NETSCOUT

NEWS RELEASE

NETSCOUT Releases 14th Annual Worldwide Infrastructure Security Report

2019-03-20

DDoS Attack Size Explodes Worldwide: SaaS and Cloud Services Increasingly Targeted

WESTFORD, Mass.--(BUSINESS WIRE)-- **NETSCOUT SYSTEMS, INC.,** (NASDAQ: NTCT), a leading provider of service assurance, security, and business analytics, today released its **14th annual Worldwide Infrastructure Security Report (WISR),** offering direct insights into a wide range of security and operational challenges facing service provider and enterprise network operators around the world, and the strategies adopted to address and mitigate them.

In addition to the survey results, the WISR is supplemented with global threat intelligence from NETSCOUT's **Active Threat Level Analysis System (ATLAS®)infrastructure**. ATLAS has visibility into approximately one-third of all internet traffic, delivering a truly comprehensive view into internet traffic, trends, and threats.

KEY FINDINGS

Digital Transformation strategies are under attack. Digital Transformation is critical to service providers looking to capture new revenue opportunities and enterprises looking to run efficient, scalable, high performing businesses. This has the attention of attackers, who are increasingly targeting these new services.

- SaaS Services: Threefold YoY increase in the number of DDoS attacks against SaaS services, from 13 percent to 41 percent.
- Third Party Data Center and Cloud Services: Threefold YoY increase in the number of DDoS attacks against third party data centers and cloud services, from 11 to 34 percent.

- Targeting Encrypted Traffic: The increasing use of encrypted traffic was reflected in the growing rate of attacks targeting it. In 2018, 94 percent observed such attacks, nearly twice the percentage as the previous year.
- For Service Providers: Cloud-based services were increasingly targeted by DDoS attacks, up from 25 percent in 2016 to 47 percent in 2018.

Getting Political. DDoS has long been a tool for online protests, thanks to the combination of increasingly sophisticated for-hire DDoS attack services and free attack tools that enable anyone with basic online skills to launch an attack.

- In 2018, 60 percent of service providers witnessed attacks traversing their networks that were targeting governments, up from 37 percent last year. As political instability increases around the world, expect DDoS to continue to be used as a form of protest.

DDoS Attacks Continue to Evolve. In 2018, DDoS attack size exploded to a record-breaking 1.7Tbps in size, and the targets and techniques continue to evolve.

- 91 percent of enterprises who experienced a DDoS attack indicated that one or more completely saturated their internet bandwidth.
- Attackers shifted their focus to stateful infrastructure attacks targeting Firewalls and IPS devices. These attacks almost doubled from 16 percent to 31 percent.
- Of those who experienced stateful attacks, 43 percent reported that their Firewall and/or IPS contributed to an outage during the attack.
- 36 percent of enterprises experienced complex multi-vector attacks targeting bandwidth, stateful infrastructure and applications.

High Cost of Downtime. For 2018, the average global cost of one hour of downtime associated with internet service outages caused by DDoS attacks was $221,836.80. Germany had the highest downtime costs, at $351,995. Meanwhile, Japan paid the least for an hour of network downtime at $123,026.

Survey Overview

NETSCOUT surveyed our service provider customers who can offer direct insights into a wide range of topics, from cyber-attacks to major industry trends such as SDN/NFV and Digital Transformation, to key organizational issues such as incident response training, staffing, and budgets. This year, for the first time, NETSCOUT also surveyed enterprise security, network and IT decision makers across seven countries, US, Canada, Brazil, UK, France, Germany and Japan.

Additional Resources

- Visit the NETSCOUT ASERT **blog** for insight on various aspects of the report and to download the full report.
- Find us on **Facebook** and follow @Netscout on Twitter for more key findings.

About NETSCOUT

NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) assures 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.

©2019 NETSCOUT SYSTEMS, INC. All rights reserved. NETSCOUT and the NETSCOUT logo are registered trademarks of NETSCOUT SYSTEMS, INC. and/or its subsidiaries and/or affiliates in the USA and/or other countries.

View source version on **businesswire.com**: **https://www.businesswire.com/news/home/20190320005120/en/**

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

Source: NETSCOUT SYSTEMS, INC.