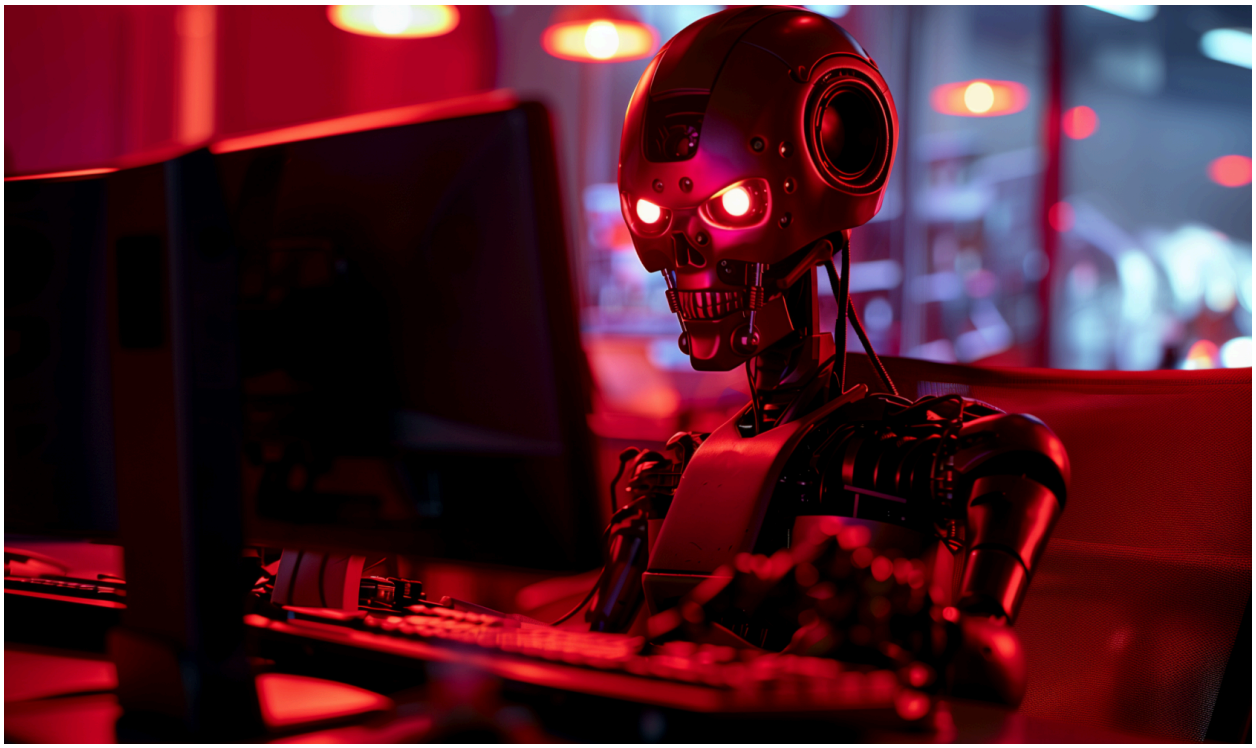


Equipo GXC desenmascarado: grupo cibercriminal que comete delitos informáticos y afecta a usuarios de bancos españoles a través del uso de herramientas de *phishing* con IA y un programas maliciosos para Android

Autores:
Anton Ushakov, jefe de investigaciones de delitos cibernéticos, Europa
Martijn van den Berk, analista de programas maliciosos, Europa

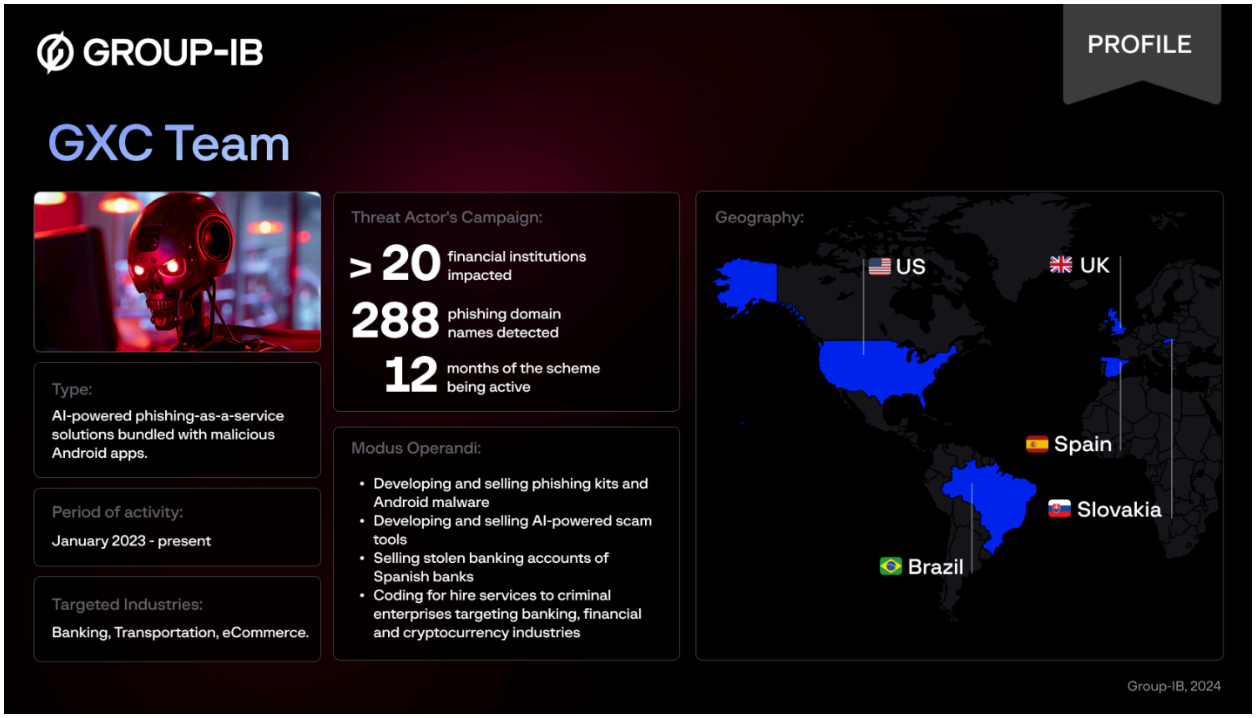
Metadescripción: Equipo GXC, especializado en el *phishing* como servicio con IA y un programa malicioso para Android capaz de interceptar códigos OTP, que afecta a usuarios de bancos españoles y a 30 instituciones de todo el mundo.

