Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°191	Fecha: 15-08-2023
		Página: 4 de 15

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Gigabud RAT, Malware Bancario móvil, se dirige a instituciones en varios países, incluido Perú		
Tipo de Ataque	Troyanos	Abreviatura	Troyanos
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

Los titulares de cuentas de numerosas instituciones financieras en Tailandia, Indonesia, Vietnam, Filipinas y Perú están siendo atacados por un malware bancario para Android llamado Gigabud RAT.

Troyano RAT.- Un troyano de acceso remoto (o RAT, del inglés Remote Access Trojan) es una herramienta que los desarrolladores de malware usan para obtener acceso total y controlar remotamente el sistema de un usuario, incluyendo su teclado y mouse, accediendo a sus archivos y recursos de red. En vez de destruir archivos o robar datos, un RAT les brinda a los atacantes el control total de un dispositivo móvil o de sobremesa, de modo de que puedan explorar furtivamente las aplicaciones y archivos; esto lo hace evadiendo las medidas de seguridad normales, como cortafuegos, sistemas de detección de intrusiones y controles de autenticación.

Los RAT suelen incluir otros malware para ayudar a los atacantes a lograr sus objetivos. Por ejemplo, un keylogger, el cual se ejecuta furtivamente en segundo plano, registrando las pulsaciones de teclas del usuario, y obteniendo sus credenciales. Con las credenciales adecuadas, un atacante puede obtener datos financieros, propiedad intelectual o elevar sus privilegios en la red para controlar remotamente otros dispositivos en una red corporativa.

2. DETALLES:

"Una de las características únicas de Gigabud RAT es que no ejecuta ninguna acción maliciosa hasta que un estafador autorice al usuario en la aplicación maliciosa, lo que hace que sea más difícil de detectar", dijeron los investigadores del Grupo-IB, Pavel Naumov y Artem Grischenko.

Durante la investigación, se descubrió que el certificado utilizado para firmar esta aplicación maliciosa se encontró en más de 50 muestras maliciosas similares que usan el mismo código fuente. El malware se disfraza utilizando los íconos de las agencias gubernamentales de estos países, así como también bancos, empresas de TI, aerolíneas, como las siguientes:

- Banco de Comercio - Banco de Perú.
- Thai Lion Air – Aerolínea de Tailandia.
- Shopee - E-commerce de Singapur.
- SUNAT – Superintendencia Nacional de Aduanas y de Administración Tributaria de Perú.
- DSI - Departamento de Investigaciones Especiales de Tailandia.
- BIR - Oficina de Impuestos Internos de Filipinas.
- Kasikornbank - Entidad financiera de Tailandia.

Íconos de agencias gubernamentales y bancos utilizados por el malware

La característica definitoria de Gigabud es su enfoque cauteloso para ejecutar acciones maliciosas.

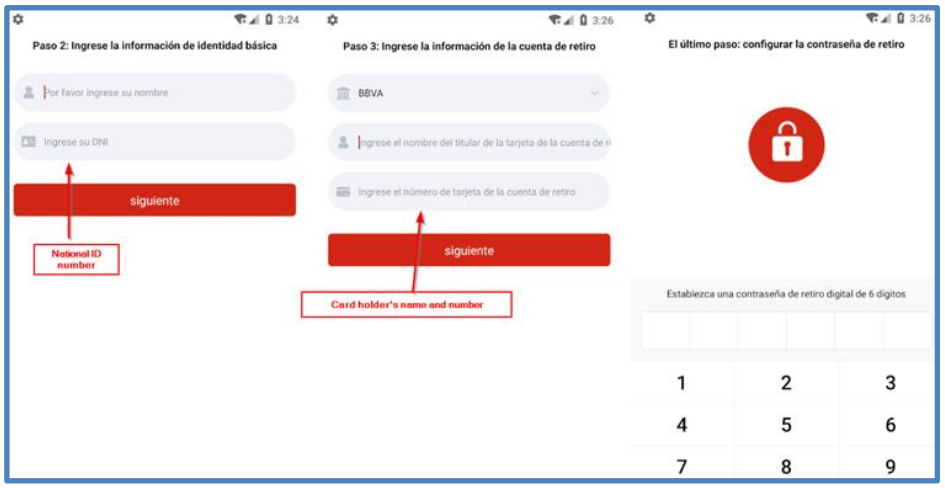
A diferencia del malware convencional que actúa inmediatamente después de la infiltración, Gigabud espera la autorización del usuario dentro de la aplicación maliciosa, una estrategia que lo hace notablemente esquivo. En lugar de confiar en los ataques de superposición de HTML, Gigabud emplea la grabación de pantalla para recopilar información confidencial, lo que complica aún más su detección.

