Investigadores en ciberseguridad están alertando sobre un nuevo malware de tipo botnet denominado HTTPBot, el cual ha sido utilizado principalmente para atacar a la industria de los videojuegos, así como a empresas tecnológicas e instituciones educativas en China.

> *«En los últimos meses, su propagación ha sido acelerada, utilizando de forma constante los dispositivos infectados para llevar a cabo ataques externos. Mediante ataques HTTP Flood altamente simulados y técnicas dinámicas de ofuscación, logra evadir los métodos tradicionales de detección basados en reglas»,* señaló NSFOCUS en un informe publicado esta semana.

Detectado por primera vez en agosto de 2024, HTTPBot recibe su nombre por utilizar el protocolo HTTP para ejecutar ataques de denegación de servicio distribuido (DDoS). Está desarrollado en Golang, lo cual resulta inusual dado que se enfoca en sistemas operativos Windows.

Este troyano tipo botnet enfocado en Windows es relevante por su aplicación en ataques dirigidos a servicios empresariales críticos, como los sistemas de inicio de sesión y pagos en plataformas de videojuegos.

«Este tipo de ataque, tan preciso como un bisturí, representa una amenaza sistémica para sectores que dependen de la interacción en tiempo real», afirmó la empresa con sede en Pekín. «HTTPBot marca un cambio de paradigma en los ataques DDoS, al pasar de la supresión indiscriminada de tráfico a la interrupción específica de funciones comerciales clave.»

Desde abril de 2025, se estima que HTTPBot ha emitido al menos 200 comandos de ataque, con el objetivo de afectar directamente a sectores como el de los videojuegos, la tecnología, la educación y el turismo dentro de China.

Una vez que se instala y ejecuta, el malware oculta su interfaz gráfica para evitar ser detectado tanto por los usuarios como por herramientas de seguridad, aumentando así su

capacidad para operar sin ser descubierto. También realiza modificaciones no autorizadas en el Registro de Windows para asegurarse de ejecutarse automáticamente al iniciar el sistema.

Posteriormente, establece comunicación con un servidor de comando y control (C2), desde donde recibe órdenes para llevar a cabo ataques HTTP Flood, enviando grandes volúmenes de solicitudes HTTP contra objetivos específicos. El malware es capaz de ejecutar distintos tipos de módulos de ataque, entre ellos:

- BrowserAttack: Emula tráfico legítimo usando instancias ocultas de Google Chrome, con el fin de agotar los recursos del servidor.
- HttpAutoAttack: Utiliza cookies para replicar con precisión sesiones reales.
- HttpFpDlAttack: Usa el protocolo HTTP/2 para sobrecargar la CPU del servidor forzándolo a entregar respuestas grandes.
- WebSocketAttack: Establece conexiones WebSocket mediante los protocolos «ws://» y «wss://».
- PostAttack: Emplea solicitudes HTTP POST para realizar los ataques.
- CookieAttack: Incorpora un sistema de procesamiento de cookies, basado en el método de BrowserAttack.

«Normalmente, las familias de botnets DDoS se enfocan en plataformas Linux o en dispositivos IoT», explicó NSFOCUS. «Sin embargo, HTTPBot se ha orientado de manera específica al ecosistema de Windows.»

«Al simular de forma profunda los protocolos y replicar el comportamiento de navegadores reales, HTTPBot evade las defensas que dependen de la integridad del protocolo. En lugar de saturar con tráfico masivo, mantiene activas las sesiones del servidor mediante rutas URL aleatorias y mecanismos de renovación de cookies.»