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, 22 de junio de 2022

N° 167-2022-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

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 167**	**Fecha: 22-06-2022**
		Página 4 de 10

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidades en 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:

Cisco ha reportado dos vulnerabilidades de severidad MEDIA de tipo manejo inadecuado de parámetros no definidos y verificación insuficiente de la autenticidad de los datos en varios de sus productos. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto autenticado ejecutar comandos arbitrarios en el sistema afectado.

2. Detalles:

- La vulnerabilidad de severidad **media** identificada como CVE-2022-20828 de manejo incorrecto de parámetros de comandos no definidos en el analizador de la interfaz de línea de comandos (CLI) del módulo FirePOWER de Cisco FirePOWER Software for Adaptive Security Appliance (ASA) podría permitir a un atacante remoto autenticado ejecutar comandos arbitrarios en el sistema operativo subyacente de un módulo ASA FirePOWER afectado como usuario raíz. Esta vulnerabilidad se debe a un manejo incorrecto de parámetros de comandos no definidos. Un atacante podría aprovechar esta vulnerabilidad mediante un comando diseñado en la CLI o enviando una solicitud HTTPS especialmente diseñada a la interfaz de administración basada en web de Cisco ASA que hospeda el módulo ASA FirePOWER. Para explotar con éxito esta vulnerabilidad, el atacante debe tener acceso administrativo a Cisco ASA.
- La vulnerabilidad de severidad **media** identificada como CVE-2022-20829 de verificación insuficiente de la autenticidad de los datos en el empaquetado de imágenes de Cisco Adaptive Security Device Manager (ASDM) y la validación de esas imágenes por Cisco ASA Software podría permitir a un atacante remoto autenticado con privilegios administrativos cargar una imagen ASDM que contiene código malicioso en un dispositivo que ejecuta Cisco ASA Software. Esta vulnerabilidad se debe a una validación insuficiente de la autenticidad de una imagen ASDM durante su instalación en un dispositivo que ejecuta Cisco ASA Software. Un atacante podría aprovechar esta vulnerabilidad instalando una imagen ASDM diseñada en el dispositivo que ejecuta Cisco ASA Software y, a esperar que un usuario de destino tenga acceso a ese dispositivo mediante ASDM.

  Un exploit exitoso podría permitir a un atacante ejecutar código arbitrario en la máquina del usuario objetivo con los privilegios de ese usuario en esa máquina. Para aprovechar esta vulnerabilidad, el atacante debe tener privilegios administrativos en el dispositivo que ejecuta Cisco ASA Software.

3. Productos afectados:

- La vulnerabilidad CVE-2022-20828 afecta a los módulos Cisco ASA FirePOWER si ejecutan una versión vulnerable del software Cisco FirePOWER (versión 6.2.2 y anteriores, 6.2.3, 6.3.0, 6.4.0, 6.5.0, 6.60, 6.7.0, y 7.0) y si están configurados para bloquear todo el acceso al shell de Linux mediante el comando en la CLI: **system lockdown[-sensor]**;
- La vulnerabilidad CVE-2022-20829 afecta a los dispositivos Cisco si ejecutan una versión de Cisco ASA Software anterior a la versión 9.18.2, si el dispositivo se configuró con una versión ASDM de Cisco anterior a la versión 7.18.1.150, si la imagen de Cisco ASDM utiliza una versión de Cisco ASDM-IDM Launcher anterior a la versión 1.9(4) y si el dispositivo se configuró para el acceso de administración HTTPS.

4. Solución:

- Cisco ha publicado actualizaciones de software que abordan esta vulnerabilidad;
- Cisco FirePOWER Software para las versiones del módulo ASA FirePOWER 6.2.2 y anteriores, así como las versiones 6.3.0 y 6.5.0, han llegado al final del mantenimiento del software. Se recomienda migrar a una versión compatible que incluya la corrección de esta vulnerabilidad;
- Cisco FirePOWER Software Release 7.0 es la versión final para el módulo ASA FirePOWER.

Fuentes de información	▪ hxxps://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asasfr-cmd-inject-PE4GfdG ▪ hxxps://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-asdm-sig-NPKvwDjm

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 167	Fecha: 22-06-2022
		Página 6 de 10

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad crítica en Siemens WinCC OA		
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:

Los investigadores Daniel dos Santos y Jos Wetzels de Forecout Technologies, han reportado una vulnerabilidad de severidad CRÍTICA de tipo uso de autenticación del lado del cliente que afecta al sistema SCADA HMI "SIMATIC WinCC OA" de Siemens. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto se haga pasar por otros usuarios y explote el protocolo cliente-servidor sin estar autenticado.

