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, 17 de junio de 2022

N° 162-2022-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° 162**	**Fecha: 17-06-2022**
		Página 4 de 8

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades en productos de AutomationDirect		
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:

La empresa de controles industriales, AutomationDirect, ha reportado múltiples vulnerabilidades de severidad ALTA de tipo elemento de ruta de búsqueda no controlada, transmisión de texto sin cifrar de información confidencial y consumo descontrolado de recursos que afecta a varios de sus productos. La explotación exitosa de estas vulnerabilidades podría causar una pérdida de información confidencial, ejecución de código con privilegios elevados, cambios no autorizados y generar una condición de denegación de servicio (DoS).

2. Detalles:

- La vulnerabilidad de severidad **alta** identificada como CVE-2022-2006 de elemento de ruta de búsqueda no controlada, se debe a que el producto afectado tiene una vulnerabilidad DLL en el directorio de instalación que podría permitir a un atacante remoto ejecutar código durante el proceso de instalación.
- La vulnerabilidad de severidad **alta** identificada como CVE-2022-2005 de transmisión de texto sin cifrar de información confidencial, se debe a que el servidor web HTTP de los productos afectados utiliza un mecanismo inseguro para transportar credenciales del cliente al servidor web, lo que podría permitir a un atacante remoto obtener las credenciales de inicio de sesión e iniciar sesión como usuario válido.
- La vulnerabilidad de severidad **alta** identificada como CVE-2022-2004 de consumo de recursos no controlado, se debe a que un paquete especialmente diseñado se puede enviar continuamente al PLC para evitar el acceso desde DirectSoft y otros dispositivos, causando una condición de denegación de servicio.
- La vulnerabilidad de severidad **alta** identificada como CVE-2022-2003 de transmisión de texto claro de información confidencial, se debe a que el producto es vulnerable a un mensaje en serie específicamente diseñado para el puerto en serie de la CPU que hará que el PLC responda con la contraseña del PLC en texto sin cifrar. De igual forma, el producto es vulnerable a un paquete Ethernet específicamente diseñado que hará que el PLC responda con la contraseña del PLC en texto sin cifrar. Esto podría permitir a un atacante acceder al sistema y realizar cambios no autorizados.
- Estas vulnerabilidades afectan a múltiples sectores de infraestructura crítica en todo el mundo.

3. Productos afectados:

- C-more EA9 con los siguientes números de pieza, todas las versiones anteriores a la versión 6.73: EA9-T6CL, EA9-T6CL-R, EA9-T7CL, EA9-T7CL-R, EA9-T8CL, EA9-T10CL, EA9-T10WCL, EA9-T12CL, EA9-T15CL, EA9-T15CL-R, EA9-RHMI y EA9-PGMSW.
- DirectLOGIC D0-06 series CPUs, versiones anteriores a 2.72 (incluye todas las versiones de H0-ECOM y H0-ECOM100 instaladas): D0-06DD1, D0-06DD2, D0-06DR, D0-06DA, D0-06AR, D0-06AA, D0-06DD1-D, D0-06DD2-D y D0-06DR-D.

4. Solución:

AutomationDirect recomienda actualizar C-more EA9 a la versión de firmware 6.73 o posterior, que admite opciones de seguridad TLS para el servidor web y actualizar DirectLOGIC D0-06 series CPUs y CPU DL06 a la versión de firmware 2.72 o posterior, que ya no responderá con la contraseña cuando se solicite con el mensaje especialmente diseñado.

Fuentes de información	▪ hxxps://www.cisa.gov/uscert/ics/advisories/icsa-22-167-01 ▪ hxxps://www.cisa.gov/uscert/ics/advisories/icsa-22-167-02 ▪ hxxps://www.cisa.gov/uscert/ics/advisories/icsa-22-167-03

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 162**	**Fecha: 17-06-2022**
		Página 5 de 8

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad crítica en el complemento Ninja Forms de WordPress		
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:

Se ha reportado una vulnerabilidad de severidad CRÍTICA en el complemento Ninja Forms de WordPress. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto la ejecución remota de código. El complemento Ninja Forms contiene varias clases y funciones que podrían aprovecharse como parte de múltiples cadenas de explotación

