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

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

Lima, 17 de noviembre de 2023

275-2023-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°275	Fecha: 17-11-2023
		Página: 4 de 12

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	CISA advierte sobre errores explotados activamente en Windows, Sophos y Oracle		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. **ANTECEDENTES:**

La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. ha agregado a su catálogo de vulnerabilidades explotadas conocidas (KEV) tres problemas de seguridad que afectan a los dispositivos de Microsoft, un producto de Sophos y una solución empresarial de Oracle.

El catálogo KEV contiene fallas que se ha confirmado que son explotadas por piratas informáticos en ataques y sirve como depósito de vulnerabilidades que las empresas de todas partes deberían tratar con prioridad.

2. **DETALLES:**

La agencia insta a las agencias federales a aplicar las actualizaciones de seguridad disponibles para los tres problemas antes del 7 de diciembre. Las tres vulnerabilidades se rastrean de la siguiente manera:

CVE-2023-36584: omisión de la característica de seguridad "Marca de la Web" (MotW) en Microsoft Windows.

CVE-2023-1671: Vulnerabilidad de inyección de comandos en Sophos Web Appliance que permite la ejecución remota de código (RCE).

CVE-2020-2551: Vulnerabilidad no especificada en Oracle Fusion Middleware, que permite a un atacante no autenticado con acceso a la red a través de IIOP comprometer el servidor WebLogic.

Aunque el catálogo KEV de CISA está dirigido principalmente a agencias federales de EE. UU., se recomienda a las empresas de todo el mundo que lo utilicen como un sistema de alerta para vulnerabilidades explotadas y tomen las medidas necesarias para actualizar sus sistemas o aplicar las mitigaciones recomendadas por los proveedores.

3. **RECOMENDACIONES:**

- Actualizar el paquete afectado según los parches de octubre del 2023 que Microsoft lanzó para abordar la vulnerabilidad CVE-2023-36584.
- Actualizar las versiones anteriores a la 4.3.10.4 del software Sophos Web Appliance según las correcciones del 4 de abril del 2023 que el proveedor lanzó para abordar la vulnerabilidad CVE-2023-1671.

Fuente de Información:	• hxxps://www.bleepingcomputer.com/news/security/cisa-warns-of-actively-exploited-windows-sophos-and-oracle-bugs/

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°275**	**Fecha: 17-11-2023**
		Página: 5 de 12

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad de denegación de servicio en productos Cisco		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Cisco ha reportado una vulnerabilidad de severidad **ALTA** de tipo denegación de servicio (DoS) en la inspección ICMPv6 cuando se configura con el motor de detección Snort 2 para el software Cisco Firepower Threat Defense (FTD) o los servicios Cisco Firepower. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado generar una condición de denegación de servicio.

2. DETALLES:

La vulnerabilidad de severidad **media**, identificada por MITRE como CVE-2023-20083 de tipo denegación de servicio, en la inspección ICMPv6 cuando se configura con el motor de detección Snort 2 para el software Cisco FTD o los servicios Cisco Firepower podría permitir que un atacante remoto no autenticado haga que la CPU de un dispositivo afectado aumente al 100 %, lo que podría detener todo el procesamiento del tráfico y resulta en una condición de DoS. El tráfico de gestión de FTD no se ve afectado por esta vulnerabilidad.

Esta vulnerabilidad se debe a una comprobación incorrecta de errores al analizar campos dentro del encabezado ICMPv6. Un atacante podría aprovechar esta vulnerabilidad enviando un paquete ICMPv6 especialmente diseñado a través de un dispositivo afectado. Un exploit exitoso podría permitir al atacante hacer que el dispositivo agote los recursos de la CPU y deje de procesar el tráfico, lo que resultaría en una condición de DoS.

Para recuperarse de la condición de DoS, es necesario reiniciar el motor de detección Snort 2, el dispositivo Cisco FTD o el dispositivo Cisco Firepower Services.

