NETSCOUT

NEWS RELEASE

New Paper from 451 Research Delivers Real-world Insights Into Adversary Attack Campaign Strategies, Planning and Execution

2017-06-21

Tech Industry Doppelgangers: Campaign Innovation in the World of Cybercrime

BURLINGTON, Mass.--(BUSINESS WIRE)--Jun. 21, 2017-- **Arbor Networks Inc.**, the security division of NETSCOUT (NASDAQ: NTCT), today announced the availability of a provocative new research paper produced by 451 Research, a preeminent information technology research and advisory company. The goal of the paper is to help security professionals understand the persona and capabilities of their adversaries and also how attack campaigns can be more easily stopped, disrupted or frustrated by a better knowledge of the attacker's tactics, techniques and procedures.

This Smart News Release features multimedia. View the full release here:
http://www.businesswire.com/news/home/20170621005325/en/

451 Research interviewed several white-hats experienced in dealing with black-hat tactics in various roles, including incident responders, malware researchers, penetration testers and all-around cybersecurity veterans. Together, these individuals have over 100 years of security experience, have investigated hundreds of incidents and given hundreds of talks on the subject.

"We have produced a very compelling paper with valuable insights and specific recommendations to enhance your security posture. Attackers aren't Hollywood movie hackers and are more likely to think, act and use the tools of an IT administrator," said Scott Crawford, Director for the Information Security Channel at 451 Research. "They don't rely on malware, custom or commodity. They don't attack from the outside in. They work from the inside out. They use common IT tools to access and escalate through internal systems. As an industry, we need to think more like

the adversary, with less emphasis on tools and more on attacker strategy."

Read this paper to learn:

- The persona and capabilities of your adversaries and how attack campaigns can be more easily stopped, disrupted or frustrated by having a better understanding the attacker's tactics, techniques and procedures.
- The people targeting your business are not who you expect. Many attackers are professionals and have basic IT skills. They are more likely to think, act and use the tools of an IT administrator than those of a Hollywood movie hacker.
- How attackers use common IT tools to access and escalate through internal systems.

Think about what this means for your security posture. What do you need when dealing with an adversary with a high degree of technical skills and familiarity with the tools IT administrators use? Where are the gaps? And what are they after?

Learn more by reading the complete 451 Research paper **here**.

About Arbor Networks

Arbor Networks, the security division of **NETSCOUT**, is driven to protect the infrastructure and ecosystem of the internet. It is the principle upon which we were founded in 2000; and remains the common thread that runs through all that we do today. Arbor's approach is rooted in the study of network traffic. Arbor's suite of visibility, DDoS protection and advanced threat solutions provide customers with a micro view of their network enhanced by a macro view of global internet traffic and emerging threats through our ATLAS infrastructure. Sourced from more than 300 service provider customers, ATLAS delivers intelligence based on insight into approximately 1/3 of global internet traffic. Supported by Arbor's Security Engineering & Response Team (ASERT), smart workflows and rich user context, Arbor's network insights help customers see, understand and solve the most complex and consequential security challenges facing their organizations.

To learn more about Arbor products and services, please visit our website at **arbornetworks.com** or follow on Twitter **@ArborNetworks**. Arbor's research, analysis and insight is shared via the **ASERT blog**. For a global data visualization of DDoS attacks that leverages our ATLAS intelligence, visit the **Digital Attack Map**, a collaboration with Jigsaw, an incubator within Alphabet, Google's parent company (NASDAQ: GOOGL).

Safe Harbor

Forward-looking statements in this release are made pursuant to the safe harbor provisions of Section 21E of the Securities Exchange Act of 1934 and other federal securities laws. Investors are cautioned that statements in this press release, which are not strictly historical statements, including without limitation, the statements related to

Arbor's portfolio of solutions, constitute forward-looking statements which involve risks and uncertainties. Actual results could differ materially from the forward-looking statements due to known and unknown risk, uncertainties, assumptions and other factors. For a more detailed description of the risk factors associated with NETSCOUT, please refer to NETSCOUT's Annual Report on Form 10-K for the fiscal year ended March 31, 2016 and NETSCOUT's subsequent Quarterly Reports on Form 10-Q, which are on file with the Securities and Exchange Commission. NETSCOUT assumes no obligation to update any forward-looking information contained in this press release or with respect to the announcements described herein.

Trademark Notice: Arbor Networks, the Arbor Networks logo and ATLAS are all trademarks of Arbor Networks, Inc. All other brands may be the trademarks of their respective owners.

View source version on businesswire.com: **http://www.businesswire.com/news/home/20170621005325/en/**

Source: Arbor Networks Inc.

Arbor Networks
Kevin Whalen, 781-362-4377
kwhalen@arbor.net