NETSCOUT

NEWS RELEASE

Arbor Networks' 12th Annual Worldwide Infrastructure Security Report Finds Attacker Innovation and IoT Exploitation Fuel DDoS Attack Landscape

2017-01-24

Weaponization of IoT Devices Drives Attack Size Higher by 60%;

800 Gbps in 2016 versus 500 Gbps in 2015

BURLINGTON, Mass--(BUSINESS WIRE)--Jan. 24, 2017-- **Arbor Networks Inc.**, the security division of NETSCOUT (NASDAQ: NTCT), today released its 12th Annual Worldwide Infrastructure Security Report (WISR) offering direct insights from network and security professionals at the world's leading service provider, cloud/hosting and enterprise organizations. The report covers a comprehensive range of issues from threat detection and incident response to managed services, staffing and budgets. Its focus is on the operational challenges internet operators face daily from network-based threats and the strategies adopted to address and mitigate them.

This Smart News Release features multimedia. View the full release here:
http://www.businesswire.com/news/home/20170124005370/en/

(Graphic: Business Wire) This year's report shows the stakes have changed for network and security teams. The threat landscape has been transformed by the emergence of Internet of Things (IoT) botnets. As IoT devices proliferate across networks, bringing tremendous benefits to businesses and consumers, attackers are able to weaponize them due to inherent security vulnerabilities. This year's report goes in-depth, covering how attackers exploit and recruit IoT devices, how IoT botnets enabled by Mirai source code operate and offers practical advice on how to defend against them.

The largest distributed denial-of-service (DDoS) attack reported this year was 800 Gbps, a 60% increase over 2015's largest attack of 500 Gbps. Not only are DDoS attacks getting larger, but they are also becoming more frequent and complex. This increased scale and complexity has led more businesses to deploy purpose-built DDoS protection solutions, implement best practice hybrid defenses and increase time for incident response practice – all positive developments in an otherwise gloomy threat environment.

"The survey respondents have grown accustomed to a constantly evolving threat environment with steady increases in attack size and complexity over the past decade," said Darren Anstee, Arbor Networks Chief Security Technologist. "However, IoT botnets are a game changer because of the numbers involved. There are billions of these devices deployed, and they are being easily weaponized to launch massive attacks. Increasing concern over the threat environment is reflected in the survey results, which show significant improvements in the deployment of best practice technologies and response processes."

Key Findings

Innovation and Exploitation Fuel DDoS Attack Landscape: The emergence of botnets that exploit inherent security weaknesses in IoT devices and the release of the Mirai botnet source code have increased attackers' abilities to launch extremely large attacks.

Scale: The massive growth in attack size has been driven by increased attack activity on all reflection/amplification protocols, and by the weaponization of IoT devices and the emergence of IoT botnets.

- Since Arbor began the WISR in 2005, DDoS attack size has grown 7,900%, for a compound annual growth rate (CAGR) of 44%.
- In the past five years alone, DDoS attack size has grown 1,233%, for a CAGR of 68%.

Frequency: The chances of being hit by a DDoS attack have never been higher, with respondents showing increased rates of attack.

- 53% of service providers indicated they are seeing more than 21 attacks per month – up from 44% last year.
- 21% of data-center respondents saw more than 50 attacks per month, versus only 8% last year.
- 45% of enterprise, government and education respondents experienced more than 10 attacks per month – a 17% year over year increase.

Complexity: Multiple simultaneous attack vectors are increasingly being used to target different aspects of a victim's infrastructure at the same time. These multi-vector attacks are popular because they can be difficult to defend against and are often highly effective, driving home the need for an agile, multi-layer defense.

- 67% of service providers and 40% of Enterprise, Government and Education (EGE) reported seeing multi-vector attacks on their networks.

Consequences of DDoS Attacks Are Becoming Clear: DDoS attacks have successfully made many leading web properties unreachable – costing thousands, sometimes millions, of dollars in revenue. This has led the C-suite and company boards to make DDoS defense a top priority.

- 61% of data center operators reported attacks totally saturating data center bandwidth.
- 25% of data center and cloud providers saw the cost of a major DDoS attack rise above $100,000, and 5% cited costs of over $1 million.
- 41% of EGE organizations reported DDoS attacks exceeding their total internet capacity. Nearly 60% of EGE respondents estimate downtime costs above $500/minute.

More Appreciation of Risk Leads to Better Behavior: This year's survey results indicate a better understanding of the brand damage and operational expense of successful DDoS attacks, driving focus on best-practice defensive strategies. Across the board, in every industry, there has been an increase in the use of purpose-built DDoS protection solutions and best practice methods.

- 77% of service provider respondents are capable of mitigating attacks in less than 20 minutes.
- Nearly 55% of EGE respondents now carry out DDoS defense simulations, with approximately 40% carrying them out at least quarterly.
- The proportion of data center and cloud provider respondents that are using firewalls for DDoS defense has fallen from 71% to 40%.

Additional Resources

- Download the full report here (registration required).
- Attend this webinar series for a deeper dive on the WISR key findings.
    - Register here for a deep dive on DDoS key findings.
- Visit the Arbor Networks blog for insight on various aspects of the report.
- Video summary of key findings.
- Like us on Facebook and follow @ArborNetworks on Twitter for more key findings.

Survey Scope & Demographics

- The WISR survey data is based upon 356 responses from a mix of Tier 1, Tier 2 and Tier 3 service providers, hosting, mobile, enterprise and other types of network operators from around the world.
- Two-thirds of all respondents identify as security, network or operations professionals.

- Data covers November 2015 through October 2016.

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).

View source version on businesswire.com: **http://www.businesswire.com/news/home/20170124005370/en/**

Source: Arbor Networks Inc

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