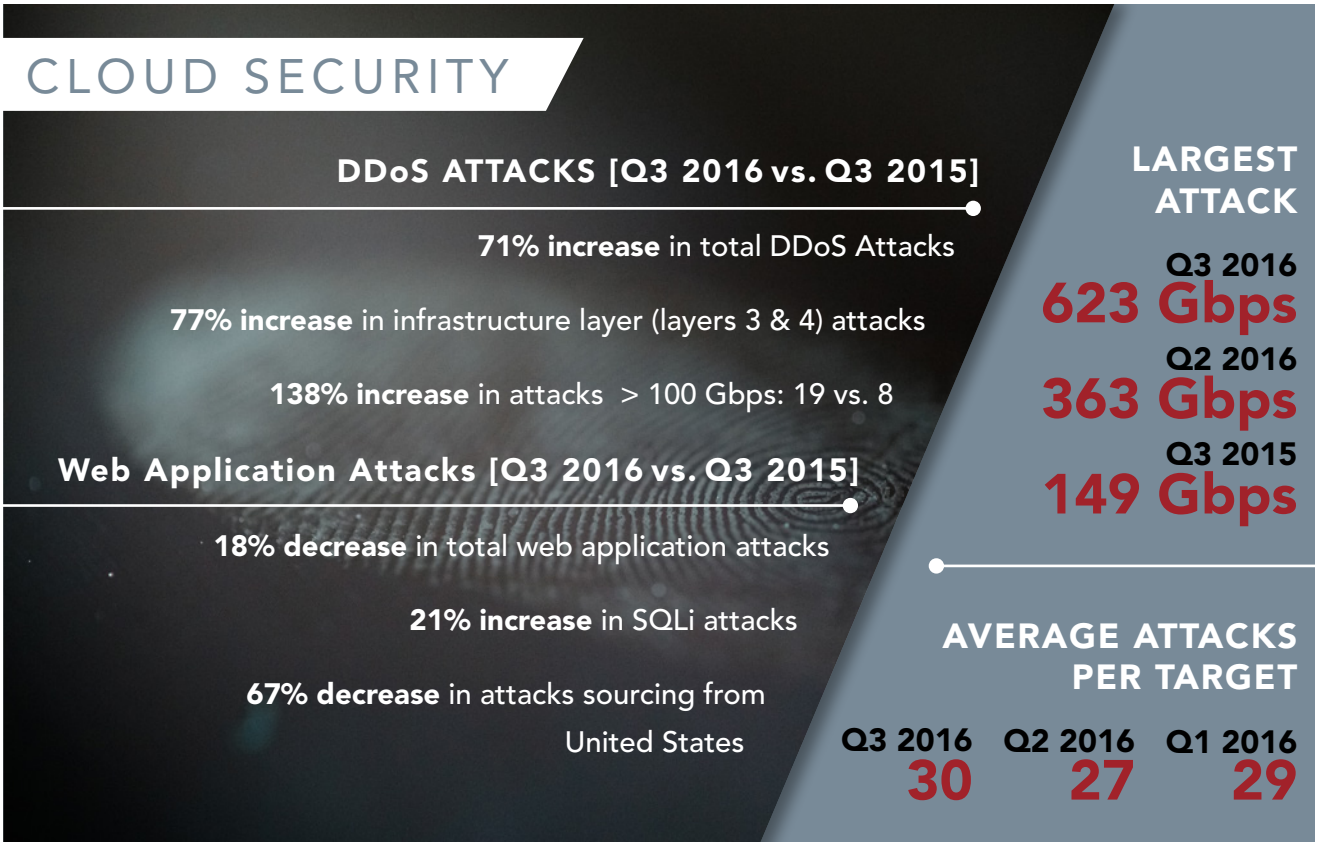
akamai's [state of the internet] / security

Q3 2016 executive summary

ABOUT THE SUMMARY / 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.