Introducción

En septiembre de 2023, Group-IB expuso al grupo criminal hispanohablante llamado Equipo GXC, hasta ese momento desconocido, que operaba una sofisticada plataforma de *phishing* como servicio con IA. Equipo GXC, cuyo objetivo eran los usuarios de bancos españoles, utilizaba técnicas inusuales que constituían una amenaza regional significativa. Este grupo, que surgió por primera vez en enero de 2023 en Telegram y Exploit.in, se especializaba en el desarrollo y la venta de kits de *phishing*, un programa malicioso para Android y herramientas fraudulentas con IA. Sus servicios incluían la venta de credenciales bancarias robadas y codificación personalizada para fines maliciosos. La operación se llevaba a cabo a través de un modelo de programa malicioso como servicio en el que los clientes pueden comprar recursos de *phishing* adaptados para emular dominios de bancos. En particular, su programa malicioso para Android se diseñó para interceptar códigos OTP (contraseñas de un solo uso), lo que afecta específicamente a usuarios de más de 36 bancos españoles, organismos gubernamentales y 30 instituciones en todo el mundo. Los analistas de Group-IB han detectado al menos 250 dominios de *phishing* que se le atribuían al actor malicioso y han descubierto 9 variantes del programa malicioso para Android.

A pesar de que sus herramientas no son extremadamente sofisticadas, las funciones innovadoras de Equipo GXC hicieron que se convirtiera en una amenaza grave para la seguridad bancaria en España. En esta entrada de blog, se analizan sus métodos operativos, las características distintivas de sus herramientas maliciosas y sus estrategias de ataque, así como estrategias defensivas efectivas contra esas amenazas.

—----------



Actividades criminales de Equipo GXC

Equipo GXC apareció en el radar de Group-IB en enero de 2023, cuando comenzó a ofrecer sus servicios criminales a través de su canal privado de Telegram y el foro clandestino Exploit.in. El precio de su kit de *phishing* oscilaba entre los 150 $ y los 900 $, mientras que el paquete que incluye el kit de *phishing* y el programa malicioso para Android costaba 500 $ por mes aproximadamente. Equipo GXC se centraba particularmente en el desarrollo y la distribución de kits de *phishing* y el programa malicioso para Android destinados a afectar a usuarios de instituciones financieras españolas, además de otros organismos, entre los que se incluyen servicios tributarios y gubernamentales, comercio electrónico, bancos e intercambios de criptomonedas en Estados Unidos, Reino Unido, Eslovaquia y Brasil.

Estas son las actividades criminales de Equipo GXC:

- Desarrollo y venta de kits de *phishing*.
- Desarrollo y venta de programas maliciosos para Android.
- Desarrollo y venta de herramientas fraudulentas con IA.
- Venta de cuentas bancarias robadas de bancos españoles.
- Servicios de codificación para fines maliciosos.

En el núcleo de las actividades de Equipo GXC se encuentra un modelo clásico de programa malicioso como servicio donde otros actores maliciosos pagan una tarifa mensual solo por el kit de *phishing* o por el paquete con la aplicación maliciosa para Android. Luego, Equipo GXC se

ocupa del resto: instala y configura la infraestructura y registra los nombres de dominio para entregar las credenciales robadas.

Al comprar los servicios de Equipo GXC, otros actores maliciosos generalmente reciben un recurso de *phishing* completamente configurado, junto con un nombre de dominio (que generalmente contiene un error tipográfico o simula ser el dominio de un banco), así como un servidor y un kit de *phishing* configurado. También se los incluirá en un chat creado especialmente en Telegram, donde un bot actúa como servidor de comando y control (C2), y envía las credenciales robadas desde el panel de *phishing* al chat.

¿Qué tienen de especial las herramientas de GXC?

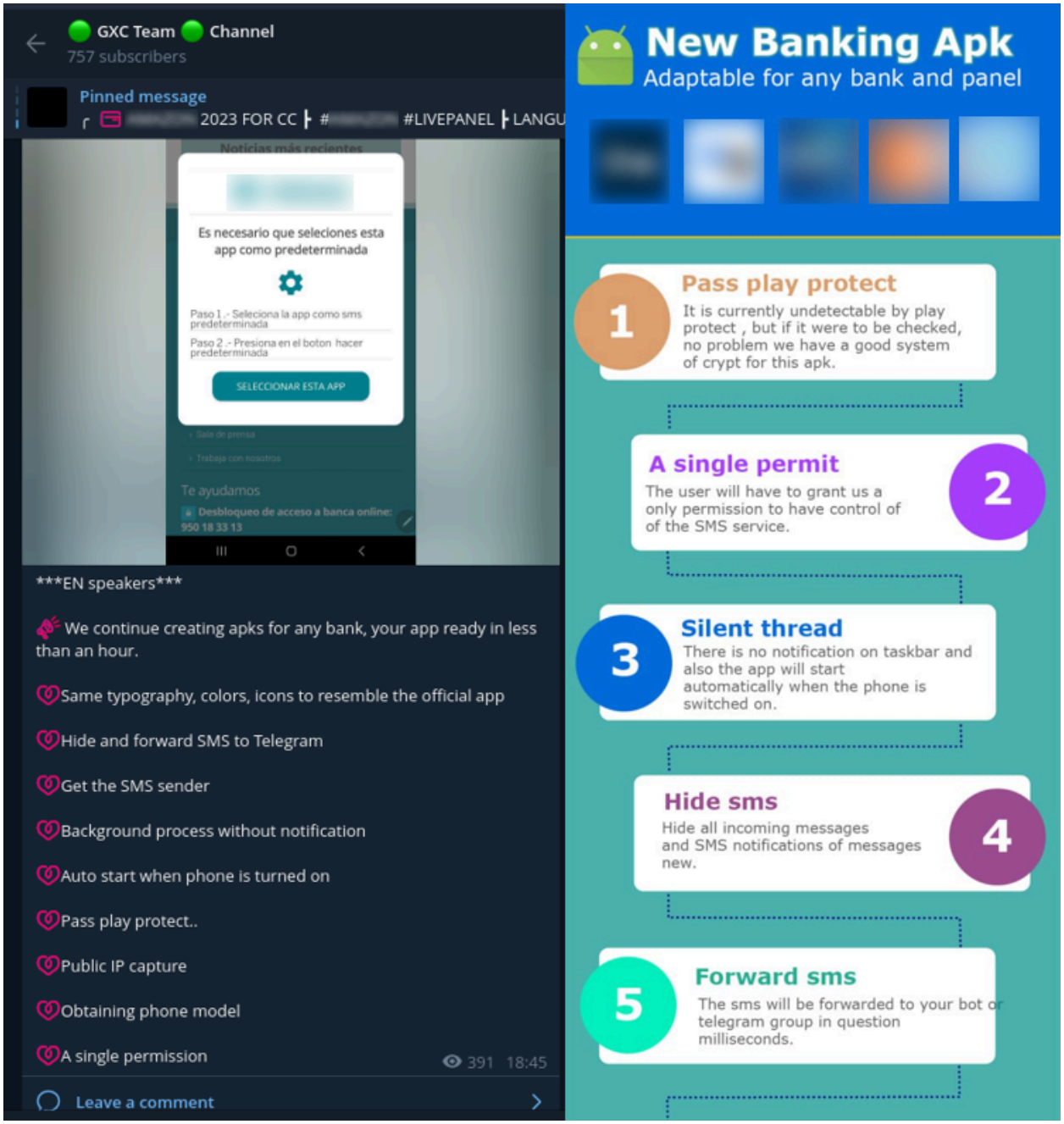
La herramienta principal de las actividades de Equipo GXC incluía kits de *phishing* personalizados y un programa malicioso para Android. Los kits de *phishing* que ofrecía Equipo GXC estaban disponibles para **36 bancos que funcionan en España** y otras 30 instituciones de otros países. Además, Equipo GXC ofrecía un programa malicioso para Android que simulaba ser una aplicación bancaria, diseñado para interceptar códigos OTP que emiten los bancos legítimos. Según la investigación de Group-IB, se detectó que se utilizaba ese programa malicioso para afectar a clientes de al menos **10 bancos que actualmente operan en España**.

