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

Lima, 28 de setiembre de 2022

N° 265-2022-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° 265	Fecha: 28-09-2022
		Página 04 de 15

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Vulnerabilidades de ejecución remota de código en WhatsApp		
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

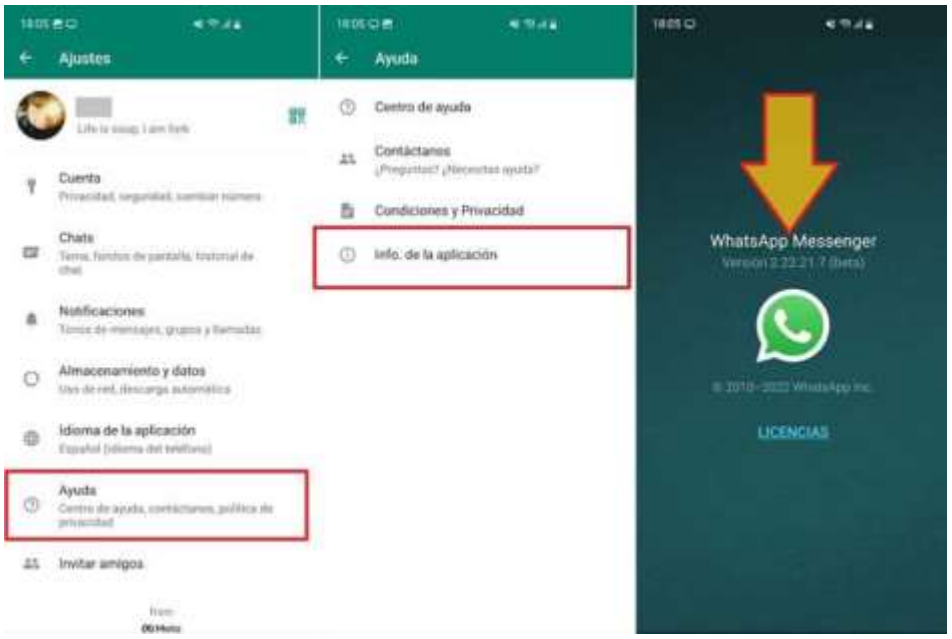
En una reciente publicación de WhatsApp, se lanzó una serie de actualizaciones de seguridad para abordar las vulnerabilidades de ejecución de código remoto en Android e iOS, recientemente descubiertas.

ANTECEDENTES:

- En enero y febrero del presente año, WhatsApp lanzó actualizaciones de seguridad para vulnerabilidades críticas asignadas como CVE-2021-24042 y CVE-2021-24043 respectivamente. Estas vulnerabilidades se daban mediante una llamada establecida por un actor de amenaza.

DETALLES:

- En el portal de avisos de seguridad de la popular aplicación de mensajería "WhatsApp", se publicaron una serie de actualizaciones de seguridad para dos vulnerabilidades clasificadas con gravedad crítica y alta respectivamente, las cuales permitirían la ejecución de código remoto.
- La primera vulnerabilidad con gravedad crítica, que ha sido asignada como CVE-2022-36934 (puntuación CVSS: 9,8), permite la ejecución de código arbitrario en el celular de la víctima, simplemente estableciendo una videollamada. Esta vulnerabilidad es conocida también como "integer overflow" o "desbordamiento aritmético".
- Dado que este error se produce en la función de las videollamadas, el atacante tendría que enviar una solicitud de videollamada manipulada a la víctima para poder aprovechar la vulnerabilidad y tomar el control completo de su aplicación. Esta vulnerabilidad afecta a las siguientes versiones de la aplicación:
    - WhatsApp para Android e iOS en versiones anteriores a v2.22.16.12
    - WhatsApp Business para Android e iOS en versiones anteriores a v2.22.16.12
- La segunda vulnerabilidad con gravedad alta, que ha sido asignada como CVE-2022-27492 (puntaje CVSS: 7.8), permite la ejecución de código arbitrario en el celular de la víctima, al recibir un archivo de video manipulado. Esta vulnerabilidad afecta a las siguientes versiones de la aplicación:
    - WhatsApp para Android antes de las versiones 2.22.16.2
    - WhatsApp para iOS versión 2.22.15.9
- La explotación de desbordamientos y subdesbordamientos de enteros es un trampolín para inducir un comportamiento no deseado, lo que provoca bloqueos inesperados, daños en la memoria y ejecución de código arbitrario. Las vulnerabilidades en WhatsApp pueden ser un vector de ataque lucrativo para los actores de amenazas que buscan instalar software malicioso en dispositivos comprometidos.
- Finalmente, WhatsApp recomendó a los usuarios, de las versiones afectadas, actualizar de inmediato la aplicación móvil a la última versión. Puede revisar su versión de WhatsApp abriendo la aplicación e ingresando a "Ajustes -> Ayuda -> Info de la aplicación".



