVG se actualizaron automáticamente y están protegidos contra cualquier riesgo de

explotación. Sin embargo, la naturaleza de las vulnerabilidades está presente.

V. RECOMENDACIÓN:

- Se sugiere seguir las recomendaciones de los desarrolladores del software. La firma antivirus se ha pronunciado:

"A nuestros usuarios de Avast y AVG que actualicen constantemente su software a la última versión para estar protegidos. La divulgación coordinada es una forma excelente de evitar que los riesgos se manifiesten en ataques, y alentamos la participación en nuestro programa de recompensas por errores».

Fuentes de información	▪ hxxps://thehackernews.com/2022/05/researchers-disclose-10-year-old.html ▪ hxxps://www.adslzone.net/noticias/seguridad/vulnerabilidades-antivirus-avast-avg-2022/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 123	Fecha: 05-05-2022
		Página 7 de 10

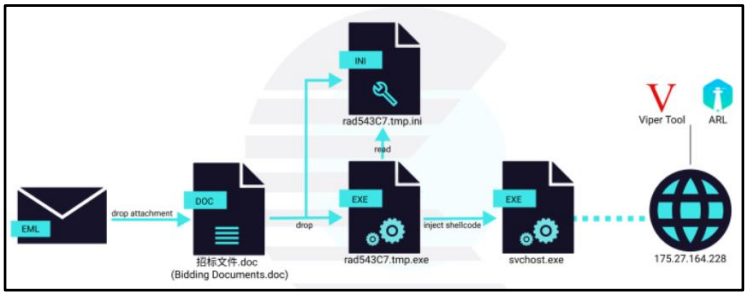
Componente que reporta	**COMANDO OPERACIONAL DE CIBERDEFENSA DEL COMANDO CONJUNTO DE LAS FUERZAS ARMADAS**		
Nombre de la alerta	Los piratas informáticos chinos "Override Panda"		
Tipo de ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de subfamilia	G02
Clasificación temática familia	Fraude		

Descripción

1. El 05 de mayo del 2022, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se tuvo conocimiento de un grupo de espionaje patrocinado por el estado chino conocido como “Override Panda” este grupo de piratas informáticos en las últimas semanas lanzó un nuevo ataque de phishing con el objetivo de robar información confidencial.

2. Según Cluster25, el grupo de piratas informáticos chinos usó un correo electrónico de phishing para enviar una baliza de un marco del Equipo Rojo conocido como “Viper”, mediante un documento adjunto diseñado para atraer a las víctimas para que abran y se comprometan con el malware.

3. El ataque inicia con un correo electrónico de spear phishing que contiene un documento llamado "Documentos de licitación para la adquisición centralizada de equipos de firewall de aplicaciones web (WAF) de China Mobile de 2022 a 2024". Este documento contiene “HexINI”, es un ejecutable que actúa como un cargador para un shellcode.



4. El objetivo de este ataque es desconocido en la actualidad, pero con alta probabilidad, dada la historia previa del ataque perpetrado por el grupo, podría ser una institución gubernamental de un país del sur de Asia.

5. Override Panda, también conocido como Naikon, Hellsing y Bronze Geneva, opera en nombre de los intereses chinos desde año 2005 para llevar a cabo operaciones de recopilación de inteligencia dirigidas a los países de la ASEAN.

6. Este grupo estuvo vinculado a una amplia campaña de ciberespionaje dirigida contra organizaciones militares en el sureste asiático. Asimismo, estuvo implicado en ataques cibernéticos dirigidos al sector de las telecomunicaciones.

7. Se recomienda:
   - Implementar y configurar la plataforma de protección de Virus y Spam en equipos para detectar, proteger y desinfectar en forma activa la instalación de códigos maliciosos como troyanos, malware.
   - Contar con herramientas de seguridad, para prevenir la entrada de amenazas.

