NETSCOUT

NEWS RELEASE

NETSCOUT's Threat Intelligence Report Reveals Alarming Complexity, Resilience, and Frequency of Cybercrime Threats

2020-02-18

More than 8.4 million DDoS attacks targeting IT infrastructures, cloud, mobile networks, and IoT devices reinforce increased risk for global enterprises and service providers

WESTFORD, Mass.--(BUSINESS WIRE)-- **NETSCOUT SYSTEMS, INC.**, (NASDAQ: NTCT), a leading provider of service assurance, security, and business analytics, today released the findings of its **Threat Intelligence Report for the second half of 2019**, which also incorporates insights from its 15th Annual Worldwide Infrastructure Security Report™ (WISR™) survey. The report underscores the proliferation of risks faced by global enterprises and service providers. These organizations must now not only defend IT infrastructures, but also manage risks caused by increased Distributed Denial of Service (DDoS) attacks on customer-facing services and applications, mobile networks, and unsecured IoT devices.

"We've uncovered some disturbing statistics," stated Hardik Modi, AVP, engineering, threat and mitigation products, NETSCOUT. "By weaponizing new attack vectors, leveraging mobile hotspots, and targeting compromised endpoint IoT devices, attackers are increasingly finding ways to infiltrate our internet-connected world. They are getting more sophisticated by using a minuscule portion of the available vulnerable devices to carry out a successful attack. The largest OpenVPN DDoS attack we observed used less than one percent of the available reflectors connected to the internet. Botmasters are waiting in the wings, since the risk will only increase in 2020 when an estimated 20.4 billion more devices are connected to the internet."

NETSCOUT's Threat Intelligence Report analyzes the global threat landscape, including DDoS campaigns, advanced persistent threat (APT) groups, IoT vulnerabilities, and crimeware. This report also includes findings from the WISR,

an annual global survey of network, security, and IT decision-makers across enterprise and service provider organizations.

Key findings from the Threat Intelligence Report and WISR include:

- Attackers weaponized seven new UDP reflection/amplification vectors and combined variations of existing well-known attack vectors to launch pinpoint-focused DDoS attacks.
- Carpet-bombing tactics increased vertical sector attack activity; satellite telecommunications witnessed a 295% increase in attacks.
- Adversaries discovered how to use advanced reconnaissance to target client services at well-protected targets like ISPs and financial institutions to amplify attacks against specific enterprises and network operators.
- Wireless communications companies experienced a 64% increase in DDoS attack frequency from 2H 2018 to 2H 2019, mainly due to the increased tendency of gamers to use their phone services as wireless hotspots, as well as the popularity of gaming on mobile devices with 4G or LTE connectivity.
- Mirai-based variants dominated the second half of 2019 with a 57% increase targeting 17 system architectures; ASERT honeypots reflect this growth with an 87% increase in the number of exploit attempts.
- Service provider respondents to the WISR reported a 52% increase in DDoS attacks on publicly exposed service infrastructures compared to 38% the previous year.

The analysts and engineers of NETSCOUT's **ATLAS Security Engineering and Response Team (ASERT)** leverage **Active Level Threat Analysis System (ATLAS™)** data–in conjunction with original research and infrastructure such as automated malware analysis pipelines, sinkholes, scanners, and honeypots–to provide unparalleled visibility and insights into the growing threat landscape.

To download NETSCOUT's semi-annual Threat Intelligence Report, please click **here**. Find us on Facebook, LinkedIn, or Twitter to receive the latest threat intelligence updates.

You can also register for a webinar on the report results. **Register Here.**

About NETSCOUT

NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) helps assure digital business services against disruptions in availability, performance, and security. Our market and technology leadership stems from combining our patented smart data technology with smart analytics. We provide real-time, pervasive visibility, and insights customers need to accelerate, and secure their digital transformation. Our approach transforms the way organizations plan, deliver, integrate, test, and deploy services and applications. Our nGenius service assurance solutions provide real-time, contextual analysis of service, network, and application performance. Arbor security solutions help protect against

DDoS attacks that threaten availability, and advanced threats that infiltrate networks to steal critical business assets. To learn more about improving service, network, and application performance in physical or virtual data centers, or in the cloud, and how NETSCOUT's performance and security solutions, powered by service intelligence can help you move forward with confidence, visit **www.netscout.com** or follow **@NETSCOUT** and **@ArborNetworks** on **Twitter**, **Facebook**, or **LinkedIn**.

©2020 NETSCOUT SYSTEMS, INC. All rights reserved. NETSCOUT, the NETSCOUT logo, Guardians of the Connected World, Adaptive Service Intelligence, NETSCOUT Arbor, the NETSCOUT Arbor logo, ATLAS, InfiniStream, InfiniStreamNG, nGenius, and nGeniusONE are registered trademarks or trademarks of NETSCOUT SYSTEMS, INC., and/or its subsidiaries and/or affiliates in the USA and/or other countries. Third-party trademarks mentioned are the property of their respective owners.

View source version on **businesswire.com**: **https://www.businesswire.com/news/home/20200218005118/en/**

Media
Maribel Lopez
Manager, Marketing & Corporate Communications
781-362-4330
Maribel.Lopez@netscout.com

Erica McDonald
Finn Partners for NetScout
+1 646 202 9784
NETSCOUT-US@FinnPartners.com

Source: NETSCOUT SYSTEMS, INC.