2. Detalles:

- SIMATIC WinCC Open Architecture (OA) forma parte de la familia SIMATIC HMI. Está diseñado para su uso en aplicaciones que requieren un alto grado de adaptabilidad específica del cliente, aplicaciones grandes o complejas y proyectos que imponen requisitos o funciones específicas del sistema.
- La vulnerabilidad de severidad **crítica** identificada como CVE-2022-331139 de uso de la autenticación del lado del cliente en las aplicaciones afectadas utilizan la autenticación sólo del lado del cliente cuando no están habilitadas la autenticación del lado del servidor (SSA) ni la autenticación Kerberos. En esta configuración, los atacantes podrían hacerse pasar por otros usuarios y/o explotar el protocolo cliente-servidor sin estar autenticados.
- La vulnerabilidad de uso de la autenticación del lado del cliente, se deba a que un producto cliente/servidor realiza la autenticación dentro del código de cliente, pero no en el código de servidor, lo que permite omitir la autenticación del lado del servidor a través de un cliente modificado que omite la comprobación de autenticación.

3. Productos afectados:

Las siguientes versiones de SIMATIC WinCC OA, un sistema SCADA HMI, se ven afectadas:

- SIMATIC WinCC OA v3.16: Todas las versiones en configuración por defecto;
- SIMATIC WinCC OA v3.17: Todas las versiones en configuración no por defecto;
- SIMATIC WinCC OA v3.18: Todas las versiones en configuración no por defecto.

4. Solución:

- Siemens recomienda proteger el acceso a la red a los dispositivos con los mecanismos adecuados. Para operar los dispositivos en un entorno de TI protegido, se recomienda configurar el entorno de acuerdo con las pautas operativas de Siemens para la Seguridad Industrial y seguir las recomendaciones de los manuales de los productos.
- Asimismo, se debe habilitar la autenticación del lado del servidor (SSA) o la autenticación Kerberos para todos los proyectos de WinCC OA (se requiere inicio de sesión).
  - ✓ SIMATIC WinCC OA v3.16 SSA;
  - ✓ SIMATIC WinCC OA v3.17 SSA;
  - ✓ SIMATIC WinCC OA v3.18 SSA.

Fuentes de información	▪ hxxps://www.cisa.gov/uscert/ics/advisories/icsa-22-172-06 ▪ https://cert-portal.siemens.com/productcert/news.html?id=21 ▪ hxxps://cert-portal.siemens.com/productcert/html/ssa-111512.html ▪ hxxps://www.siemens.com/cert/operational-guidelines-industrial-security ▪ hxxps://www.siemens.com/industrialsecurity

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 167	Fecha: 22-06-2022
		Página 7 de 10

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Nueva campaña de phishing que suplanta la identidad bancaria de la Caja Trujillo		
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 que suplanta la identidad bancaria de la Caja Trujillo, mediante la creación de un sitio web falso similar al oficial, con el objetivo robar credenciales de acceso, datos personales y/o financieros de los clientes de la Caja Trujillo.

2. Proceso del ataque phishing:

Imagen 1: Sitio web que suplanta la identidad de la Caja Trujillo, solicita a la víctima ingresar sus datos bancarios (N° de Tarjeta y DNI).