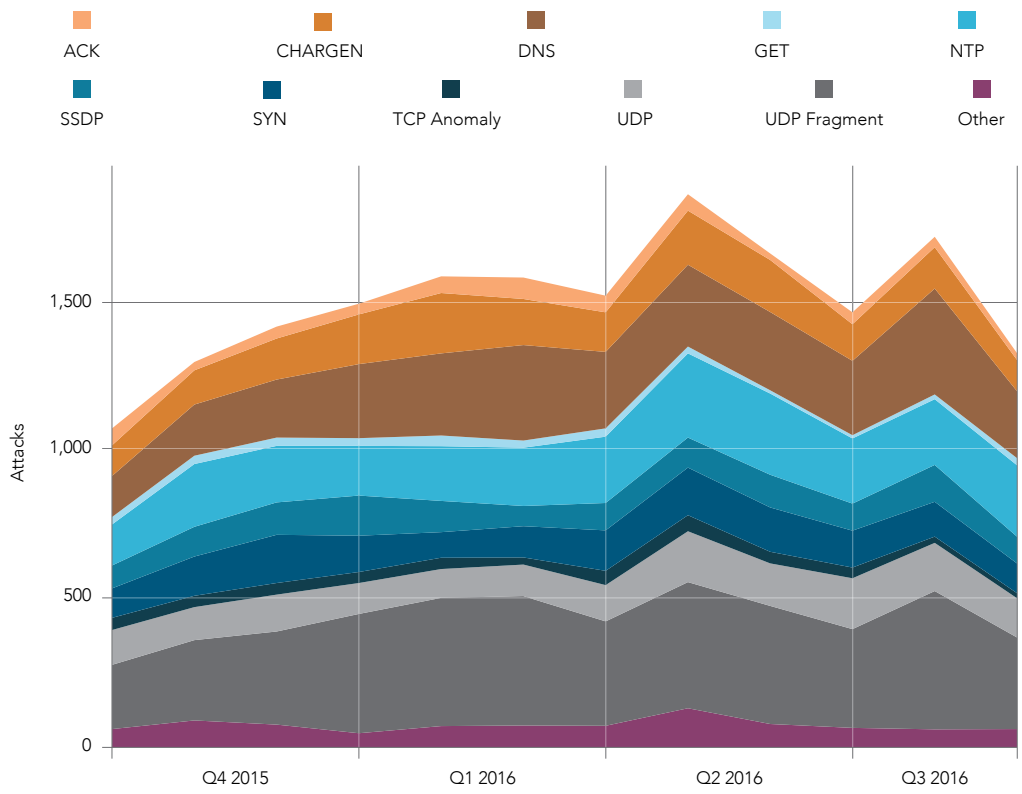
Cloud Security / The *Q3 2016 State of the Internet / Security Report* combines Distributed Denial-of-Services (DDoS) attack data on the routed network with web application and DDoS attack data from the Akamai Intelligent Platform™.

DDoS Update / The size of the largest attacks almost doubled this quarter. Two DDoS attacks occured at a new high of 623 Gigabits per second (Gbps) and 555 Gbps, a significant increase from the previous record of 363 Gbps. Both of these record attacks targeted cybersecurity writer and blogger, Brian Krebs (www.krebsonsecurity.com), who became a lightning rod for the Mirai botnet following a recent publication. The 555 Gbps attack used ACK floods and NTP reflection, but the source of traffic in the 623 Gbps attack was unusual: a malware-based botnet called Mirai, fueled by infected Internet-of-Things (IoT) devices.

Mirai botnets spread like a worm, using telnet and default usernames and passwords to infect devices that then listen for attack commands while scanning for additional vulnerable devices. Attacks include UDP, GRE, ACK, SYN, DNS, Valve Engine, and HTTP floods.

