	EC-2022-045	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	08-marzo-2022	**Troyano Bancario para Android**	V 1.1

I. DATOS GENERALES:

Clase de alerta: Código Malicioso
Tipo de incidente: Malware
Nivel de riesgo: Alta

II. ALERTA

Troyano SharkBot es una aplicación móvil que se hace pasar por un antivirus; pero su objetivo principal, es realizar transferencias de dinero en el dispositivo de las víctimas; este malware se encontraba disponible en el repositorio oficial de aplicaciones Android.

Figura 1. Ilustración asociada a Troyano Bancario

III. INTRODUCCIÓN

SharkBot es un troyano bancario, detectado por primera vez en octubre del 2021. En semanas previas, este troyano se encontraba en Play Store disponible para su descarga y hoy en día; su APK[1] se encuentra disponible en ciertas páginas web.

[1] Android Application Package: Paquete de instalación que contiene los datos de una aplicación.

Play Store establece controles para las aplicaciones a ser descargadas; sin embargo, en ciertas ocasiones; determinadas aplicaciones escapan a dichos controles. En este caso, SharkBot eludió los controles de seguridad de Play Store y por un período de tiempo; estuvo disponible para su descarga, a través del nombre "**Antivirus, Super Cleaner**". En la siguiente gráfica se indica la imagen asociada a esta aplicación.

Figura 2. Ilustración asociada a Troyano Bancario SharkBot
Fuente: Propia

IV. VECTOR DE ATAQUE: Sistemas de Transferencia Automática

El objetivo de este malware es realizar transferencia de dinero a través de la técnica de Sistemas de Transferencia Automática[2] (ATS). La característica de ATS permite:

[2] Es una técnica empleada por el malware bancario y en lugar de reunir credenciales para su posterior uso/venta, se encargan directamente de iniciar automáticamente transferencias electrónicas desde el dispositivo de las víctimas.

- Recibir y simular una lista de eventos, entre ellos; simular la transferencia de dinero.
- Simular clics, pulsaciones de botones; permitiendo instalar otras aplicaciones maliciosas.

A continuación, se mencionan las funciones asociadas a SharkBot para robar credenciales bancarias en los dispositivos Android infectados.

INYECCIONES

Con el objetivo de robar credenciales de acceso, el malware SharkBot se vale del Phishing, abriendo un sitio web de inicio de sesión falso tan pronto como detecta que se abrió la aplicación bancaria oficial.

REGISTRO DE TECLAS

Para el robo de credenciales, SharkBot emplea el registro de eventos de accesibilidad y envía los registros al C2 correspondiente.

INTERCEPCIÓN DE SMS

Este Malware tiene la capacidad de interceptar/ocultar mensajes SMS.

CONTROL REMOTO

A través de los servicios de accesibilidad, este Malware obtiene el control remoto completo de un dispositivo Android.

Figura 3. Ilustración asociada a funciones de SharkBot
Fuente: Research NCCGROUP

Cabe señalar que, para que se cumplan dichas funcionalidades es necesario habilitar los "**Permisos y Servicios de Accesibilidad**" para que el malware intercepte todos los eventos de accesibilidad.

SharkBot emplea HTTP para comunicarse con el Servidor de Comando & Control (C2).

La información enviada y recibida se envía de una manera cifrada a través de RC4, se emplea una clave pública RSA la misma que se genera aleatoriamente; en la siguiente gráfica se observa el intercambio de mensajes entre el dispositivo infectado y el C2.

