Investigadores en ciberseguridad han descubierto que actores maliciosos están creando sitios web engañosos, alojados en dominios recién registrados, con el fin de propagar un malware conocido para Android llamado SpyNote.

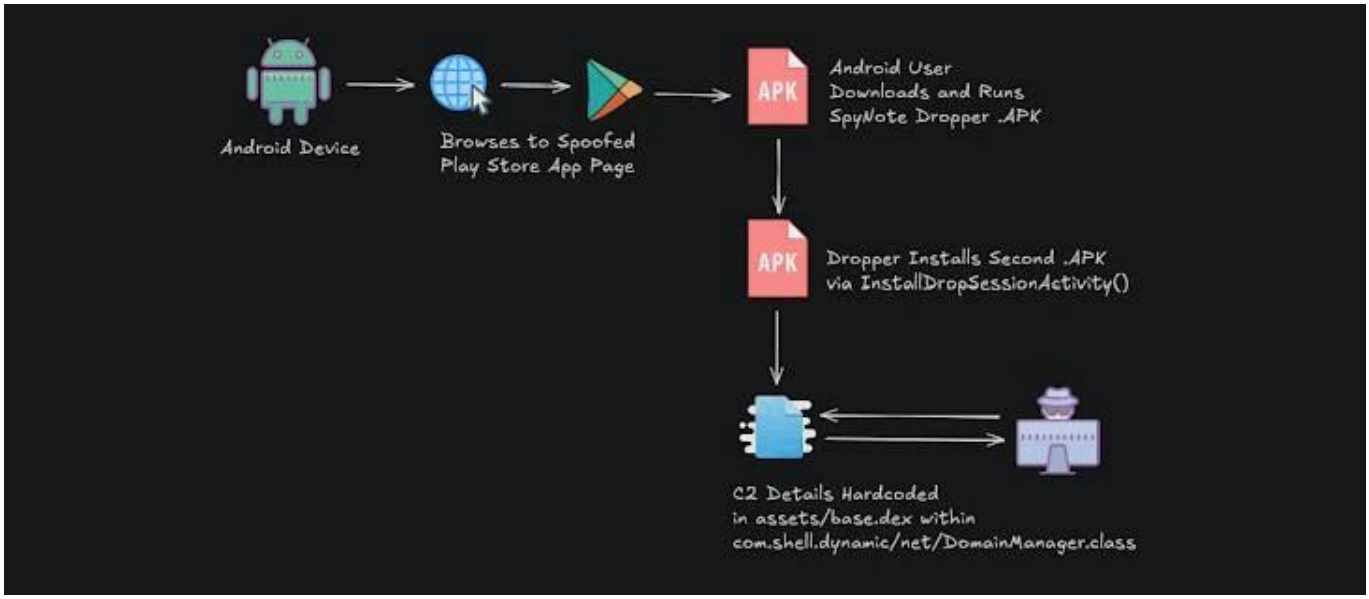
Estos sitios falsos imitan páginas de instalación de la Google Play Store, presentándose como descargas de aplicaciones populares como el navegador Chrome, con el objetivo de engañar a los usuarios y hacer que instalen el malware sin darse cuenta.

Según un informe del equipo de DomainTools Investigations (DTI), los atacantes han utilizado una combinación de sitios en inglés y en chino, y han incluido comentarios en chino tanto en el código del sitio como en el del malware.

SpyNote (también conocido como SpyMax) es un troyano de acceso remoto (RAT), que se aprovecha de los servicios de accesibilidad de Android para robar datos sensibles de los dispositivos infectados. En mayo de 2024, este malware también fue distribuido a través de un sitio falso que se hacía pasar por el antivirus Avast.

Un análisis posterior de la firma de seguridad móvil Zimperium reveló similitudes entre SpyNote y otro malware llamado Gigabud, lo que sugiere que podrían haber sido desarrollados por los mismos atacantes. Se cree que Gigabud está vinculado a un grupo de habla china llamado GoldFactory.

Además, se ha detectado que SpyNote ha sido utilizado por grupos de hackers patrocinados por estados, como OilAlpha, y otros actores no identificados.



Los sitios falsificados descubiertos por DTI contienen una galería de imágenes que, al hacer clic, descargan un archivo APK malicioso en el dispositivo del usuario. Este archivo actúa como instalador para introducir una segunda aplicación maliciosa, que se activa al interactuar con una ventana emergente.

Una vez instalado, el malware solicita numerosos permisos invasivos para obtener un control total del dispositivo comprometido, permitiéndole robar mensajes SMS, contactos, registros de llamadas, ubicación, archivos, y activar remotamente la cámara, el micrófono, manipular llamadas y ejecutar comandos.

El informe coincide con una advertencia de la empresa Lookout, que reportó más de 4 millones de ataques de ingeniería social enfocados en móviles en 2024, incluyendo 427,000 apps maliciosas en dispositivos empresariales y 1.6 millones de aplicaciones vulnerables detectadas.

Lookout también informó que, en los últimos cinco años, los usuarios de iOS han sido más atacados por campañas de phishing que los de Android, y que en 2024 los dispositivos iOS fueron atacados más del doble que los Android.

Advertencia Global sobre los Malware BadBazaar y MOONSHINE

Por otro lado, agencias de inteligencia de Australia, Canadá, Alemania, Nueva Zelanda, Reino Unido y Estados Unidos emitieron una advertencia conjunta sobre el uso de los malware BadBazaar y MOONSHINE para atacar a comunidades uigur, taiwanesa y tibetana.

Los objetivos de estos ataques incluyen ONG, periodistas, empresas y miembros de la sociedad civil vinculados con estas comunidades. Las agencias alertaron que el uso indiscriminado de estos programas espía podría afectar incluso a personas fuera de los objetivos previstos.

Tanto BadBazaar como MOONSHINE son troyanos capaces de recolectar datos sensibles en dispositivos Android e iOS, como ubicación, mensajes, fotos y archivos. Estos se distribuyen comúnmente disfrazados como apps de mensajería, utilidades o religiosas.

BadBazaar fue documentado por primera vez en 2022 por Lookout, aunque se sospecha que ha estado activo desde 2018. MOONSHINE, por su parte, ha sido utilizado por un grupo identificado como Earth Minotaur para vigilar durante largo tiempo a tibetanos y uigures.

El uso de BadBazaar ha sido vinculado a un grupo de hackers chinos conocido como APT15, también llamado Flea, Nickel, Royal APT, entre otros nombres.

Aunque la versión para iOS de BadBazaar tiene capacidades más limitadas que la de Android, aún puede extraer datos personales del dispositivo, según Lookout. Se cree que esta variante se dirigía principalmente a la comunidad tibetana dentro de China.

Los datos recolectados por MOONSHINE son enviados a una infraestructura controlada por los atacantes, gestionada a través de un panel llamado SCOTCH ADMIN, que muestra información de los dispositivos infectados. En enero de 2024, se registraron 635 dispositivos comprometidos en tres de estos paneles.

Como hecho relacionado, las autoridades suecas arrestaron a Dilshat Reshit, un ciudadano

uigur residente en Estocolmo, bajo sospecha de espiar a otros miembros de la comunidad uigur en el país. Reshit ha sido portavoz en chino del Congreso Mundial Uigur desde 2004.