Se descubrió que un troyano de acceso remoto (RAT) basado en Android previamente indocumentado, utiliza funciones de grabación de pantalla para robar información confidencial en el dispositivo, incluyendo credenciales bancarias y así abrir una puerta al fraude en el dispositivo.

Apodado como Vultur debido a su uso de la tecnología de uso compartido de pantalla remota de Virtual Network Computing (VNC) para obtener una visibilidad de los usuarios específicos, el malware móvil se distribuyó a través de la tienda oficial de Google Play y se hizo pasar por una aplicación llamada *«Protection Guard»*, atrayendo a más de 5000 instalaciones. Las aplicaciones bancarias y de criptomonedas de entidades ubicadas en Italia, Australia y España fueron los principales objetivos.

> *«Por primera vez estamos viendo un troyano bancario Android que tiene la grabación de pantalla y el keylogging como la estrategia principal para recolectar credenciales de inicio de sesión de una forma automatizada y escalable»,* dijeron los investigadores de ThreatFabric.
>
> *«Los actores optaron por alejarse del desarrollo de superposición HTML común que por lo genera se ve en otros troyanos bancarios de Android: este enfoque generalmente requiere una mayor inversión de tiempo y esfuerzo por parte de los actores para crear múltiples superposiciones capaces de engañar al usuario. En su lugar, optaron por simplemente registrar lo que se muestre en la pantalla, obteniendo efectivamente el mismo resultado final»,* agregaron.

Mientras que el malware bancario como MysteryBot, Grandoreiro, Banker.BR y Vizom se han basado por tradición en ataques de superposición, es decir, creando una versión falsa de la página de inicio de sesión del banco y superponiéndola sobre la aplicación legítima, con el fin de engañar a las víctimas para que revelen sus contraseñas y otra información privada, se está acumulando evidencia de que los actores de amenazas se están alejando de dicho enfoque.

En un informe publicado a inicios de esta semana, la compañía italiana de seguridad cibernética Cleafy, descubrió UBEL, una variante actualizada de Oscorp, que se observó utilizando WebRTC para interactuar con el teléfono Android comprometido en tiempo real.

Vultur adopta una táctica similar en el sentido de que aprovecha los permisos de accesibilidad para capturar las pulsaciones de teclas y aprovecha la función de grabación de pantalla de VNC para registrar de forma sigilosa todas las actividades en el teléfono, obviando así la necesidad de registrar un nuevo dispositivo y dificultando que los bancos detecten el fraude.

Además, el malware emplea ngrok, una utilidad multiplataforma que se utiliza para exponer servidores locales detrás de NAT y cortafuegos a la Internet pública a través de túneles seguros, para proporcionar acceso remoto al servidor VNC que se ejecuta localmente en el teléfono.

Además, también establece conexiones con un servidor de comando y control (C2) para recibir comandos a través de Firebase Cloud Messaging (FCM), cuyos resultados, incluidos los datos extraídos y las capturas de pantalla, se transmiten al servidor.

La investigación de ThreatFabric también conectó a Vultur con otra conocida pieza de software malicioso llamada Brunhilda, un cuentagotas que utiliza Play Store para distribuir distintos tipos de malware en lo que se llama una operación de *«cuentagotas como servicio»* (DaaS), citando superposiciones en el código fuente y la infraestructura C2 utilizada para facilitar los ataques.

Estos vínculos, dijo la compañía de servicios de seguridad cibernética con sede en Ámsterdam, indican que Brunhilda es un actor de amenazas de operación privada que tiene su propio cuentagotas y RAT Vultur patentado.

> *«La historia de Vultur muestra una vez más cómo los actores pasan de utilizar troyanos alquilados (MaaS) que se venden en los mercados clandestinos a malware*

> *patentado/privado adaptado a las necesidades de este grupo. Estos ataques son escalables y automatizados, ya que las acciones para realizar fraudes pueden programarse en el backend del malware y enviarse en forma de secuencia de comandos, lo que facilita que los actores se ejecuten»*, dijeron los investigadores.