RECOMENDACIONES:

- Contar con la última versión de la aplicación WhatsApp.
- Habilitar las actualizaciones automáticas de WhatsApp en IOS App Store y Android Play Store.
- Contar con estrictos controles de seguridad.

Fuentes de información	▪ hxxps://www.whatsapp.com/security/advisories/2022/?lang=en ▪ hxxps://thehackernews.com/2022/09/critical-whatsapp-bugs-could-have-let.html ▪ Análisis propio de fuentes abiertas.

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 265	Fecha: 28-09-2022
		Página 06 de 15

Componente que reporta	**CIBERDEFENSA Y TELEMÁTICA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Nueva campaña de malware NullMixer que roba los datos y credenciales de pago de los usuarios.		
Tipo de ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Subfamilia	C02
Clasificación temática familia	Código Malicioso		

Descripción

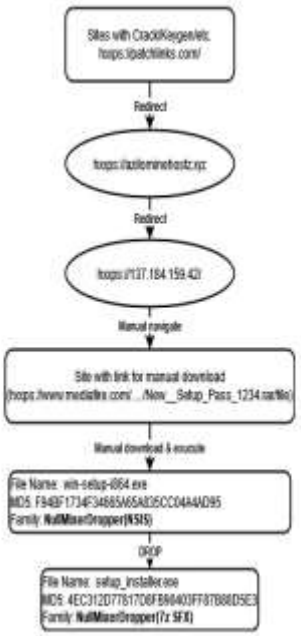
FECHA DEL EVENTO

A través del monitoreo y búsqueda de amenazas en el ciberespacio del día 27 de setiembre del 2022, se detectó que ciberdelincuentes continúan aprovechándose de los usuarios que buscan software crackeado dirigiéndolos a sitios web fraudulentos que alojan instaladores armados que implementan malware llamado NullMixer en sistemas comprometidos.

ANTECEDENTES:

Cuando un usuario extrae y ejecuta NullMixer, deja caer una serie de archivos de malware a la máquina comprometida. Deja caer una amplia variedad de binarios maliciosos para infectar la máquina, como puertas traseras, banqueros, descargadores, spyware y muchos otros.

El malware desvía las credenciales de diversas plataformas, como cuentas de datos bancarios, redes sociales, correos corporativos, contraseñas de administrador, endpoints, cookies, etc, lo que hace que NullMixer sea insidioso es su capacidad para descargar docenas de troyanos a la vez, ampliando significativamente la escala de las infecciones.
Las cadenas de ataque generalmente comienzan cuando un usuario intenta descargar software descifrado de uno de los sitios, lo que conduce a un archivo protegido por contraseña que contiene un archivo ejecutable que, por su parte, deja caer y lanza un segundo binario de configuración diseñado para entregar una serie de archivos maliciosos.
Estos sitios web maliciosos aprovechan las técnicas de envenenamiento de la optimización de motores de búsqueda (SEO), como el relleno de palabras clave, para incluirlos en gran medida en los resultados de los motores de búsqueda.
NullMixer, el mes pasado, se vinculó a la distribución de una extensión de Google Chrome llamada FB Stealer, que es capaz de robar credenciales de Facebook y sustituir motores de búsqueda.



RECOMENDACIONES:

- Se recomienda bloquear las descargas de archivos ejecutables de Windows de categorías no deseadas.
- Se recomienda que las organizaciones, capaciten a los empleados para que abran documentos solo de fuentes confiables y se aseguren de que el contenido descargado coincida con el contenido que se pretende descargar.

