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, 09 de junio de 2022

N° 155-2022-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

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 155	Fecha: 09-06-2022
		Página 4 de 9

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidades en el gestor de arranque U-Boot para dispositivos integrados basados en Linux		
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:

Investigadores de NCC Group, han detectado dos vulnerabilidades de severidad CRÍTICA y ALTA de tipo sobreescritura del descriptor de agujeros y desbordamiento de búfer en el algoritmo de desfragmentación IP implementado en U-Boot. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante local comprometer dispositivos integrados basados en Linux y/o generar una condición de denegación de servicio.

2. Detalles:

- U-Boot es un gestor de arranque (o bootloader) utilizado en sistemas integrados basados en Linux, y se encarga del proceso de arranque del sistema operativo. Tiene, asimismo, capacidad de conectarse a la red y obtener imágenes de arranque. U-Boot se utiliza en varios tipos de sistemas integrados, incluidos ChromeOS y Android. Admite múltiples arquitecturas, incluidas 68k, ARM, x86, MIPS, Nios, PPC y más.
- La vulnerabilidad de severidad **crítica** identificada como CVE-2022-30790 de sobreescritura del descriptor de agujeros en la desfragmentación de paquetes IP de U-Boot conduce a una escritura arbitraria fuera de los límites. La implementación U-Boot de RFC815 IP DATAGRAM RFC815 IP DATAGRAM REARTHMS es susceptible a un ataque de sobreescritura de "Hole Descriptor" que, en última instancia, conduce a una escritura arbitraria.
- La vulnerabilidad de severidad **alta** identificada como CVE-2022-30552 de desbordamiento de búfer, podría conducir o generar una condición de DoS en el código de desfragmentación de paquetes IP de U-Boot. La implementación U-Boot de RFC815 IP DATAGRAM REASSEMBLY ALGORITTHS es susceptible a un desbordamiento de búfer a través de un datagrama IP fragmentado especialmente diseñado con una longitud total no válida que provoca una denegación de servicio.
- Estas vulnerabilidades sólo se pueden explotar desde la red local, ya que requiere la elaboración de un paquete con formato incorrecto que probablemente se descartaría durante el enrutamiento.

3. Productos afectados:

- Estas vulnerabilidades afectan al cargador de arranque U-Boot 2022.01.

4. Solución:

- Los mantenedores de U-boot están trabajando para lanzar un parche de seguridad que corrijan estas vulnerabilidades, luego de lo cual se recomienda a los usuarios actualizar a la última versión.

Fuentes de información	▪ hxxps://github.com/u-boot/u-boot/tags ▪ hxxps://research.nccgroup.com/2022/06/03/technical-advisory-multiple-vulnerabilities-in-u-boot-cve-2022-30790-cve-2022-30552/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 155	**Fecha: 09-06-2022**
		Página 5 de 9

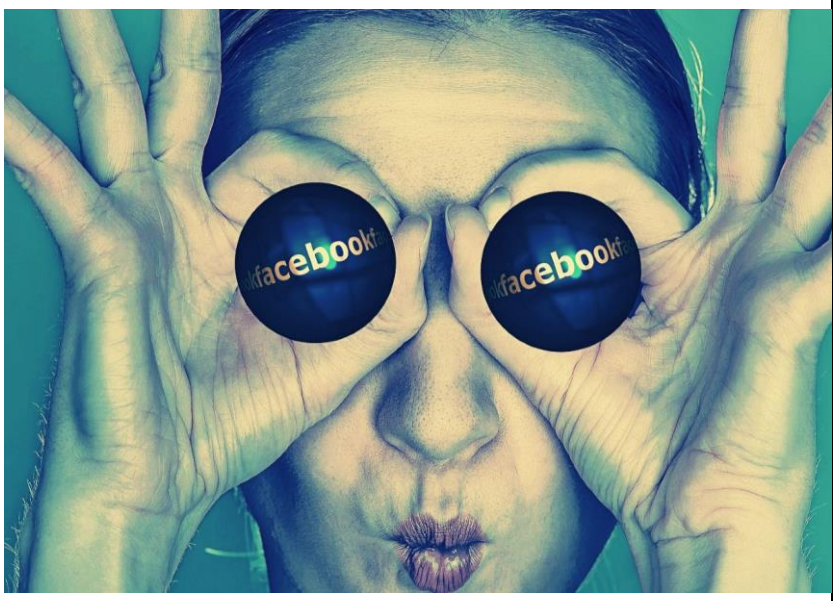
Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Operación masiva de phishing en Facebook Messenger		
Tipo de ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de subfamilia	G01
Clasificación temática familia	Fraude		

Descripción

A través del monitoreo y búsqueda de amenazas en el ciberespacio del día 08 de junio del 2022, se ha observado una operación masiva de phishing de Facebook Messeger distribuyendo más enlaces de phishing entre los contactos de las cuentas robadas y al mismo tiempo extrayendo credenciales.

ANTECEDENTES:

Los investigadores han descubierto una operación de phishing a gran escala que abusó de Facebook y Messenger para atraer a millones de usuarios a páginas de phishing, engañándolos para que ingresaran las credenciales de su cuenta y vieran anuncios.



