Las instituciones financieras en la región de Asia-Pacífico (APAC) y Medio Oriente y Norte de África (MENA) están siendo objeto de un nuevo tipo de amenaza llamada JSOutProx, que se está desarrollando rápidamente.

> Según un informe técnico publicado recientemente por Resecurity, *«JSOutProx es un sofisticado marco de ataque que combina JavaScript y .NET. Este malware utiliza la función de (des)serialización .NET para comunicarse con un módulo principal de JavaScript en la máquina de la víctima. Una vez que se ejecuta, JSOutProx permite cargar varios complementos que realizan actividades maliciosas adicionales en el objetivo».*

Yoroi identificó por primera vez JSOutProx en diciembre de 2019. Se cree que los primeros ataques fueron llevados a cabo por Solar Spider, un actor de amenazas conocido por atacar bancos y grandes empresas en Asia y Europa.

En 2021, Quick Heal Security Labs informó sobre ataques que utilizaban un troyano de acceso remoto (RAT) para dirigirse a empleados de pequeños bancos en la India. Otras oleadas de ataques han tenido como objetivo a instituciones gubernamentales indias desde abril de 2020.

Los ataques de JSOutProx suelen comenzar con correos electrónicos de spear-phishing que contienen archivos JavaScript maliciosos, haciéndose pasar por documentos PDF o archivos ZIP. Estos archivos ejecutan un implante fuertemente ofuscado que se encarga de llevar a cabo las acciones maliciosas.

El malware cuenta con varios complementos que permiten la exfiltración de datos, operaciones en el sistema de archivos y otras acciones ofensivas. Además, puede obtener información del host comprometido, controlar la configuración del proxy, acceder a cuentas de Microsoft Outlook y recopilar contraseñas de un solo uso de Symantec VIP. JSOutProx también utiliza el campo de encabezado Cookie para las comunicaciones de control de comando (C2).

A pesar de ser un RAT completamente funcional implementado en JavaScript, JSOutProx tiene limitaciones en comparación con los archivos ejecutables tradicionales. Sin embargo, la popularidad de JavaScript en los sitios web hace que este tipo de malware pase desapercibido más fácilmente para los usuarios comunes y los sistemas de detección de antivirus.

Resecurity ha documentado recientemente una nueva ola de ataques que utilizan notificaciones de pago falsas de SWIFT o MoneyGram para engañar a las víctimas y ejecutar el código malicioso. Estos ataques han aumentado en frecuencia desde febrero de 2024.

Los artefactos de estos ataques han sido encontrados alojados en repositorios de GitHub y GitLab, aunque estos han sido bloqueados y eliminados rápidamente. Los atacantes suelen eliminar y recrear los repositorios para gestionar múltiples cargas maliciosas y diferenciar objetivos.

Aunque los orígenes exactos del grupo de cibercriminales detrás de JSOutProx aún son desconocidos, la distribución de los ataques y la complejidad del malware sugieren una posible conexión con China o grupos afiliados.

Este desarrollo se produce en un momento en que los criminales cibernéticos están promocionando en la dark web un nuevo software llamado GEOBOX, que utiliza dispositivos Raspberry Pi para llevar a cabo actividades fraudulentas y de anonimización.

GEOBOX, disponible por una tarifa mensual o de por vida, permite a los usuarios falsificar ubicaciones GPS, emular configuraciones de red y software, imitar puntos de acceso Wi-Fi conocidos y evitar filtros antifraude.

El fácil acceso a herramientas como GEOBOX plantea preocupaciones de seguridad debido a su potencial para facilitar una amplia gama de delitos, como ataques patrocinados por el estado, espionaje corporativo, fraude financiero y distribución de malware.