NEWS RELEASE

NETSCOUT Highlights Dawn of the TerrorBit Era

2019-02-26

Latest Report from NETSCOUT Threat Intelligence Reveals New Findings on IoT Vulnerabilities, Nation State Actors, and Increase in DDoS Frequency and Attack Size

WESTFORD, Mass.--(BUSINESS WIRE)--

NETSCOUT SYSTEMS, INC., (NASDAQ: NTCT), a leading provider of service assurance, security, and business analytics, today released its latest **Threat Landscape Report**, offering globally scoped internet threat intelligence together with analysis from its security research arm. Examining findings from the second half of 2018, the report covers the latest trends and activities including nation-state advanced persistent threat (APT) groups, IoT vulnerabilities, crimeware operations, and Distributed Denial of Service (DDoS) attack campaigns.

“Our global findings reveal that the threat landscape in the second half of 2018 represents the equivalent of attacks on steroids,” said Hardik Modi, NETSCOUT’s senior director of Threat Intelligence. “With DDoS attack size and frequency, volume of nation state activity and speed of IoT threats all on the rise, the modern world can no longer ignore the digital threats we regularly face from malicious actors capable of capitalizing on the interdependencies that wind through our pervasively connected world.”

KEY HIGHLIGHTS:

By drawing on the internet-scale visibility of its **Active Level Threat Analysis System (ATLAS)** in conjunction with analysis from its ATLAS Security Engineering and Response Team (ASERT), NETSCOUT Threat Intelligence provides a unique view into the threat landscape, demonstrated by a steady stream of discoveries during the second half of 2018.

During the course of the last six months, NETSCOUT Threat Intelligence saw attackers bulk up existing tactics, rapidly evolve new performance enhancements, and apply smart business techniques to vastly accelerate attack growth rate. Key findings from the report include:

IoT's Countdown to Attack

- Constant targets of DDoS malware, IoT devices come under attack within five minutes of being plugged in and targeted by specific exploits within 24 hours.
- IoT security is minimal to nonexistent on many devices, making this an increasingly dangerous and vulnerable sector, particularly as items ranging from medical devices to cars are IoT-equipped.

The 'TerrorBit Attack' and Beyond

- Overall, the number of DDoS attacks in 2018 was up 26 percent compared to the year previously, and attacks in the 100-400 Gbps range exploded, showing continued interest by bad actors in this attack vector and maturity of tooling in the mid-range of attacks.
- The global maximum DDoS attack size grew by 19 percent in the second half of 2018 versus the same period in the year previously, as threat actors launched strategic campaigns that compromised and used a vast array of devices related solely by internet connectivity. And "carpet bombing," a new variant of the more common reflection or flooding DDoS attack, emerged, requiring different detection techniques.

Nation-State Innovation

- DDoS attacks against the international affairs sector, which includes the United Nations, the International Monetary Fund and the State Department, increased by nearly 200 percent between 2H 2017 and 2H 2018.
- The volume of nation state APT group activity has increased in the space of the last year, as have the number of targets. Subsequently, NETSCOUT is now monitoring the activities of at least 35 groups across several countries, which include Iran, China, Russia, and North Korea.
- These groups are employing new techniques, combining custom-made tools with commodity crimeware as in the case of **STOLEN PENCIL** to extend their reach and impact.

Commercialization of Crimeware

- The cybercriminal underground operates much like legitimate businesses using the conventional business practice of the affiliate model to rapidly generate profits. Increases in attack size reflect the continued monetization of the threat landscape.

- Campaigns like **DanaBot** increased distribution efficiency and cut labor costs by using an affiliate model to rapidly establish its presence across the globe, with 12 separate affiliates targeting financial institutions in many countries.
- However, collaborative crime fighting is also on the rise, illustrated by recent efforts with the ASERT team and the Federal Bureau of Investigation (FBI) during an investigation into MedusaHTTP DDoS, a botnet from a hacker known as stevenkings, that ultimately led to charges being filed.

Through telemetry on a massive scale, ATLAS delivers visibility into the backbone networks at the core of the internet. NETSCOUT gathers data shared by organizations around the world, including 90 percent of Tier 1 service providers, representing approximately one third of internet traffic. NETSCOUT correlates this and other data sets to provide automated data sharing and intelligence, facilitating usage by all internet users, business and private, and giving them a broader perspective to better understand and react to the threats they face.

Additional Resources

- Visit the NETSCOUT ASERT **blog** for insight on various aspects of the report and to download the full **report**.
- Attend a **webinar** on key findings hosted by Hardik Modi, Sr. Director of NETSCOUT Threat Intelligence and Richard Hummel, Threat Intelligence Manager, NETSCOUT, on Thursday, February 28 at 10:30 am ET.
- 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 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/20190226005707/en/**

Maribel Lopez
Manager, Marketing & Corporate Communications
NETSCOUT
maribel.lopez@netscout.com
617-308-8551

Source: NETSCOUT SYSTEMS, INC.