Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 115	Fecha: 17-05-2023 Página 4 de 10

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Hackers utilizan la variante Golang de Cobalt Strike para atacar los sistemas Apple macOS		
Tipo de ataque	Malware	Abreviatura	Malware
Medios de propagación	Red, Internet, Correo electrónico		
Código de familia	C	Código de subfamilia	C01
Clasificación temática familia	Código malicioso		

Descripción

Una implementación de Golang de Cobalt Strike llamada Geacon atraiga la atención de los actores de amenazas que buscan apuntar a los sistemas macOS de Apple.

DETALLES:

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

- 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. 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 360 360 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.

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

RECOMENDACIONES:

- Evitar hacer clic en enlaces de mensajes de spam e ingresar en sitios web desconocidos.
- Evitar hacer clic en la URL o abrir archivos adjuntos en correos electrónicos desconocidos y no deseados.
- Mantener actualizado el Sistema operativo y software antivirus en las estaciones de trabajo.

Fuentes de información	▪ https://thehackernews.com/2023/05/hackers-using-golang-variant-of-cobalt.html ▪ Análisis propio de fuentes abiertas.