Investigadores de seguridad cibernética han descubierto un nuevo programa de robo de información dirigido a los sistemas Apple macOS que está diseñado para establecer una presencia continua en los dispositivos infectados y funcionar como un programa espía.

Apodado Cuckoo por Kandji, el malware es un binario Mach-O universal capaz de ejecutarse tanto en Macs con procesadores Intel como en aquellos basados en Arm.

Actualmente, no está claro el método exacto de distribución, aunque hay indicios de que el binario se encuentra alojado en sitios como dumpmedia[.]com, tunesolo[.]com, fonedog[.]com, tunesfun[.]com y tunefab[.]com, los cuales afirman ofrecer versiones gratuitas y de pago de aplicaciones dedicadas a extraer música de servicios de streaming y convertirla a formato MP3.

El archivo de imagen de disco descargado desde estos sitios web es responsable de ejecutar un shell de bash para recopilar información del dispositivo y asegurarse de que la máquina comprometida no se encuentre en Armenia, Bielorrusia, Kazajistán, Rusia o Ucrania. El binario malicioso solo se ejecuta si la verificación de la ubicación es exitosa.

Además, establece una presencia continua mediante un LaunchAgent, una técnica previamente utilizada por diferentes familias de malware como RustBucket, XLoader, JaskaGO y un backdoor de macOS que comparte características con ZuRu.

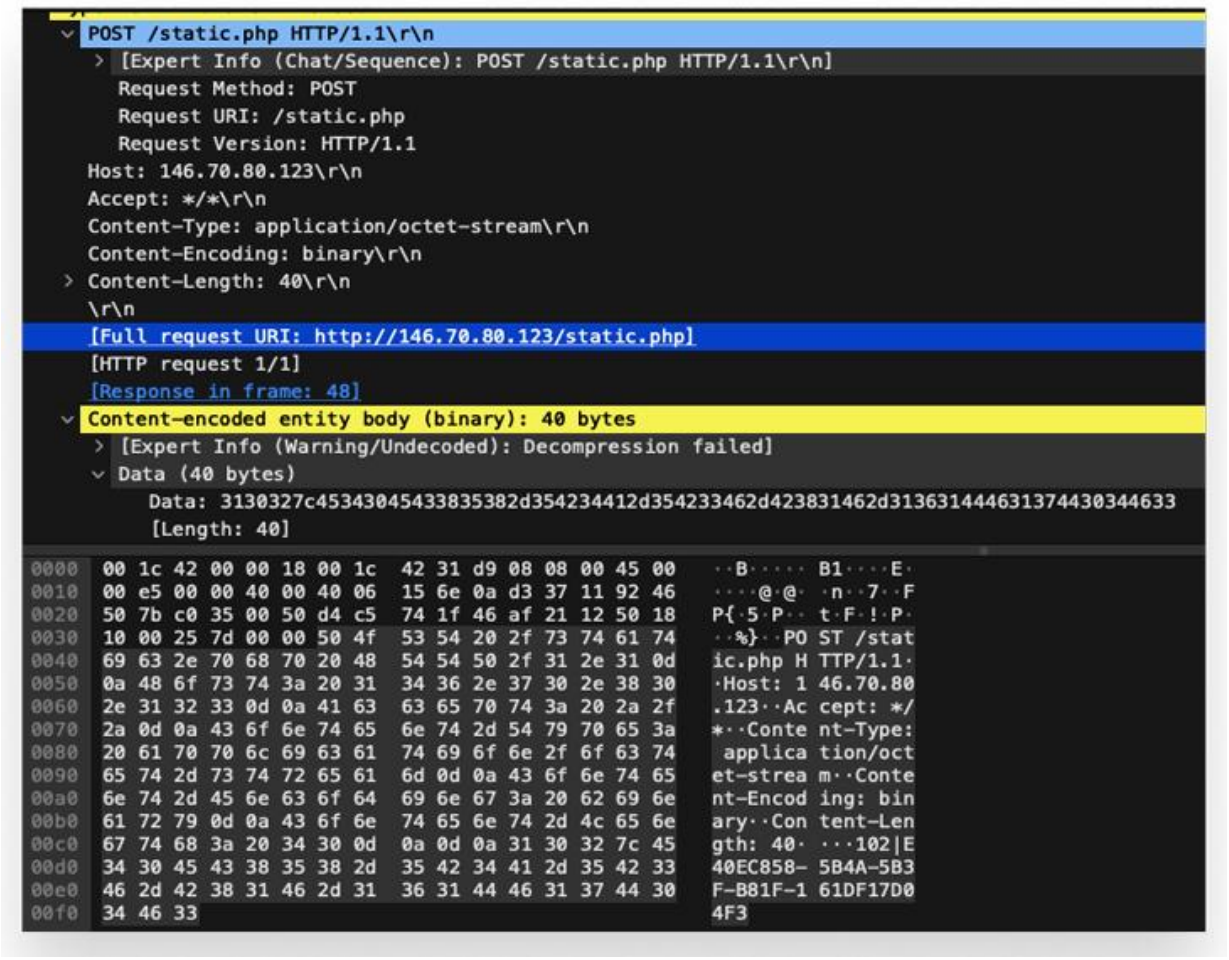
Al igual que el malware MacStealer macOS, Cuckoo también utiliza osascript para mostrar un falso cuadro de diálogo de contraseña y engañar a los usuarios para que ingresen las contraseñas de sus sistemas y obtener así privilegios de administrador.

