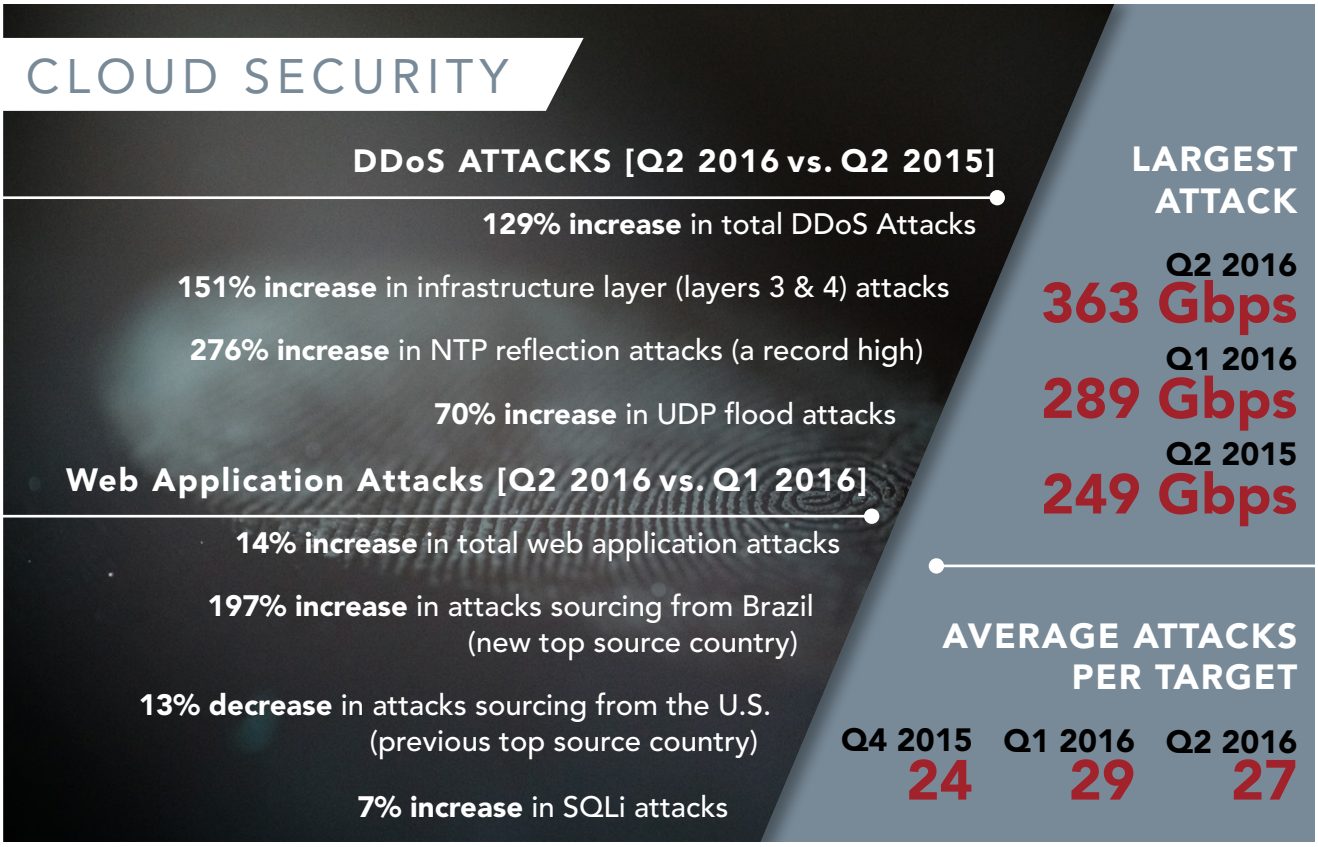
akamai's [state of the internet] / security

Q2 2016 executive review

ABOUT THE REVIEW / Akamai, the world's leading content delivery network (***CDN***) provider, uses its globally distributed Intelligent Platform™ to process trillions of Internet transactions each day. This allows Akamai to gather massive amounts of data on metrics related to broadband connectivity, cloud security, and media delivery. The *State of the Internet* program was built to leverage that data in order to better enable businesses and governments to make intelligent, strategic decisions. Each quarter, Akamai uses this data to publish reports in the *State of the Internet* program focused on broadband connectivity and cloud security.