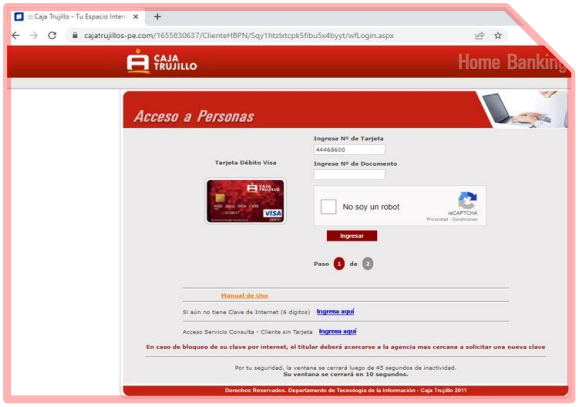
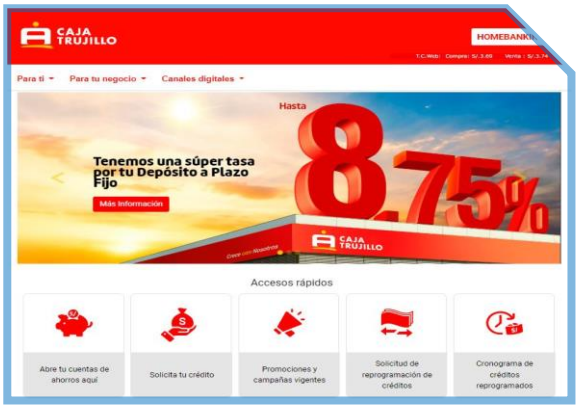
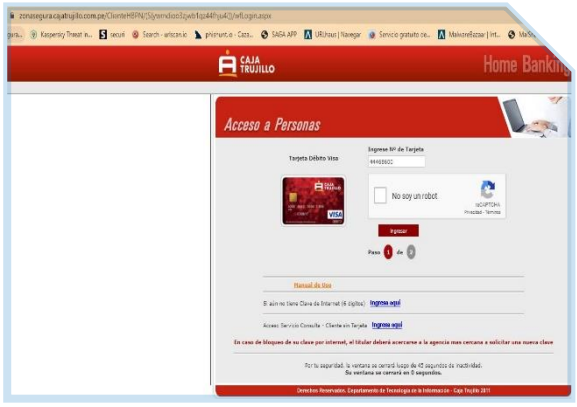


Imagen 2: Una vez que se ingresó los datos bancarios, es redirigido al sitio web oficial de la Caja Trujillo, aludiendo un aparente error de autenticación; sin embargo, los datos fueron capturados por los cibercriminales.

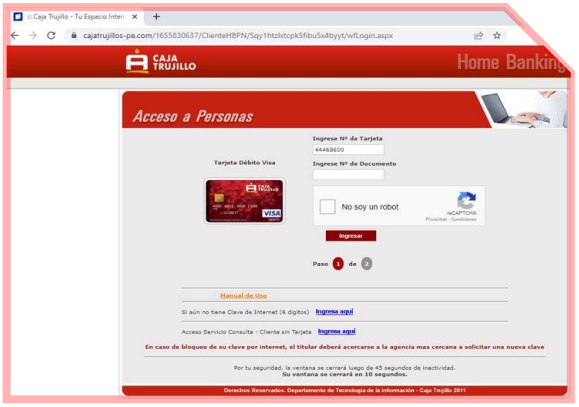


3. Comparación del sitio web oficial y sitio web fraudulento:

SITIO WEB OFICIAL
URL: https://zonasegura.cajatrujillo.com.pe/



SITIO WEB FRAUDULENTO
URL: hXXps[:]//cajatrujillos-pe[.]com/



Observación: El sitio apócrifo utiliza el diseño gráfico de la Caja Trujillo, con el objetivo de engañar a la víctima. La diferencia se encuentra en la dirección URL, de ambos sitios web.

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

- URL : https[:]//cajatrujillos-pe[.]com/
- Dominio : cajatrujillos-pe[.]com
- IP. : 104[.]21[.]0[.]226
- Código : 200
- Tamaño : 800.38 KB
- SHA-256 : 382858d0998997bab390a1dfe93aab076d7e31ad8c6d4b806c5f931e6ee46534

DETECCIÓN | DETALLES | ENLACES | COMUNIDAD

Análisis De Proveedores De Seguridad

alphaMountain.ai	Suplantación de identidad	Avira	Suplantación de identidad
BitDefender	Malware	CRDF	Malicioso
CASO	Suplantación de identidad	Buscador de amenazas de Forcepoint	Suplantación de identidad
Fortinet	Suplantación de identidad	G-datos	Malware
Seguridad Heimdal	Suplantación de identidad	kaspersky	Suplantación de identidad
ue de phishing	Suplantación de identidad	Sanar rapido	Suplantación de identidad

- Otros resultados del análisis:

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:**

- Confirmar el sitio web al que se ingresa sean los oficiales.
- Verificar la redacción y ortografía de la URL.
- Evitar proporcionar información personal y/o bancaria en sitios webs fraudulentas.
- Evitar guardar información bancaria en el dispositivo móvil.
- Contar con una solución de seguridad, constantemente actualizada tanto en dispositivos de escritorio como en móviles, ya que sirven como barrera inicial protectora ante sitios web maliciosos.