Fuentes de información	▪ https://thehackernews.com/2022/09/new-nullmixer-malware-campaignstealing.html

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 265	Fecha: 28-09-2022
		Página 07 de 15

Componente que reporta	**COMANDANCIA DE CIBERDEFENSA DE LA MARINA DE GUERRA DEL PERÚ**		
Nombre de la alerta	Nuevos hashes maliciosos		
Tipo de ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de subfamilia	C03
Clasificación temática familia	Código malicioso		

Descripción

1. El día 28 de setiembre del 2022, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectaron nuevas firmas de hash maliciosas, entre ellas:

ITEM	HASH SHA256	TIPO DE ARCHIVO	NOMBRE DEL ARCHIVO
1	6df677c8cfda8d63b0d089a2cac515cfff04a32433d70c29a1f3625be5388f70	android	Reflection4.apk
2	9d75b3cecc84c446e9d91008fbcaebde79cede7f4f2c0e442e977c575d665766	android	Reflection3.apk
3	3c595ae6d6ec1e78187db308324e6894dbdbb84221aa9c2c0ceebb094b0e32aa	android	PrivateDataLeak1.apk
4	151291871d430fb1cf95d984e21b711f2da3baa525ada5048bb612016b96202e	isoimage	Gallery#7044.iso
5	ed1ab1a1f8d1a8a6d5d113c71460473f0cbcc312c62161cf3e8121f060e39499	zip	590528.zip
6	f79656defa1f651ebb941033781b1532b7d11d303dd183f046dea24ea2d438df	zip	Quotation_inquiry_html.zip
7	a7ef884c5f4686d2bee093f5d3281f663ced80ac7aa8e4a55b9410f6fbb6d15e	zip	BOOKINGS COPY.zip
8	0b6079d8adfa53591e5cc61949464a26723b6c809b3f56c793903d981e95e14c	zip	BSE.zip
9	1da21647c13409f1f65983afad1b9d9ce074fde79ff26f11660f947ffde1d4c8	html	87228.html
10	1ae37c18f98cae208449efb83ab537cfc9d84f5f0be2d8c3b34ad6ad2fbf4065	gzip	1ae37c18f98cae208449efb83ab537cfc9d84f5f0be2d8c3b34ad6ad2fbf4065.gz
11	a26d870e1e5afce73df367f469d5b95f3ca42a17f4a9809edb3d817cdc3e1ea0	dll	Sneaky.dll
12	a168b6af9704af6cbc0429ce4bb13896aa24b5089529fa0966392e47f09659ca	dmg	a168b6af9704af6cbc0429ce4bb13896aa24b5089529fa0966392e47f09659ca.img
13	13db3db7122c31473978f0a80011592e766a033946563e239c80e6fd0abb64c8	pdf	13db3db7122c31473978f0a80011592e766a033946563e239c80e6fd0abb64c8.pdf
14	4ebf9c82531470eef9c7e3ae8bc2084d3c40031f0fdf3cc3c42d021816578458	dll	No Determinado
15	65bd41c708439c4a1c71b3d842e9cc174b5137b504eb8ba572508079538b347c	7zip	catalogue_28092022_samples_list_revise_0.7z

2. Recomendaciones:
   a. Evitar descargar archivos y/o enlaces de dudosa procedencia.
   b. Mantener los equipos protegidos, con el software actualizado.

Fuentes de información	▪ Comandancia de Ciberdefensa de la Marina, Osint

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 265	Fecha: 28-09-2022
		Página 08 de 15

Componente que reporta	COMANDANCIA DE CIBERDEFENSA DE LA MARINA DE GUERRA DEL PERÚ		
Nombre de la alerta	Suplantación de página web de empresa		
Tipo de ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Correo Electrónico		
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 detectaron varios sitios webs fraudulentos activos, donde suplantan páginas web de diversas empresas, con la finalidad de obtener las credenciales del usuario y robar información:

