[state of the internet] / security

Q2 2017 executive summary

Akamai, the world's largest and most trusted cloud delivery platform, 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* 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 on the *State of the Internet* focused on broadband connectivity and cloud security.

Editor's Overview/ Throughout the *State of the Internet / Security Report*, we talk about how the landscape is constantly changing. The second quarter of 2017 saw a number of significant changes in the nature of traffic, including a large reduction in the number of IP addresses participating in volumetric attacks, and a lack of large attacks. Web application attacks continue to increase in frequency, with SQL Injection (SQLi) attacks as the most numerous.

The number of DDoS attacks seen by Akamai is higher this quarter. The largest attacks we're used to seeing, those over 100 Gigabits per second (Gbps), are conspicuously absent for the first time in more than three years. Businesses across the globe were hit by the WannaCry and Petya malware strains, potentially costing the economy in excess of $4 billion. The Mirai botnet continues to be used to attack organizations, while at the same time older strains of malware are being retooled for new uses, such as the PBot botnet that Akamai's Security Intelligence Response Team (SIRT) examines in this quarter's report.

Akamai's researchers examined the traffic created by a malware process called Domain Generation Algorithm (DGA). Botnets use DGA to create a multitude of domains to use as command and control channels, hiding a few real channels in the noise, like a needle in the haystack. We also took a first look at more than nine months of Mirai command and control traffic to understand how the bots are connected. This is another step in our drive toward ever more in-depth research.

Download the full *State of the Internet / Security* report at www.akamai.com/stateoftheinternet-security

DDoS Update / The number of Distributed Denial of Service (DDoS) attacks rose 28% in Q2, following three quarters of decline. The average number of DDoS attacks per targeted customer rose to a high of 32 — an average of a new attack every three days. A single gaming customer was attacked 558 times in this quarter alone.

The Mirai botnet continues to use large numbers of unsecured Internet of Things devices, but this quarter an old strain of malware, called PBot, was retooled to attack its target with hundreds, rather than tens of thousands, of compromised nodes. This botnet was used in the biggest attack of the quarter, measured at 75 Gbps, targeting a financial organization.

DoS attack sizes quickly fluctuate with the popularity and availability of new malware variants and attack tools. The largest DDoS attacks in 2016 were 500–600 Gbps or more, a significant jump from 100 Gbps attacks in 2014 and 2015. Even though the largest attack this quarter was relatively tame at 75 Gbps, experience tells us this calm cannot last long.

Infrastructure-layer, volume-based attacks accounted for 99% of DDoS attacks in Q2, in large part due to the availability of "for rent" botnets. This is primarily because volumetric attacks that attack the application layer are rare. It's more likely for this type of attack to target the application, such as the web or database weaknesses, than it is for them to rely on brute force for their effect.

A majority of DDoS traffic is being generated using reflection techniques, in which common Internet protocols are queried excessively using spoofed IP addresses, and their responses are directed at the attacker's target. The most popular types of reflectors, Domain Name Services (DNS) and Network Time Protocol (NTP), amplify traffic by factors up to 100 times or more, and are readily available globally.

DDoS ATTACKS [Q2 2017 vs. Q1 2017]

- 28% increase in total DDoS attacks
- 27% increase in infrastructure layer (layers 3 & 4) attacks
- 21% increase in reflection-based attacks
- 28% increase in average number of attacks per target

LARGEST DDoS ATTACKS

- Q2 2017: 75 Gbps
- Q1 2017: 120 Gbps
- Q4 2016: 517 Gbps
- Q3 2016: 623 Gbps
- Q2 2016: 363 Gbps

Web Application Attacks / The number of web application attacks continues to grow each quarter. Where volumetric DDoS attacks might affect a site for minutes, hours, or possibly weeks, web application attacks can lead to the compromise of an organization's site, with much longer-lasting and important business implications.

