| | | | |
|---|---|---|---|
| Nro. Alerta: | EC-2022-072 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS<br>**ALERTAS DE SEGURIDAD** | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT |
| TLP: | TLP:BLANCO | | |
| Fecha: | 20-mayo-2022 | Apps para dispositivos móviles infectadas con malware FACESTEALER | V 1.1 |

## I. DATOS GENERALES:

**Clase de alerta:** Malware
**Tipo de incidente:** Sistema infectado
**Nivel de riesgo:** Medio

## II. ALERTA

Se han identificado varias aplicaciones en la tienda de apps de Google (Google Play) cuyo objetivo es realizar actividades de tipo maliciosas, como robar las credenciales de usuarios e información confidencial como claves de acceso.

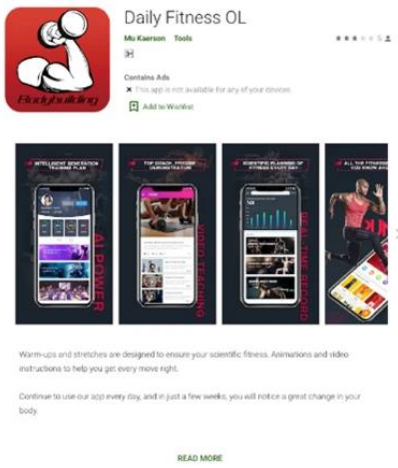


**Figura 1:** Ilustración app maliciosa
**Fuente:** Trend Micro

## III. INTRODUCCIÓN

La empresa de seguridad Trend Micro ha identificado varias aplicaciones que se distribuyen a través de Google Store que están infectadas con el malware "*Facestealer*", el cual obtiene clave de los usuarios para acceder a otras aplicaciones o servicios. Se han identificado aproximadamente 200 apps infectadas, las cuales ya han se han instalado en teléfonos móviles. A continuación se muestra los temas de las aplicaciones utilizadas por el malware "*Facestealer*":



**Dirección:** Av. 9 de Octubre N27-75 y Berlín
**Código Postal:** 170513 / Quito - Ecuador
**Teléfono:** 593-2 2946 400 - www.arcotel.gob.ec

Gobierno del Encuentro | Juntos lo logramos

| | | | |
|---|---|---|---|
| Nro. Alerta: | EC-2022-072 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS<br>**ALERTAS DE SEGURIDAD** | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT |
| TLP: | TLP:BLANCO | | |
| Fecha: | 20-mayo-2022 | Apps para dispositivos móviles infectadas con malware FACESTEALER | V 1.1 |

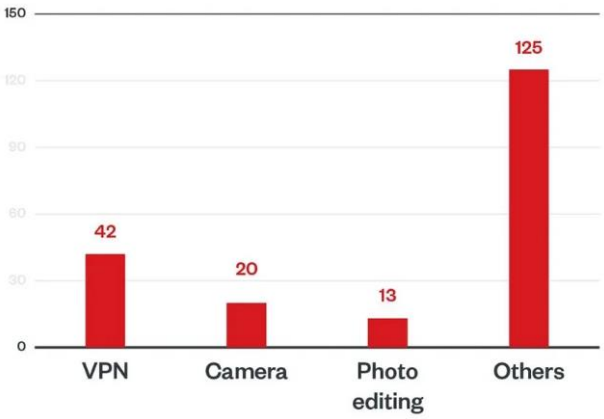


**Figura 2:** Ilustración app maliciosa
**Fuente:** Trend Micro

Una de las aplicaciones llamada Daily Fitness OL, aparentemente era un aplicación de tipo fitness, con ejercicios y demostraciones en video, pero fue diseñada para robar credenciales de Facebook de usuarios.

Cuando se inicia la aplicación, se envía una solicitud al usuario para que inicie sesión en Facebook, y una vez que el usuario inicia sesión, la aplicación inicia una WebView (un navegador integrable) para cargar una URL, por ejemplo, hxxps://touch[.]facebook[.]com/home[.]php?sk=h_nor. Posteriormente, se inyecta un fragmento de código JavaScript en la página web cargada para robar las credenciales ingresadas por el usuario.