2. Detalles:

- El equipo de Wordfence de la empresa de seguridad de WordPress Defiant, señalo que, más de un millón de sitios web de WordPress se ven potencialmente afectados por una vulnerabilidad crítica del complemento Ninja Forms y que está siendo explotado activamente en la naturaleza.
- Los investigadores indicaron que una característica de Ninja Forms es la capacidad de agregar "Combinar etiquetas" a los formularios que autocompletarán los valores de otras áreas de WordPress, como las ID de publicación y los nombres de los usuarios registrados.
- Debido a esta vulnerabilidad, los investigadores dijeron que fue posible llamar a varias clases de Ninja Forms y abusar de ellas para una amplia gama de exploits dirigidos a sitios vulnerables de WordPress. Indicaron además que la forma en que la clase "NF_MergeTags_Other" maneja las etiquetas de combinación hace posible que los atacantes no autenticados proporcionen etiquetas de combinación. El complemento Ninja Forms contiene varias clases y funciones que podrían aprovecharse como parte de múltiples cadenas de explotación.
- Una cadena de explotación potencialmente crítica, en particular, implica el uso de la clase "NF_Admin_Processes_ImportForm para lograr la ejecución remota de código a través de la deserialización, aunque sería necesario instalar otro complemento o tema en el sitio con un dispositivo utilizable.
- Esta vulnerabilidad afecta a más de un millón de sitios web de WordPress en todo el mundo.

3. Productos afectados:

- Múltiples versiones del complemento Ninja Forms.

4. Solución:

- El equipo de Wordfence indicó que esta vulnerabilidad se corrigió con el lanzamiento de las versiones: 3.0.34.2, 3.1.10, 3.2.28, 3.3.21.4, 3.4.34.2, 3.5.8.4 y 3.6.11 de Ninja Forms.

Fuentes de información	▪ hxxps://www.wordfence.com/blog/2022/06/psa-critical-vulnerability-patched-in-ninja-forms-wordpress-plugin/ ▪ hxxps://www.securityweek.com/exploited-vulnerability-patched-wordpress-plugin-over-1-million-installations

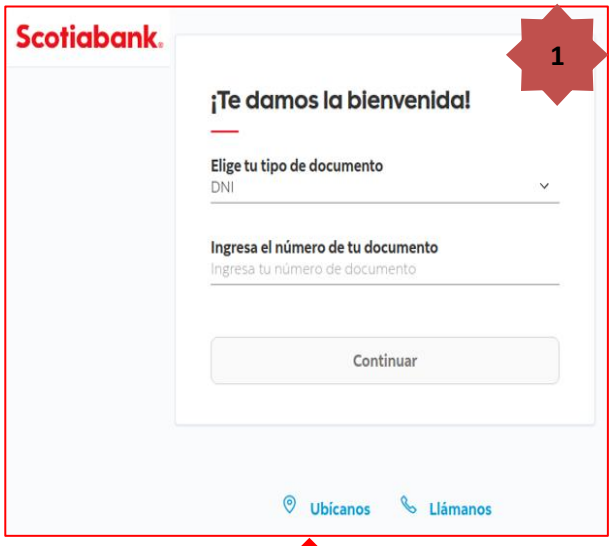
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 162	Fecha: 17-06-2022
		Página 6 de 8

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Phishing, suplantando la identidad de la entidad Bancaria Scotiabank		
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		

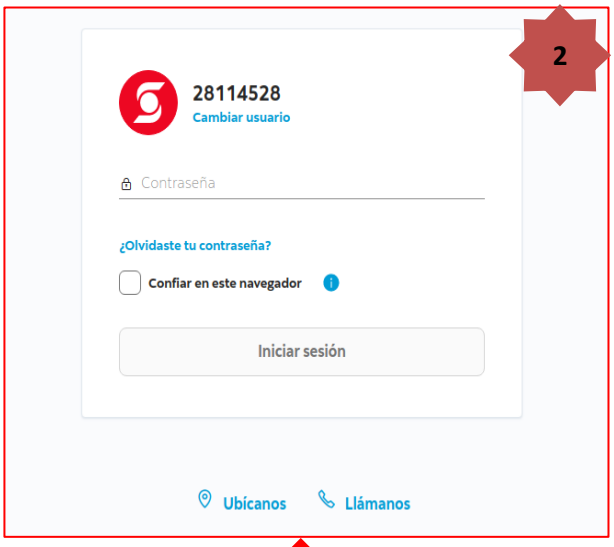
Descripción

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, por medio de los diferentes navegadores web, dirigido a los clientes y/o usuarios de la entidad bancaria Scotiabank; el cual, mediante la creación de un sitio web similar al original, solicitan a las posibles víctimas ingresar las credenciales de inicio de sesión como DNI y contraseña.