A. Productos afectados:

Esta vulnerabilidad afecta a los productos de Cisco si ejecutan una versión vulnerable del software de Cisco y están configurados con una política de descubrimiento de red que permite la detección de hosts y aplicaciones e invoca el motor de detección Snort 2:

- Servicios Firepower: todas las plataformas.
- Software Firepower Threat Defense (FTD): todas las plataformas.

Cabe indicar, que, de forma predeterminada, la política de descubrimiento de red está configurada solo para la detección de aplicaciones. Para que se aproveche esta vulnerabilidad, Snort 2 debe estar activo. Puede haber una o más instancias de Snort que estén activas en un dispositivo Cisco FTD o Cisco Firepower Services.

3. RECOMENDACIÓN:

- Aplicar las actualizaciones que Cisco ha lanzado para abordar esta vulnerabilidad. No existen soluciones alternativas que aborden esta vulnerabilidad.

Fuente de Información:	• hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-icmpv6-dos-4eMkLuN

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°275	Fecha: 17-11-2023
		Página: 6 de 12

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades críticas en productos Fortinet		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha reportado dos vulnerabilidades de severidad **CRÍTICA** de tipo inyección de comando del sistema operativo e Inyección SQL en varios productos Fortinet. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto la ejecución de código o comandos no autorizados.

2. DETALLES:

La vulnerabilidad de severidad **crítica**, identificada por MITRE como CVE-2023-36553 de tipo inyección de comando del sistema operativo, podría permitir a un atacante remoto no autenticado ejecutar comandos no autorizados a través de solicitudes de API manipuladas.

La vulnerabilidad de severidad **crítica**, identificada por MITRE como CVE-2023-34991 de tipo inyección SQL, podría permitir a un atacante remoto no autenticado ejecutar consultas SQL no autorizadas a través de una solicitud HTTP maliciosa.

A. Productos afectados:

- FortiSIEM, versiones: 5.4.0, 5.3.3, 5.3.2, 5.3.1, 5.3.0, 5.2.8, 5.2.7, 5.2.6, 5.2.5, 5.2.2, 5.2.1, 5.1.3, 5.1.2, 5.1.1, 5.1.0, 5.0.1, 5.0.0, 4.10.0, 4.9.0 y 4.7.2.
- FortiWLM, versiones: 8.6.5, 8.6.4, 8.6.3, 8.6.2, 8.6.1, 8.6.0, 8.5.4, 8.5.3, 8.5.2, 8.5.1, 8.5.0, 8.4.2, 8.4.1, 8.4.0, 8.3.2, 8.3.1, 8.3.0 y 8.2.2.

3. RECOMENDACIONES:

- Actualizar FortiSIEM a las siguientes versiones de software disponibles que abordan estas vulnerabilidades: versión 7.1.0, 7.0.1, 6.7.6, 6.6.4, 6.5.2, 6.4.3 o superiores).
- Actualizar FortiWLM a la versión 8.6.6, 8.5.5 o superior.

Fuente de Información:	• hxxps://www.fortiguard.com/psirt/FG-IR-23-135 • hxxps://www.fortiguard.com/psirt/FG-IR-23-142

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°275	Fecha: 17-11-2023
		Página: 7 de 12

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades en Microsoft Edge		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. **ANTECEDENTES:**

   Se ha reportado múltiples vulnerabilidades de severidad **ALTA** y **MEDIA** de tipo uso después de la liberación, error de validación de entrada y ataque suplantación de identidad en Microsoft Edge. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar código arbitrario y comprometer el sistema vulnerable.

2. **DETALLES:**

   La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-5997 y CVE-2023-6112 de tipo uso después de la liberación, existe debido a un error de uso después de la liberación dentro del componente de recolección de basura y de navegación en Google Chrome. Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite, provocar un error de uso después de la liberación y ejecutar código arbitrario en el sistema de destino.

   La vulnerabilidad de severidad **media**, identificada por MITRE como CVE-2023-36008 de tipo error de validación de entrada, existe debido a una validación insuficiente de la entrada proporcionada por el usuario. Un atacante remoto puede engañar a la víctima para que abra un archivo especialmente diseñado con el navegador y ejecute código arbitrario en el sistema.