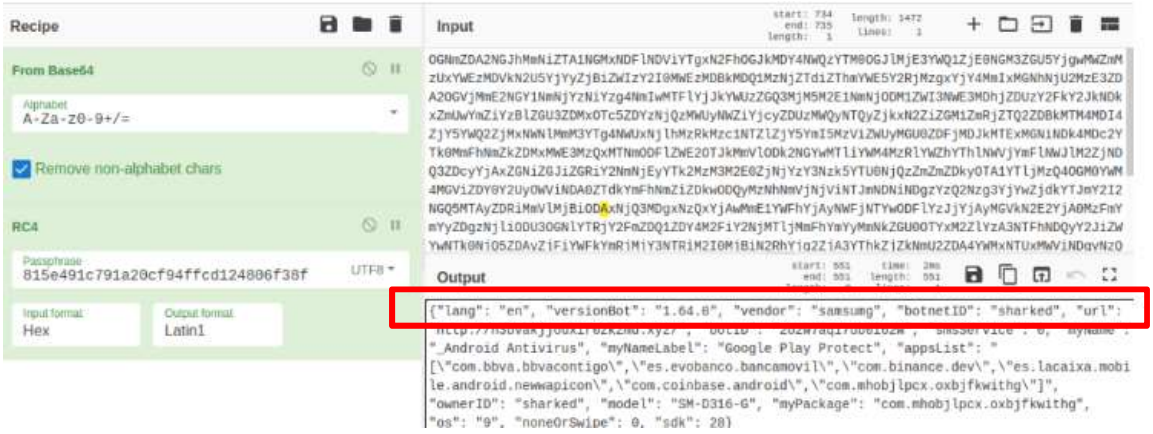


Figura 4. Ilustración asociada a la comunicación entre el dispositivo y el C2.
Fuente: Research NCCGROUP

SharkBot puede recibir diferentes comandos del servidor C2 para ejecutar diferentes acciones en el dispositivo infectado; en la siguiente gráfica se observan los comandos empleados:

	EC-2022-045	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	08-marzo-2022	**Troyano Bancario para Android**	V 1.1

```
String v9 = v2.getString("command");
switch(v9.hashCode()) {
    case -2081903487: {
        boolean v9_2 = v9.equals("smsSend");
        v9_1 = v9_2 ? 6 : -1;
        break;
    }
    case 0x8BD150FC: {
        v9_1 = v9.equals("updateLib") ? 15 : -1;
        break;
    }
    case -1949210555: {
        v9_1 = v9.equals("updateSQL") ? 11 : -1;
        break;
    }
    case 0x8FAEE23F: {
        v9_1 = v9.equals("stopAll") ? 1 : -1;
        break;
    }
    case -1403048597: {
        v9_1 = v9.equals("updateConfig") ? 14 : -1;
        break;
    }
    case 0xB42095DF: {
        v9_1 = v9.equals("uninstallApp") ? 9 : -1;
        break;
    }
    case -416707258: {
        v9_1 = v9.equals("changeSmsAdmin") ? 12 : -1;
        break;
    }
    case -75592340: {
        v9_1 = v9.equals("getDoze") ? 8 : -1;
        break;
    }
    case 0xB7F9F39: {
        v9_1 = v9.equals("sendInject") ? 13 : -1;
        break;
    }
```

Figura 5. Ilustración asociada comandos de SharkBot.
Fuente: Research NCCGROUP

	EC-2022-045	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	08-marzo-2022	**Troyano Bancario para Android**	V 1.1

En la siguiente tabla se describen el uso de los diferentes comandos.

Ítem	Comando	Descripción
1	smsSend	Utilizado para enviar un mensaje de texto al número de teléfono especificado por los TA.
2	updateLib	Se utiliza para solicitar que el malware descargue un nuevo archivo JAR desde la URL especificada, que debe contener una versión actualizada del malware.
3	updateSQL	Se usa para enviar la consulta SQL para que se ejecute en la base de datos SQLite que Sharkbot usa para guardar la configuración del malware (inyecciones, etc.)
4	stopAll	Se utiliza para restablecer/detener la función ATS, deteniendo la automatización en curso.
5	updateConfig	Se utiliza para enviar una configuración actualizada al malware.
6	uninstallApp	Se utiliza para desinstalar la aplicación especificada del dispositivo infectado.
7	changeSmsAdmin	Se utiliza para cambiar la aplicación del administrador de SMS.
8	getDoze	Se usa para verificar si los permisos para ignorar la optimización de la batería están habilitados y mostrar la configuración de Android para deshabilitarlos si no lo están.
9	sendInject	Se usa para mostrar una superposición para robar las credenciales del usuario.
10	getNotify	Se usa para mostrar la configuración del detector de notificaciones si no está habilitada para el malware. Con estos permisos habilitados, Sharkbot podrá interceptar notificaciones y enviarlas al C2
11	APP_STOP_VIEW	Se usa para cerrar la aplicación especificada, por lo que cada vez que el usuario intenta abrir esa aplicación, el Servicio de Accesibilidad la cierra.
12	downloadFile	Se utiliza para descargar un archivo desde la URL especificada.
13	updateTimeKnock	Se utiliza para actualizar la marca de tiempo de la última solicitud para el bot.

	EC-2022-045	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	08-marzo-2022	**Troyano Bancario para Android**	V 1.1

Ítem	Comando	Descripción
14	localATS	Se utiliza para habilitar los ataques ATS. Incluye una matriz JSON con los diferentes eventos/acciones que debe simular para realizar ATS (clics de botones, etc.)

Tabla 1. Comandos SharkBot.
Fuente: Research NCCGROUP

INDICADORES DE COMPROMISO

A continuación, se mencionan los indicadores de compromiso asociados a SharkBot.

Inicialmente se considera el sitio web de descarga

Ítem	Descripción	IOC
1	Números de Serie de los certificados	https://apkplz[.]net/app/com.abbondioendrizzi.antivirus.supercleaner **DNS requests** apkplz.net apksos.com ocsp.digicert.com **IP** 104[.]26[.]4[.]67 172[.]67[.]69[.]200 104[.]26[.]5[.]67 8[.]248[.]139[.]254 104[.]26[.]9[.]204

Tabla 2. IOC asociados a sitio Web de descarga de SharkBot
Fuente: Any Run

	EC-2022-045	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	08-marzo-2022	**Troyano Bancario para Android**	V 1.1

Realizando el análisis en Virus Total se obtiene la siguiente información:

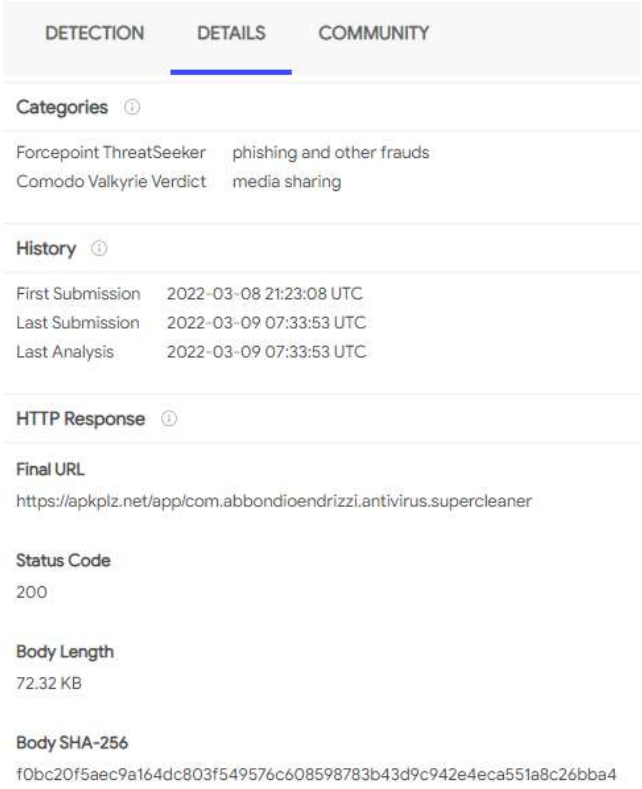
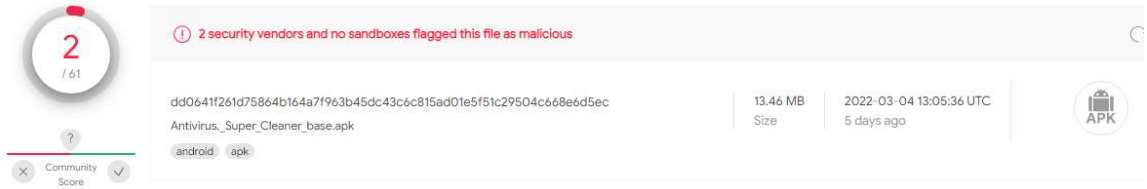


Figura 6. Ilustración asociada a WEB de descarga de SharkBot
Fuente: Virus total

En referencia a la APK de descarga, se obtiene:



	EC-2022-045	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	08-marzo-2022	**Troyano Bancario para Android**	V 1.1

Summary

Android Type	APK
Package Name	com.abbondioendrizzi.antivirus.supercleaner
Main Activity	com.abbondioendrizzi.antivirus.supercleaner.screen.main.MainActivity
Internal Version	5
Displayed Version	1.5
Minimum SDK Version	26
Target SDK Version	30

Certificate Attributes

Valid From	2022-01-29 11:40:42
Valid To	2052-01-29 11:40:42
Serial Number	cb81bbca19b19f0628aecb9b1a61f6e1aad1b5b5
Thumbprint	7ff554b2fc5b9e34ed703b1b13e833f62363f459

Certificate Subject

Distinguished Name	C:US, CN:Android, L:Mountain View, O:Google Inc., ST:California, OU:Android
Common Name	Android
Organization	Google Inc.
Organizational Unit	Android
Country Code	US
State	California
Locality	Mountain View

Figura 6. Análisis APK SharkBot
Fuente: Virus total

A continuación, se listan los IOC de la aplicación SharkBot

Item	Propiedades	Detalle
1	MD5	f30078ce385ef7ebd9864c8a70ff20f8
2	SHA-1	1ef621c0a39bd158f56ca4727b19173d1a81b534
3	SHA-256	dd0641f261d75864b164a7f963b45dc43c6c815ad01e5f51c29504c668e6d5ec
4	Vhash	fa2f3720a95e6362f7810f091e47a42f
5	SSDEEP	393216:INIvvMaH5macX7X52NWdXJq2TNhUfwplpMrfum7t:INs0aZqgY5jNqt
6	TLSH	T111E6238BFB98C62FD9731632C917453372A31E0824929BBA2315F3281977D425F56FCA
7	File type	Android
8	Magic	Zip archive data
9	TrID	VYM Mind Map (34.7%)
10	TrID	Sweet Home 3D design (generic) (29.1%)
11	TrID	Mozilla Firefox browser extension (22.2%)
12	TrID	ZIP compressed archive (11.1%)
13	TrID	PrintFox/Pagefox bitmap (640x800) (2.7%)
14	File size	13.46 MB (14112506 bytes)
15	SharkBotDropper C2	hxxp://statscodicefiscale[.]xyz/stats/
16	Auto/Direct Reply' URL used to distribute the malware	hxxps://bit[.]ly/34ArUxI
17	C2 servers/Domains for SharkBot	n3bvakjjouxir0zkzmd[.]xyz (185.219.221.99) mjayoxbvakjjouxir0z[.]xyz (185.219.221.99)

Figura 6. IOC APK SharkBot
Fuente: Virus total

	EC-2022-045	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	08-marzo-2022	**Troyano Bancario para Android**	V 1.1

V. RECOMENDACIONES:

El EcuCert recomienda a su comunidad objetivo:

- Descargar aplicaciones solamente desde fuentes oficiales y verificadas.
- Prestar atención si el teléfono móvil presenta las siguientes características: funciona lentamente, la configuración del sistema se modifica sin el permiso del usuario, si el uso de datos y batería aumenta significativamente.
- No abrir links provenientes de correos desconocidos, de anuncios maliciosos o de sitios web fraudulentos.
- Escanear el dispositivo Android con un software antimalware legítimo.
- Verificar las aplicaciones que tienen privilegios de administrador.

VI. REFERENCIAS:

GROUP, N. (03 de 03 de 2022). *NCC GROUP*. Obtenido de NCC GROUP: https://research.nccgroup.com/2022/03/03/sharkbot-a-new-generation-android-banking-trojan-being-distributed-on-google-play-store/

Meskauskas, T. (04 de 03 de 2022). *PC RISK*. Obtenido de PC RISK: https://www.pcrisk.com/removal-guides/22402-sharkbot-malware-android

Rankia. (12 de 05 de 2017). *Rankia*. Obtenido de Rankia: https://www.rankia.com/foros/bancos-cajas/temas/3568859-peligro-virus-nuevas-formas-ataque-bancos-sistemas-transferencia-automatica-ats

Toulas, B. (05 de 03 de 2022). *Bleepingcomputer*. Obtenido de Bleepingcomputer: https://www.bleepingcomputer.com/news/security/sharkbot-malware-hides-as-android-antivirus-in-google-play/