a. Facebook

PAIS DE PROCEDENCIA	FECHA	IP	URL
United States	2022-09-28	50.62.198.124	xxxxs://markitem4122284959395.com/Facebook/metas/Facebook.html?QwujosJ82t5ihq3KfHcAVxySUM1PGpCDaETL4bze0BYR9mg7lIW6FvnXkZdOrN12937256709
United States	2022-09-28	199.36.158.100	xxxx://meta-business-appeal-129861666.web.app/
United States	2022-09-28	2620:0:890::100	xxxxs://meta-business-page-129869812.web.app
United States	2022-09-28	199.36.158.100	xxxx://meta-business-page-129869812.firebaseapp.com
United States	2022-09-28	199.36.158.100	xxxx://meta-business-appeal-19787675.web.app
United States	2022-09-28	199.36.158.100	xxxxs://meta-business-page-921869281.web.app/
United States	2022-09-28	199.36.158.100	xxxxs://meta-business-page-921869281.firebaseapp.com/
United States	2022-09-28	199.36.158.100	xxxxs://meta-business-page-192892225.web.app/
United States	2022-09-28	199.36.158.100	xxxxs://meta-business-page-192892225.firebaseapp.com/
United States	2022-09-28	2620:0:890::100	xxxxs://meta-business-page-192689926.web.app/
United States	2022-09-28	199.36.158.100	xxxxs://meta-business-page-192689926.firebaseapp.com/
United States	2022-09-28	2620:0:890::100	xxxxs://meta-business-page-129869812.firebaseapp.com/
United States	2022-09-28	199.36.158.100	xxxxs://meta-business-appeal-19787675.web.app/
United States	2022-09-28	2620:0:890::100	xxxxs://meta-business-appeal-19787675.firebaseapp.com/
United States	2022-09-28	2620:0:890::100	xxxxs://meta-business-page-129869812.web.app/%22%7D
United States	2022-09-28	199.36.158.100	xxxxs://meta-business-page-129869812.web.app/
United States	2022-09-28	2620:0:890::100	xxxx://meta-business-page-129869812.firebaseapp.com/
United States	2022-09-28	2620:0:890::100	xxxx://meta-business-appeal-19787675.web.app/

Vietnam	2022-09-28	125.212.224.192	xxxx://astsesksrercovveryi-554542.click/
United States	2022-09-28	199.36.158.100	xxxxs://meta-business-apoeal-8291938.web.app
United States	2022-09-28	199.36.158.100	xxxxs://meta-business-apoeal-8291938.firebaseapp.com
United States	2022-09-28	2620:0:890::100	xxxxs://copyright-support-appeal901310.web.app/
United States	2022-09-28	199.36.158.100	xxxxs://copyright-support-appeal901310.firebaseapp.com/
United States	2022-09-28	199.36.158.100	xxxxs://copyright-support-appeal83394.web.app/
United States	2022-09-28	199.36.158.100	xxxxs://copyright-support-appeal83394.firebaseapp.com/
United States	2022-09-28	2620:0:890::100	xxxxs://copyright-support-appeal29381.web.app/
United States	2022-09-28	199.36.158.100	xxxxs://copyright-support-appeal29381.firebaseapp.com/
United States	2022-09-28	2620:0:890::100	xxxxs://copyright-support-appeal29302.web.app/
United States	2022-09-28	2620:0:890::100	xxxxs://copyright-support-appeal29302.firebaseapp.com/
United States	2022-09-28	2620:0:890::100	xxxxs://copyright-support-appeal29283.web.app/
United States	2022-09-28	2620:0:890::100	xxxxs://copyright-support-appeal29283.firebaseapp.com/
United States	2022-09-28	199.36.158.100	xxxxs://copyright-support-appeal192038.web.app/
United States	2022-09-28	199.36.158.100	xxxxs://copyright-support-appeal192038.firebaseapp.com/
United States	2022-09-28	199.36.158.100	xxxxs://copyright-support-appeal10293.web.app/
United States	2022-09-28	199.36.158.100	xxxxs://copyright-support-appeal10293.firebaseapp.com/
United States	2022-09-28	199.36.158.100	xxxxs://meta-business-apoeal-8291938.web.app/
United States	2022-09-28	199.36.158.100	xxxxs://meta-business-apoeal-8291938.firebaseapp.com/

b. Instagram

PAIS DE PROCEDENCIA	FECHA	IP	URL
United States	2022-09-28	172.67.217.127	xxxxs://loginst0-id.greenlink.my.id/logins.php
United States	2022-09-28	104.21.70.7	xxxxs://loginst0-id.greenlink.my.id/
Desconocido	2022-09-28	2606:50c0:8002::153	xxxxs://thanosdadeepweb.github.io/instadothanos
United States	2022-09-28	185.199.110.153	xxxxs://thanosdadeepweb.github.io/instadothanos/

c. Google

PAIS DE PROCEDENCIA	FECHA	IP	URL
Desconocido	2022-09-28	45.148.116.57	xxxxs://netflix-support-fr.info/

d. Netflix

PAIS DE PROCEDENCIA	FECHA	IP	URL
United States	2022-09-28	104.21.72.167	xxxx://www.dfgoidfgfd7dfg.shop/
United States	2022-09-28	185.199.109.153	xxxxs://orkube.github.io/Netflix-bootstrap/
United States	2022-09-28	76.76.21.98	xxxx://netflix.visakhsr.com/
United States	2022-09-28	107.21.131.38	xxxx://caresure.duckdns.org/50285433069b9faf53c900cd2642fa9d
Desconocido	2022-09-28	163.123.142.135	xxxx://updatepayment.anondns.net/937ea3f7714dc0d01475da7bff33b596
Desconocido	2022-09-28	163.123.142.135	xxxx://updatepayment.anondns.net/7c792a8279211dece3b4df04719c818a
Desconocido	2022-09-28	163.123.142.135	xxxx://updatepayment.anondns.net/5523d651bfb642be33057a3b78d02c9e
Desconocido	2022-09-28	163.123.142.135	xxxx://updatepayment.anondns.net/937ea3f7714dc0d01475da7bff33b596/
Desconocido	2022-09-28	163.123.142.135	xxxx://updatepayment.anondns.net/7c792a8279211dece3b4df04719c818a/
Desconocido	2022-09-28	163.123.142.135	xxxx://updatepayment.anondns.net/5523d651bfb642be33057a3b78d02c9e/
United States	2022-09-28	185.199.109.153	xxxxs://ajaymadhavan14.github.io/Netflix-clone

e. Outlook

PAIS DE PROCEDENCIA	FECHA	IP	URL
United States	2022-09-28	162.244.81.35	xxxxs://siasky.net/AAB47UZGKna37kA-kcyOZW7Go7kmhElOX2_ABMTsGHLICA
Ukraine	2022-09-28	89.184.89.137	xxxxs://shop.starpom.com.ua/wp-content/fonts/css/modules.html

f. Microsoft Login

PAIS DE PROCEDENCIA	FECHA	IP	URL
United States	2022-09-28	104.18.7.145	xxxxs://storageapi.fleek.co/acf60efc-1273-4d1a-97e1-744aa07ef8bf-bucket/003888899.html
United States	2022-09-28	2604:1380:4641:6104:5000:5dff:fe88:c725	xxxxs://s6k7q-liaaa-aaaad-qd6ha-cai.raw.ic0.app/
Netherlands	2022-09-28	139.178.83.202	xxxxs://qewxm-vyaaa-aaaad-qd6ia-cai.raw.ic0.app/
Brazil	2022-09-28	159.138.208.202	xxxxs://f0w3e498ifr0k-0fdlk-3rje4kf-gjkwre-jgv-wr09jv-9rejc.obs.sa-brazil-1.myhuaweicloud.com:443/kve9o04r5-tgkl-erlfg-ew0kr5g-4rjkflefd-ekf-0klef.html?AWSAccessKeyId=Y33AQWKH1XTGWG0XAF5T&Expires=1666467209&Signature=usBPzNrY9xw453v6IQnbynhFlAA%3D#jjones@nesf.com
Desconocido	2022-09-28	103.153.183.146	xxxxs://puadre.info/not
United States	2022-09-28	104.18.6.145	xxxxs://storageapi.fleek.co/e61eeede-3cd0-4c0c-a107-08833c0ec841-bucket/swclassics776372.html
United States	2022-09-	2606:4700::681	xxxxs://storageapi.fleek.co/2e59aa00-2800-4a3a-9109-