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



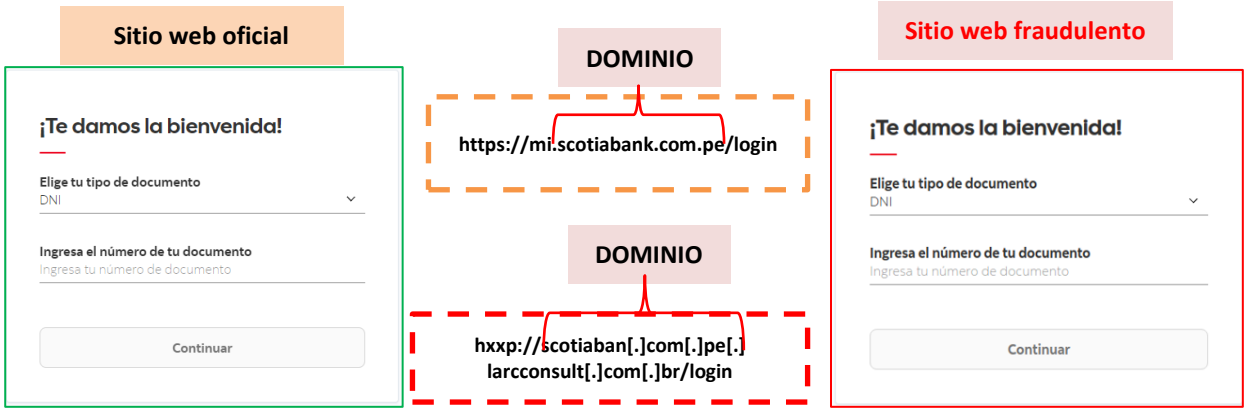
Los ciberdelincuentes requieren ingresar el tipo y número del documento nacional de identidad (DNI).



Luego piden ingresar la contraseña del usuario de las posibles víctimas o realizar un cambio de usuario.

Al ingresar las credenciales de acceso y hacer clic en iniciar sesión el supuesto sitio web informa que la información es inválida.

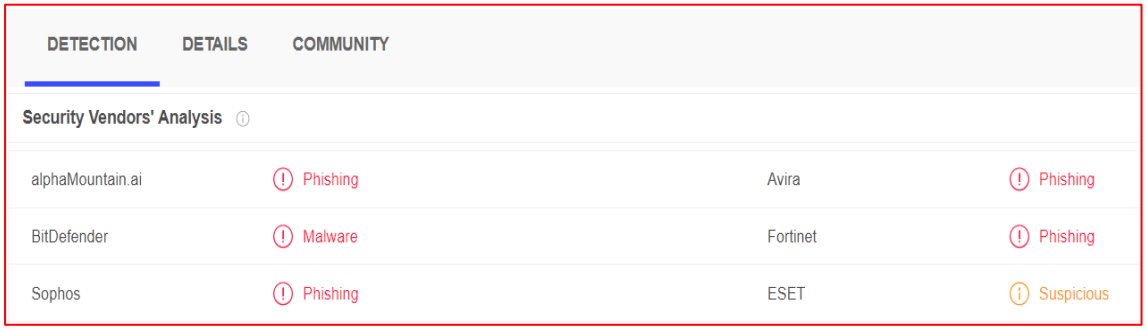
3. Comparación del sitio web oficial y fraudulento.



- Existe una similitud entre el fondo y forma de cada sitio web.
- La URL hxxp://scotiaban[.]com[.]pe[.]larcconsult[.]com[.]br/login del sitio web fraudulento NO POSEE EL PROTOCOLO DE SEGURIDAD DE RED (https).

4. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como Phishing (suplantación de identidad):

- Indicadores de compromiso:
  - **URL:** hxxp[:]//scotiaban[.]com[.]pe[.]larcconsult[.]com[.]br/login
  - **Dominio:** larcconsult[.]com[.]br
  - **IP:** 108[.]179[.]253[.]83
  - **Tamaño:** 674 B
  - **SHA-256:** 9341a2a96bfb6b523a8cf02cf79e9d1d858898a1ad1fe18c378ff4af80cc5ab3



5. Apreciación de la información:

- La presente campaña de Phishing, permite a los actores de amenazas obtener información bancaria de los usuarios del Banco Scotiabank.
- 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.

6. Recomendaciones:

- Verificar la información en la entidad correspondiente
- Las entidades bancarias no solicitan realizar actualización de datos de manera online o virtual.
- 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