   Se ha asignado el siguiente identificador para la vulnerabilidad de severidad baja: CVE-2023-36026.

   A. Productos afectados:

   - Microsoft Edge: versión 79.0.309.71 - 119.0.2151.58.

3. **RECOMENDACIÓN:**

   - Actualizar el producto afectado a la última versión de software disponible que aborda estas vulnerabilidades.

Fuente de Información:	• hxxp://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-5997 • hxxp://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-6112 • hxxp://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36008 • hxxp://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36026

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°275	Fecha: 17-11-2023
		Página: 8 de 12

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidades críticas en Sixnet RTU de Red Lion		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha reportado dos vulnerabilidades de severidad **CRÍTICA** de tipo anulación de autenticación utilizando una ruta o canal alternativo y método de función peligrosa expuesta en Sixnet RTU de Red Lion. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado ejecutar comandos con altos privilegios.

2. DETALLES:

La vulnerabilidad de severidad **crítica**, identificada por MITRE como CVE-2023-42770 de tipo anulación de autenticación utilizando una ruta o canal alternativo, provoca que cuando se reciba el mismo mensaje a través de TCP/IP, la RTU simplemente aceptará el mensaje sin desafío de autenticación. Esta vulnerabilidad, requiere autenticación, pero el producto tiene una ruta o canal alternativo que no requiere autenticación.

La vulnerabilidad de severidad **crítica**, identificada por MITRE como CVE-2023-40151 de tipo método de función peligrosa expuesta, se produce cuando la autenticación de usuario no está habilitada, la *shell* podrá ejecutar comandos con los privilegios más altos. Esta vulnerabilidad, proporciona una interfaz de programación de aplicaciones (API) o una interfaz similar para la interacción con actores externos, pero la interfaz incluye un método o función peligroso que no está debidamente restringido.

A. Productos afectados:

- ST-IPm-8460: versión de firmware 6.0.202 y posterior.
- ST-IPm-6350: versiones de firmware 4.9.114 y posteriores.
- VT-mIPm-135-D: versiones de firmware 4.9.114 y posteriores.
- VT-mIPm-245-D: versiones de firmware 4.9.114 y posteriores.
- VT-IPm2m-213-D: versiones de firmware 4.9.114 y posteriores.
- VT-IPm2m-113-D: versiones de firmware 4.9.114 y posteriores.

3. RECOMENDACIÓN:

- Aplicar los últimos parches a sus productos que abordan estas vulnerabilidades.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-23-320-01

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°275	**Fecha: 17-11-2023**
		Página: 9 de 12

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Detección de sitio web fraudulento del Banco Crédito del Perú		
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 Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que actores de amenazas vienen realizando una campaña de Phishing, suplantando el sitio web del Banco de Crédito del Perú (servicio online de préstamo personal), con la finalidad de robar información bancaria de los usuarios de la entidad financiera como números de tarjetas bancarias, clave intranet de seis dígitos, documento de identidad, correo electrónico, etc.

2. DETALLES:

Paso N.º 01

Solicitan a la víctima registrar lo siguiente:

- El monto solicitado del préstamo.
- Documento Nacional de identidad (DNI).
- Número de Celular.
- Correo electrónico.

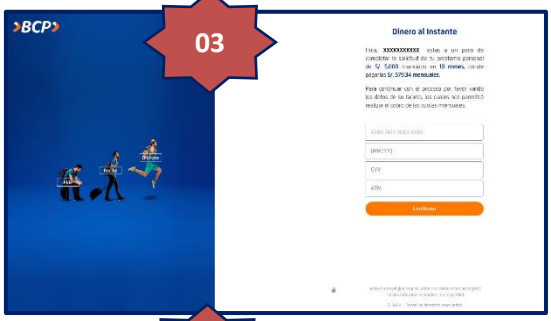
Para luego dar clic en <**Empezar**>.