Los operadores de la campaña utilizaron estas cuentas robadas para enviar más mensajes de phishing a sus amigos, lo que generó importantes ingresos a través de las comisiones de publicidad en línea.

Según PIXM, una empresa de ciberseguridad centrada en la IA con sede en Nueva York, la campaña alcanzó su punto máximo entre abril y mayo de 2022, pero ha estado activa al menos desde septiembre de 2021.

Escala masiva de abuso

Si bien se desconoce cómo comenzó inicialmente la campaña, PIXM afirma que las víctimas llegaron a las páginas de destino de phishing a partir de una serie de redireccionamientos que se originaron en Facebook Messenger. A medida que se robaban más cuentas de Facebook, los atacantes usaban herramientas automatizadas para enviar más enlaces de phishing a los amigos de la cuenta comprometida, lo que generaba un crecimiento masivo en las cuentas robadas. "La cuenta de un usuario se vería comprometida y, probablemente de forma automatizada, el atacante iniciaría sesión en esa cuenta y enviaría el enlace a los amigos del usuario a través de Facebook Messenger", explica PIXM en el informe .

Si bien Facebook tiene medidas de protección para detener la difusión de URL de phishing, los actores de amenazas utilizaron un truco para eludir estas protecciones. Los mensajes de phishing usaban servicios legítimos de generación de URL como litch.me, celebrity.co, amaze.co y funnel-preview.com, lo que sería un problema para bloquear ya que las aplicaciones legítimas los usan. Los investigadores creen que estos 405 nombres de usuario representan sólo una fracción de las cuentas utilizadas para la campaña.

Después de que la víctima ingrese sus credenciales en la página de inicio de phishing, comienza una nueva ronda de redireccionamientos, llevándolos a páginas de publicidad, formularios de encuestas, etc. Los actores de amenazas reciben ingresos por referencia de estos redireccionamientos, que se estiman en millones de dólares a esta escala de operación.

Rastreando al actor de la amenaza

PIXM encontró un fragmento de código común en todas las páginas de destino, que contenía una referencia a un sitio web que ha sido incautado y forma parte de una investigación contra un colombiano identificado como Rafael Dorado.

No está claro quién se apoderó del dominio y colocó el aviso en el sitio.

Una búsqueda inversa de whois reveló enlaces a una empresa legítima de desarrollo web en Colombia y sitios antiguos que ofrecían "bots similares" de Facebook y servicios de piratería.

PIXM compartió los resultados de su investigación con la Policía de Colombia y la Interpol, pero como señalan, la campaña sigue en curso, a pesar de que muchas de las URL identificadas se han desconectado.

RECOMENDACIONES:

- Evite abrir enlaces sospechosos en Facebook.
- Mantenga actualizado el sistema operativo e instale aplicaciones de antivirus.
- Realice periódicamente respaldos de seguridad.

Fuentes de información	▪ https://www.bleepingcomputer.com/news/security/massive-facebook-messenger-phishing-operation-generates-millions/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 155	Fecha: 09-06-2022
		Página 7 de 9

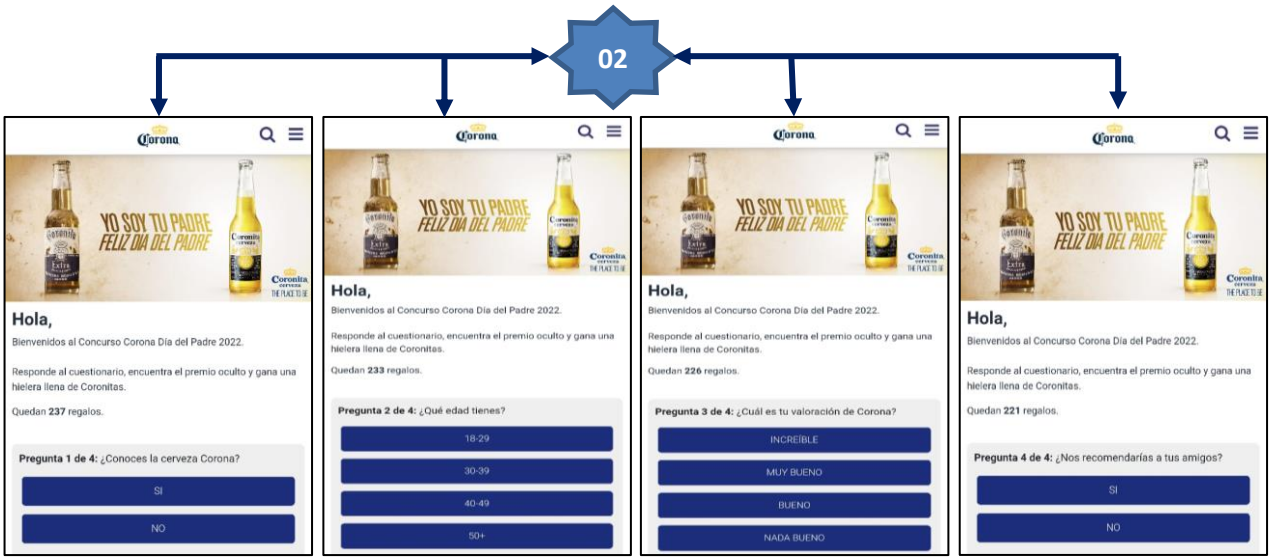
Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Distribución de malware publicitario- Adware.		
Tipo de ataque	Adware	Abreviatura	Adware
Medios de propagación	Enlaces de internet		
Código de familia	C	Código de subfamilia	C07
Clasificación temática familia	Código malicioso		

Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se tomó conocimiento que, actores de amenazas vienen llevando a cabo una campaña de distribución de malware publicitario – ADWARE, por medio de las diferentes aplicaciones de mensajería instantánea (WhatsApp, Telegram, etc.), mediante el envío de un enlace fraudulento con la temática de un supuesto concurso por el día del Padre y organizado por la compañía cervecera Corona.

2. **Imagen**: Detalle del proceso del Malware Publicitario:

➢ A través de las aplicaciones de mensajería instantánea (WhatsApp, Telegram, etc.), envían un link malicioso sobre un supuesto concurso organizado por la compañía cervecera CORONA.

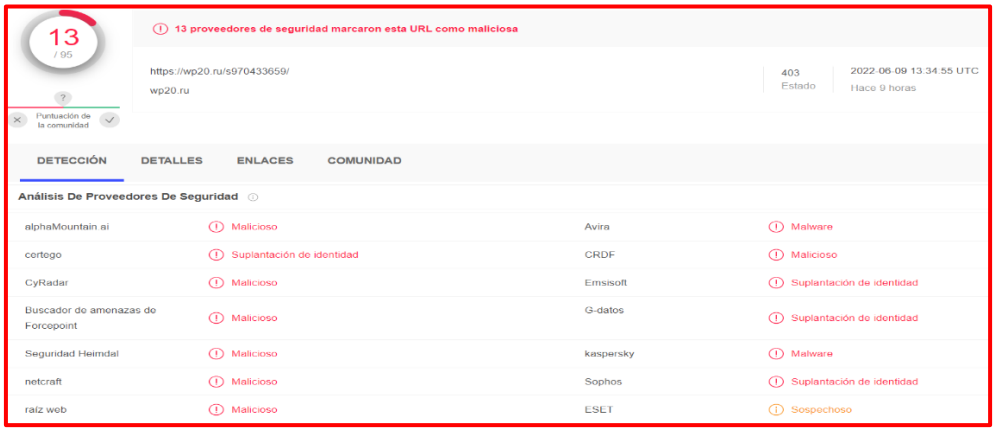


➢ Una vez dado clic en el enlace malicioso (Paso Nº 01), redirige a un cuestionario de cuatro (04) preguntas, para poder ganar un supuesto premio, organizado por la compañía cervecera Corona.

➢ Culminado el cuestionario de preguntas (Paso Nº 02), aparece una pantalla, señalando que las preguntas respondidas han sido guardadas con éxito, solicitando dar clic en <OK>.

- Una vez dado <Ok> (Paso Nº 03), aparece una pantalla, señalando que ha logrado ganar un premio, indicando que la víctima debe compartir el link fraudulento, para luego dar clic en <OK>; sin embargo, redirige al navegador donde abrió el link malicioso.

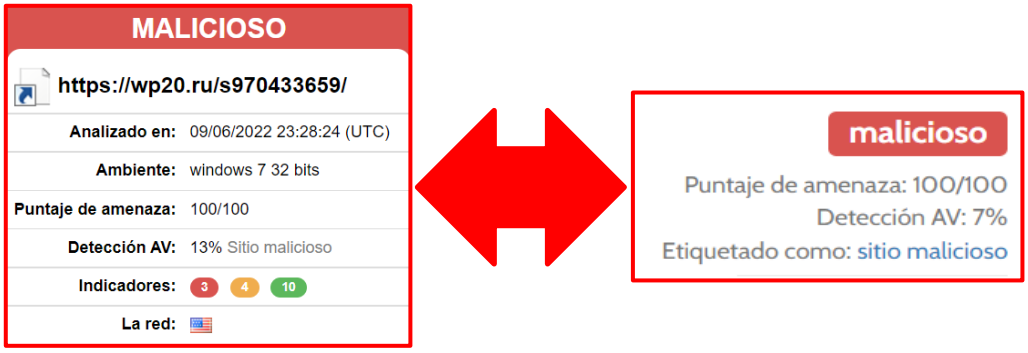
3. ***Proveedores de seguridad informática alertan como MALICIOSO.***



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

- URL : hxxps://wp20[.]ru/s970433659/
- DOMINIO : wp20[.]ru
- SHA-256 : 65f097e010e77586ff9ab4153554982698d5ca24dc73abb4deb1823a279c6457
- IP : 172[.]67[.]181[.]197

5. ***Otras detecciones***



6. ***Algunas 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 de dudosa procedencia.
- Mantener actualizado el sistema operativo y aplicaciones del equipo de cómputo.
- Mantener actualizado el sistema antivirus (el antivirus debe ser licenciado).
- 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