WEB APPLICATION ATTACKS [Q2 2017 vs. Q1 2017]

- 5% increase in total web application attacks
- 4% increase in attacks sourcing from the U.S. (top source country)
- 21% increase in SQLi attacks

TOP WEB APPLICATION ATTACK VECTORS (Q2 2017)

- SQL Injection (SQLi): 51%
- Local File Inclusion (LFI): 33%
- Cross-Site Scripting (XSS): 9%

Web application attacks differ from volumetric attacks because they aren't aimed at choking services with too much traffic. Instead, they target weaknesses in the servers to try to compromise the underlying services and systems. The most common attacks, SQLi, Local File Inclusion, and Cross-Site Scripting, are attempts to get to data or exploit weaknesses on web servers.

In many cases, Akamai uses behavioral analysis techniques to detect potentially malicious activity and block web application attacks. In Q2, we examined DNS-related traffic logged to Akamai's Cloud Security Intelligence (CSI) platform to understand anomalous behavior seen on networks infected with malware. Some popular botnets use Domain Generation Algorithms (DGA), a technique that generates new domain names daily and shifts command and control infrastructure to avoid takedown. Identifying the relevant characteristics and practicing machine learning algorithms allow us to identify abnormal behaviors that lead to detecting and blocking malware activity.

Business Implications / This quarter saw a rise in the number of both DDoS and web application attacks targeting organizations Akamai protects. The numbers show a rebound in DDoS attacks compared to the last three quarters. Does this indicate that we're going to see future increases in the number of attacks? There's no way to be certain, but we do know that both web application and DDoS attacks are cyclical, and that they often return more powerful than ever. It would require a tectonic shift to the nature of the Internet to change this fact. So, like planning for the holiday season, we have to plan for the next high tide of attack traffic.

Understanding the tools attackers currently use, like Mirai and PBot, enables us to infer what we might see in the future. Researching the methods used by malware to hide, such as Domain Generation Algorithms, leads to unmasking the traffic controlling the malware. The more we can see what the ill-intentioned wizard is doing behind the curtain, the more we can protect the systems we're charged with guarding.

For more analysis and research, download the full report.

The Q2 2017 *State of the Internet / Security Report* combines attack data from across Akamai's global infrastructure and represents the research of a diverse set of teams throughout the company.

State of the Internet / Security Team
Jose Arteaga, Akamai SIRT Lead, Data Wrangler — Attack Spotlight
Dave Lewis, Global Security Advocate — DDoS Activity, Web Application Attack Activity
Chad Seaman, Akamai SIRT — Attack Spotlight, Mirai Command and Control Clusters
Wilber Mejia, Akamai SIRT — Attack Spotlight
Alexandre Laplume, Akamai SIRT — Attack Spotlight
Elad Shuster, Security Data Analyst, Threat Research Unit
Or Katz, Principal Lead & Security Researcher — Domain Generation Algorithm
Jon Thompson, Custom Analytics
Shrijita Bhattacharya, Intern — Mirai Command and Control Clusters

Editorial Staff
Martin McKeay, Senior Security Advocate, Senior Editor
Amanda Fakhreddine, Sr. Technical Writer, Editor

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

Contact
sotisecurity@akamai.com
Twitter: *@akamai_soti* / *@akamai*
www.akamai.com/stateoftheinternet-security

Download the Full Report

[state of the internet] / security
Q2 2017 full report

About Akamai
As the world's largest and most trusted cloud delivery platform, Akamai makes it easier for its customers to provide the best and most secure digital experiences on any device, anytime, anywhere. Akamai's massively distributed platform is unparalleled in scale with over 200,000 servers across 130 countries, giving customers superior performance and threat protection. Akamai's portfolio of web and mobile performance, cloud security, enterprise access, and video delivery solutions are supported by exceptional customer service and 24/7 monitoring. To learn why the top financial institutions, e-commerce leaders, media & entertainment providers, and government organizations trust Akamai please visit *www.akamai.com*, *blogs.akamai.com*, or *@Akamai* on Twitter. You can find our global contact information at *www.akamai.com/locations*. Published 08/17