Paso N.º 02

Instan a la víctima que registre datos como:

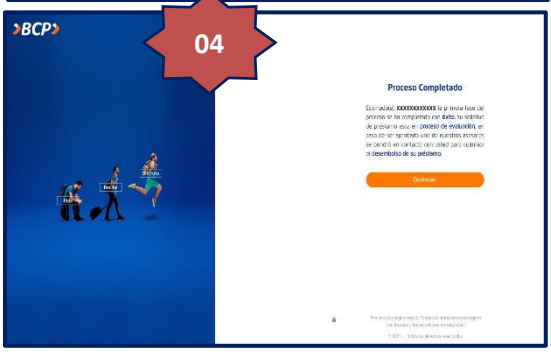
- El número de la tarjeta bancaria.
- Clave de seis dígitos del intranet.
- Código captcha.

Para luego dar clic en <**Continuar**>.



Paso N.º 03

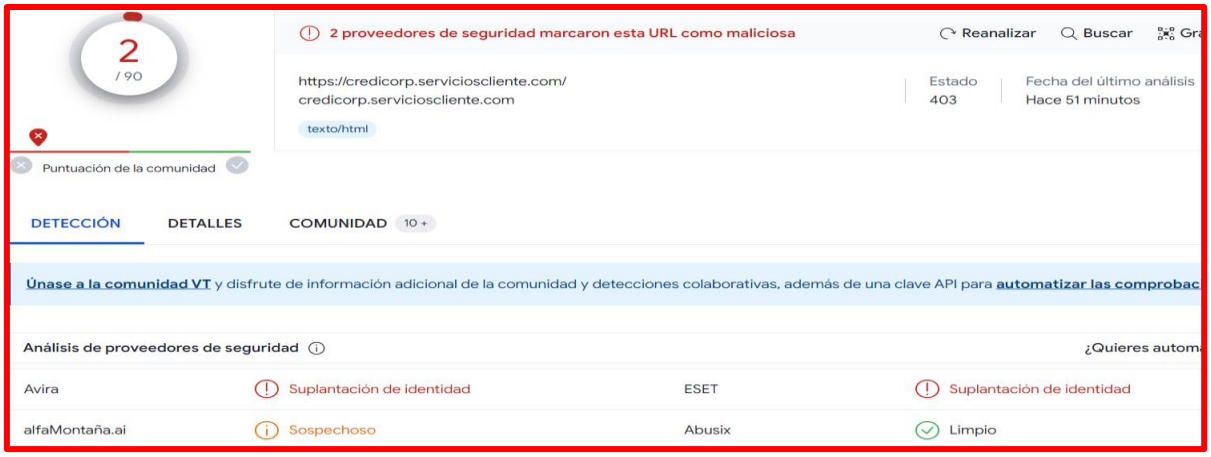
Una vez brindado los datos solicitados en el paso N.º 02, aparece una pantalla requiriendo información de la tarjeta bancaria como la fecha de expedición, el código de seguridad (CVV) y la clave de cuatro dígitos utilizado en el cajero automático, para luego dar clic en <**Continuar**>.



Paso N.º 04

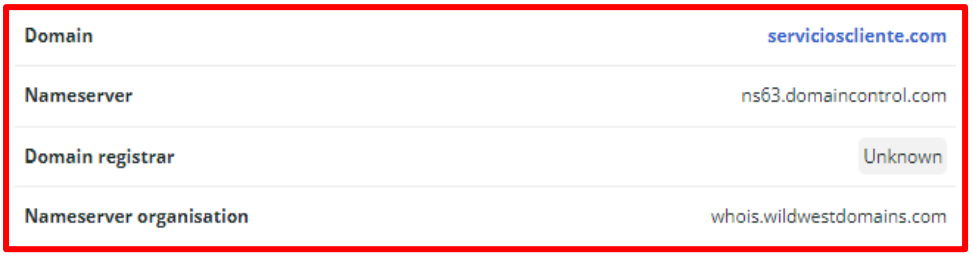
Luego, aparece una pantalla indicando que se ha completado con éxito el registro de datos y en el transcurso del día asesores de la entidad bancaria se pondrán en contacto con la víctima, para luego dar clic en <**Continuar**>. Redirigiendo al sitio web oficial de la entidad bancaria; sin embargo, los ciberdelincuentes obtuvieron los datos proporcionados por la víctima.

