Un cargador de malware reciente desarrollado en Go, denominado JinxLoader, está siendo explotado por grupos maliciosos para enviar cargas de software malicioso avanzado, como Formbook y su variante posterior XLoader.

Estas revelaciones provienen de las compañías de ciberseguridad Palo Alto Networks Unit 42 y Symantec. Ambas entidades destacaron estrategias de ataque complejas que culminaron con la introducción de JinxLoader mediante tácticas de engaño digital.

> *«Este software malicioso rinde tributo al personaje Jinx del juego League of Legends, presentando al personaje en su publicidad y en el panel de acceso [de comando y control]. El propósito principal de JinxLoader es simple: instalar malware en sistemas comprometidos»*, mencionó Symantec.

En noticias anteriores, Unit 42 informó en noviembre de 2023 que esta herramienta maliciosa se ofreció por primera vez en un foro de hacking en línea el 30 de abril de 2023, con precios de $60 mensuales, $120 anuales o una suscripción vitalicia por $200.

Los ataques inician mediante correos electrónicos fraudulentos que simulan ser de la organización petrolera ADNOC de Abu Dhabi, incitando a los usuarios a abrir archivos RAR con contraseña. Al acceder a estos archivos, se instala el software JinxLoader, facilitando la entrada de Formbook o XLoader.

Simultáneamente, ESET detectó un incremento en infecciones relacionadas, introduciendo una nueva familia de malware denominada Rugmi, diseñada para difundir programas que roban información valiosa.

Estas acciones ocurren paralelamente a un aumento en la circulación de otros programas dañinos como DarkGate y PikaBot. Además, un grupo de ciberdelincuentes identificado como TA544 o Narwal Spider está usando variantes de malware denominadas IDAT Loader para desplegar el software malicioso Remcos RAT o SystemBC.

En otro frente, los creadores del malware Meduza Stealer han lanzado una versión mejorada (versión 2.2) en la web profunda, ahora con capacidad para atacar billeteras digitales y con un mecanismo mejorado para capturar datos de tarjetas de crédito.

Indicando la persistencia del negocio ilegal en la venta de datos robados, expertos en seguridad también han identificado una nueva amenaza llamada Vortex Stealer, capaz de extraer información de navegadores web, tokens de Discord, sesiones activas de Telegram, datos del sistema y archivos de pequeño tamaño.

> *«La información sustraída se almacena y se envía a plataformas como Gofile o Anonfiles. Además, el malware puede compartir estos datos en canales de Discord mediante enlaces web. También cuenta con la capacidad de distribuir esta información a través de bots en Telegram»*, añadió Symantec.