BOLETÍN DE ALERTA

Boletín Nro.: 2020-33

Fecha de publicación: 13/11/2020

Tema: Troyano bancario en Android llamado “Ghimob” dirigido a aplicaciones financieras, afecta a Paraguay.

Descripción:

Investigadores de seguridad han descubierto recientemente un nuevo **troyano bancario en Android**, llamado “Ghimob” dirigido a **aplicaciones financieras** de bancos que operan en países como **Brasil, Paraguay, Perú, Portugal, Alemania, Angola y Mozambique**.

Este troyano fue denominado por los investigadores como un “espía completamente desarrollado en tu bolsillo” que puede ser accedido remotamente por los operadores. Además, cuenta con características que permite a los ciberdelincuentes **eludir las medidas antifraude y de seguridad implementadas por las instituciones financieras**, con el objetivo de **realizar transacciones fraudulentas** desde el dispositivo móvil de la víctima.

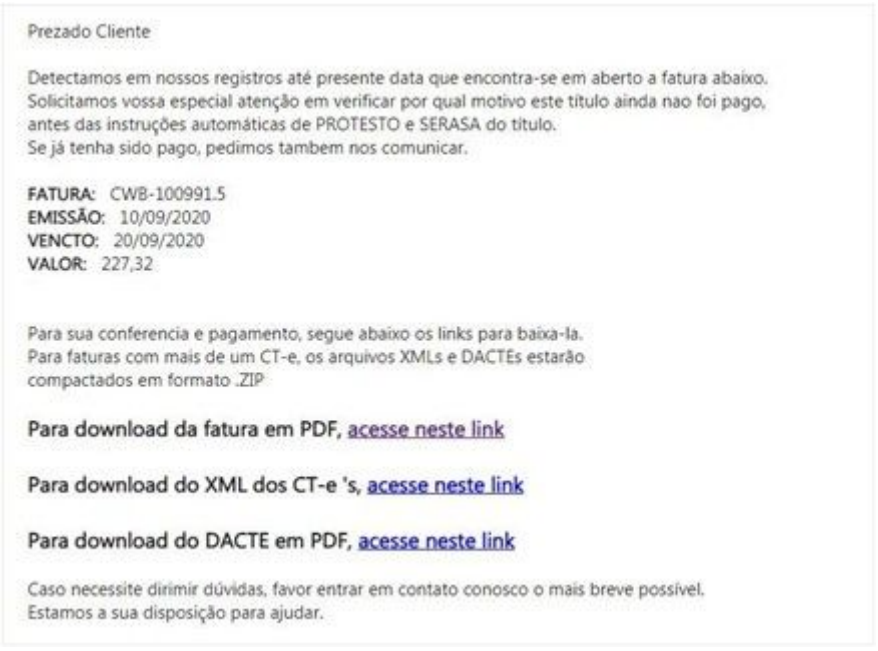
¿Cómo infecta a sus víctimas?

Primeramente, los ciberdelincuentes engañan a la potencial víctima mediante **técnicas de ingeniería social** para que la misma instale un archivo malicioso enviado a través de un correo electrónico phishing.

En los ejemplos vistos, un supuesto acreedor envía el correo electrónico donde proporciona un enlace para que la víctima pueda ver “**más información**”. Sin embargo, dicho enlace redirige a una aplicación que pretende ser una **herramienta legítima como Google Defender, Google Docs o WhatsApp Updater**; que en realidad se trata del **instalador APK de Ghimob**.

Existe una alerta mundial sobre este malware ya que el mismo se está propagando en muchos países y también en latinoamérica. En el caso de Paraguay, hasta el

momento Ghimob tiene en su mira **dos aplicaciones bancarias**, según las investigaciones realizadas.



Prezado Cliente

Detectamos em nossos registros até presente data que encontra-se em aberto a fatura abaixo.
Solicitamos vossa especial atenção em verificar por qual motivo este titulo ainda nao foi pago,
antes das instruções automáticas de PROTESTO e SERASA do titulo.
Se já tenha sido pago, pedimos tambem nos comunicar.

FATURA: CWB-100991.5
EMISSÃO: 10/09/2020
VENCTO: 20/09/2020
VALOR: 227,32

Para sua conferencia e pagamento, segue abaixo os links para baixa-la.
Para faturas com mais de um CT-e, os arquivos XMLs e DACTEs estarão
compactados em formato .ZIP

Para download da fatura em PDF, acesse neste link

Para download do XML dos CT-e 's, acesse neste link

Para download do DACTE em PDF, acesse neste link

Caso necessite dirimir dúvidas, favor entrar em contato conosco o mais breve possível.
Estamos a sua disposição para ajudar.