	28	2:791	8c82ee58664d-bucket/uyt/Personal.html
United States	2022-09-28	104.18.7.145	xxxxs://storageapi.fleek.co/2e59aa00-2800-4a3a-9109-8c82ee58664d-bucket/ho/Personal.html
United States	2022-09-28	162.244.80.76	xxxxs://siasky.net/PAAwdxJ--Av5SYmeYrAyW-PwO309dcOIixa4uS4SQJ2rYA
Desconocido	2022-09-28	103.153.183.146	xxxxs://puadre.info/not/
France	2022-09-28	51.195.62.12	xxxxs://fibromyalgiaservices.co.uk/invoice_po7564/PDFfiles/accessms/index.html
United States	2022-09-28	162.241.127.62	xxxxs://evplugpower.com/wp-error/of/realm_xxx.html
United States	2022-09-28	162.241.127.62	xxxxs://alaskariverdomes.com/mssl/
Australia	2022-09-28	110.238.127.235	xxxxs://0uj-yt08ty0-ghj-0j0gtycytyt-sdy-by9u-bb-nun-u9u.obs.ap-southeast-2.myhuaweicloud.com/l-ge305rg3e5r-gi-rflkw-rekfg-wejkr5tg9kjr-0fjkg-refkjf.htm
South Africa	2022-09-28	154.0.164.93	xxxx://fencandgate.co.za/office
United States	2022-09-28	2604:1380:4641:6104:5000:5dff:fe88:c725	xxxxs://frbnu-riaaa-aaaad-qd53a-cai.raw.ic0.app
Netherlands	2022-09-28	139.178.83.202	xxxxs://eoj6d-sqaaa-aaaad-qd57q-cai.raw.ic0.app
Australia	2022-09-28	110.238.127.235	xxxxs://0uj-yt08ty0-ghj-0j0gtycytyt-sdy-by9u-bb-nun-u9u.obs.ap-southeast-2.myhuaweicloud.com:443/l-ge305rg3e5r-gi-rflkw-rekfg-wejkr5tg9kjr-0fjkg-refkjf.htm?AWSAccessKeyId=Y33AQWKH1XTGWG0XAF5T&Expires=1666807620&Signature=Mp2WXGOXqDM88pNNxVBw3rKtjvI%3D#accounts@centrica.com
United States	2022-09-28	2604:1380:4641:6103:5000:fdff:feb3:2faf	xxxxs://frbnu-riaaa-aaaad-qd53a-cai.raw.ic0.app/
United States	2022-09-28	2604:1380:4641:6103:5000:fdff:feb3:2faf	xxxxs://eoj6d-sqaaa-aaaad-qd57q-cai.raw.ic0.app/
Australia	2022-09-28	110.238.127.235	xxxxs://v3e0rpohgjv-0wrjh-vjwmr-vj-ewrhnvb-0wnhsd-vcnr-v.obs.ap-southeast-2.myhuaweicloud.com/8ih0-be0-rbgv0-wb0-vgf4bw0-bvf0-wbevc0-w84re0f.html

g. Office 365

PAIS DE PROCEDENCIA	FECHA	IP	URL
United States	2022-09-28	104.250.174.241	xxxxs://watchtoearn.sa.com/office365/office
United States	2022-09-28	104.250.174.241	xxxxs://watchtoearn.sa.com/office365/office/

2. Recomendaciones:

   a. Evitar ingresar datos personales a enlaces de dudosa procedencia.
   b. Mantener los equipos protegidos, con el software actualizado.

Fuentes de información	▪ Comandancia de Ciberdefensa de la Marina, Osint

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 265	Fecha: 28-09-2022
		Página 12 de 15

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Smishing o fraude por mensaje de texto simulando ser la entidad legitima del Registro Nacional de Identificación y Estado Civil (RENIEC)		
Tipo de ataque	Suplantación	Abreviatura	Suplantación
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 una campaña de Smishing que consiste en él envió de un mensaje de texto (SMS/MMS), simulando ser la entidad legitima del Registro Nacional de Identificación y Estado Civil (RENIEC), donde advierte a la víctima, sobre una supuesta ***"NOTIFICACIÓN INFORMATIVA"***, adjunto un enlace que contiene un archivo APK, con el objetivo infectar el dispositivo móvil y robar información confidencial.

   - Proceso del ataque Smishing:

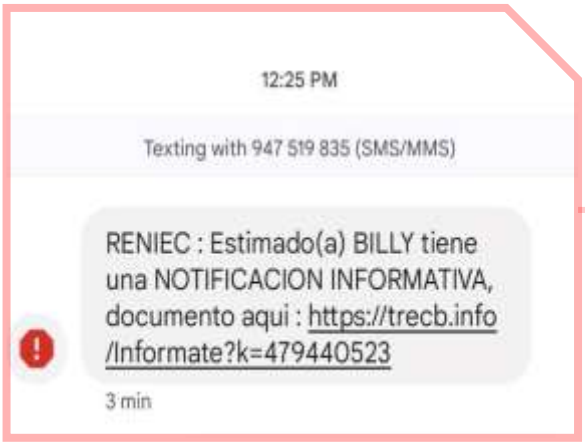


Imagen 1: Mensaje de texto enviado desde el número de teléfono 947519835 simula ser la entidad de RENIEC, advierte a la persona de ***"BILLY"*** que tiene una ***"NOTIFICACIÓN INFORMATIVA",*** adjunto un enlace que, al hacer clic, descarga un archivo APK.