Lo que diferencia a las herramientas de Equipo GXC no es su sofisticación técnica, sino varias funciones notables que se implementaron y hacían que sus herramientas fueran una amenaza significativa para clientes bancarios de España.

Paquete de kit de *phishing* y programa malicioso para Android

La primera implementación notable es el paquete que incluye un kit de *phishing* y una aplicación maliciosa para Android. A diferencia de los desarrolladores de *phishing* típicos, Equipo GXC combinó kits de *phishing* con un programa malicioso que robaba códigos OTP enviados por SMS, lo que hace que una situación típica de ataque de *phishing* tenga una característica levemente diferente. En lugar de solo obtener credenciales y otros datos directamente desde una página de *phishing*, el programa malicioso les solicitaba a las víctimas que descargaran e instalaran una aplicación bancaria que aparentemente evitaba un «intento

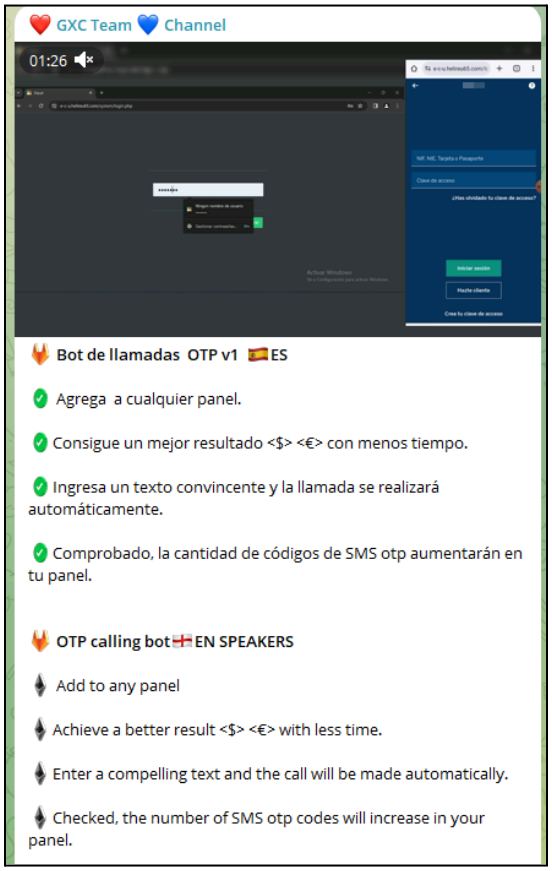
de *phishing*». Una vez que las víctimas la instalaban, la aplicación solicitaba permiso para manipular mensajes SMS, lo que permitía que los atacantes enviaran mensajes SMS de manera encubierta desde el dispositivo de la víctima a un bot de Telegram controlado por Equipo GXC, lo que a su vez permitía vaciar las cuentas bancarias de su víctima muy fácilmente.



Captura de pantalla de un anuncio hecho por Equipo GXC en su chat de Telegram acerca del robo de códigos OTP enviados por mensajes SMS que afectaba a bancos españoles.