Cloud Security / The *Q2 2016 State of the Internet / Security Report* combines DDoS attack data on the routed network with web application and DDoS attack data from the Akamai Intelligent Platform™.

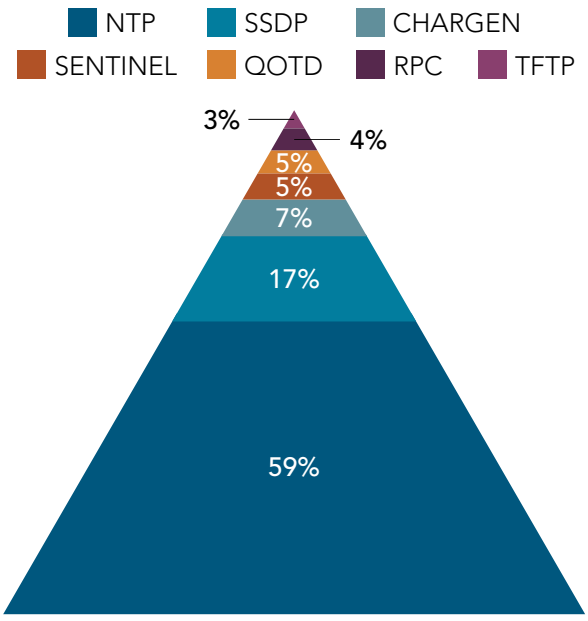
DDoS Update / Attack activity over the routed network continued to rise, setting another record for the number of DDoS attacks — more than double that of a year earlier. In contrast, attack size dropped precipitously — down 36% — to 3.85 Gigabits per second (Gbps), an average size Akamai has not seen since first tracking the statistic. The smaller attack size corresponded with 10% fewer multi-vector attacks. Although average attack size decreased, few organizations can withstand even these smaller attacks without help.

Higher packet rate was a new trend this quarter. A record-setting 21 attacks measured more than 30 Million packets per second (Mpps) compared with six recorded in Q1. Of these high packet rate attacks, only six also peaked at more than 100 Gbps.

