Una implementación de Golang de Cobalt Strike llamado Geacon ha estado atrayendo la atención de los hackers que buscan apuntar a los sistemas macOS de Apple.

Según hallazgos de SentinelOne, se observó un aumento en la cantidad de cargas útiles de Geacon que aparecen en VirusTotal en los últimos meses.

> *«Aunque algunas de estas son probablemente operaciones de equipo rojo, otras tienen las características de ataques maliciosos genuinos»*, dijeron en un informe los investigadores de seguridad, Phil Stokes y Dinesh Devadoss.

Cobalt Strike es una conocida herramienta de simulación de equipos rojos y adversarios desarrollada por Fortra. Debido a sus innumerables capacidades, los atacantes han abusado de las versiones hackeadas del software a lo largo de los años.

Aunque la actividad posterior a la explotación asociada con Cobalt Strike se ha centrado principalmente en Windows, dichos ataques contra macOS son raros.

En mayo de 2022, la empresa de cadena de suministro de software Sonatype, reveló detalles de un paquete de Python malicioso llamado «*pymafka*«, que fue diseñado para lanzar un Cobalt Strike Beacon en hosts Windows, macOS y Linux comprometidos.

Sin embargo, eso puede cambiar con la aparición de artefactos Geacon en la naturaleza. Geacon es una variante Go de Cobalt Strike que está disponible en GitHub desde febrero de 2020.

El análisis adicional de dos nuevas muestras de VirusTotal que se cargaron en abril de 2023 ha rastreado sus orígenes en dos variantes de Geacon (geacon_plus y geacon_pro), que fueron desarrolladas a fines de octubre por dos desarrolladores chinos anónimos z3ratu1 y H4de5.

Ya no se puede acceder al proyecto geacon_pro en GitHub, pero una instantánea de Internet

Archive capturada el 6 de marzo de 2023 revela su capacidad para eludir motores antivirus como Microsoft Defender, Kaspersky y Qihoo 360 Core Crystal.

H4de5, el desarrollador detrás de geacon_pro, afirma que la herramienta está diseñada principalmente para admitir las versiones 4.1 y posteriores de CobaltStrike, mientras que geacon_plus admite la versión 4.0 de CobaltStrike. La versión actual del software es la 4.8.

Resume_20230320.app de Xu Yiqing, uno de los artefactos descubiertos por SentinelOne, emplea un AppleScript de solo ejecución para comunicarse con un servidor remoto y descargar una carga útil de Geacon. Es compatible con las arquitecturas de silicio de Apple e Intel.

> *«La carga útil de Geacon sin firmar se recupera de una dirección IP en China. Antes de que comience su actividad de señalización, al usuario se le presenta un documento señuelo de dos páginas incrustado en el binario de Geacon. Se abre un PDF que muestra el currículum de una persona llamada Xu Yiqing»,* dijeron los investigadores.

El binario de Geacon, compilado a partir del código fuente de geacon_plus, incluye una multitud de funciones que le permiten descargar cargas útiles de próxima etapa y filtrar datos, y facilitar las comunicaciones de red.

La segunda muestra, según la empresa de ciberseguridad, está integrada en una aplicación troyana que se hace pasar por la aplicación de soporte remoto SecureLink (SecureLink.app) y se dirige principalmente a dispositivos Intel.

Los barebones, solicitudes de aplicaciones no firmadas para el permiso de los usuarios para acceder a contactos, fotos, recordatorios, así como a la cámara y el micrófono del dispositivo. Su componente principal es una carga útil de Geacon construida a partir del proyecto geacon_pro, que se conecta a un conocido servidor de comando y control (C2) en Japón.

El desarrollo se produce cuando el ecosistema macOS está siendo atacado por una amplia variedad de hackers, incluyendo grupos patrocinados por el estado, para implementar puertas traseras y ladrones de información.

> *«El aumento de las muestras de Geacon en los últimos meses sugiere que los equipos de seguridad deberían prestar atención a esta herramienta y asegurarse de que cuentan con protecciones»,* dijeron los investigadores.