La compañía de seguridad cibernética Imperva, dijo el viernes que mitigó recientemente un ataque de denegación de servicio distribuido (DDoS) de rescate dirigido a un sitio web sin nombre que alcanzó un máximo de 2.5 millones de solicitudes por segundo (RPS).

> *«Si bien los ataques DDoS de rescate no son nuevos, parecen estar evolucionando y volviéndose más interesantes con el tiempo y con cada nueva fase. Por ejemplo, hemos visto casos en los que la nota de rescate se incluye en el ataque incrustado en una solicitud de URL»,* dijo Nelli Klepfish, analista de seguridad de Imperva.

Las principales fuentes de los ataques provinieron de Indonesia, seguida de Estados Unidos, China, Brasil, India, Colombia, Rusia, Tailandia, México y Argentina.

Los ataques de denegación de servicio distribuido (DDoS) son una subcategoría de ataques de denegación de servicio (DoS) en los que se utiliza un ejército de dispositivos en línea conectados, conocido como botnet, para abrumar un sitio web de destino con tráfico falso en un intento para que no esté disponible para los usuarios legítimos.

La compañía con sede en California dijo que la entidad afectada recibió varias notas de rescate incluidas como parte de los ataques DDoS, exigiendo que la empresa hiciera un pago de bitcoin para permanecer en línea y evitar perder *«cientos de millones en capitalización de mercado»*.

En un giro interesante, los atacantes se hacen llamar REvil, el cártel de ransomware como servicio que sufrió un gran revés después de que algunos de sus operadores fueran arrestados por las autoridades policiales rusas a inicios de enero.

> *«Sin embargo, no está claro si las amenazas fueron hechas recientemente por el*

> *grupo REvil original o por un impostor»,* dijo Klepfish.

El ataque de 2.5 millones de RPS duró menos de un minuto, y uno de los sitios hermanos operados por la misma compañía sufrió un ataque similar que duró aproximadamente 10 minutos, incluso cuando las tácticas empleadas se cambiaron constantemente para evitar una posible mitigación.

La evidencia recopilada por Imperva apunta a los ataques DDoS que se originaron en la botnet Meris, que ha seguido aprovechando una vulnerabilidad de seguridad ahora abordada en los enrutadores Mikrotik (CVE-2018-14847) para atacar objetivos, incluido Yandex, en septiembre pasado.

> *«Los tipos de sitios que buscan los actores de amenazas parecen ser sitios comerciales que se centran en las ventas y las comunicaciones. Los objetivos tienden a estar ubicados en Estados Unidos o Europa, y todos tienen en común que son empresas que cotizan en bolsa y los actores de amenazas usan esto para su ventaja al referirse al daño potencial que un ataque DDoS podría causar al precio de las acciones de la empresa»,* dijo Klepfish.

Los hallazgos se producen cuando se detectó a actores maliciosos armando una nueva técnica de amplificación llamada TCP Middlebox Reflection por primera vez en la naturaleza para afectar a las industrias de banca, viajes, juegos, medios y alojamiento web con una avalancha de tráfico falso.

El ataque DDoS de rescate es también la segunda actividad relacionada con la botnet evitada por Imperva desde principios de año, ya que la compañía detalla un ataque de raspado web que apuntó a una plataforma de listado de trabajos no identificada a fines de enero.

> *«El atacante usó una red de bots a gran escala, generando no menos de 400*

> *millones de solicitudes de bots de casi 400,000 direcciones IP únicas durante cuatro días, con la intención de recopilar los perfiles de los solicitantes de empleo»*, dijo la compañía de seguridad.