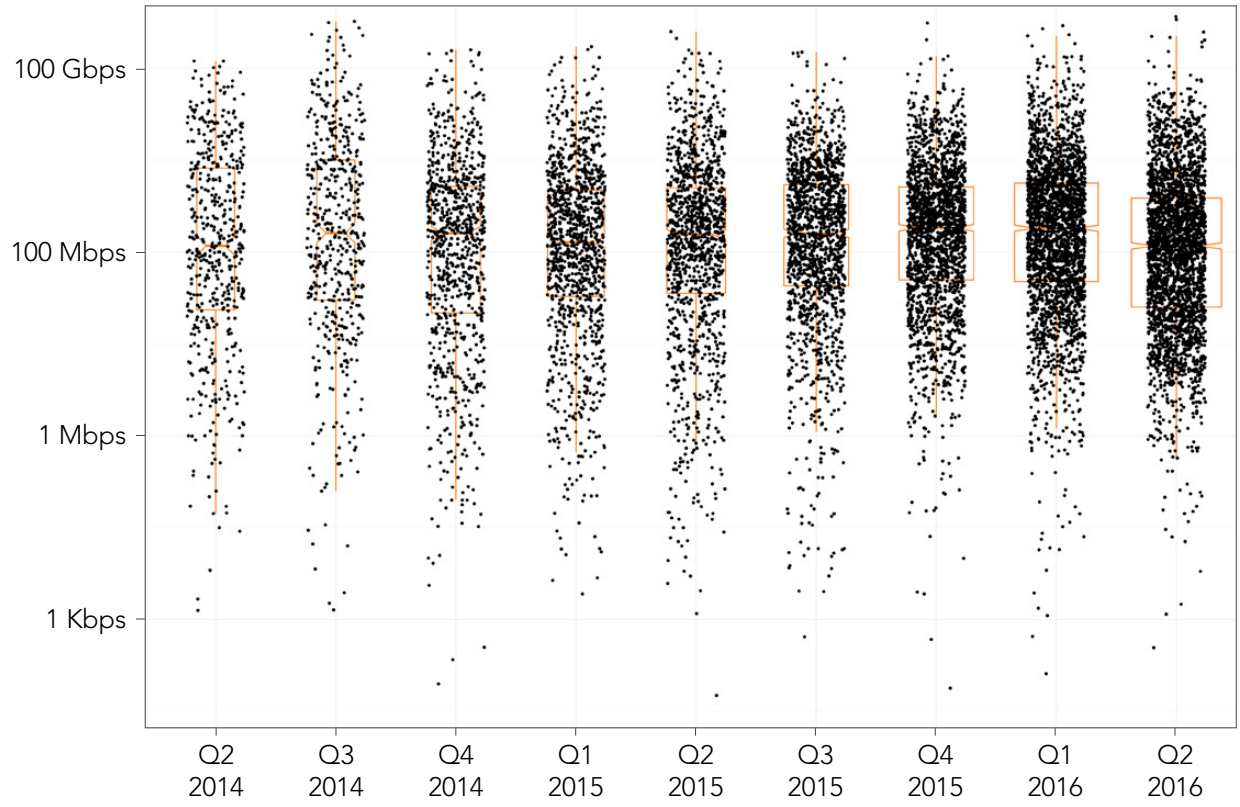
The composition of vectors in attacks greater than 300 Gbps changed this quarter. Previously, these attacks were composed primarily of padded SYN and UDP flood payloads, but the latest attacks contained other vectors including reflection attacks. These attacks could indicate a new hybrid botnet that combines traditional attack tools spread on a wider scale.

More than half of the DDoS attacks (57%) targeted gaming companies, with another 26% targeting the software & technology industry — some of which serve the gaming sector. Those industries were followed by financial services (5%), media & entertainment (4%), Internet & telecom (4%), education (1%), and other sectors made up the remainder (3%). One customer was targeted with 373 attack events.

NTP reflection attacks increased 44% compared with Q1 2016 and accounted for 16% of all DDoS attacks. Reflection attack tools, which are popular among booter/stressor sites, bounce traffic off of servers running vulnerable services such as DNS, CHARGEN, and NTP. Of the nearly 80,000 reflectors we tracked worldwide in Q2 2016, 59% were NTP reflectors.



Once again, NTP was the top source of reflection attacks (59%) in Q2 2016



While the median size of DDoS attacks decreased slightly in Q2 2016, the number of attacks continued to rise