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

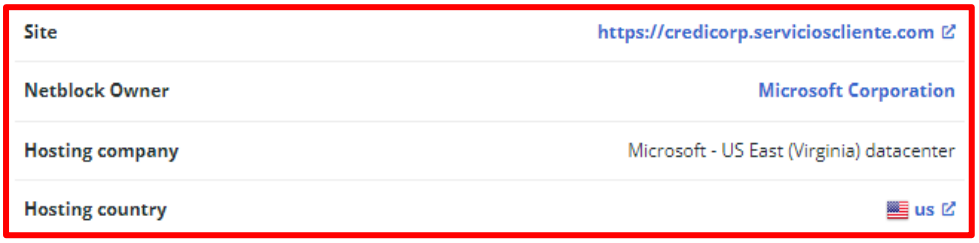


a) Indicadores de compromiso (IoC)

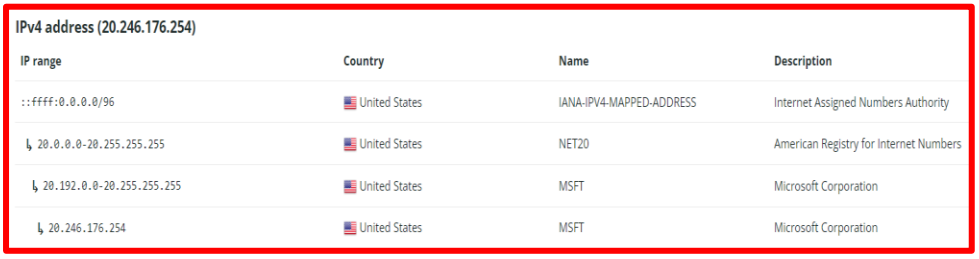
- Dominio : serviciosclientе[.]com



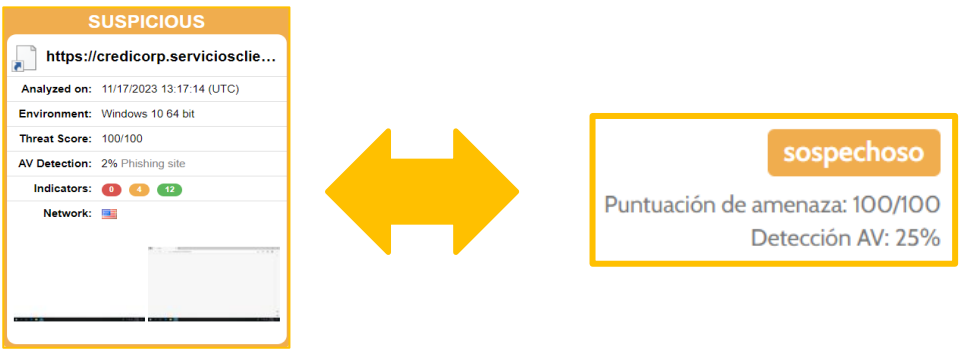
- Url : hxxps://credicorp[.]serviciosclientе[.]com/



- SHA-256 : afca372f9959cb6c46bde573d25172c1b223dac52cba20ffad3c8fc2ea09cc8e



- IP : 20[.]246[.]176[.]254
- Tipo de tex. : Text/Html
- Otras detecciones



B. Apreciación de la información:

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

- 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, a través de las aplicaciones de mensajería instantánea entre ellos WhatsApp, Telegram, Messenger, etc. y mensajes de textos SMS.

3. RECOMENDACIONES:

- Verificar detalladamente las URL de los sitios web.
- No abrir o descargar archivos sospechosos.
- No seguir las instrucciones de sitio web sospechoso.
- No aceptar permisos de instalación de archivos desconocidos o dudosa procedencia.
- Mantener actualizado el sistema operativo y aplicaciones del equipo de cómputo.
- Mantener actualizado el sistema antivirus (el antivirus debe ser licenciado).

Fuente de Información:	Análisis propio de redes sociales y fuente abierta.

Índice alfabético