> *«Este malware busca archivos específicos asociados con aplicaciones particulares, con el objetivo de recopilar la mayor cantidad posible de información del sistema»,* señalaron los investigadores Adam Kohler y Christopher Lopez.

Está equipado para ejecutar una serie de comandos que extraen información del hardware,

capturan los procesos en ejecución, buscan aplicaciones instaladas, toman capturas de pantalla y recopilan datos de iCloud Keychain, Notas de Apple, navegadores web, billeteras de criptomonedas y aplicaciones como Discord, FileZilla, Steam y Telegram.

> *«Cada aplicación maliciosa contiene otro paquete de aplicación dentro del directorio de recursos. Todos esos paquetes (excepto los alojados en fonedog[.]com) están firmados y tienen un ID de desarrollador válido de Yian Technology Shenzhen Co., Ltd (VRBJ4VRP)»,* agregaron los investigadores.



> *«El sitio web fonedog[.]com alojaba una herramienta de recuperación de Android, entre otras cosas; el paquete de aplicación adicional en este caso tiene un ID de desarrollador de FoneDog Technology Limited (CUAU2GTG98)».*

La divulgación se produce casi un mes después de que la empresa de gestión de dispositivos Apple también expusiera otro programa de robo de información llamado CloudChat, que se hace pasar por una aplicación de mensajería centrada en la privacidad y es capaz de comprometer a usuarios de macOS cuyas direcciones IP no se ubican en China.

El malware funciona al capturar claves privadas de criptomonedas copiadas al portapapeles y datos asociados con extensiones de billetera instaladas en Google Chrome.

También sigue al descubrimiento de una nueva variante del conocido malware AdLoad escrito en Go llamado Rload (también conocido como Lador), que está diseñado para evadir la lista de firmas de malware Apple XProtect y está compilado únicamente para la arquitectura Intel x86_64.

«Los binarios funcionan como lanzadores iniciales para la carga útil de la siguiente etapa», dijo el investigador de seguridad de SentinelOne, Phil Stokes, en un informe la semana pasada, agregando que los métodos de distribución específicos permanecen actualmente oscuros.

Dicho esto, estos lanzadores suelen estar incrustados típicamente en aplicaciones crackeadas o troyanizadas distribuidas por sitios web maliciosos.

AdLoad, una campaña extendida de adware que afecta a macOS desde al menos 2017, es conocida por manipular los resultados de los motores de búsqueda e inyectar anuncios en páginas web con el fin de obtener ganancias monetarias mediante un proxy web adversario que redirige el tráfico web del usuario a través de la infraestructura del atacante.