INFONETICS RESEARCH SPECIAL REPORT

DDoS Security Report

November 2014

By Analyst Jeff Wilson

Infonetics RESEARCH

Table of Contents

Exhibit

DRIVERS FOR INVESTING IN DDOS PREVENTION SOLUTIONS

DDoS prevention appliances are the first line of defense for most hosting providers around the globe looking to protect themselves from brute-force attacks on network or resource availability, and with the unprecedented number, size, and coverage of DDoS attacks over the last 3 years, vendors who build DDoS prevention solutions have seen and continue to see a significant increase in demand.

The key drivers for increased investment in DDoS prevention solutions include:

- Emergence of new varieties of **amplification attacks** like the DNS amplification attack aimed at Spamhaus in 2013 that topped 300G, and the NTP amplification attack earlier this year that topped 400G; these attacks are pushing the boundaries of mitigation performance

- **Demand for on-premise solutions** is growing every day even though conventional wisdom says that many customers are looking at cloud-based solutions for DDoS mitigation

- **Data center consolidation,** data center upgrades, and the rollout of the cloud infrastructure that will underpin the next generation of cloud services; large data centers and cloud providers are highly visible targets who must protect their own infrastructure and the customers who trust them to host data and applications; in the last 5 years the scale and architecture of most medium and large data centers have changed significantly, and hosting/cloud providers need DDoS solutions with improved performance, faster physical interfaces, and advanced detection and mitigation technologies

- **Managed DDoS mitigation services;** in addition to purchasing DDoS solutions to protect their own infrastructure, hosting providers around the globe are buying DDoS products to build out managed services for their customers

- **SDN and NFV** are pervasive trends in network and telecom infrastructure, and they will eventually touch all areas of security; though virtual appliance solutions for DDoS mitigation aren't widely available, it's not hard to imagine (particularly in an NFV context) a world where DDoS mitigation can be dynamically provisioned via software

- The increasing volume of **highly visible attacks**, including a mix of politically motivated attacks, state-sponsored electronic warfare, social activism, organized crime, and good old fashioned pointless mischief and mayhem, driven by the easy availability of bots/botnets for hire and easily distributed crowd-sourced attack tools

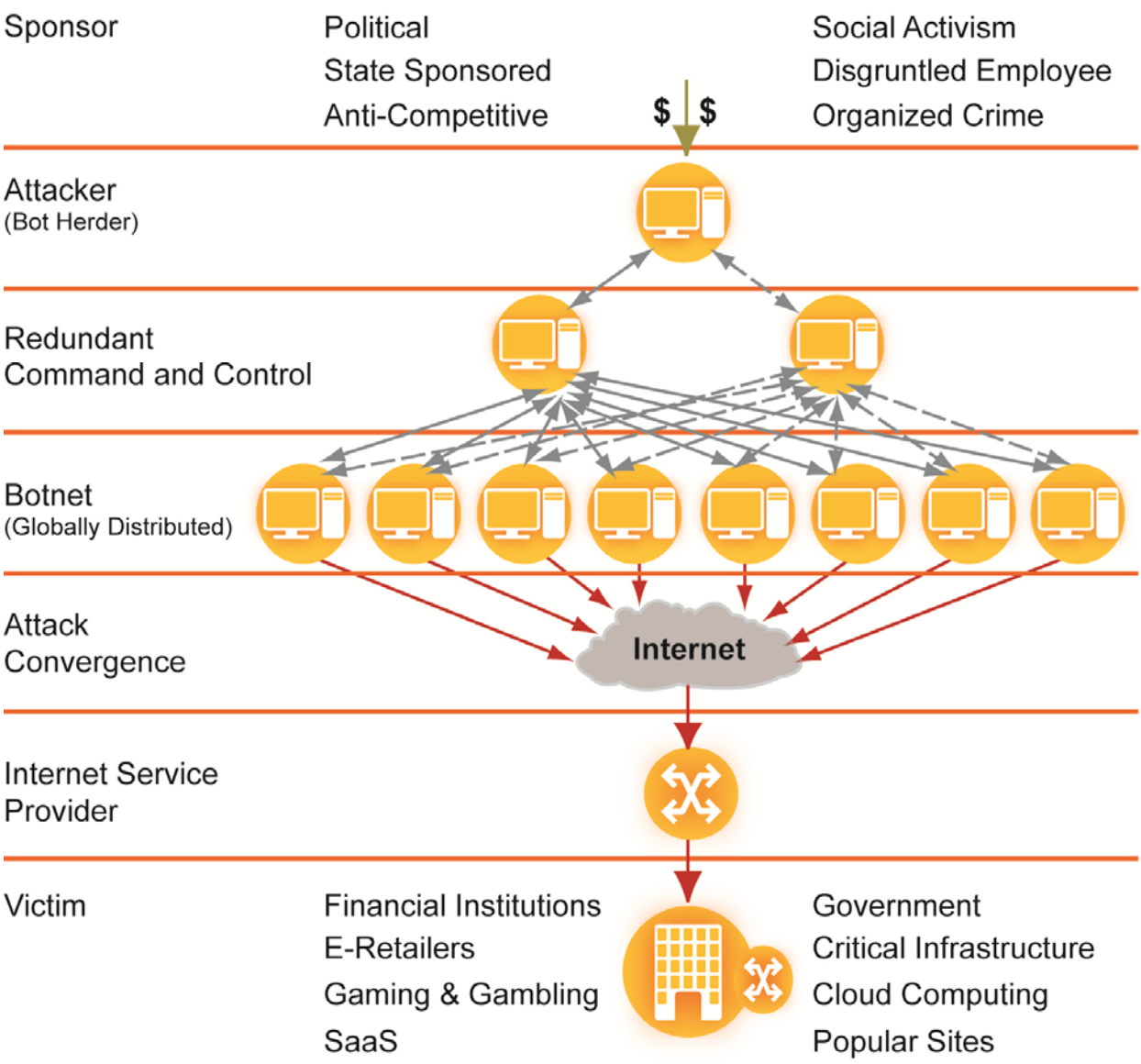
- Increasing number of **sophisticated application-layer attacks** like R.U.D.Y and Slowloris that some DDoS detection and mitigation infrastructure can't identify and block, forcing companies to make new investments in DDoS solutions