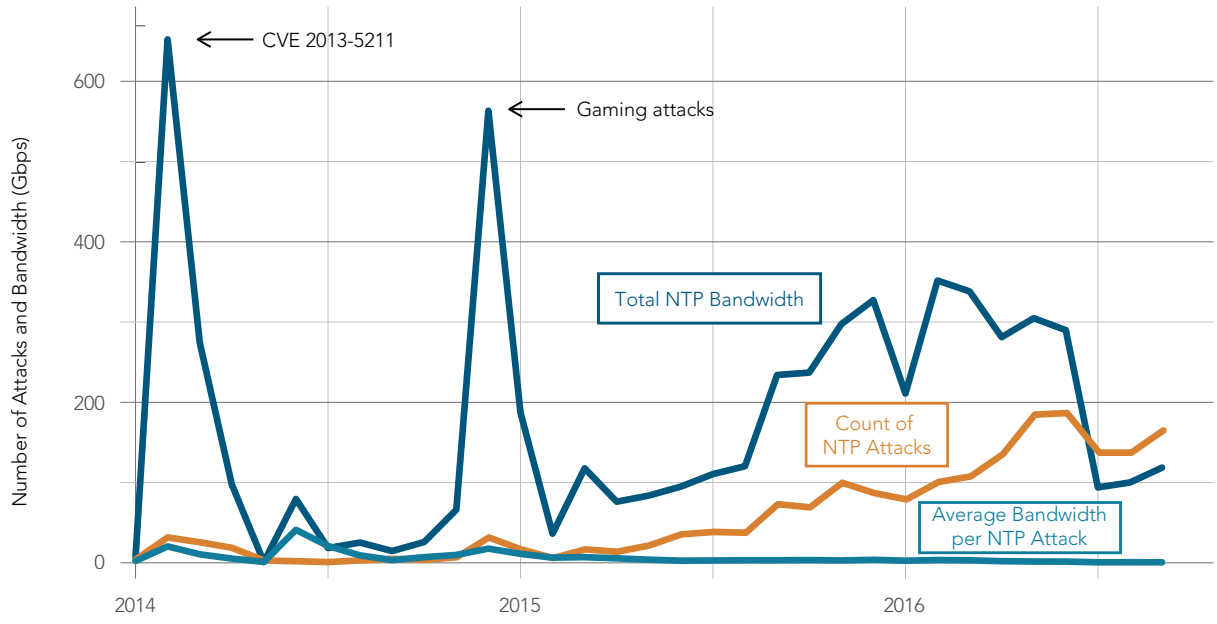
Q1 marked a high point in the number of attacks peaking at more than 100 Gbps, and Q3 matched it with another 19 mega attacks. While the overall number of attacks fell by 8% this quarter, the number and size of large attacks increased. Of the 19 mega attacks, 13 targeted Media & Entertainment, 4 targeted Gaming, and 2 targeted Software & Technology.

The total number of DDoS attacks over the routed network was 4,556, which is up 71% over Q3 a year ago but down 8% compared with last quarter. It is encouraging to see a drop in overall attack numbers, but this trend is unlikely to continue. The winter holiday season has long been characterized by a rise in the number of DDoS attacks, and malicious actors now have a new tool, IoT-fueled botnets, that is likely to be used again.



While there was a surge of attacks in August, the overall number of attacks in the third quarter was down compared with Q2 2016

Last quarter we reported a 276% increase in NTP attacks compared with Q2 2015. Our analysis this quarter indicates that although the number of attacks was high, the amount of traffic each generates has plummeted because the number of unpatched NTP servers available for malicious use continues to shrink. During the 2014 holiday season, the average NTP flood attack delivered over 40 Gbps, while the average NTP attack in this quarter could barely generate 700 Million bits per second (Mbps) – a 98% drop in bandwidth.

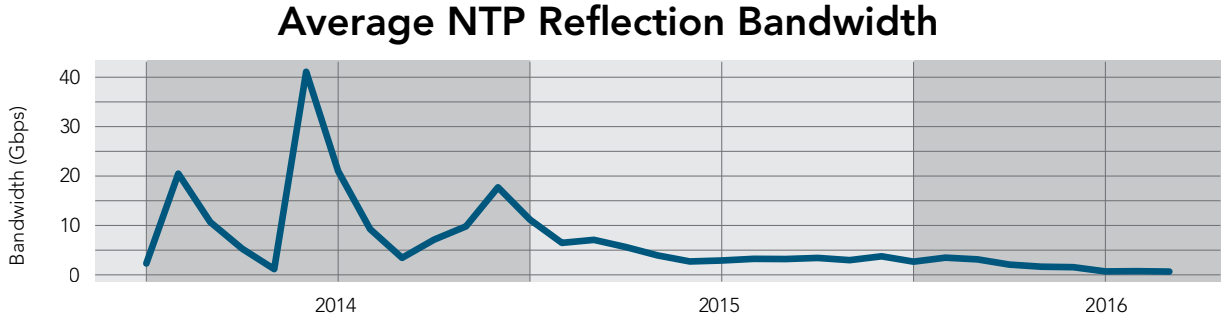


The release of the NTP monlist vulnerability caused a huge spike in NTP attack traffic, followed by a concentrated attack on gaming companies in December 2014

Even though the Mirai botnet used Generic Routing Encapsulation (GRE) floods heavily in Q3, GRE remains a minor component of the overall attack landscape. It is likely, however, that the popularity of GRE floods will grow due to awareness of the recent attacks. Unlike reflection-based attacks, GRE flooding relies heavily upon the capability of the botnet nodes, and it doesn't support amplification of the attack traffic.

This quarter marks a full year with China as the top source country for DDoS attacks. In Q3, China sourced 30% of DDoS attack traffic. On a positive note, the proportion of traffic from China is down 56%, which contributed to the 8% drop in total attacks. The U.S., U.K., France, and Brazil were also among the top five source countries for attacks.