Fuentes de información	▪ https://thehackernews.com/2022/05/chinese-override-panda-hackers.html ▪ https://cluster25.io/2022/04/29/lotus-panda-awake-last-strike/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 123	Fecha: 05-05-2022
		Página 8 de 10

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Smishing, Campaña de envió de SMS fraudulentos, suplantando la identidad del banco Interbank.		
Tipo de ataque	Smishing	Abreviatura	Smishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de subfamilia	G03
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 diferentes delitos informáticos empleando la modalidad "Smishing" (SMS), quienes suplantan la identidad del Banco Interbank, indicando que el cliente cuenta con un depósito de S/. 210.00 correspondiente al Bono Subsidio, para ello se quiere ingresar a un link adjuntado en el mensaje enviado.

2. **Imagen**: Detalle del proceso del Smishing:

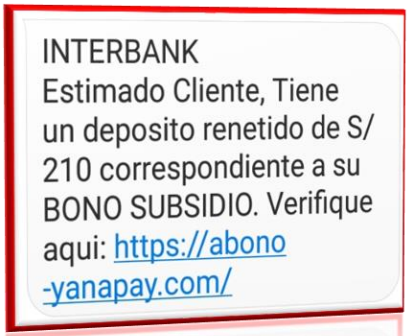


Imagen 1: Mensaje enviado a la víctima.

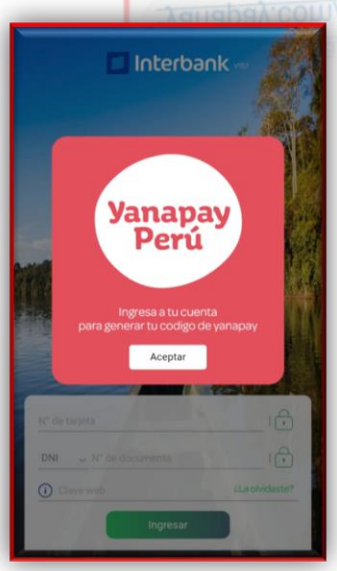


Imagen 2: Una vez hecho clic, en el enlace del mensaje, es redirigido a un sitio falso que suplanta la identidad del Banco Interbank, con el fondo de Yanapay Perú.

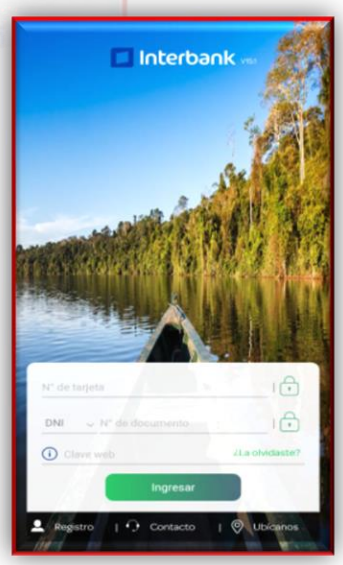


Imagen 3: Sitio web falso, donde requiere el ingreso de las credenciales de acceso (número de tarjeta, DNI y clave web).

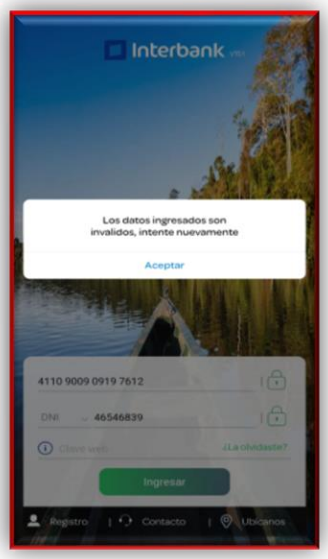
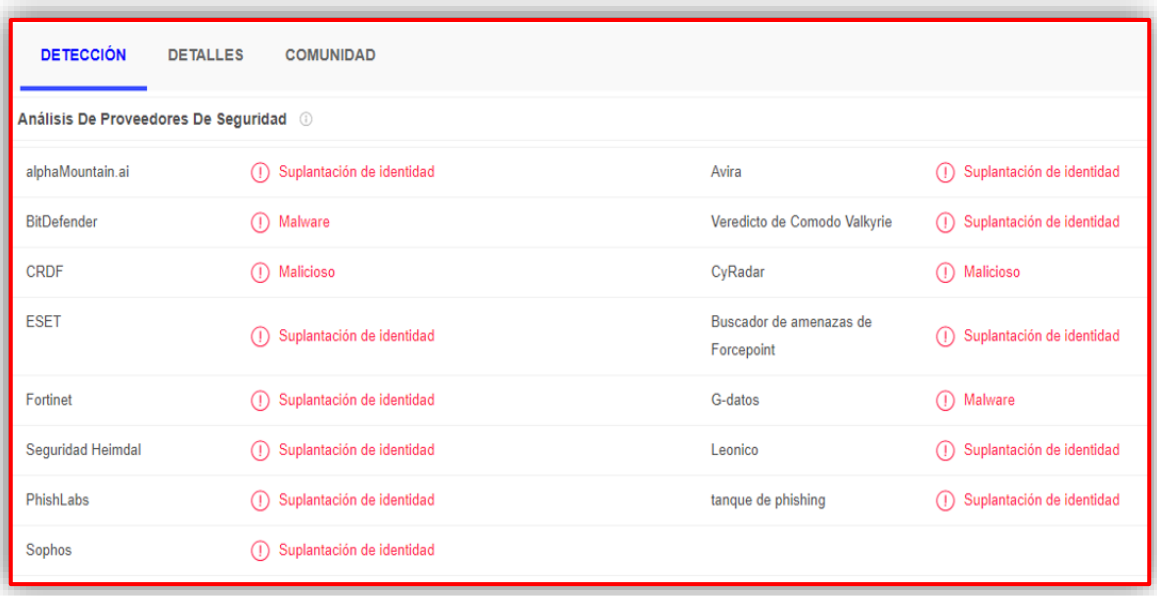


Imagen 4: Pasado unos segundos, aparece un mensaje indicando "Los datos ingresados son inválidos, intente nuevamente", aludiendo un aparente error de autenticación, sin embargo, los datos fueron capturados.

3. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD:**

- **INDICADORES DE COMPROMISO:**

  - ✓ **URL:** hxxps://abono-yanapay[.]com/
  - ✓ **Dominio:** abono-yanapay[.]com
  - ✓ **IP:** 45[.]13[.]252[.]188
  - ✓ **SHA-256**: 2c578007dfbc320d7e6358bb8f3b9be343487b64130d69259b94eb3b1d3e7162



DETECCIÓN | DETALLES | COMUNIDAD

Análisis De Proveedores De Seguridad

alphaMountain.ai	Suplantación de identidad	Avira	Suplantación de identidad
BitDefender	Malware	Veredicto de Comodo Valkyrie	Suplantación de identidad
CRDF	Malicioso	CyRadar	Malicioso
ESET	Suplantación de identidad	Buscador de amenazas de Forcepoint	Suplantación de identidad
Fortinet	Suplantación de identidad	G-datos	Malware
Seguridad Heimdal	Suplantación de identidad	Leonico	Suplantación de identidad
PhishLabs	Suplantación de identidad	tanque de phishing	Suplantación de identidad
Sophos	Suplantación de identidad		

- **OTRAS DETECCIONES:**

4. ALGUNAS RECOMENDACIONES:

- Verificar la información en la entidad correspondiente.
- Acceder al sitio web a través de fuentes oficiales.
- No abrir enlaces de dudosa procedencia.
- No seguir indicaciones de sitios web fraudulentos.
- No compartir la información con terceras personas, amigos o familiares.
- Mantener instalado un servicio de antivirus en el dispositivo.

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

Índice alfabético