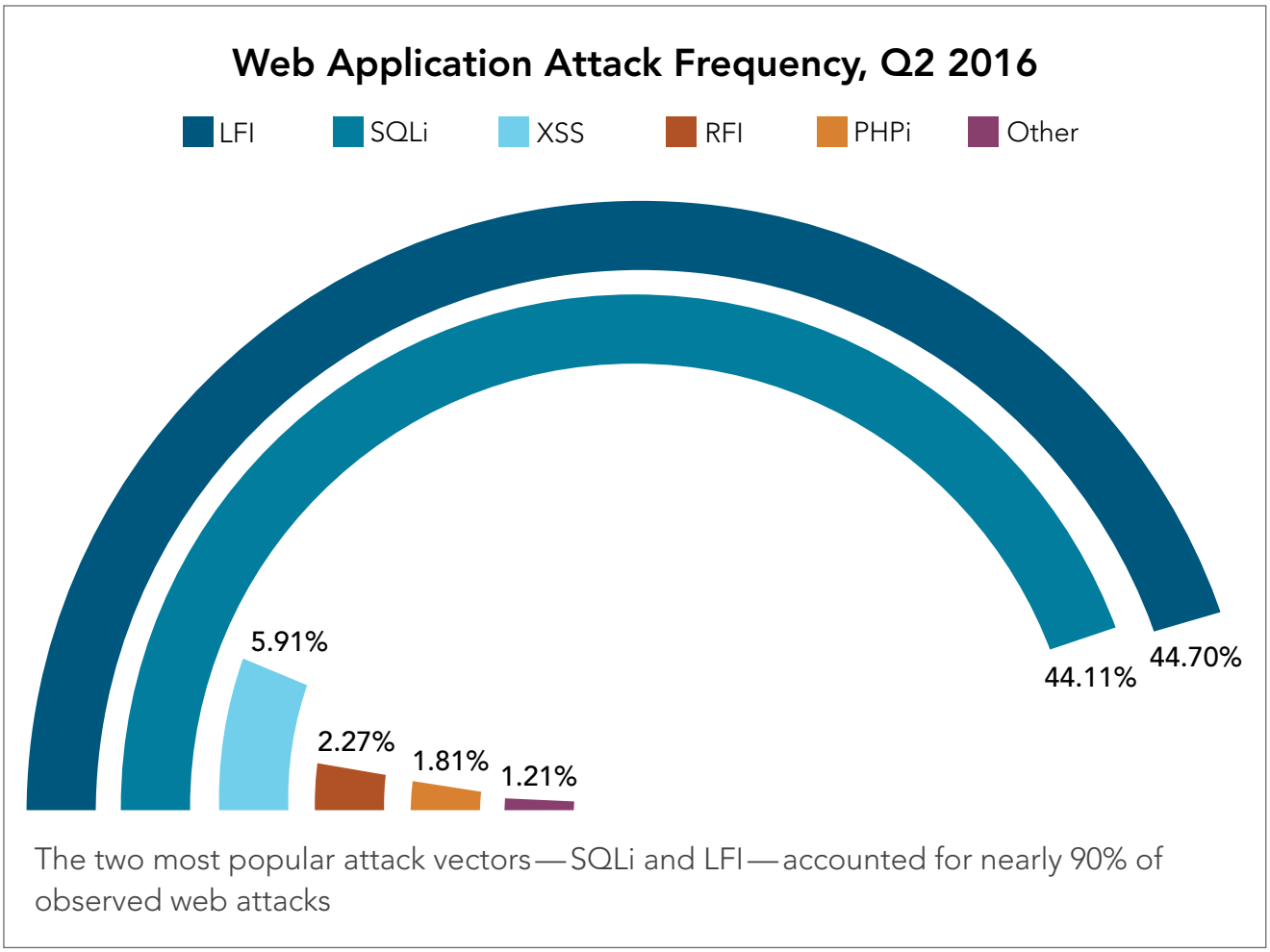
The boxes for each quarter represent the middle 50% of attacks by attack size, while each dot represents an individual attack. The vertical axis has a logarithmic scale; the upper attacks are many thousands of times larger than the bottom ones.

Bot Activity / In a single-day analysis, 43% of web traffic across the Akamai Intelligent Platform was bot traffic. Of the bot traffic, 63% was comprised of malicious automation tools and scraping campaigns.

In addition, Akamai documented an Account Takeover (ATO) botnet. These IP addresses targeted more than 20,000 domains and subdomains. Although the targets ranged across nearly all verticals we track, most targeted financial services and retail organizations.

