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, 20 de octubre de 2022

N° 285-2022-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° 285	Fecha: 20-10-2022
		Página 04 de 10

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Malware en aplicaciones Android con más de 20 millones de descargas		
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

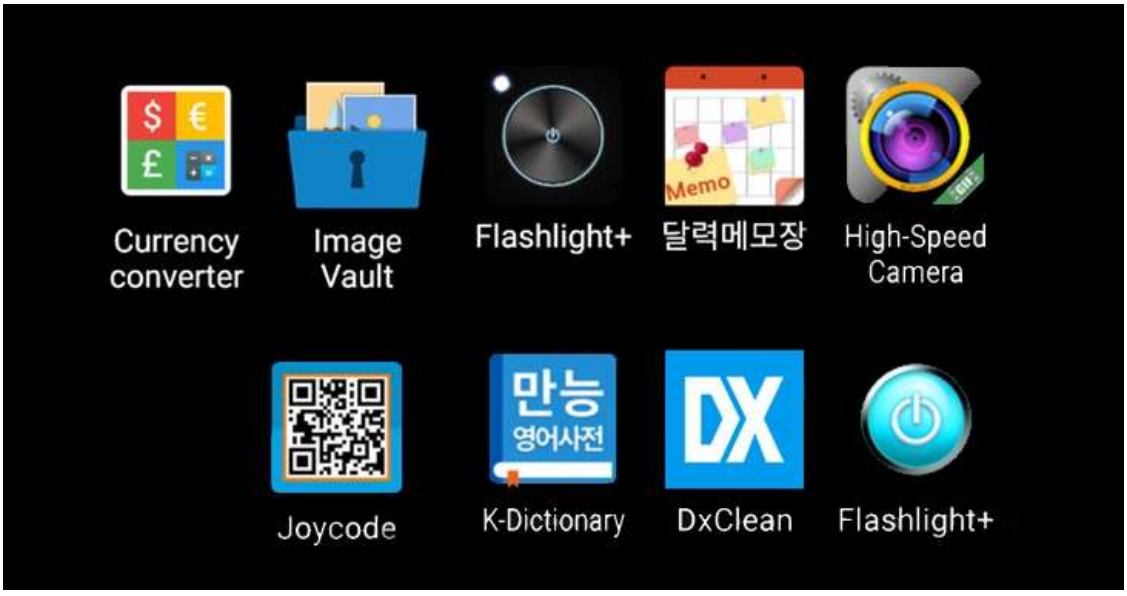
En una reciente investigación realizada por McAfee, se identificaron 16 aplicaciones con más de 20 millones de descargas en Google Play Store.

ANTECEDENTES:

- Clicker es un malware de tipo troyano, cuyo objetivo es el fraude publicitario. Estos "clickers" se conectan continuamente a sitios web, lo que otorga a los actores de amenazas ingresos en base a un pago por clic.
- Hace dos meses, McAfee descubrió una docena de aplicaciones de adware de Android distribuidas en Google Play Store, que albergaban una cepa de malware llamada “HiddenAds”, la cual se ejecutaba automáticamente sin ninguna interacción del usuario.

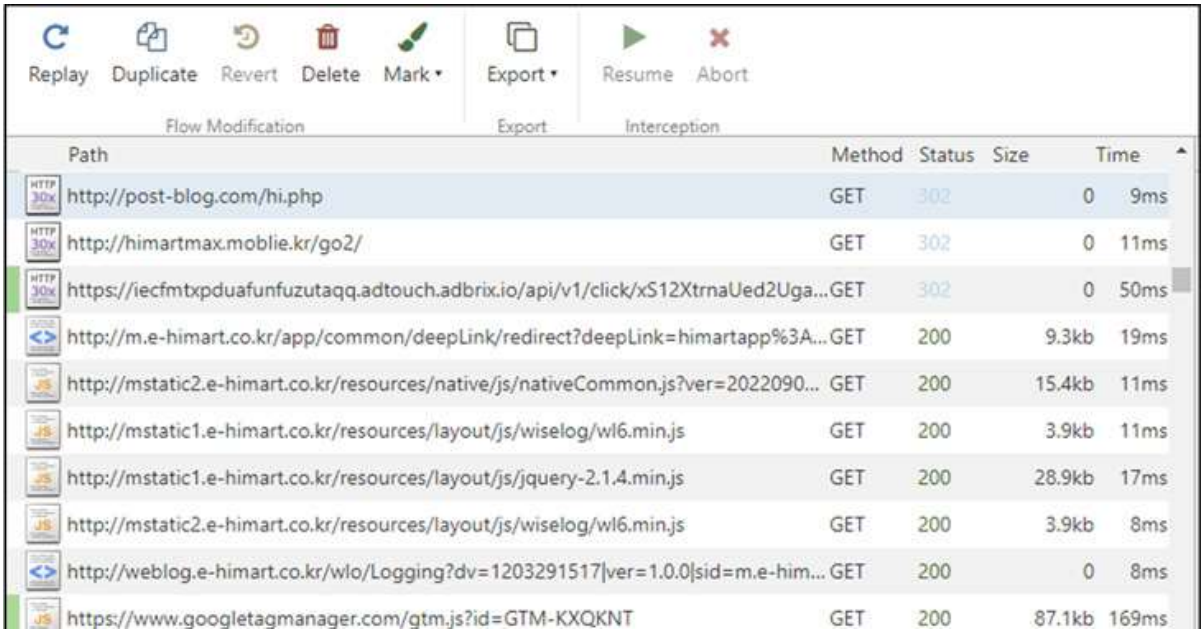
DETALLES:

