Investigadores de Google revelaron este jueves que encontraron un ataque de abrevadero a fines de agosto explotando un sistema operativo de día cero ahora en MacOS y dirigido a sitios web de Hong Kong, relacionados con un medio de comunicación y un prominente grupo político y laboral a favor de la democracia para entregar una backdoor nunca antes vista en máquinas comprometidas.

> *«Según nuestros hallazgos, creemos que este actor de amenazas es un grupo con buenos recursos, probablemente respaldado por el estado, con acceso a su propio equipo de ingeniería de software basado en la calidad del código de carga útil»*, dijo Erye Hernández, investigador del Grupo de Análisis de Amenazas de Google (TAG).

Rastreada como CVE-2021-30869 con puntuación CVSS de 7.8, la vulnerabilidad de seguridad se refiere a un error de confusión de tipos que afecta al componente del kernel XNU y que podría hacer que una aplicación maliciosa ejecute código arbitrario con los privilegios más altos. Apple abordó el problema el 23 de septiembre.

Los ataques observados por TAG involucraron una cadena de exploits que unió CVE-2021-1789, un error de ejecución de código remoto en Webkit que se corrigió en febrero de 2021, y el mencionado CVE-2021-30869 para salir del sandbox de Safari y elevar los privilegios y descargar y ejecutar una carga útil de segunda etapa denominada MACMA desde un servidor remoto.

Este malware previamente indocumentado, un implante con todas las funciones, está marcado por una *«ingeniería de software extensa»* con capacidades para grabar audio y pulsaciones de teclas, tomar huellas dactilares del dispositivo, capturar pantalla, descargar y cargar archivos arbitrarios y ejecutar comandos de terminal maliciosos, dijo Google TAG.

Las muestras de la puerta trasera subidas a VirusTotal revelan que ninguno de los motores anti-malware detecta actualmente los archivos como maliciosos.

Según el investigador de seguridad Patrick Wardle, una variante de 2019 de MACMA se hace

pasar por Adobe Flash Player, y el binario muestra un mensaje de error en el idioma chino luego de la instalación, lo que sugiere que «el malware está dirigido a usuarios chinos y que esta versión del malware está diseñada para implementarse mediante métodos de ingeniería social». La versión 2021, por otro lado, está diseñada para la explotación remota.

Los sitios web que contenía código malicioso para servir exploits desde un servidor controlado por el atacante, también actuaron como un abrevadero para apuntar a los usuarios de iOS, aunque utilizando una cadena de exploits diferente entregada al navegador de las víctimas. Google TAG dijo que solo pudo recuperar una parte del flujo de infección, donde se utilizó un error de confusión de tipos (CVE-2019-8506) para obtener la ejecución de código en Safari.

Se puede acceder aquí a los indicadores de compromiso adicionales (IoC) asociados con la campaña.