[notasdeprensa.jpg](http://www.mexicopress.com.mx)Publicado en WESTFORD, Mass el 03/10/2022

# [Ataques DDOS en Ucrania, afectan a varios países, según informe de amenazas DDoS de NETSCOUT 2022](http://www.notasdeprensa.es)

## NETSCOUT SYSTEMS, INC. anunció hoy los resultados de su informe de inteligencia sobre amenazas DDoS del primer semestre de 2022

Los hallazgos del informe de NETSCOUT demuestran cuán sofisticados se han vuelto los ciberdelincuentes para eludir las defensas con nuevos vectores de ataque DDoS y metodologías exitosas. "Al innovar y adaptarse constantemente, los atacantes diseñan vectores de ataque DDoS nuevos y más efectivos o duplican las metodologías efectivas existentes", dijo Richard Hummel, líder de inteligencia de amenazas de NETSCOUT. "En la primera mitad de 2022, los atacantes realizaron más reconocimiento previo al ataque, ejercieron un nuevo vector de ataque llamado TP240 PhoneHome, crearon un tsunami de ataques de inundación de TCP y expandieron rápidamente botnets de alta potencia para plagar los recursos conectados a la red. Además, Los malos actores han abrazado abiertamente la agresión en línea con campañas de ataques DDoS de alto perfil relacionadas con los disturbios geopolíticos, que han tenido implicaciones globales". El sistema de análisis de amenazas de nivel activo (ATLAS™) de NETSCOUT compila estadísticas de ataques DDoS de la mayoría de los ISP del mundo, grandes centros de datos y redes gubernamentales y empresariales. Estos datos representan inteligencia sobre ataques que ocurren en más de 190 países, 550 industrias y 50 000 números de sistemas autónomos (ASN). El equipo de ingeniería y respuesta de seguridad ATLAS (ASERT) de NETSCOUT analiza y selecciona estos datos para proporcionar información única en su informe semestral. Los hallazgos clave del Informe de inteligencia sobre amenazas DDoS de NETSCOUT del primer semestre de 2022 incluyen: • Hubo 6,019,888 ataques DDoS globales en la primera mitad de 2022. • Los ataques de inundación basados en TCP (SYN, ACK, RST) siguen siendo el vector de ataque más utilizado, con aproximadamente el 46 % de todos los ataques que continúan una tendencia que comenzó a principios de 2021. • Los ataques de tortura de agua de DNS se aceleraron en 2022 con un aumento del 46 % principalmente mediante inundaciones de consultas UDP, mientras que los ataques de bombardeo de alfombras experimentaron un gran regreso hacia el final del segundo trimestre; en general, los ataques de amplificación de DNS se redujeron en un 31 % del segundo semestre de 2021 al primer semestre de 2022. • El nuevo vector DDoS de reflexión/amplificación TP240 PhoneHome se descubrió a principios de 2022 con una relación de amplificación sin precedentes de 4.293.967.296:1; las acciones rápidas erradicaron la naturaleza abusiva de este servicio. • La proliferación de redes de bots de malware creció a un ritmo alarmante, con 21 226 nodos rastreados en el primer trimestre a 488 381 nodos en el segundo, lo que resultó en más ataques directos a la capa de aplicación. Los disturbios geopolíticos generan un aumento de los ataques DDoSCuando las tropas terrestres rusas ingresaron a Ucrania a fines de febrero, hubo un aumento significativo en los ataques DDoS dirigidos a departamentos gubernamentales, organizaciones de medios en línea, empresas financieras, proveedores de alojamiento y empresas relacionadas con criptomonedas, como se documentó anteriormente. Sin embargo, el efecto dominó resultante de la guerra tuvo un impacto dramático en los ataques DDoS en otros países, incluidos: • Irlanda experimentó un aumento en los ataques después de brindar servicios a organizaciones ucranianas. • India experimentó un aumento medible en los ataques DDoS luego de su abstención en las votaciones del Consejo de Seguridad y la Asamblea General de la ONU condenando las acciones de Rusia en Ucrania. • El mismo día, Taiwán soportó su número más alto de ataques DDoS después de hacer declaraciones públicas de apoyo a Ucrania, al igual que Belice. • Finlandia experimentó un aumento del 258 % en los ataques DDoS año tras año, coincidiendo con su anuncio de solicitar la membresía en la OTAN. • Polonia, Rumania, Lituania y Noruega fueron objeto de ataques DDoS vinculados a Killnet; un grupo de atacantes en línea alineados con Rusia. • Si bien la frecuencia y la gravedad de los ataques DDoS en América del Norte se mantuvieron relativamente constantes, los proveedores de telecomunicaciones satelitales experimentaron un aumento en los ataques DDoS de alto impacto, especialmente después de brindar soporte para la infraestructura de comunicaciones de Ucrania. • Rusia experimentó un aumento de casi tres veces en los ataques DDoS diarios desde que comenzó el conflicto con Ucrania y continuó hasta el final del período del informe. De manera similar, a medida que aumentaron las tensiones entre Taiwán, China y Hong Kong en el primer semestre de 2022, los ataques DDoS contra Taiwán ocurrieron regularmente en concierto con eventos públicos relacionados. Nadie ve y sabe más sobre la actividad de ataques DDoS y las mejores prácticas en protección contra ataques que NETSCOUT. Además de publicar el Informe de inteligencia de amenazas DDoS, NETSCOUT también presenta sus datos de ataques DDoS en tiempo real altamente seleccionados en su portal Omnis Threat Horizon para brindar a los clientes visibilidad del panorama global de amenazas y comprender el impacto en sus organizaciones. Estos datos también alimentan ATLAS Intelligence Feed (AIF) de NETSCOUT, que arma continuamente la cartera de seguridad Omnis y Arbor de NETSCOUT. Junto con AIF, los productos Omnis y Arbor detectan y bloquean automáticamente la actividad de amenazas para empresas y proveedores de servicios en todo el mundo.

**Datos de contacto:**

Rosi Romero

5522851828

Nota de prensa publicada en: [https://www.mexicopress.com.mx/ataques-ddos-en-ucrania-afectan-a-varios](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Internacional Nacional Finanzas Programación E-Commerce Software Ciberseguridad

[notasdeprensa.jpg](http://www.mexicopress.com.mx)

[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)