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.

**DDoS Update** / Attack activity over the routed network continued to surge, once again setting a record for the number of DDoS attacks, more than doubling when compared with the previous year. This increase was largely driven by repeat attacks on customers, rather than a broadening of the number of targets. In Q1, targets were attacked an average of 29 times each. One customer was attacked a staggering 283 times — about three times per day.

More than half of the attacks (55%) targeted gaming companies, with another 25% targeting the software & technology industry. Those industries were followed by media & entertainment (5%), financial services (4%), Internet & telecom (4%), education (3%), the public sector (2%), and retail & consumer goods (2%).
As in recent quarters, the vast majority of DDoS attacks were based on reflection attacks using stresser/bother-based tools. These tools bounce traffic off servers running vulnerable services such as DNS, CHARGEN, and NTP. In fact, 70% of the DDoS attacks in Q1 used the reflection-based DNS, CHARGEN, NTP, or UDP fragment vectors.

Nearly 60% of the DDoS attacks mitigated in Q1 used at least two attack vectors at once, making defense more difficult. This multi-vector functionality is no longer confined to the most clever attackers; it is now a standard capability in the DDoS-for-hire marketplace and accessible to even the least skilled actors.

Q1 2016 also set a record for the number of DDoS attacks exceeding 100 Gigabits per second (Gbps). There were 19 of these mega attacks, with the largest peaking at 289 Gbps. Fourteen of them relied on DNS reflection methods. Last quarter
there were only five mega attacks; the previous record was 17, set in Q3 2014. The largest of these attacks targeted the software & technology, gaming, and media & entertainment sectors.

While the median size of DDoS attacks has varied only slightly in recent quarters, the number of attacks has continued to grow dramatically since 2013.

**DDoS Size and Frequency as a Function of Time**

While the median size of DDoS attacks has varied only slightly in recent quarters, the number of attacks has grown dramatically since 2013.

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** For the first time, we’ve included an analysis of bot activity in the *State of the Internet / Security Report*. Looking at bot activity over 24 hours, we tracked and analyzed more than 2 trillion bot requests. While known, so-called good bots represented 40% of the bot traffic, 50% of the bot requests were determined to be malicious and were engaged in scraping campaigns and related activity.
**Web Application Attack Statistics** / Web application attacks increased nearly 26% compared with Q4 2015. As in past quarters, the retail sector remained the most popular attack target, targeted in 43% of the attacks. But in a shift from last quarter, we saw a 2% decrease in web application attacks over HTTP and a 236% increase in web application attacks over HTTPS. There was also an 87% increase in SQLi attacks compared with the previous quarter.

As in recent quarters, the US was both the most frequent source of web application attack traffic (43%) and the most frequent target (60%).

As in previous quarters, the retail industry was most frequently targeted with web application attacks in Q1 2016.
state of the internet / security

State of the Internet / Security Team
David Fernandez, Akamai sIRT
Bill Brenner, 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
Q1 2016

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 05/16.