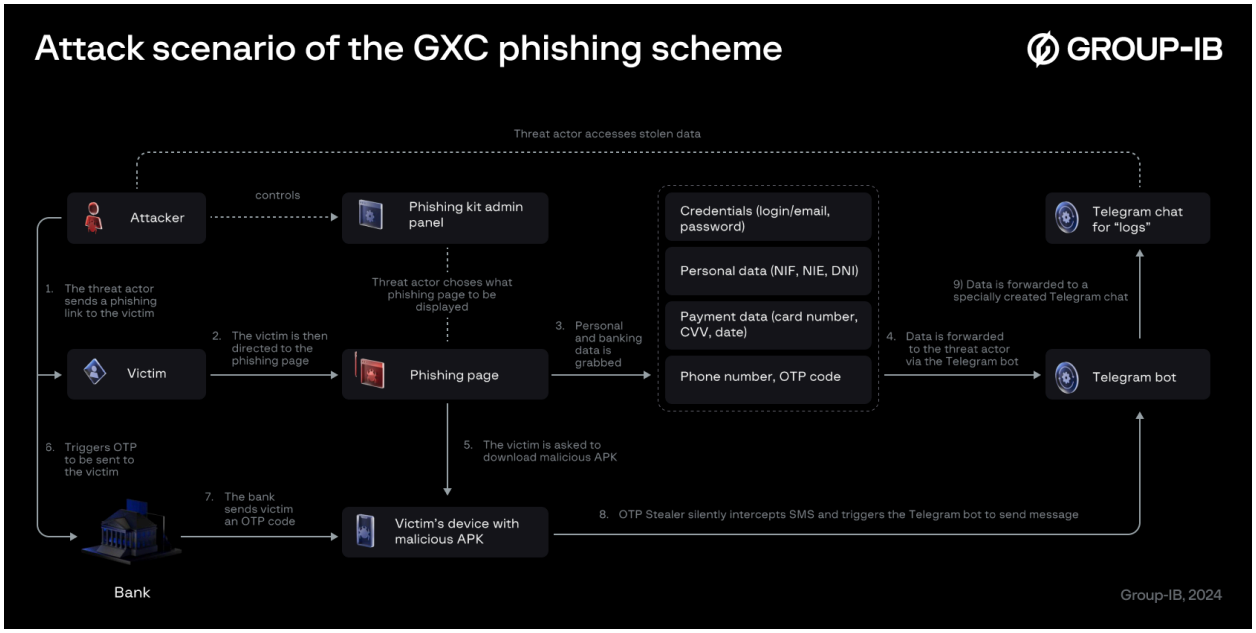
Función de llamadas de voz mediante uso de IA en el kit de *phishing*

Los desarrolladores también integraron una función con IA actualizada que permite que otros actores maliciosos realicen llamadas de voz a sus víctimas siguiendo sus indicaciones, directamente desde el kit de *phishing*. Las víctimas reciben llamadas supuestamente de sus bancos en las que se les pide que brinden sus códigos de autenticación en dos pasos (2FA), que instalen aplicaciones que resultan ser programas maliciosos o que realicen cualquier otra acción que deseen los demás actores maliciosos. Utilizando este mecanismo simple pero efectivo, se aumenta aún más la situación fraudulenta y se convence a las víctimas, y esto demuestra lo rápido y fácil que los criminales adoptan e implementan las herramientas con IA en sus esquemas, lo que hace que las situaciones de fraude tradicionales se transformen en nuevas tácticas más sofisticadas.



Captura de pantalla de un anuncio de Equipo GXC en su canal de Telegram acerca de la función de llamadas de voz mediante IA.

Situación de ataque

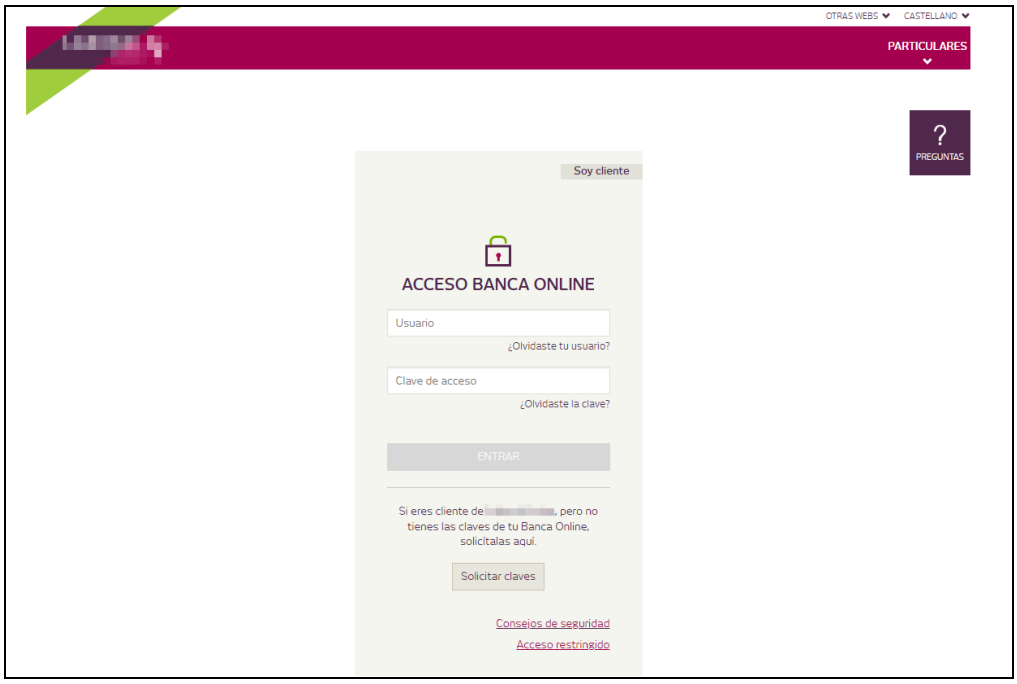


Situación de ataque generalizado del kit de *phishing* y el programa malicioso para el robo de OTP de Equipo GXC.

Desde la perspectiva de la víctima, el fraude comienza cuando recibe un señuelo de *phishing* a través de un mensaje SMS de *smishing* y continúa con los siguientes pasos:

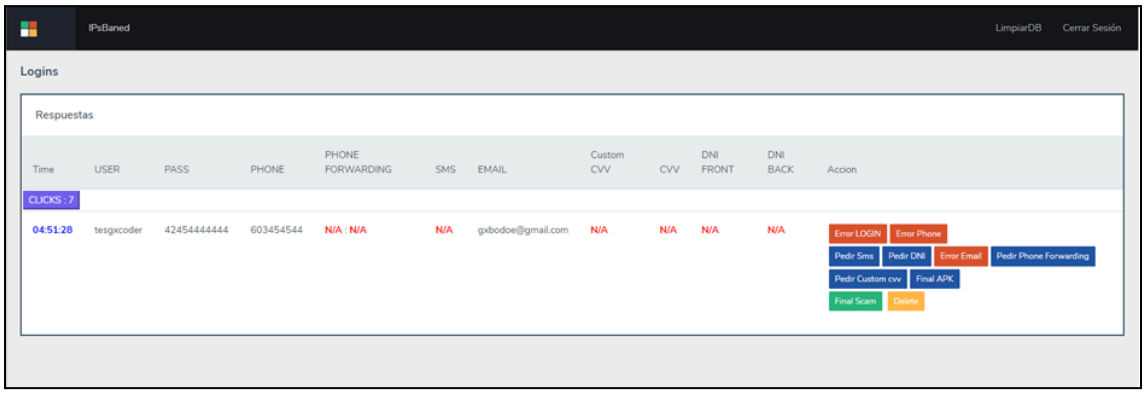
Ruta de phishing

1. A la víctima se le solicita que acceda a un sitio web de *phishing* mediante mensajes SMS de *smishing* u otro método de distribución de enlaces.
2. Una vez que la víctima llega al sitio web de *phishing*, se le solicita que ingrese sus credenciales iniciales, incluso los detalles de inicio de sesión, utilizando el número de identificación fiscal español (NIF) u otros datos, junto con una contraseña. Al mismo tiempo, el actor malicioso recibe una notificación en el panel de administración o el chat de Telegram que le informa que la víctima ha ingresado al sitio web de *phishing*.