Una característica destacada de Gigabud es su uso de servicios de accesibilidad, lo que le permite realizar acciones en el dispositivo de la víctima de forma remota. Esta capacidad, conocida como "TouchAction", permite al atacante realizar gestos en el dispositivo del usuario, dándole el poder de evadir los mecanismos de defensa, incluida la autenticación de dos factores (2FA).

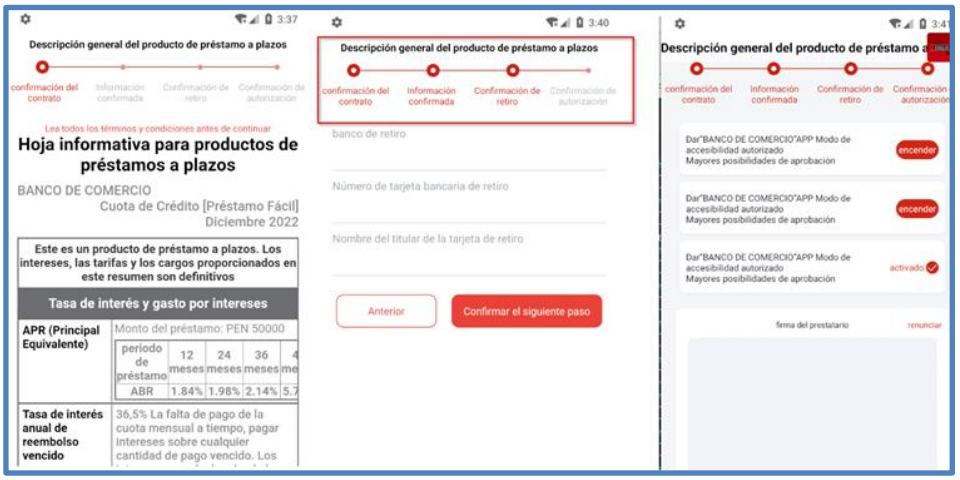
También se identificó una segunda variante del malware sin las capacidades RAT, apodado Gigabud.Loan. Éste se presenta bajo la apariencia de una solicitud de préstamo que es capaz de filtrar los datos ingresados por el usuario.

"Los objetivos eran individuos atraídos a completar un formulario de solicitud de tarjeta bancaria para obtener un préstamo a bajo interés", dijeron los investigadores. "Se convence a las víctimas de proporcionar información personal durante el proceso de solicitud".

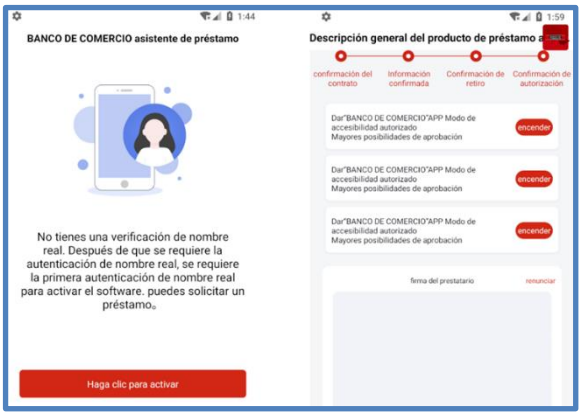
Durante el registro, el malware solicita a la víctima que proporcione su nombre y número de identificación y también les permite seleccionar el nombre de un banco de una lista recibida del servidor Command-and-Control con el nombre y el número del titular de la tarjeta.