Después de que el usuario inicia sesión en su cuenta, la aplicación recopilaba la cookie, la aplicación cifra toda la información de identificación personal (PII) y la envía a un servidor remoto ubicado en Rusia. La clave de cifrado y la dirección del servidor remoto se obtienen de la configuración descargada.

Con el malware Facestealer, además de las credenciales de Facebook, obtiene fotografías, direcciones físicas y también datos bancarios que estén asociados.

Otras de las aplicaciones maliciosas identificadas son:


Dirección: Av. 9 de Octubre N27-75 y Berlín
Código Postal: 170513 / Quito - Ecuador
Teléfono: 593-2 2946 400 - www.arcotel.gob.ec
Gobierno del Encuentro Juntos lo logramos

| | | | |
|---|---|---|---|
| Nro. Alerta: | EC-2022-072 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS<br>**ALERTAS DE SEGURIDAD** | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT |
| TLP: | TLP:BLANCO | | |
| Fecha: | 20-mayo-2022 | Apps para dispositivos móviles infectadas con malware FACESTEALER | V 1.1 |

Enjoy Photo Editor

Panorama Camera

Photo Gaming Puzzle

Swarm Photo

Business Meta Manager

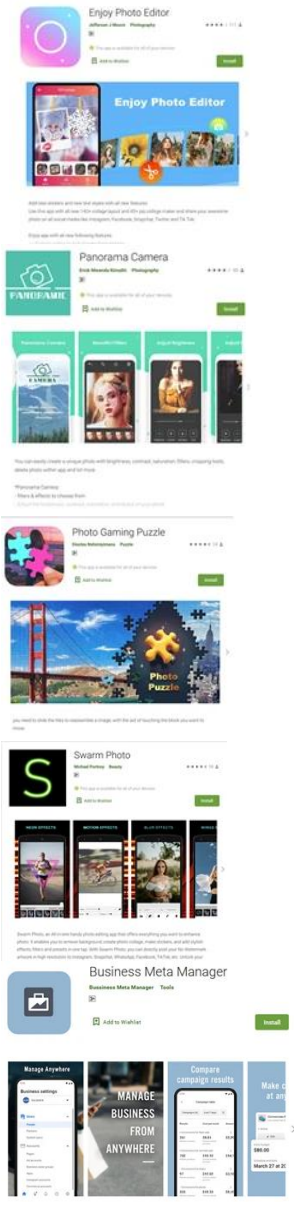


**Figura 3:** Ilustración aplicaciones maliciosas
**Fuente:** Trend Micro

| | | | |
|---|---|---|---|
| Nro. Alerta: | EC-2022-072 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS<br>**ALERTAS DE SEGURIDAD** | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT |
| TLP: | TLP:BLANCO | | |
| Fecha: | 20-mayo-2022 | Apps para dispositivos móviles infectadas con malware FACESTEALER | V 1.1 |

## IV. VECTOR DE ATAQUE: Aplicaciones móviles infectadas

## V. IMPACTO:

El malware "*Facestealer*" afecta a la confidencialidad de los datos de los usuarios que han instalado las aplicaciones infectadas, ya que roba credenciales e información personal para mandarlos a un servidor remoto.

## VI. INDICADORES DE COMPROMISO:

En la siguiente tabla, se indican los IOC asociados:

| SHA-256 | Nombre del paquete | Nombre de detección | Conteo de descargas antes de ser eliminado |
|---|---|---|---|
| 7ea4757b71680797cbce66a8ec922484fc25f87814cc4f811e70ceb723bfd0fc | com.olfitness.android | AndroidOS_FaceStealer.HRXH | 10,000+ |
| b7fe6ec868fedaf37791cf7f1fc1656b4df7cd511b634850b890b333a9b81b9d | com.editor.xinphoto | AndroidOS_FaceStealer.HRXF | 100,000+ |
| 40580a84b5c1b0526973f12d84e46018ea4889978a19fcdcde947de5b2033cff | com.sensitivity.swarmphoto | AndroidOS_FaceStealer.HRXE | 10,000+ |
| 6ccd0c0302cda02566301ae51f8da4935c02664169ad0ead4ee07fa6b2f99112 | com.meta.adsformeta3 | AndroidOS_FaceStealer.HRXG | 100+ |
| 4464b2de7b877c9ff0e4c904e9256b302c9bd74abc5c8dacb6e4469498c64691 | com.photo.panoramacamera | AndroidOS_FaceStealer.HRXF | 50,000+ |
| 3325488a8df69a92be92eb11bf01ab4c9b612c5307d615e72c07a4d859675e3f | com.photo.move | AndroidOS_FaceStealer.HRXF | 10,000+ |

