Se ha descubierto una nueva versión de un sofisticado spyware para Android llamado Mandrake en cinco aplicaciones que estaban disponibles para su descarga en Google Play Store y que permanecieron sin ser detectadas durante dos años.

Kaspersky informó el lunes que las aplicaciones acumularon más de 32,000 instalaciones antes de ser eliminadas de la tienda de aplicaciones. La mayoría de las descargas provino de Canadá, Alemania, Italia, México, España, Perú y el Reino Unido.

> *«Las nuevas muestras incluyeron capas adicionales de ofuscación y técnicas de evasión, como trasladar la funcionalidad maliciosa a bibliotecas nativas ofuscadas, usar fijación de certificados para las comunicaciones de C2 y realizar diversas pruebas para comprobar si Mandrake se ejecutaba en un dispositivo rooteado o en un entorno emulado»*, explicaron los investigadores Tatyana Shishkova e Igor Golovin.

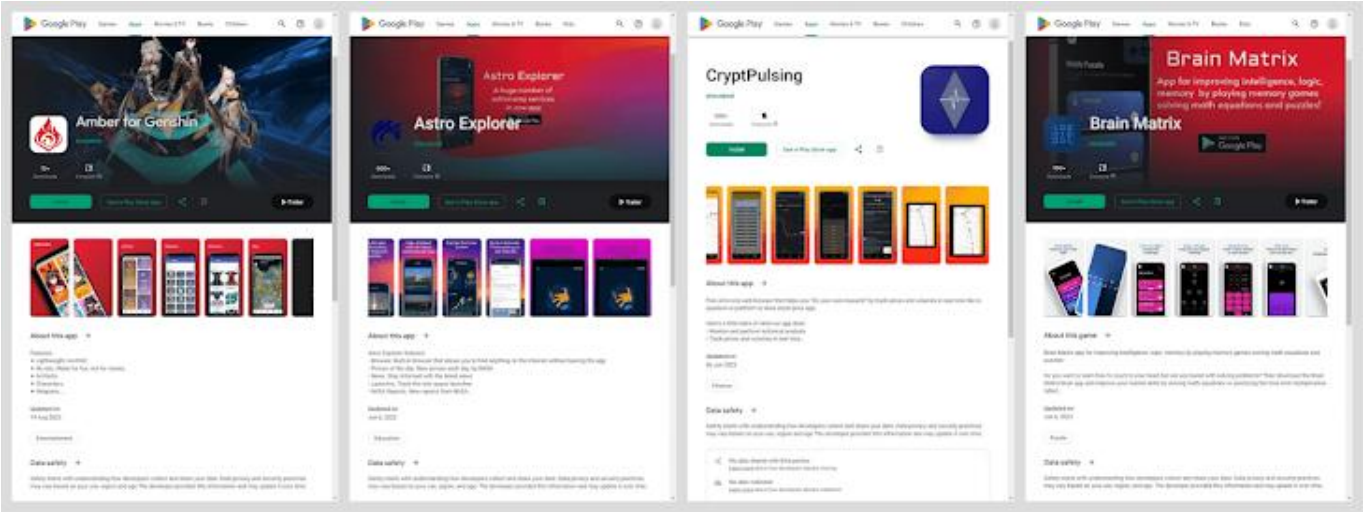
Mandrake fue documentado por primera vez por el proveedor rumano de ciberseguridad Bitdefender en mayo de 2020, describiendo su enfoque deliberado para infectar un número reducido de dispositivos mientras se mantenía oculto desde 2016.

Las variantes actualizadas se caracterizan por el uso de OLLVM para esconder la funcionalidad principal, además de incorporar una serie de técnicas para evadir la detección y el análisis en entornos controlados por analistas de malware.

La lista de aplicaciones que contienen Mandrake es la siguiente:

- AirFS (com.airft.ftrnsfr)
- Amber (com.shrp.sght)
- Astro Explorer (com.astro.dscvr)
- Brain Matrix (com.brnmth.mtrx)
- CryptoPulsing (com.cryptopulsing.browser)

Las aplicaciones se estructuran en tres etapas: Un dropper que inicia un cargador responsable de ejecutar el componente principal del malware después de descargarlo y desencriptarlo desde un servidor de comando y control (C2).



La carga útil de la segunda etapa también puede recopilar información sobre el estado de conectividad del dispositivo, aplicaciones instaladas, porcentaje de batería, dirección IP externa y la versión actual de Google Play. Además, puede eliminar el módulo principal y solicitar permisos para dibujar superposiciones y ejecutarse en segundo plano.

La tercera etapa permite comandos adicionales para cargar una URL específica en un WebView, iniciar una sesión de compartición de pantalla remota y grabar la pantalla del dispositivo con el objetivo de robar las credenciales de las víctimas y descargar más malware.

> *«Android 13 introdujo la función 'Ajustes Restringidos', que prohíbe a las aplicaciones sideloaded solicitar directamente permisos peligrosos. Para eludir esta función, Mandrake gestiona la instalación con un instalador de paquetes 'basado en sesión'»*, dijeron los investigadores.

La empresa de seguridad rusa describió a Mandrake como un ejemplo de una amenaza en constante evolución que está refinando continuamente sus técnicas para evadir los mecanismos de defensa y evitar la detección.

> *«Esto destaca las formidables habilidades de los actores de amenazas, y también que controles más estrictos para las aplicaciones antes de ser publicadas en los mercados solo resultan en amenazas más sofisticadas y difíciles de detectar que se infiltran en los mercados de aplicaciones oficiales»,* dijo la empresa.

Cuando se le pidió un comentario, Google dijo que está reforzando continuamente las defensas de Google Play Protect a medida que se identifican nuevas aplicaciones maliciosas y que está mejorando sus capacidades para incluir detección de amenazas en tiempo real para abordar técnicas de ofuscación y evasión.

> *«Los usuarios de Android están protegidos automáticamente contra versiones conocidas de este malware por Google Play Protect, que está activado por defecto en dispositivos Android con Google Play Services. Google Play Protect puede advertir a los usuarios o bloquear aplicaciones que se sabe que exhiben un comportamiento malicioso, incluso cuando esas aplicaciones provienen de fuentes externas a Play»,* dijo un portavoz de Google.