- En un aviso de seguridad publicado por McAfee, se detalla el descubrimiento de 16 nuevas aplicaciones asociadas al malware “Clicker”, que se encontraban disponibles bajo la apariencia de utilidades de cámara, convertidores, aplicaciones de notas, diccionarios, lectores de códigos QR, entre otros. Se descubrieron más de 20 millones de descargas acumuladas en Google Play Store.



- La aplicación Clicker, una vez instalada y lanzada, desata su funcionalidad fraudulenta que permite que el malware visite de forma encubierta sitios web falsos y simule clics en anuncios sin el conocimiento de las víctimas. Según los investigadores, esto puede causar tráfico pesado en la red y consumir energía sin que el usuario sea consciente que genera ganancias para el actor de amenazas al tener este malware en su dispositivo móvil.

- Para ocultar aún más su verdadero objetivo, la aplicación tiene en cuenta el tiempo de instalación de la aplicación para que la actividad sospechosa no se active dentro de la primera hora de la descarga de la aplicación. Además, incorpora un retraso aleatorio en el medio para permanecer bajo el radar.



- Los investigadores catalogaron esta actividad como "fraude publicitario en móviles", dado que estas aplicaciones se distribuían como una publicidad atractiva para engañar a usuarios Android. A continuación, se detalla la lista de aplicaciones maliciosas:

Nombre del paquete	Nombre de la aplicación	Cantidad de descargas
com[.]hantor[.]CozyCamera	High-Speed Camera	10,000,000+
com[.]james[.]SmartTaskManager	Smart Task Manager	5,000,000+
kr[.]caramel[.]flash_plus	Flashlight+	1,000,000+
com[.]smh[.]memocalendar	달력메모장	1,000,000+
com[.]joysoft[.]wordBook	K-Dictionary	1,000,000+
com[.]kmshack[.]BusanBus	BusanBus	1,000,000+
com[.]candlencom[.]candleprotest	Flashlight+	500,000+
com[.]movinapp[.]quicknote	Quick Note	500,000+
com[.]smartwho[.]SmartCurrencyConverter	Currency Converter	500,000+
com[.]joysoft[.]barcode	Joycode	100,000+
com[.]joysoft[.]ezdica	EzDica	100,000+
com[.]schedulezero[.]instapp	Instagram Profile Downloader	100,000+
com[.]meek[.]tingboard	Ez Notes	100,000+
com[.]candlencom[.]flashlite	손전등	1,000+
com[.]doubleline[.]calcul	계산기	100+
com[.]dev[.]imagevault	Flashlight+	100+

- En la investigación también se comparten los siguientes IoCs:
    - liveposting[.]net
    - sideup[.]co[.]kr

- msideup[.]co[.]kr
- post-blog[.]com
- pangclick[.]com
- modooalba[.]net

- Finalmente, los investigadores de seguridad de McAfee notificaron a Google, por lo que las aplicaciones identificadas ya no se encuentran disponibles en Google Play.

RECOMENDACIONES:

- Eliminar inmediatamente las aplicaciones de la lista en caso las tuviese descargadas.
- Contar con una aplicación de antivirus.
- Revisar las reseñas de las aplicaciones antes de descargarlas.

Fuentes de información	▪ hxxps://www.mcafee.com/blogs/other-blogs/mcafee-labs/new-malicious-clicker-found-in-apps-installed-by-20m-users/ ▪ hxxps://thehackernews.com/2022/10/these-16-clicker-malware-infected.html ▪ Análisis propio de fuentes abiertas.

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 285	**Fecha: 20-10-2022**
		Página 07 de 10

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Campaña de phishing que tiene como objetivo robar credenciales de acceso de cuentas de Yahoo!		
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 actores de amenazas vienen llevando a cabo una campaña de phishing "tipo de robo de identidad en línea", que utilizando correos electrónicos falsos afirma ser enviado por la empresa "Yahoo!" para atraer la atención de la víctima, en el texto del mensaje se advierte que se ha detectado una actividad de acceso inusual, por lo que será cancelada a menos que se ingrese en el enlace que se adjunta, con el objetivo robar los datos personales (la contraseña de la cuenta).

2. Proceso del ataque phishing:

Imagen 1: Mensaje de correo electrónico enviado supuestamente de "Yahoo!" incita a la víctima, hacer << Click para continuar>>.

