Investigadores de seguridad cibernética advierten sobre los servicios que rompen CAPTCHA que son ofrecidos a la venta para eludir los sistemas diseñados para distinguir a los usuarios legítimos del tráfico de bots.

> *«Debido a que los ciberdelincuentes están interesados en descifrar los CAPTCHA con precisión, se han creado varios servicios que están orientados principalmente a esta demanda del mercado»,* dijo Trend Micro en un informe.

> *«Estos servicios de resolución de CAPTCHA no usan técnicas [de reconocimiento óptico de caracteres] o métodos avanzados de aprendizaje automático; en cambio, rompen los CAPTCHA al asignar tareas de ruptura de CAPTCHA a solucionadores humanos reales».*

CAPTCHA, abreviatura de Prueba de Turing Pública Completamente Automatizada para Diferenciar a las Computadoras y los Humanos, es una herramienta para diferenciar a los usuarios humanos reales de los usuarios automatizados con el objetivo de combatir el correo no deseado y restringir la creación de cuentas falsas.

Aunque los mecanismos CAPTCHA pueden ser una experiencia disruptiva para el usuario, se consideran un medio eficaz para contrarrestar los ataques del tráfico web que se origina en bots.

Los servicios ilícitos de resolución de CAPTCHA funcionan canalizando las solicitudes enviadas por los clientes y delegándolas a sus solucionadores humanos, quienes elaboran la solución y envían los resultados a los usuarios.

Esto, a su vez, se logra llamando a una API para enviar el CAPTCHA e invocando una segunda API para obtener los resultados.

> *«Esto facilita que los clientes de los servicios de ruptura de CAPTCHA desarrollen herramientas automatizadas contra los servicios web en línea. Y debido a que los humanos reales están resolviendo CAPTCHA, el propósito de filtrar el tráfico automatizado de bots a través de estas pruebas se vuelve ineficaz»,* dijo el investigador de seguridad Joey Costoya.

Además de esto, se ha observado que los hackers compran servicios que rompen CAPTCHA y los combinan con ofertas de proxyware para ocultar la dirección IP de origen y evadir las barreras antibot.

Proxyware, aunque se comercializa como una utilidad para compartir el ancho de banda de Internet no usado de un usuario con otras partes a cambio de un *«ingreso pasivo»*, esencialmente convierte los dispositivos que los ejecutan en proxies residenciales.

En una instancia de un servicio de ruptura de CAPTCHA dirigido al popular mercado de comercio social Poshmark, las solicitudes de tareas que emanan de un bot se enrutan por medio de una red de proxyware.

> *«Los CAPTCHA son herramientas comunes que se usan para prevenir el spam y el abuso de bots, pero el uso cada vez mayor de servicios de ruptura de CAPTCHA ha ocasionado que los CAPTCHA sean menos efectivos. Si bien los servicios web en línea pueden bloquear las IP de origen de los abusadores, el aumento de la adopción de proxyware hace que este método sea tan inútil como los CAPTCHA»,* dijo Costoya.

Para mitigar dichos riesgos, se recomienda que los servicios web en línea complementen los CAPTCHA y las listas de bloqueo de IP con otras herramientas contra el abuso.