Ejemplo del sitio web de *phishing* inicial.

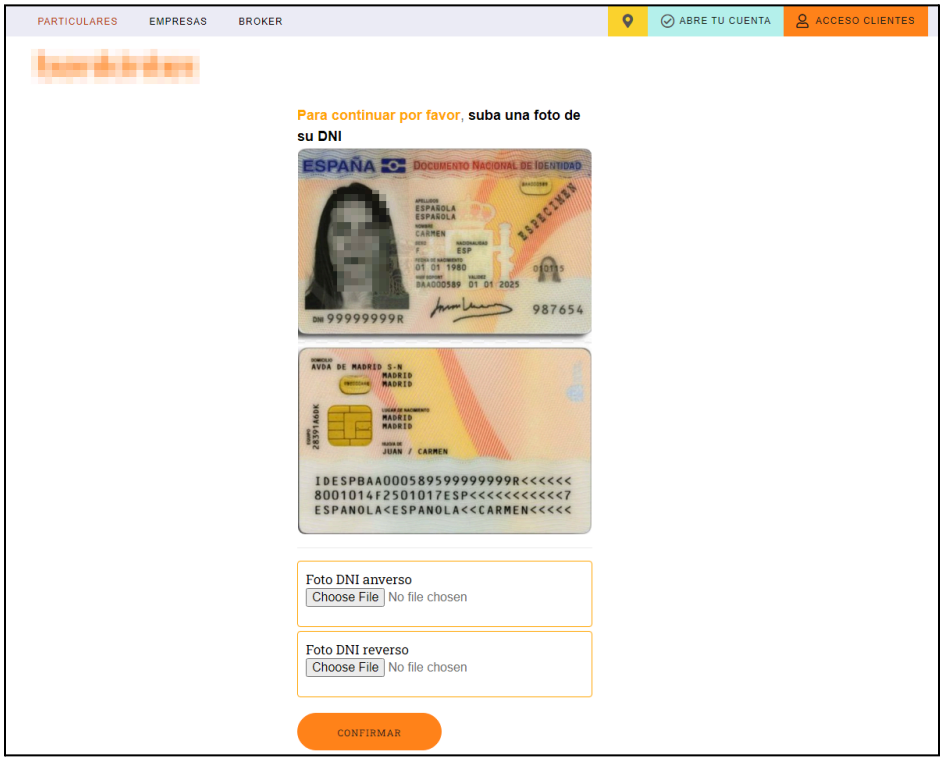
Una vez establecidos, el actor malicioso tendrá un control absoluto en tiempo real mediante un denominado “panel en vivo”, un tipo de kit de *phishing,* específicamente un panel de administración, en el que el atacante puede elegir de forma manual qué tipo de datos deben solicitarse a las víctimas y qué página debe mostrarse posteriormente. En función de lo que seleccione la víctima y dependiendo de esta estrategia de manipulación dinámica, el actor malicioso puede solicitar más información personal.



Captura de pantalla del panel de administración en vivo del kit de phishing.

3. Dependiendo de la institución financiera que se simula y la selección del actor malicioso, es posible que se le solicite una fotografía del documento de identidad (DNI) a las víctimas, su dirección física, dirección de correo electrónico, número de teléfono, código OTP enviado por SMS, etc. Luego, se muestran los datos en el panel de administración

del kit de *phishing* o se los envía al chat de Telegram que controla el actor malicioso utilizando el bot de Telegram.

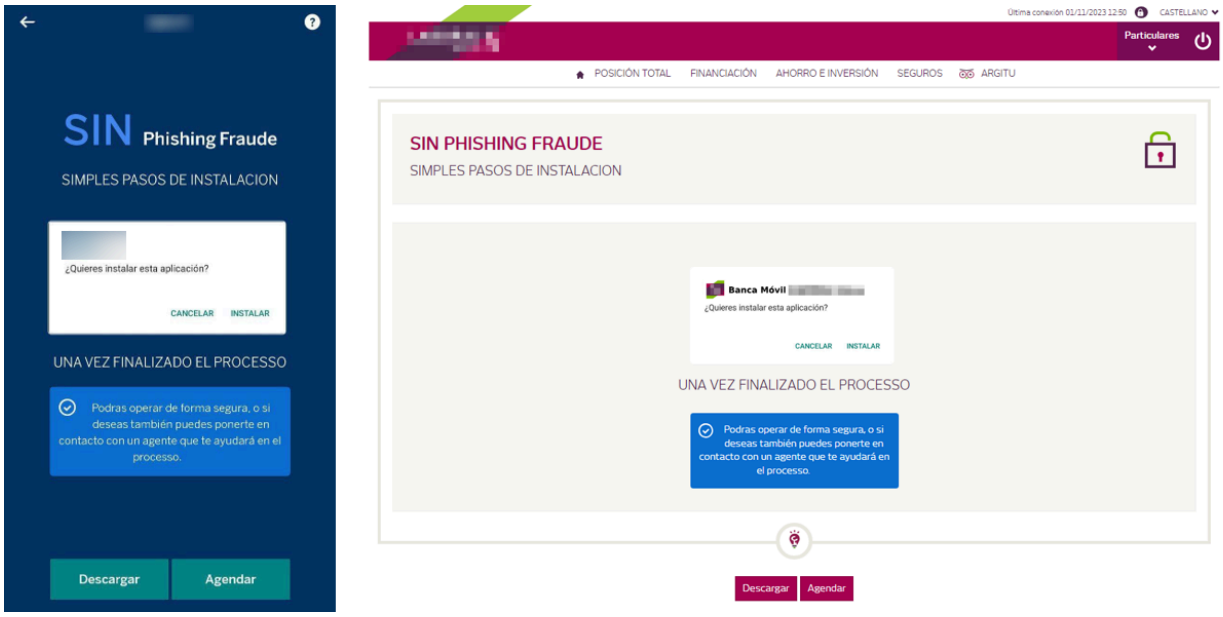


Captura de pantalla de una página de *phishing* que solicita el DNI (documento de identidad) utilizando un documento de muestra.