Figura: Correo malicioso utilizado para la distribución del malware, en portugués

Una vez que el malware es instalado en el dispositivo de la víctima, el delincuente toma el control del dispositivo de la víctima de forma remota, lo primero que realiza es intentar detectar cualquier posible **emulador** o **depurador** y en caso de encontrarlo el **malware se termina**. Caso contrario, el malware envía un mensaje al **servidor C2C (Command & Control)** con los datos del dispositivo de la víctima, que incluyen el modelo del dispositivo, si tiene el bloqueo de pantalla activado o no y la lista de todas las aplicaciones específicas de interés instaladas en el dispositivo (con las versiones incluidas).

Ghimob cuenta con capacidades de **grabación de pantalla**, permitiéndole grabar cuando la víctima ingresa su **patrón de bloqueo de pantalla** para repetirlo más tarde y **desbloquear el dispositivo**. También tiene la capacidad de **impedir** que el usuario víctima **desinstale el malware** y **reinicie o apague el dispositivo**.

Cuando el usuario-agente hace clic en el enlace malicioso desde un navegador para Android, se descarga el archivo APK que instala Ghimob, que se presenta como instalador de aplicación conocido o legítimo, sin embargo, no se encuentra alojado en Google Play Store, sino que se aloja en varios dominios maliciosos. Una vez que el dispositivo se infecta, la aplicación maliciosa toma provecho del **Modo de Accesibilidad** de Android para obtener persistencia y deshabilitar la desinstalación manual permitiendo así al malware capturar pulsaciones del teclado, manipular el contenido de la pantalla y proporcionar al ciberdelincuente un control remoto total del dispositivo.

Durante un ataque, el ciberdelincuente utiliza una **técnica común en otros troyanos bancarios móviles** de **Android** para evitar la detección, en donde inserta una **pantalla negra** en el dispositivo o abre una página web en pantalla completa, con el fin de que, mientras que el usuario visualiza la pantalla superpuesta, el ciberdelincuente en segundo plano lleve a cabo el ataque realizando una transacción ilícita en una aplicación financiera abierta o activada en el dispositivo de la víctima.

Impacto:

Una infección exitosa permitiría a un ciberdelincuente contar un control remoto total del dispositivo infectado, obtener información confidencial y realizar transacciones fraudulentas en nombre de la víctima.

Recomendaciones:

En usuarios de dispositivos móviles

- No ingresar a enlaces sospechosos enviados a través de correo electrónico o redes sociales.
- Algunos aspectos a tener en cuenta para identificar un dispositivo móvil infectado:
    - En general, un mal funcionamiento del dispositivo de forma lenta o anormal,

  - Las aplicaciones se bloquean o no funcionan de manera correcta o en algunos casos no pueden iniciarse,
  - Un aumento inusual del consumo de datos y de batería y
  - La presencia de una gran cantidad de anuncios.
- En caso de una infección o sospecha, se recomienda contar con una **solución de seguridad** que permita realizar análisis de malware en el dispositivo y eliminarlo del sistema. De no solucionarse el problema se puede **restaurar el dispositivo a los valores de fábrica** (borrado completo de los datos), en este caso es importante contar con una copia de seguridad o backup de datos importantes del dispositivo.
- Prestar atención antes de descargar cualquier archivo, o programa de internet y asegurarse de que estos provengan de fuentes confiables (páginas web o tiendas oficiales).
- Mantener actualizado el dispositivo a la última versión disponible en las tiendas oficiales, para evitar que delincuentes aprovechen posibles vulnerabilidades ya abordadas en parches de seguridad lanzados por los fabricantes.

En instituciones financieras

- Estar alertas ante estas amenazas y mejorar los procesos de autenticación, tecnologías anti-fraude e inteligencia de datos de amenazas,
- Mitigar todos los riesgos asociados con esta nueva familia de troyanos de acceso remoto móviles.

Información adicional:

- https://securelist.lat/ghimob-tetrade-threat-mobile-devices/91704/
- https://thehackernews.com/2020/11/watch-out-new-android-banking-trojan.html
- https://threatpost.com/ghimob-android-banking-trojan/161075/