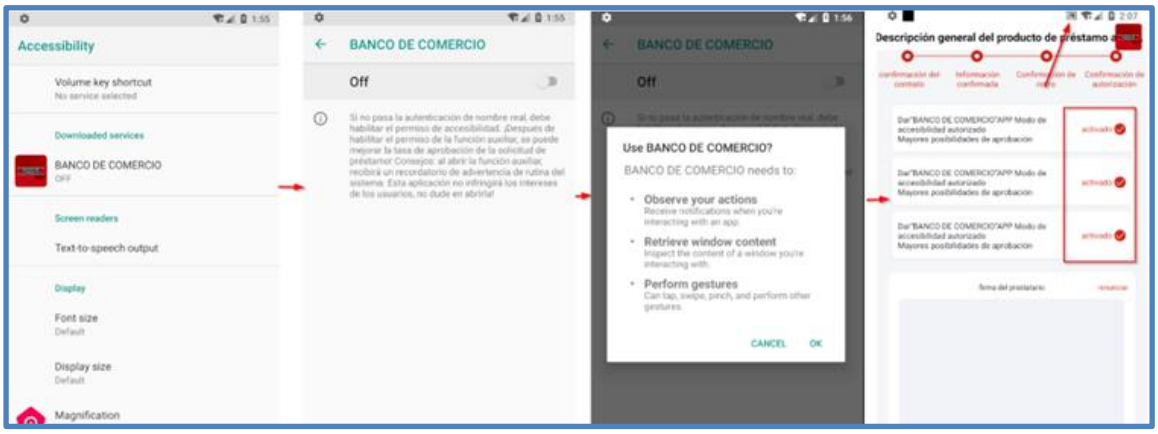
Una vez que se completa el registro o el inicio de sesión, el malware muestra un contrato de préstamo falso recibido del servidor y luego solicita a la víctima que confirme su información.



El malware no muestra ninguna actividad maliciosa hasta la etapa final, donde presenta una página de "Autenticación de nombre real" y solicita a la víctima que presione el botón "Hacer clic para activar" para solicitar un préstamo. Una vez que se hace clic en el botón, el malware solicita a la víctima que otorgue permisos de accesibilidad, incluido el permiso para la grabación de pantalla y la superposición de pantalla.



Después de que la víctima otorga el permiso de accesibilidad, el malware comienza a explotarlo al habilitar automáticamente la función de grabación de pantalla. Además, el malware solicita permiso para mostrarse sobre otras aplicaciones.



Ambas versiones de malware se propagan a través de sitios web de phishing, cuyos enlaces se entregan a las víctimas a través de SMS o mensajes instantáneos en las redes sociales. Gigabud.Loan también se distribuye directamente en forma de archivos APK enviados a través de mensajes en WhatsApp.

Los objetivos a los que se contacta en las redes sociales a menudo se ven obligados a visitar los sitios con el pretexto de completar una auditoría fiscal y reclamar un reembolso.

En el transcurso de 2022 a 2023, los investigadores de Group-IB detectaron más de 400 muestras Gigabud RAT y más de 20 muestras Gigabud.Loan utilizando técnicas de caza avanzadas.

3. RECOMENDACIONES:

- Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.
- Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecuten en ellos.
- Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.
- Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.
- No abrir correos electrónicos de dudosa procedencia (remitente desconocido), ni dar clic en enlaces, ni descargar archivos adjuntos desconocidos.
- Informar a los encargados de seguridad de la información de su institución en caso se detecte cualquier actividad anómala en su equipo.

Fuente de Información:	• hxxps://thehackernews.com/2023/08/gigabud-rat-android-banking-malware.html • hxxps://www.securesoftcorp.com/es/w/novedades/ss_alerta054 • hxxps://www.hackread.com/gigabud-financial-android-malware-bypass-2fa/ • hxxps://cyble.com/blog/gigabud-rat-new-android-rat-masquerading-as-government-agencies/