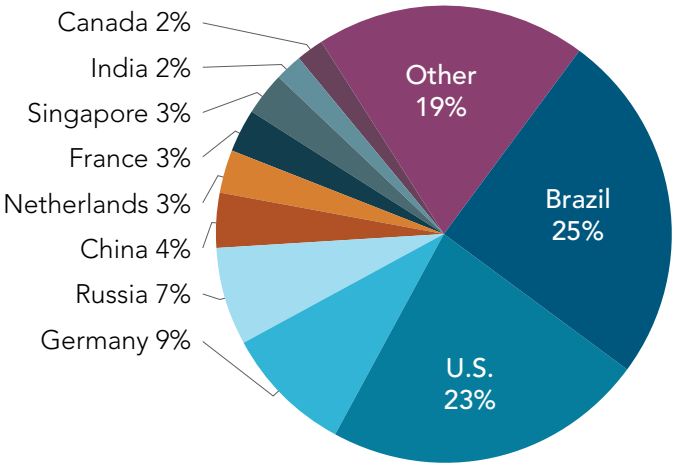
Web Application Attack Statistics / For the first time, Brazil was the top source country for web application attacks (25%), based largely on a series of attack campaigns in April against the hotel industry. The U.S. was a close second at 23%, a huge drop from 43% in Q1. Akamai has seen a steady increase in the amount of malicious traffic coming from Brazil, specifically from cloud-based Infrastructure-as-a-Service (IaaS) data centers. Overall, the U.S. was the top target of web application attacks, receiving 64% overall.

Local File Inclusion (LFI) and SQL Injection (SQLi) accounted for almost 90% of the web application attacks in Q2. This quarter we removed Shellshock from the list of attack vectors. In our experience, Shellshock alerts are most commonly an indicator of companies scanning their own sites for the vulnerability, not actual attacks.



The two most popular attack vectors—SQLi and LFI—accounted for nearly 90% of observed web attacks

Top 10 Source Countries for Web Application Attacks, Q2 2016



Only 23% of attacks originated in the US this quarter, down from 43% last quarter, replaced by Brazil as the top source for web attacks

***State of the Internet / Security* Team**
David Fernandez, Akamai SIRT
Jose Arteaga, Akamai SIRT
Ezra Caltum, Threat Research Unit
Martin McKeay, Sr Security Advocate
Dave Lewis, Security Advocate
Jon Thompson, Custom Analytics
Ryan Barnett, Threat Research Unit
Larry Cashdollar, Akamai SIRT
Miguel Serrano, Security Marketing
Ory Segal, Threat Research Unit
Yossef Daya, Threat Research Unit

Design
Shawn Doughty, Creative Direction
Brendan O'Hara, Art Direction/Design

Contact
SOTIsecurity@akamai.com
Twitter: *@akamai_soti* / *@akamai*
www.akamai.com/StateOfTheInternet

Download the Full Report

[state of the internet] / security report
Q2 2016

Akamai FASTER FORWARD

As the global leader in Content Delivery Network (CDN) services, Akamai makes the Internet fast, reliable, and secure for its customers. The company's advanced web performance, mobile performance, cloud security, and media delivery solutions are revolutionizing how businesses optimize consumer, enterprise, and entertainment experiences for any device, anywhere. To learn how Akamai solutions and its team of Internet experts are helping businesses move faster forward, please visit ***www.akamai.com*** or ***blogs.akamai.com***, and follow ***@Akamai*** on Twitter.

Akamai is headquartered in Cambridge, Massachusetts in the United States with operations in more than 57 offices around the world. Our services and renowned customer care are designed to enable businesses to provide an unparalleled Internet experience for their customers worldwide. Addresses, phone numbers, and contact information for all locations are listed on ***www.akamai.com/locations***.

©2016 Akamai Technologies, Inc. All Rights Reserved. Reproduction in whole or in part in any form or medium without express written permission is prohibited. Akamai and the Akamai wave logo are registered trademarks. Other trademarks contained herein are the property of their respective owners. Akamai believes that the information in this publication is accurate as of its publication date; such information is subject to change without notice. Published 09/16.