Investigadores de seguridad cibernética descubrieron una *«interesante campaña de correo electrónico»* emprendida por un actor de amenazas que comenzó a distribuir un nuevo malware escrito en el lenguaje de programación Nim.

Nombrado como NomzaLoader por investigadores de Proofpoint, el desarrollo marca uno de los raros casos de malware Nim descubierto en el panorama de amenazas.

> *«Los desarrolladores de malware pueden optar por utilizar un lenguaje de programación poco común para evitar la detección, ya que los ingenieros inversos pueden no estar familiarizados con la implementación de Nim o no estar enfocados en desarrollar la detección para ella, y por lo tanto, las herramientas y las cajas de arena pueden tener dificultades para analizar muestras»,* dijeron los investigadores.

Proofpoint está rastreando a los operadores de la campaña bajo el nombre de TA800, quienes al parecer, comenzaron a distribuir NimzaLoader a partir del 3 de febrero de 2021. Antes de la última serie de actividad, se sabe que TA800 ha utilizado predominantemente BazaLoader desde abril de 2020.

Mientras APT28 se ha vinculado antes a la entrega de malware de Zebrocy mediante cargadores basados en Nim, la aparición de NimzaLoader es otra señal de que los actores maliciosos están reestructurando constantemente su arsenal de malware para evitar la detección.

Los hallazgos de Proofpoint también fueron corroborados de forma independiente por investigadores del equipo de inteligencia de amenazas de Walmart, que denominaron al malware «NimarLoader«.

Al igual que en el caso de BazaLoader, la campaña detectada el 3 de febrero hizo uso de señuelos de phishing de correo electrónico personalizados que contenían un enlace a un supuesto documento PDF que redirigía al destinatario a un ejecutable de NimzaLoader alojado en Slack, que usaba un icono falso de Adobe como parte de sus trucos de ingeniería

social.

Al abrirlo, el malware proporciona a los atacantes acceso a los sistemas Windows de la víctima, junto con capacidades para ejecutar comandos arbitrarios recuperados de un servidor de comando y control, incluyendo la ejecución de comandos de PowerShell, la inyección de shellcode en los procesos en ejecución e incluso la implementación de más malware.

Evidencia adicional recopilada por Proofpoint y Walmart demuestra que NimzaLoader también se está utilizando para descargar y ejecutar Cobalt Strike como su carga útil secundaria, lo que sugiere que los actores de amenazas integran distintas tácticas en sus campañas.

> *«No está claro si Nimzaloader es solo un punto en el radar para TA800 y el panorama de amenazas amplio, o si NimzaLoader será adoptado por otros actores de amenazas de la misma forma que BazaLoader ha ganado una amplia adopción»,* concluyeron los investigadores.