En ese momento, los criminales también pueden activar la función de llamadas de voz mediante el uso de IA directamente en el kit de *phishing* para que las víctimas reciban una llamada automática que logre que brinden incluso más datos valiosos.

Ruta del programa malicioso para Android

Para los clientes de varias instituciones financieras, la estafa continúa. La página de *phishing* los engaña para que descarguen e instalen una supuesta aplicación bancaria para Android que aparentemente «evita intentos de fraude». Muy desafortunadamente, en lugar de eso, las víctimas descargarán un programa malicioso diseñado para robar OTP enviados por mensajes SMS.

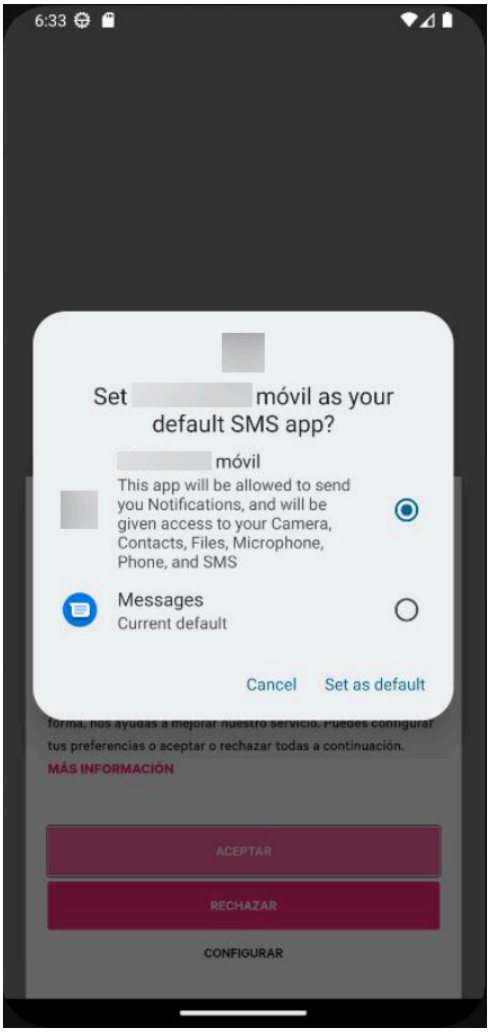


Ejemplo de una página de *phishing* que les solicita a las víctimas instalar una «aplicación bancaria» que aparentemente evita intentos de fraude.

4. El APK (kit de paquete de Android) simula ser la aplicación de un banco legítimo que utiliza el logotipo y estilo originales. Luego de instalar y abrir la aplicación, la víctima verá una página (WebView con una URL codificada de forma rígida) que le solicitará que conceda permisos a la aplicación.

Ejemplo de una aplicación falsa que solicita permisos.

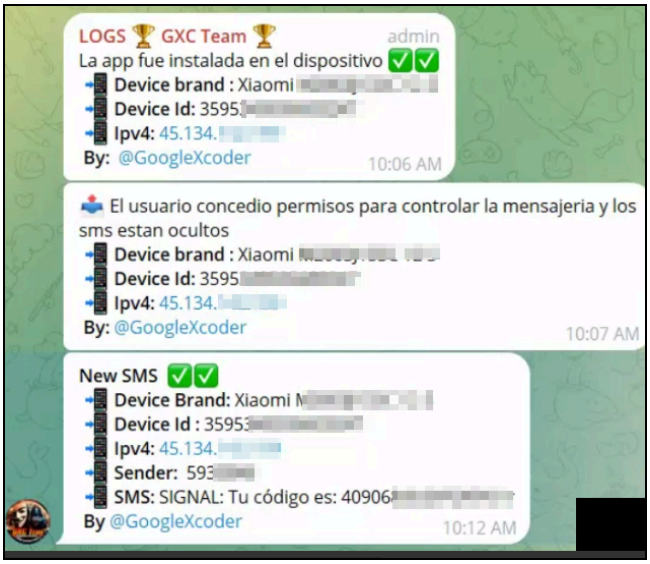
5. Al hacer clic en cualquier lugar de la ventana de la aplicación, se abrirá un cuadro de diálogo que solicitará que la víctima establezca la aplicación como predeterminada para mensajes SMS. Ese cuadro de diálogo no se podrá cerrar y se volverá a abrir mientras no se establezca la aplicación como la predeterminada para mensajes SMS.



6. Una vez que se establezca la aplicación como la predeterminada para mensajes SMS, se otorgarán varios permisos, incluidos READ_SMS y RECEIVE_SMS, lo que permitirá que los criminales lean, reenvíen y eliminen mensajes SMS de manera encubierta.

7. En la última etapa, la aplicación abrirá un sitio web legítimo del banco en WebView, lo que permitirá que los usuarios interactúen normalmente con este.

8. Luego, cuando el atacante activa la solicitud de OTP, el programa malicioso para Android, de manera desapercibida, recibe y reenvía mensajes SMS con códigos OTP al chat de Telegram que controla el actor malicioso, lo que permite que los atacantes confirmen cualquier tipo de operación, incluso transferencias de dinero, cambios en la cuenta, aumento de límites de crédito y otras operaciones financieras.



Captura de pantalla de notificaciones de Telegram enviadas al bot que controla el actor malicioso y que contienen datos de la víctima y mensajes SMS reenviados desde el dispositivo infectado.

En caso de que, al final del esquema, el ataque haya tenido éxito, el actor malicioso contará con una gran cantidad de credenciales y datos personales para llevar a cabo diferentes operaciones bancarias utilizando la cuenta bancaria de la víctima, gracias al kit de *phishing*, y podrá confirmar esas operaciones gracias al programa malicioso para el robo de OTP que se instaló.

Análisis del programa malicioso para Android de GXC

El programa malicioso que utiliza Equipo GXC es un programa malicioso para Android que roba mensajes SMS. La función principal de la aplicación es recibir mensajes SMS que contengan códigos OTP para inicio de sesión en cuentas de bancos y enviarlos a un chat de Telegram que controla el actor malicioso.