2. Como parte de la simulación se realizó el análisis del archivo APK en las diferentes plataformas virtuales de seguridad digital, obteniendo como resultado **MALICIOSO:**

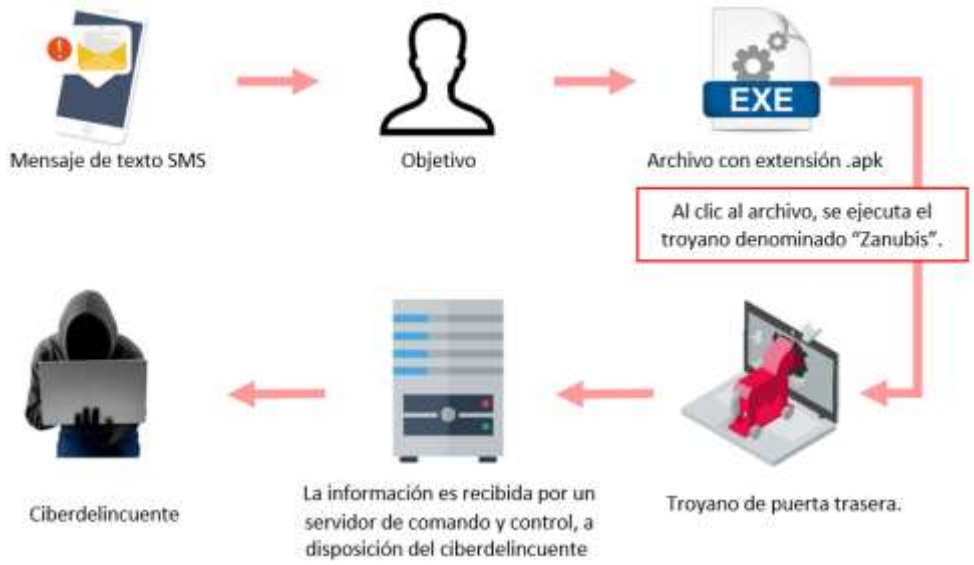
   - Indicadores de compromisos:

     - **MD5:** 70290209773e431af4a0b05d3f30577e
     - **SHA-256:** c34a3aef4e1ac60244c899e83e343fcb49c1646c38ca42b9a53bf3009bd814b3
     - **Tipo de archivo:** Android
     - **Tamaño del archivo:** 3,97 MB (4160722 bytes)
     - **Nombre del paquete:** informacion_d3b93d9.pdf.apk

Observación: Se detecta que el archivo APK, contiene Malware, uno de ellos conocido como Zanubis es un software malicioso clasificada como un troyano bancario. Este malware se dirige a los sistemas operativos (SO) de Android. La función principal de este programa es obtener sigilosamente las credenciales de la cuenta bancaria en línea y obtener acceso remoto a los fondos almacenados en ella. Zanubis apunta a los bancos latinoamericanos, en particular a los que tienen sede en Perú.

- Permisos solicitados:
  - Escribir contactos
  - Enviar SMS
  - Permite que una aplicación reciba mensajes push WAP
  - Escribir almacenamiento externo
  - Recibir SMS
  - Leer almacenamiento externo
  - Llamada telefónica
  - Leer teléfono estado
  - Leer SMS
  - Recibir MMS
  - Leer contacto
  - Otros.

3. Proceso de infección:



4. Referencia:

El smishing es una técnica que consiste en el envío de un SMS por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima, red social, banco, institución pública, etc. con el objetivo de robar información personal y/o bancario. Generalmente el mensaje contiene una URL, la cual redirige a un sitio web malicioso o descarga de un Malware.

5. Recomendaciones:

- Eliminar cualquier archivo que se haya descargado desde el SMS o un enlace adjunto en el mensaje.
- Cambiar contraseñas de las cuentas implicadas, que hayan podido ser vulneradas.
- Activar la verificación en dos pasos en las cuentas para evitar la suplantación de identidad.
- Evitar responder a mensajes enviados desde (correo electrónico, Whatsapp, SMS y otros), que contengan enlaces de dudosa procedencia.
- Verificar detenidamente la redacción y ortografía de la dirección URL, que coincidan con el sitio web oficial.
- Utilizar una firma de antivirus actualizado, ya que es la primera barrera ante posibles ataques cibernéticos.

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

Índice alfabético