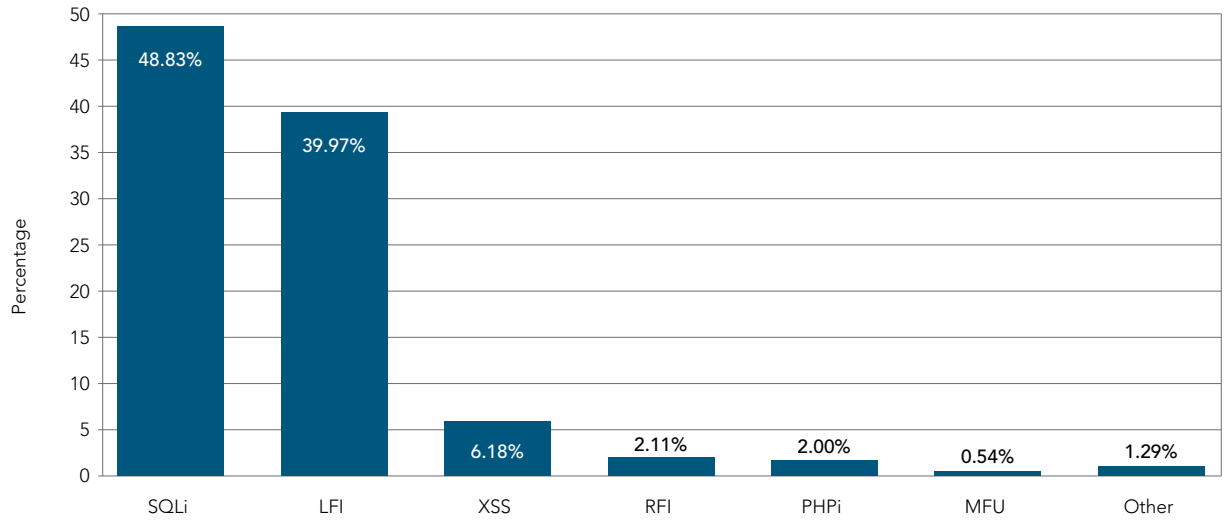
The average number of DDoS attacks increased to 30 per target this quarter, indicating that after a first attack, an organization has a high likelihood of experiencing another attack — and some organizations are under almost continuous attack. The top target organizations were targeted by three to five attacks a day. For these organizations, several short outages daily could have serious negative effect on the reputation of their business.



By June 2016, NTP reflection bandwidth had shrunk to the point that botnet owners started to move on to other protocols

Web Application Attack Statistics / Despite a drop of 13% in web application attacks from the U.S., the country reclaimed the top spot as the greatest source of attack traffic. Brazil, which held the top position last quarter, dropped to fourth place, behind the Netherlands and Russia. With 18% of attacks, the Netherlands was a surprising second-place source. Attackers often obscure the source of a web application attack with the use of proxy servers. These countries were the sources of the IP addresses for the last hop observed.

While the U.S. was the source of 20% of the web application attacks, it was the target of 66% of the attacks.



SQLi accounted for nearly 50% of observed web attacks

Three vectors accounted for 95% of all web application attacks this quarter: SQL Injection (SQLi), Local File Inclusion (LFI), and Cross-site Scripting (XSS). Remote File Inclusion (RFI), PHP Injection (PHPi), and Malicious File Upload (MFU) each accounted for 2% or less.

Out of curiosity, we looked at the relationship between major sporting events and the number of web application attacks. We found that during the UEFA Euro Championship game, attacks sourcing from France and Portugal were down 68% and 95% respectively as compared with a month later. The same trend held for the Summer Olympics in Rio. Attacks sourced from Brazil dropped from 7.3 million in the 17-day period one month earlier to only 1 million attacks during the Olympics. This is interesting, but we suggest you keep your firewall active during such events.

Resources / Access these Q3 2016 cybersecurity resources from Akamai:

1. Kaiten/STD Router DDoS Malware Threat Advisory
2. SSHowDowN Threat Advisory: Exploitation of IoT devices for Launching Mass-Scale Attack Campaigns

***State of the Internet / Security* Team**
Martin McKeay, Senior Security Advocate, Senior Editor
Jose Arteaga, Akamai SIRT
Amanda Fakhreddine, Editor
Dave Lewis, Security Advocate
Larry Cashdollar, Akamai SIRT
Chad Seaman, Akamai SIRT
Jon Thompson, Custom Analytics
Ryan Barnett, Threat Research Unit
Ezra Caltum, Threat Research Unitt

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
Q3 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***.