- **Internet traffic growth**, which has driven major carriers to upgrade their backbone infrastructure to increase capacity, driving a need for increased capacity DDoS prevention solutions; Cisco predicts global IP traffic to reach the zettabyte threshold by 2015, and to top 1.4 zettabytes by 2014, the CAGR for global IP traffic from 2012 to 2017 at 23%

DDOS RISK PROFILE

DDoS attacks, are by name, an attempt to deny a service; that can be any number of services, denied for any purpose an attacker can dream up. The diagram below shows the basic structure of a DDoS attack.

Exhibit 1 **Anatomy of a DDoS Attack**



DDoS attacks are simple: flood a resource with traffic until that resource overloads and becomes non-functional. Some attacks require vulnerabilities in the end system, while others simply require brute force. The availability of rental botnets and simple tools has made it simple for anyone to launch an attack, and the scale of the attacks is growing rapidly. Most of the technical innovation in DDoS prevention is around meeting the ever-increasing performance requirements driven by large attacks.

DEMAND-SIDE DATA

In *Data Center Security Strategies and Vendor Leadership: North American Enterprise Survey,* our March 2014 survey of 104 medium and large organizations that operate their own data centers, we found that:

- 70% are driven to deploy new security solutions because they need to upgrade to high speed network interfaces on their security appliances to match the upgrades that have happened in their switching infrastructure; 73% are driven by the need for security solutions with aggregate performance that matches their data center network performance

- Though there has been significant discussion of DDoS attacks aimed at just about everyone (with data centers bearing the brunt), protection against new DDoS attacks isn't high on the list of drivers for buying new solutions, though it's very likely that the increasing throughput and sustained nature of many current DDoS attacks is forcing performance upgrades to existing DDoS protection systems

- 44% of respondents plan to increase spending on DDoS prevention products by March 2015

In Data Center Security Strategies and Vendor Leadership: North American Enterprise Survey, our December 2013 survey of 23 major service providers around the globe, we found that:

- 100% of the providers we talked to are driven to deploy new security solutions to handle new DDoS attacks

- 48% of respondents are looking to buy security appliance solutions with >200G of aggregate throughput; 30% are looking for >500G

BOTTOM LINE

Hosting providers around the globe are being bombarded with non-stop DDoS attacks, and many are looking to deploy on-premise solutions that can help keep their infrastructure operational and give them the ability to deliver branded DDoS mitigation solutions to their hosting customers.

REPORT AUTHOR

Jeff Wilson
Principal Analyst, Security
Infonetics Research
+1 408.583.3337 | jeff@infonetics.com
Twitter: @securityjeff

ABOUT INFONETICS RESEARCH

Infonetics is an international market research and analyst firm serving the communications industry since 1990. A leader in defining and tracking emerging and established technologies in all world regions, Infonetics helps clients plan, strategize, and compete more effectively.

REPORT REPRINTS AND CUSTOM RESEARCH

To learn about distributing excerpts from Infonetics reports or custom research, please contact:

North America (West) and Asia Pacific
Larry Howard, Vice President, larry@infonetics.com, +1 408.583.3335

North America (East, Midwest, Texas), Latin America and EMEA
Scott Coyne, Senior Account Director, scott@infonetics.com, +1 408.583.3395

Greater China and Southeast Asia 大中华区及东南亚地区
Jeffrey Song, Market Analyst 市场分析师及客户经理
jeffrey@infonetics.com, +86 21.3919.8505