NEWS RELEASE

DDoS Attacks Skyrocket and Hacktivist Activity Surges Threatening Critical Global Infrastructure According to NETSCOUT’s 1H2024 Threat Intelligence Report

2024-10-02

Hacktivists Escalate Sophisticated, Multi-Vector Assaults on Banking and Financial Services, Government, and Utilities

WESTFORD, Mass.--(BUSINESS WIRE)-- NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) today released findings from its 1H2024 **DDoS Threat Intelligence Report** , citing a dramatic 43% increase in the number of application-layer attacks and a 30% increase in volumetric attacks, especially in Europe and the Middle East. Attack duration varied with 70% lasting less than 15 minutes. The escalation of attacks involves a range of threat actors, including hacktivists targeting critical infrastructure in the banking and financial services, government, and utilities sectors. These attacks pose significant threats by disrupting vital civilian services in countries that oppose hacktivists’ ideologies. Key industries, already facing frequent and intense multi-vector attacks, experienced a 55% increase over the past four years.

“Hacktivist activities continue to plague global organizations with more sophisticated and coordinated DDoS attacks against multiple targets simultaneously,” stated Richard Hummel, director, threat intelligence, NETSCOUT. “As adversaries use more resilient, take-down-resistant networks, detection and mitigation are more challenging. This report gives network operations teams insights to fine-tune their strategies to stay ahead of these evolving threats.”

Attack Sophistication Strains Networks Worldwide

DDoS attacks continue to evolve, using innovative technologies and approaches to disrupt networks. During the 1H2024, NETSCOUT observed several significant trends, including:

- NoName057(16), a pro-Russia hacktivist group, increased its focus on application-layer attacks, particularly HTTP/S GET and POST floods, leading to a 43% rise compared to 1H2023.
- Bot-infected devices increased by 50% with the emergence of the Zergeca botnet -- and the continued evolution of the DDoSia botnet used by NoName057(16) -- which uses advanced technologies like DNS over HTTPS (DoH) for command-and-control (C2).
- Distributed botnet C2 infrastructure leveraging bots as control nodes, enabling more decentralized and resilient DDoS attack coordination.

These attacks have triggered widespread disruptions, affecting industries on a global scale. Service slowdowns or outages can cripple revenue streams, delay critical operations, hinder productivity, and significantly elevate organizational risks.

Attackers Targeting New Networks

NETSCOUT also found that the emergence of new networks and autonomous system numbers (ASNs) play a pivotal role in increased DDoS activity. Over 75% of newly established networks are involved with DDoS activities, both as targets or abused participants in furthering attacks on others, within the first 42 days of coming online, as adversaries launch attacks using resilient nuisance networks and bulletproof hosting providers. Organizations need to plan for DDoS protection when splitting off a portion of a network to a new ASN rather than assume automatic protections from upstream service providers.

NETSCOUT’s global internet visibility is backed by decades of experience working with the world’s largest service providers and enterprises. It collects, analyzes, prioritizes, and disseminates data on DDoS attacks from 216 countries and territories, 470 vertical industries, and over 14,000 ASNs. Powered by its ATLAS platform, the company gains insights from more than 500 terabits per second (Tbps) of internet peering network traffic.

Visit our **interactive website** for more information on NETSCOUT's DDoS Threat Intelligence Report. For real-time DDoS attack stats, map, and insights, visit **NETSCOUT Cyber Threat Horizon** .

About NETSCOUT

NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) protects the connected world from cyberattacks and performance and availability disruptions through its unique visibility platform and solutions powered by its pioneering deep packet inspection at scale technology. NETSCOUT serves the world’s largest enterprises, service providers, and public sector organizations. Learn more at **www.netscout.com** or follow @NETSCOUT on **LinkedIn** , **X** , or **Facebook** .

Editorial:

Chris Lucas
NETSCOUT Systems, Inc.
+1 978-614-4124
chris.lucas@netscout.com

Chris Shattuck
Finn Partners for NETSCOUT
+1 404-502-6755
NETSCOUT-US@FinnPartners.com

Source: NETSCOUT SYSTEMS, INC