Funciones

- Solicitar establecer la aplicación como la predeterminada para mensajes SMS.
- Solicitar permisos específicos de manera explícita.
    - READ_SMS
    - RECEIVE_SMS
    - ACCESS_WIFI_STATE
    - FOREGROUND_SERVICE
- Recibir y leer mensajes SMS.
- Enviar mensajes SMS a un chat de Telegram utilizando un bot.

- Mostrar páginas HTML en la aplicación.
- Recopilar y enviar información sobre el dispositivo de la víctima, por ejemplo, identificadores de hardware e IP del dispositivo, etc.

Análisis de la ejecución

A continuación, se incluye una descripción por etapas de cómo opera el programa malicioso, desde la perspectiva de una víctima.

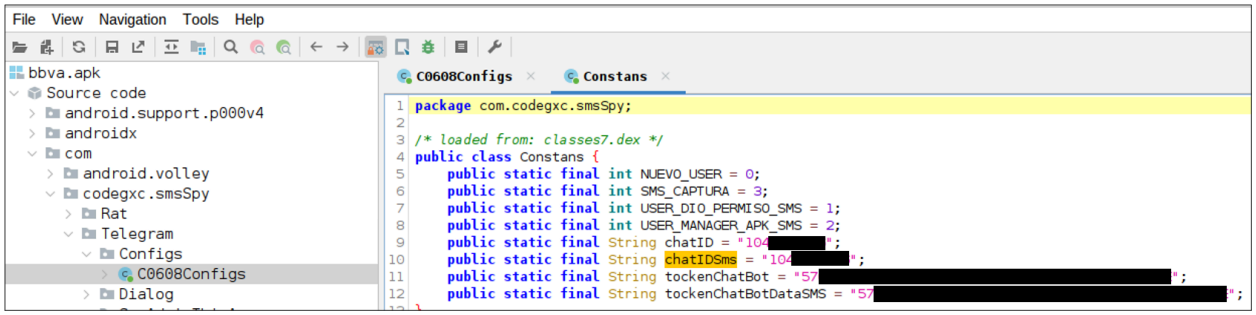
1) Al abrir la aplicación, la víctima verá una WebView. Esta WebView está configurada para ingresar a una URL codificada de manera rígida y mostrar la página web, que es un sitio web legítimo de un banco.

2) Al hacer clic en cualquier lugar de la ventana de la aplicación, se abrirá un cuadro de diálogo que solicitará que la víctima establezca la aplicación como predeterminada para mensajes SMS. Ese cuadro de diálogo no se podrá cerrar y se volverá a abrir mientras no se establezca la aplicación como la predeterminada para mensajes SMS.

3) Establecer la aplicación maliciosa como la predeterminada para mensajes SMS concederá varios permisos, sobre todo READ_SMS y RECEIVE_SMS, lo que permitirá que la aplicación lea y reciba los mensajes SMS que se envían al dispositivo de la víctima respectivamente.

4) Al volver a la aplicación, y luego de haber establecido la aplicación como la predeterminada para mensajes SMS, será posible interactuar normalmente con el sitio web a través de la URL codificada de manera rígida. El cuadro de diálogo ya no volverá a abrirse.

Funcionando en segundo plano, la aplicación enviará cualquier mensaje SMS que reciba la víctima al chat de Telegram que controla el actor malicioso mediante un bot. Las identificaciones del chat y el bot se codifican de manera rígida en el APK malicioso.



Junto con el contenido de los mensajes SMS, el actor malicioso también recibe información adicional, por ejemplo, el fabricante y modelo de dispositivo, la versión del firmware de Android

del dispositivo, la dirección IP actual, el número de teléfono del remitente del mensaje SMS y el contenido del mensaje SMS.

La idea es que la víctima, al instalar la aplicación, concederá los permisos necesarios y, por lo tanto, la aplicación será la que reciba cada mensaje SMS que incluya un código OTP para completar el inicio de sesión o confirmar una operación, y este se enviará al chat de Telegram que controla el actor malicioso.

Conclusión

El descubrimiento de Equipo GXC revela una ciberamenaza emergente dirigida específicamente a clientes de bancos españoles, que cuenta con una actividad criminal muy bien establecida, así como herramientas de *phishing* efectivas, lo que representa una amenaza significativa para la región. Es necesario prestar especial atención a la combinación inusual de un kit de *phishing* y un programa malicioso para el robo de OTP, lo que proporciona más versatilidad a los criminales y representa un riesgo mayor para los usuarios que no están al tanto de esta situación.

Se ha comenzado por páginas de *phishing* genéricas y se han implementado nuevas funciones y métodos para mejorar los señuelos y las situaciones de ataque. Equipo GXC demuestra que los criminales que utilizan técnicas simples pero creativas logran su objetivo rápidamente y, por lo tanto, representan un riesgo significativo no solo para los clientes, sino también para las instituciones financieras.
Group-IB continuará monitoreando y haciendo un seguimiento de la actividad de este actor malicioso y ya ha comenzado una investigación más integral al respecto.

Recomendaciones

Como forma de prevención y mitigación, las instituciones pueden adoptar un enfoque diversificado para abordar esta amenaza o alguna similar:

1. Monitoreo del escenario de amenazas local y seguimiento de la actividad del actor malicioso utilizando soluciones de análisis de amenazas.
2. Detección proactiva y eliminación de recursos de *phishing* para evitar el fraude en etapas iniciales.
3. Implementación de soluciones antifraude o de protección contra fraudes durante sesiones para detectar y protegerse contra riesgos asociados a cuentas.
4. Concienciación sobre los nuevos esquemas de fraude y capacitación de usuarios.
5. Aumento de los esfuerzos para combatir este tipo de amenaza mediante la autorización de investigaciones del ciberdelito.

Como cliente bancario, así es cómo puede reconocer ese tipo de amenazas y protegerse contra intentos de fraude o de *phishing*:

1. Siempre compruebe la autenticidad de la solicitud con su banco.
2. Realice absolutamente todas las comprobaciones antes de dar cualquier información personal o relacionada con su banco en línea.
3. No descargue ni transfiera ninguna aplicación bancaria o similar desde sitios web o enlaces sospechosos o no confiables.
4. Utilice únicamente canales de comunicación verificados oficialmente con su banco y los empleados bancarios.