**Tabla 1:** IOCs
**Fuente:** Trend Micro

| | | | |
|---|---|---|---|
| Nro. Alerta: | EC-2022-072 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS<br>**ALERTAS DE SEGURIDAD** | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT |
| TLP: | TLP:BLANCO | | |
| Fecha: | 20-mayo-2022 | Apps para dispositivos móviles infectadas con malware FACESTEALER | V 1.1 |

## VII. RECOMENDACIONES:

El Centro de Respuestas a Incidentes Informáticos de ARCOTEL, EcuCERT, recomienda a su comunidad objetivo y a la ciudadanía lo siguiente:

- En caso de que tenga instalada alguna de las aplicaciones antes indicadas se recomienda su desinstalación inmediata.
- Se deben cambiar todas las contraseñas de las aplicaciones y servicios a los cuales accede a través del celular.
- Al instalar una aplicación debemos verificar a que información permitimos que la aplicación quiere acceder, por lo que no se debe habilitar todos los permisos que se solicitan.
- Antes de instalar una aplicación se debe revisar sus reseñas a fin de identificar si algún usuario ha visto comportamientos extraños en el funcionamiento de la app.
- Se deben descargar las aplicaciones de sitios oficiales a fin de reducir las posibilidades de ser víctimas de aplicaciones con código malicioso.

## VIII. DESCARGO DE RESPONSABILIDAD

- La información en esta alerta es con fines informativos. El Centro de Respuestas de ARCOTEL, EcuCERT, no respalda ningún producto o servicio comercial, incluidos aquellos sujetos de análisis.
- Cualquier referencia a productos, procesos o servicios comerciales específicos por marca de servicio, marca comercial, fabricante, no constituye ni implica respaldo, recomendación o favorecimiento por parte de EcuCERT.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

## IX. REFERENCIAS:


- *Fake Mobile Apps Steal Facebook Credentials, Cryptocurrency-Related Keys*. (2022, 16 mayo). Trend Micro. Recuperado 18 de mayo de 2022, de https://www.trendmicro.com/en_us/research/22/e/fake-mobile-apps-steal-facebook-credentials--crypto-related-keys.html.

- De la Calle, R. (2022, 17 mayo). *Más de 200 aplicaciones en Android están robando las contraseñas*. MovilZona. Recuperado 18 de mayo de 2022, de




Dirección: Av. 9 de Octubre N27-75 y Berlín
Código Postal: 170513 / Quito - Ecuador
Teléfono: 593-2 2946 400 - www.arcotel.gob.ec

Gobierno del Encuentro Juntos lo logramos

| | | | |
|---|---|---|---|
| Nro. Alerta: | EC-2022-072 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS<br>**ALERTAS DE SEGURIDAD** | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT |
| TLP: | TLP:BLANCO | | |
| Fecha: | 20-mayo-2022 | Apps para dispositivos móviles infectadas con malware FACESTEALER | V 1.1 |

https://www.movilzona.es/noticias/problemas/200-aplicaciones-android-roban-contrasenas/.

- Alcántara, B. (s. f.). *Detectan 200 aplicaciones maliciosas que pueden robar tus credenciales de Facebook*. Andro4all. Recuperado 18 de mayo de 2022, de https://andro4all.com/google-play/detectan-200-aplicaciones-maliciosas-que-pueden-robar-tus-credenciales-de-facebook.



**Dirección:** Av. 9 de Octubre N27-75 y Berlín
**Código Postal:** 170513 / Quito - Ecuador
**Teléfono:** 593-2 2946 400 - www.arcotel.gob.ec

Gobierno del Encuentro | Juntos lo logramos