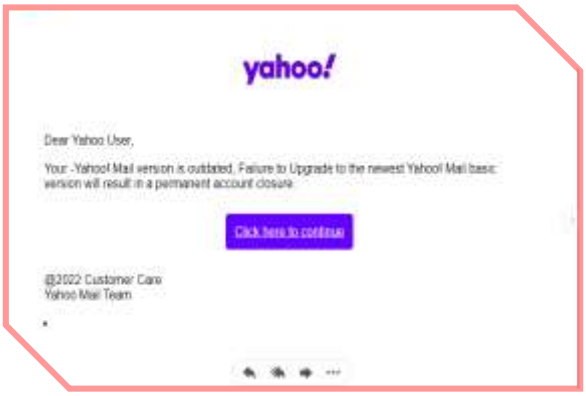
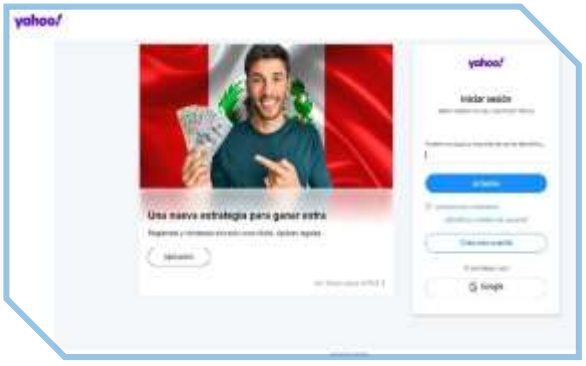


Imagen 2: Engaño, solicitud para ingresar nombre de usuario, correo electrónico o móvil.

Imagen 3: Solicitud para ingresar la contraseña.

Imagen 4: Que, al ingresar la contraseña, es redirigido al sitio oficial de Yahoo! aludiendo un aparente error; sin embargo, los datos fueron capturados por los ciberdelincuentes.



3. Comparación de sitio oficial y sitio falso:

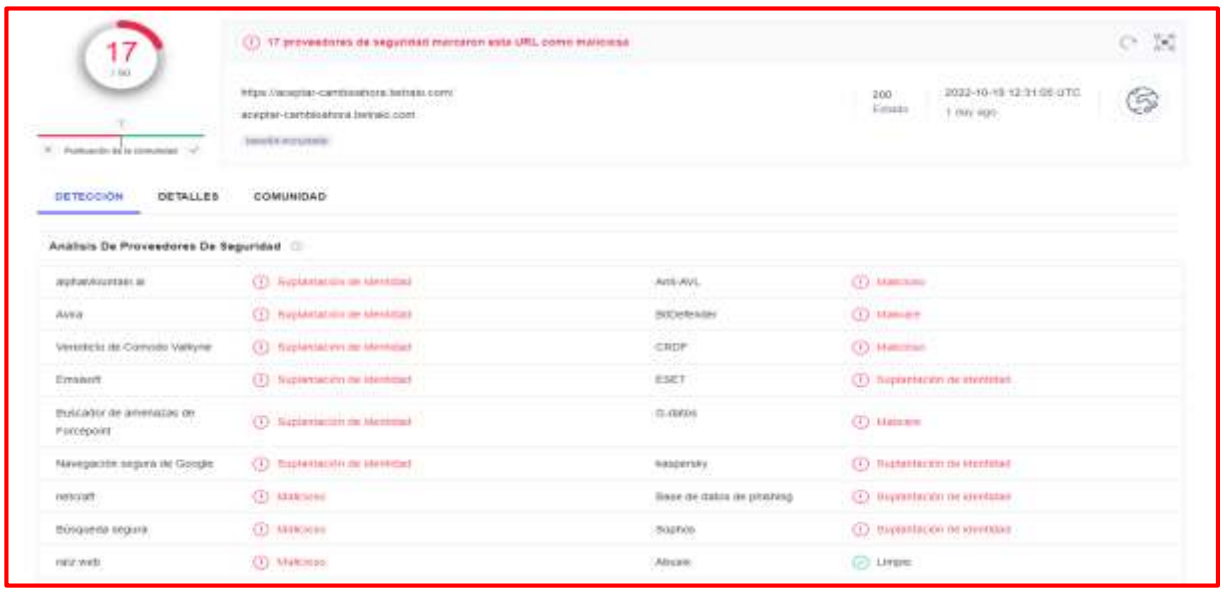
SITIO OFICIAL
URL: https://login.yahoo.com/

SITIO FRAUDULENTO
URL: hxxps://accept-changenow[.]betraio[.]com/

- Existe similitud en imagen de fondo, color y escritura.
- Tiene certificado de seguridad de protocolo HTTPS.
- El dominio se hace pasar por el sitio oficial, pero no coincide.

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

- **URL:** hxxps[:]//accept-changenow[.]betraio[.]com/
- **Dominio:** accept-changenow[.]betraio[.]com
- **Direcciones IP:** 162[.]241[.]60[.]218
- **Código De Estado:** 200
- **Tamaño:** 16.69 KB
- **SHA-256:** eb59f0ad0830031efaf3a107548de6cbd9ed5f226c3a895555389ceacf7e463d



5. **Otras detecciones del análisis**:

6. **Recomendaciones:**

- Acceder al sitio web a través de fuentes oficiales
- 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.
- Evitar proporcionar información personal y/o financiera a través de sitios webs de dudosa procedencia.
- 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