Nro. Alerta:	EC-2021-037	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DE LA AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES EcuCERT **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	29-dic-2021	Troyano bancario para Android	V 1.0

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad

Tipo de incidente: Sistemas y/o software Abierto

Nivel de riesgo: Alto

II. ALERTA

Un troyano bancario intenta realizar transacciones fraudulentas sin el conocimiento de los clientes de una entidad financiera de Brasil. Aunque en Ecuador no se han registrado casos similares, es oportuno conocer el modo de operación de este malware; para concientizar a la comunidad sobre el uso adecuado de dispositivos electrónicos.

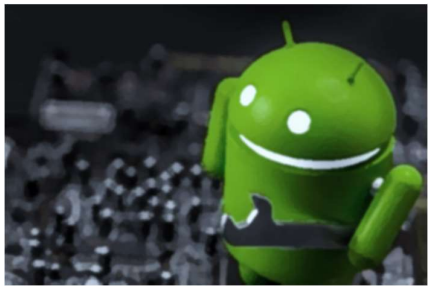

Figura No. 1: Ilustraciones relacionadas a un troyano bancario
Fuente: Cyclonis

III. INTRODUCCIÓN

Con el objetivo de recaudar dinero de una entidad financiera, los ciberdelincuentes configuraron una página web similar a la tienda de aplicaciones Play Store de Google; a través de dicha página, los ciberatacantes buscan que los usuarios instalen una aplicación falsa, muy similar a la original.

Una vez que el usuario se encuentra en la página web falsa, se le solicita al usuario que descargue una APK (Android Application Pack), el cual puede instalarse únicamente en Android.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2021-037	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DE LA AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES EcuCERT **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	29-dic-2021	Troyano bancario para Android	V 1.0

Una vez finalizada la instalación, se solicita al usuario que habilite el s*ervicio de accesibilidad*[1], entre otros. Un punto importante a destacar de este troyano es que la aplicación solicita acceso al *Servicio de accesibilidad* mostrando una superposición de WebView tomada de otras familias de malware.

Una vez que se ejecuta la aplicación falsa, está intentará abrir la aplicación real del Banco Itau Unibanco, y utilizará la aplicación oficial para realizar transacciones fraudulentas cambiando los campos de entrada del usuario y accediendo así a los datos de inicio de sesión.

IV. VECTOR DE ATAQUE:

Las aplicaciones maliciosas son un vector de ataque utilizado por los ciberdelincuentes para obtener el control de dispositivos móviles. Así mismo, los atacantes están dejando de lado la superposición de HTML optando por el desarrollo de aplicaciones propias.

V. IMPACTO:

Ante la presencia de este troyano, la confidencialidad de información es notablemente afectada.

VI. RECOMENDACIONES:

El Centro de Respuestas a Incidentes Informáticos de la ARCOTEL, EcuCERT, recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- Descargar aplicaciones móviles de sitios confiables.
- Actualizar las aplicaciones periódicamente.
- En el caso en el que se proceda a instalar un APK, se deberá examinar las solicitudes de instalación que se realizan.
- Se debe prestar mucha atención al abrir enlaces que se transmiten vía correo electrónico o SMS.
- A pesar de que este caso ocurre en otros países, se sugiere a los usuarios prestar atención al modo de operación de este ataque, a fin de conocer sobre este tipo de estafas y que debemos hacer para evitarlas.

[1] **Accessibilty Service:** Interfaz para operaciones rutinarias en el dispositivo Android, que tiene funciones para realizar casi cualquier tarea.

Nro. Alerta:	EC-2021-037	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DE LA AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES EcuCERT **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	29-dic-2021	Troyano bancario para Android	V 1.0

VII. REFERENCIAS:

- Cyclonis. (s.f.). Cyclonis. Obtenido de Cyclonis: https://www.cyclonis.com/es/el-troyano-hydra-para-android-persigue-a-los-clientes-de-commerzbank/
- Latam, C. (28 de 12 de 2021). ciberseguridadlatam. Obtenido de ciberseguridadlatam: https://www.ciberseguridadlatam.com/2021/12/28/un-troyano-bancario-para-android-se-propaga-a-traves-de-una-pagina-falsa-de-google-play-store/
- MITRE. (14 de 10 de 2019). Mitre ATT&ACK. Obtenido de Mitre ATT&ACK: https://attack.mitre.org/techniques/T1475/
- NewsEuro. (25 de 12 de 2021). NewsEuro. Obtenido de NewsEuro: https://news.eseuro.com/technology/55654.html
- Radar, T. (27 de 12 de 2021). Techradar. Obtenido de Techradar: https://global.techradar.com/es-es/news/este-peligroso-troyano-para-android-se-hace-pasar-por-una-pagina-de-google-play-store

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec