

13/04/22

Sharkbot, el nuevo malware de Android capaz de robar credenciales bancarias

Un nuevo malware apodado Sharkbot ha sido localizado en aplicaciones que se hacen pasar por antivirus en Google Play Store.

Investigadores de Check Point Research (CPR) [han localizado muestras](#) en Google Play Store de un **dropper camuflado de antivirus para Android**, apodado Sharkbot. Sharkbot es un malware con capacidad de robar credenciales bancarias, es decir, un banker.

Análisis de Sharkbot

Entre sus características, implementa técnicas de evasión para no ser ejecutado en emuladores. También **ignora a usuarios de China, India, Rumanía, Rusia, Ucrania y Bielorrusia**. Además, integra un [algoritmo de generación de dominios \(DGA\)](#) para conectar a los servidores de control. El uso de DGA permite que una muestra con una semilla fija en el código genere 7 dominios por semana. Combinando las semillas y algoritmos observados, se generan 56 dominios por semana.



```
try {
    if(!Build.FINGERPRINT.startsWith("generic") && !Build.FINGERPRINT.startsWith("unknown") && !Build.MODEL.contains("google_sdk") && !Build.MODEL.contains(
        "Emulator") && !Build.MODEL.contains("GCE x86 phone") && !Build.MODEL.contains("Standard PC") && !Build.MODEL.contains("Android SDK") && !Build.MODEL.contains("sdk_gphone")
    ) && !Build.MODEL.contains("AOSP") && !Build.MODEL.contains("X86pro") && !Build.MODEL.contains("Virtual") && !Build.MODEL.contains("Vmare") && !Build.MANUFACTURER
        .contains("LIMITED") && !Build.MANUFACTURER.contains("MOBILE") && !Build.MANUFACTURER.contains("Vmare") && !Build.MANUFACTURER.contains("Virtual") && !Build.MANUFACTURER
        .contains("QEMU") && !Build.MANUFACTURER.contains("unknown") && !Build.MANUFACTURER.contains("Genymobile") && !Build.MANUFACTURER.contains("Genymotion") && (!Build
        .BRAND.startsWith("generic") || !Build.DEVICE.startsWith("generic")) && !"google_sdk".equals(Build.PRODUCT)) {
        boolean v0 = q.h("cn|in|ro|ru|ua|by").contains(Locale.getDefault().getLanguage().toLowerCase());
        return v0;
    }
}
catch(Exception unused_ex) {
}

return true;
```

Mecanismo de evasión para no ejecutar el malware en emuladores. Fuente: [Check Point Research](#)

El proceso de robo de credenciales es típico en Android, **abusando la API del servicio de accesibilidad** para darle a la aplicación acceso a todos los datos visualizados por el usuario, permitiendo interactuar con la interfaz como si fuera una persona.

Principalmente, el malware Sharkbot induce a la víctima a introducir sus datos de acceso bancarios en una ventana aparentemente benigna. Como resultado, a través de dicho formulario se envían las credenciales al servidor de Comando y Control (C&C).

Comandos de Sharkbot

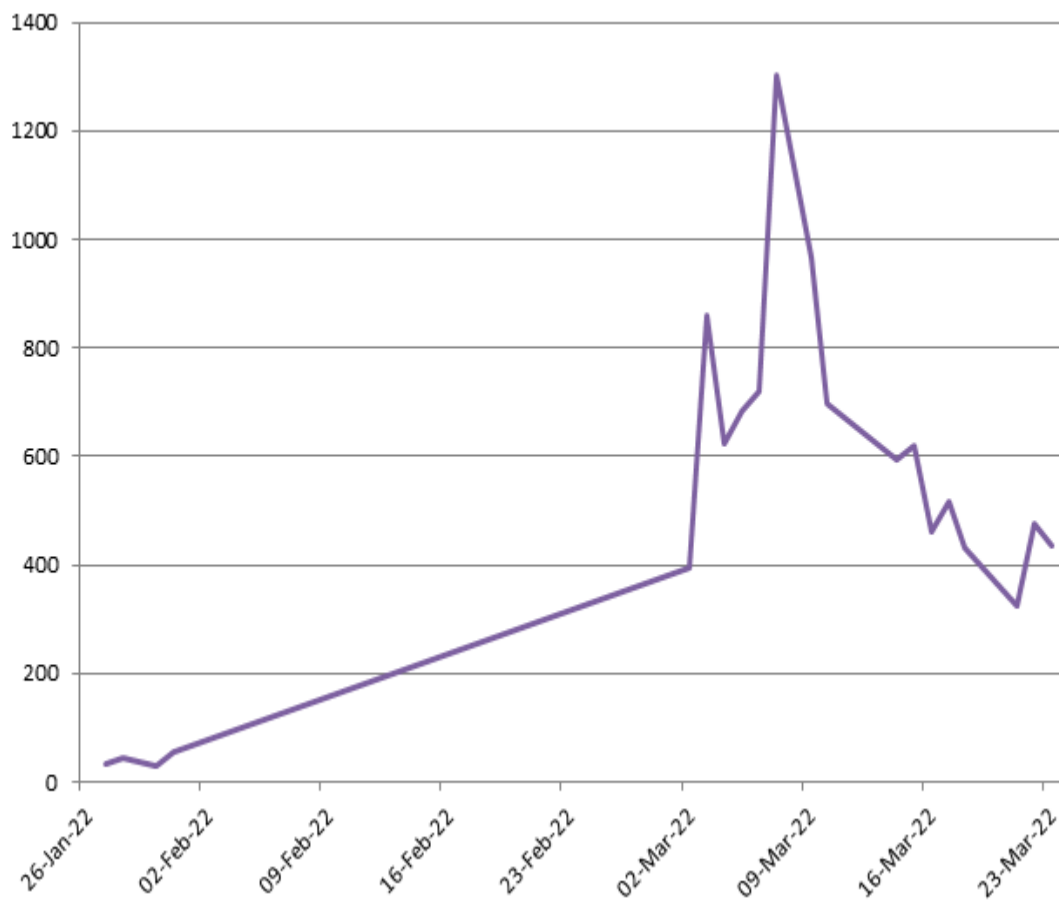
A continuación se muestra una breve descripción de los comandos de Sharkbot:

Nº	Comando	Descripción
1	smsSend	Solicita permiso para enviar SMS
2	updateLib	Descarga y almacena un fichero JAR con código Java
3	updateSQL	Actualiza una opción en una BD local
4	updateConfig	Actualiza diferentes opciones
5	uninstallApp	Desinstala una aplicación dada
6	collectContacts	Envía la lista de contactos al servidor
7	changeSmsAdmin	Cambia el gestor por defecto de SMS
8	getDoze	Desactiva la optimización de batería para que Sharkbot se ejecute en segundo plano
9	sendInject	Crea la ventana de inyección para una URL
10	iWantA11	Activa el servicio de accesibilidad para Sharkbot
11	updateTimeKnock	Actualiza la opción “TIME_KNOCK_ADMIN”
12	sendPush	Muestra una notificación Push al usuario
13	APP_STOP_VIEW	Previene que el usuario active la aplicación
14	Swipe	Imita la acción de deslizar del usuario sobre la pantalla del dispositivo
15	autoReply	Establece un mensaje de autorrespuesta en las notificaciones Push
16	removeApp	Elimina una aplicación de forma silenciosa
17	serviceSMS	Envía mensajes SMS a números de teléfonos con un texto dado
18	getNotify	Activa el «Listener» de notificaciones para la aplicación de Sharkbot
19	localATS	Activa una aplicación dada y registra todos los eventos de accesibilidad
20	sendSMS	Envía un SMS con un texto a un número de teléfono
21	downloadFile	Descarga un fichero de una URL y lo almacena localmente con extensión «.apk»
22	stopAll	Un comando se transfiere al fichero JAR, descargado con updateLib

Tabla de comandos de Sharkbot

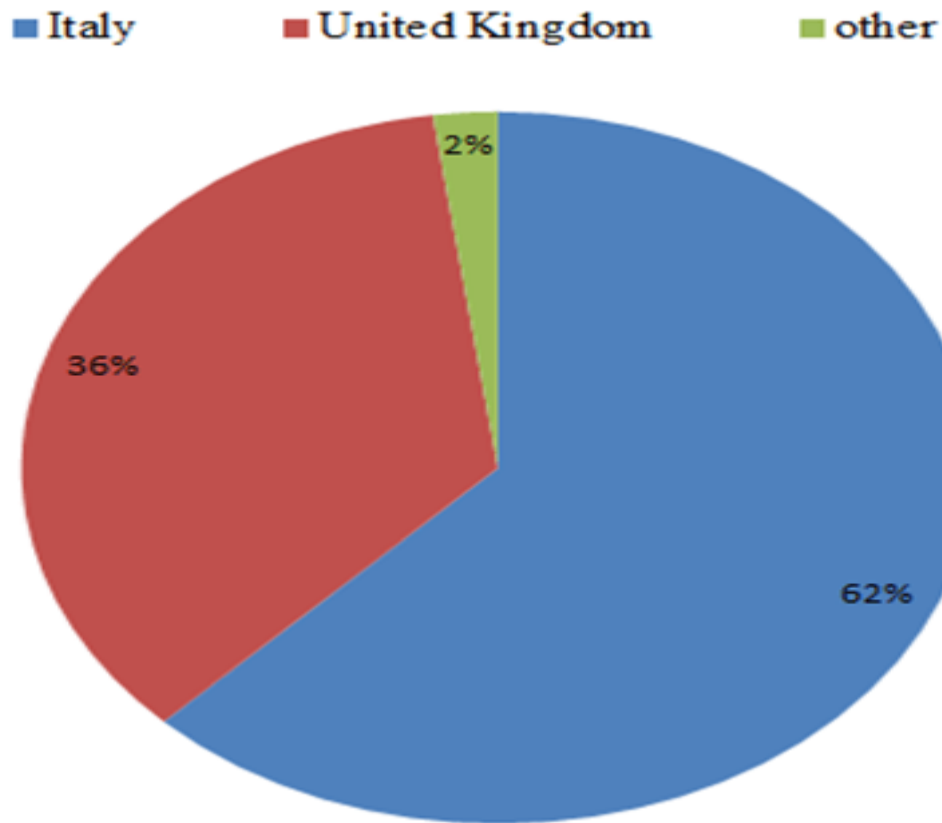
Impacto del malware

Desde Check Point Research afirman que hay un **único servidor malicioso** y que los dominios generados de forma aleatoria actúan como relés a dicho servidor



Actividad del servidor de Sharkbot. Fuente: [Check Point Research](#)

En el siguiente gráfico podemos ver que actualmente la mayoría de clientes afectados se encuentran en Reino Unido e Italia.



Distribución geográfica de las potenciales víctimas. Fuente: [Check Point Research](#)

Las aplicaciones maliciosas han sido eliminadas de Google Play, pero aún persisten en tiendas de aplicaciones no oficiales. Sin embargo, se estiman más de 15.000 descargas en total a través de la tienda de Google.

Asimismo, los nombres de los paquetes afectados son los siguientes:

Nombre de paquete

com.antivirus.centersecurity.freeforall

com.centersecurity.android.cleaner

com.pagnotto28.sellsourcecode.supercleaner

com.pagnotto28.sellsourcecode.alpha

com.abbondioendrizzi.tools.supercleaner

com.abbondioendrizzi.antivirus.supercleaner

Estas muestras aparecen detectadas como maliciosas en [Koodous](#), el antivirus social colaborativo para analistas de malware de Android.



Powerful Cleaner, Anti...

Unknown


⚠ Detected

^ -5 v



Download



Analyze


Share

 General

 Comments (1)

 Votes (5)

 Matches


Analysis information

⊗ Not static analyzed

Analyze

⊗ Not dynamic analyzed

Analyze

 Yara rules not applied

Check

Metadata

Package name	com.pagnotto28.sellsourcecode.supercleaner
Developer	Unknown
Displayed version	1.9
File size	13.46 MB
First seen	2 months ago
MD5	ab25bfce859ba1bb374eda63e1be92d3 
SHA1	065e0ef6aab548cdc764aadd4c41ad815fda78f8 
SHA256	e5b96e80935ca83bbe895f6239eabca1337dc575a066bb6ae2b56faacd29ddaa 