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

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 167	Fecha: 22-06-2022
		Página 9 de 10

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Hackers del gobierno ruso golpearon Ucrania con Cobalt Strike, malware CredoMap		
Tipo de ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de subfamilia	C01
Clasificación temática familia	Código Malicioso		

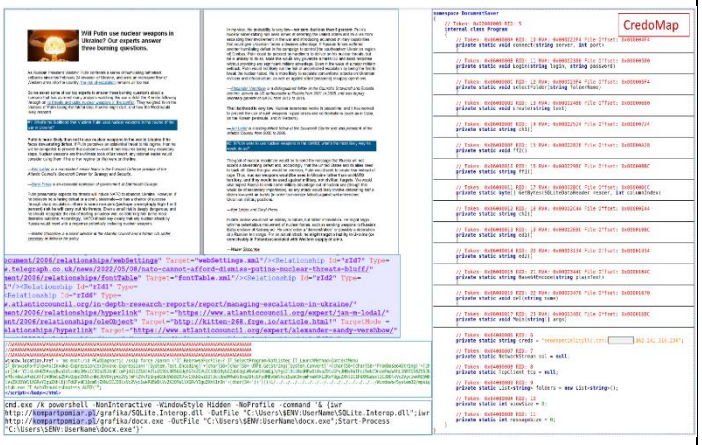
Descripción

FECHA DEL EVENTO:

A través del monitoreo y búsqueda de amenazas en el ciberespacio del día 21 de junio del 2022, se tomó conocimiento de la publicación realizada en la página web de "**BLEEPING COMPUTER**", El Equipo de Respuesta a Emergencias Informáticas de Ucrania (CERT) advierte que los grupos de piratería rusos están explotando la vulnerabilidad de ejecución de código Follina en nuevas campañas de phishing para instalar el malware CredoMap y las balizas Cobalt Strike.

ANTECEDENTES:

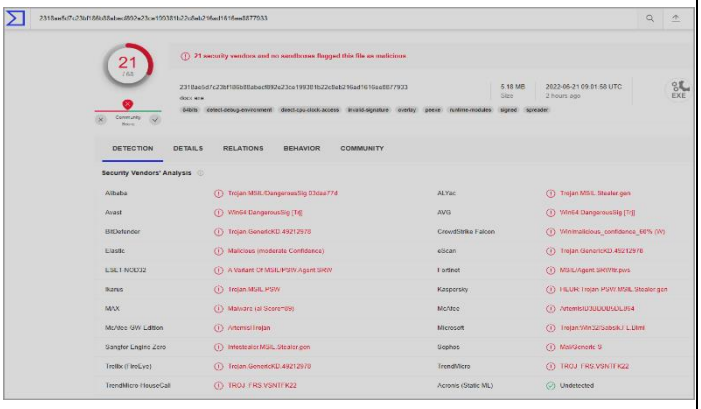
Se cree que el grupo de piratería APT28 está enviando correos electrónicos que contienen un documento malicioso llamado "Terrorismo nuclear una amenaza muy real.rtf. Los actores de amenazas seleccionaron el tema de este correo electrónico para atraer a los destinatarios a abrirlo, explotando el temor que se extiende entre los ucranianos sobre un posible ataque nuclear.



Los actores de amenazas también utilizaron una táctica similar en mayo de 2022, cuando CERT-UA identificó la difusión de documentos maliciosos que advertían sobre un ataque químico.

DETALLES:

Esta vulnerabilidad es una falla en la herramienta de diagnóstico de Microsoft, explotada en la naturaleza desde al menos abril de 2022, desencadenando descargas maliciosas simplemente abriendo un archivo de documento o, en el caso de los RTF, simplemente viéndolo en el panel de vista previa de Windows.



CredoMap es una cepa de malware desconocida detectada por varios motores AV en Virus Total, con numerosos proveedores clasificándola como un troyano que roba contraseñas.

RECOMENDACIONES:

- CERT-UA aconseja a los empleados de organizaciones críticas que permanezcan atentos a las amenazas entregadas por correo electrónico, ya que el número de ataques de spear-phishing sigue siendo alto.

Fuentes de información	▪ https://www.bleepingcomputer.com/news/security/russian-govt-hackers-hit-ukraine-with-cobalt-strike-credomap-malware/

Índice alfabético