Una campaña de malware persistente basada en Golang denominada GO#WEBBFUSCATOR aprovechó la imagen de campo profundo tomada del Telescopio Espacial James Webb (JWST) de la NASA como señuelo para desplegar cargas útiles maliciosas en sistemas infectados.

El desarrollo, revelado por Securonix, apunta a la creciente adopción de Go entre los atacantes, debido al soporte multiplataforma del lenguaje de programación, lo que permite a los operadores aprovechar de forma efectiva una base de código común para apuntar a distintos sistemas operativos.

Los binarios de Go también tienen el beneficio adicional de dificultar el análisis y la ingeniería inversa en comparación con el malware escrito en otros lenguajes como C++ o C#, sin mencionar los intentos prolongados de análisis y detección.

Los correos electrónicos de phishing que contienen un archivo adjunto de Microsoft Office actúan como punto de entrada para la cadena de ataque, que al abrirse, recupera un marco de VBA ofuscado que, a su vez, se ejecuta de forma automática si el destinatario habilita las macros.

La ejecución de la macro da como resultado la descarga de un archivo de imagen «OxB36F8GEEC634.jpg» que aparentemente es una imagen del primer campo profundo capturado por JWST pero, al inspeccionar con un editor de texto, en realidad es una carga útil codificada en Base64.

> *«El código desofuscado ejecuta un comando que descargará un archivo llamado OxB36F8GEEC634.jpg, usará certutil.exe para decodificarlo en un binario (msdllupdate.exe) y después, al final, lo ejecutará»*, dijeron los investigadores de Securonix, D. luzvyk, T. Peck y O. Kolesnikov.

El binario, un ejecutable de Windows de 64 bits con un tamaño de 1.7 MB, no solo está equipado para volar bajo el radar de los motores antimalware, sino que también se oscurece mediante una técnica llamada gobfuscation, que hace uso de una herramienta de ofuscación

de Golang públicamente disponible en GitHub.

La biblioteca gobfuscate ha sido previamente documentada como utilizada por los actores detrás de ChaChi, un troyano de acceso remoto empleado por los operadores del ransomware PYSA (también conocido como Mespinoza) como parte de su conjunto de herramientas, y el marco de comando y control (C2) de Sliver.

La comunicación con el servidor C2 se facilita a través de consultas y respuestas de DNS encriptadas, lo que permite que el malware ejecute comandos enviados por el servidor por medio del símbolo del sistema de Windows. Se cree que los dominios C2 para la campaña se registraron a fines de mayo de 2022.

La decisión de Microsoft de bloquear las macros de forma predeterminada en las aplicaciones de Office llevó a muchos adversarios a modificar sus campañas cambiando a archivos LNK e ISO no autorizados para implementar adware. Queda por ver si los atacantes de GO#WEBBFUSCATOR adoptarán un método de ataque parecido.

> *«Usar una imagen legítima para construir un binario de Golang con Certutil no es muy común. Está claro que el autor original del binario diseñó la carga útil con algunas metodologías de detección anti-EDR y contraforense triviales en mente»,* dijeron los investigadores.