Si ha sido víctima de un ataque de este tipo, no lo oculte. Los delincuentes se benefician con nuestro silencio. Al darse cuenta de que ha sido víctima de un ataque, asegúrese de denunciarlo a la policía. Aporte todo los detalles que sea posible para poder iniciar las investigaciones y castigar a los delincuentes.

Indicadores de compromiso

Nombres de dominios de *phishing*

hu-alert[.]online
caixabank-particular[.]com
mi-bancsabadell[.]com
be-ceca[.]com
lng-direct.es-miparticulares[.]com
es-miparticulares[.]com
grupos-inicio[.]com
au-myposts[.]com
es-bsnacional[.]com
mi-deustsche-bank[.]com
mi-deutschebank[.]com
es-miempresas[.]com
cuenta-app[.]com
santander.esp-aviso[.]com

esp-aviso[.]com
ing.direct-usuario[.]com
direct-usuario[.]com
grupo-inicios[.]com
santander-empresas.grupo-inicios[.]com
www.direct-cuentas[.]com
direct-cuentas[.]com
amazon-cuentas[.]com
es-registros[.]com
bancosantander-empresa[.]net
bancosantander-empresas[.]net
supportfbappeal[.]com
banca.grupocajarural-esp[.]com
esp-avisos[.]com
grupocajarural-esp[.]com
cancelar-recibos[.]net
mi-satander[.]com
aviso-laboralkutxa[.]com
movil-abanca[.]online
mi-evobanco[.]com
dispositivo-triodos[.]com
micorreo-aviso[.]com
mi-kutxabank[.]com
cornerbanks-ch[.]com
www-banca-sabadell[.]com
laboraikutxa-web[.]com
mi-caixabanca[.]com
www-laboraikutxa[.]com
mi-sabadell[.]com

usuario-e[.]com
banca-laboraikutxa[.]com
f-fb-watch[.]com
mibanca-bankinter[.]com
banca-arquia[.]com
banca-deutsche[.]com
mi-bankinter[.]com
mi-laboraikutxa[.]com
mi-laboralkutxa[.]com
opensbank[.]com
aviso-bbva[.]com
seguridad-eurocaja[.]com
seguridad-mi-abanca[.]com
laboraikuxta-usuarios[.]com
micorreo-notificacion[.]com
seguridad-mibbva[.]com
abanca-usuario[.]com
eligecamino[.]com
laboraikutxa-usuario[.]com
laborakutxa-usuario[.]com
www-bancasabadell[.]com
bancasantander-es-empresa[.]com
bancasantander-empresa-es[.]com
mi-abanca[.]com
bancaminos[.]com
bancasantander-empresa[.]com
micorreos-notificacion[.]com
bankinter-banca[.]com
antifraudes-es[.]com
bancasantander-app[.]com

bancasantander-empresas[.]com
tuscaminos[.]com
targobank-verificacion[.]com
bankinter-ingreso[.]com
bancaminos.tuscaminos[.]com
cajamar-verificacion[.]com
bbva-seguridad-es[.]com
bbva-atencion-cliente[.]com
targobank-verificaciones[.]com
caixaeginyers[.]com
tuscamino[.]com
cancelacion-transferencias[.]net
es-entra[.]online
mioficina-es[.]com
laboralkutxa.es-users[.]com
es-users[.]com
laboralkutxa.es-usuarios[.]online
es-usuarios[.]online
hanseaticsbank-da[.]com
es-html[.]com
es-iniciar[.]online
es-particular-es[.]com
incidencia-404[.]com
www.incidencia-404[.]com
bancaminos-es[.]online
bbvaempresa-es[.]com
es-enter[.]com
www.es-enter[.]com
bancsabadell-esp[.]com
ing.home-html[.]com

home-html[.]com
hanseaticbank[.]su
uk-lives[.]su
es-saldo[.]su
es-funciones[.]su
es-lives[.]su
es-live[.]su
es-funcion[.]su
au-lives[.]su
bancamarch.es-acceso[.]su
es-acceso[.]su
bancobbva.es-online[.]su
es-online[.]su
arquiabanca.es-accesos[.]su
es-accesos[.]su
es-actualizacion[.]su
bbvacuentaonline[.]su
caixaenginyers.es-cuentas[.]su
es-cuentas[.]su
es-cuenta[.]su
deutschbank.es-infos[.]su
bancosantander.es-web[.]su
es-web[.]su
es-infos[.]su
es-clientes[.]su
openbank.es-clientes[.]su
unicajabanco.es-info[.]su
es-info[.]su
liberbanconet[.]club
renta4banconet[.]club

liberbanksnet[.]club
renta4banconets[.]club
r4banconet[.]club
liberbankis[.]club
libersbanknets[.]club
etherscamorg[.]club
liberbanknets[.]club
liberbankes[.]club
liberbankiorg[.]club
liberbankorg[.]club
andbank[.]club
z-sms[.]online
binacenow[.]com
binacefull[.]net
binaceeasy[.]com
binacecoin[.]net
binacefull[.]biz
dg.esmas[.]online

APK Maliciosas

sha-256
402544C3C74924C7A9F355108F474FD3B0D643A38ABA45C933D880B1C2A206DE
E65C24D6E5F883CA02F79EDC0BD4FDBD28DC130F11FDBCA75B7FD26B2587BFA4
B1B0EB10002669BE6B32792A196227F1D595E26B0039E719EF9357E2B8F5361B
944F0568CE0394B4DB3FD618D6F1A0C53F94712F91FA162A4F28B1F93AD9F18F
2826A1C5ED1456BA00421FFDD4E331C691B39FC0334F4590EB860C38452D606B
9C718529F37A6C3EA0B128A8C15A1D1950BB350A9B5039C770651B8B73393007
E047F13914278AD4E5CC63D30CFDAC56CF20F86D3A4CF26414001E9AED5F9875
05A5CF0D0EB2A224D0326F2AC95A2D60CA9935D015070ED17439C2DD7A79D50C
AE2976F99876605DF0E043AC62081AF43426286EC5759DC3ECA080E26CB16B97

Número de serie del certificado de firma del APK
45ff9a3

Certificado de firma SHA256 del APK
492682F877607EE99DF2DDD2BD5953FD727BDF6E19D397DE9DBBAFD582BCAD75