[state of the internet] / security

Q3 2017 executive summary

Akamai

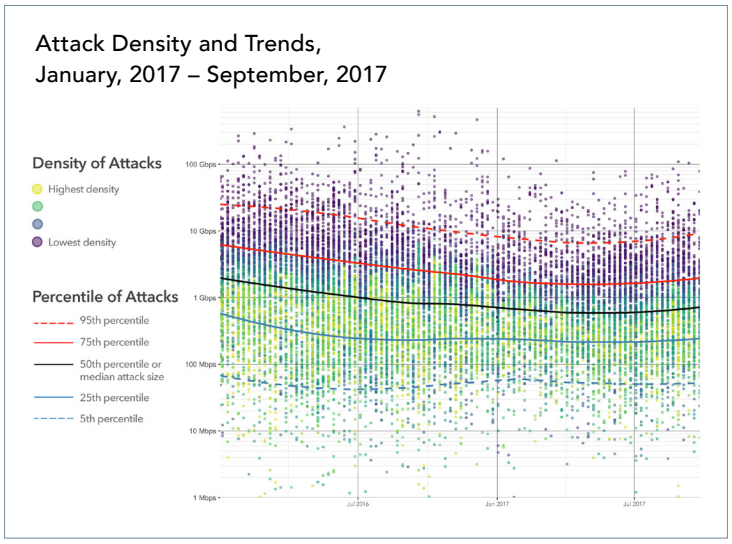
Akamai, the world's largest and most trusted cloud delivery platform, uses its globally distributed Akamai Intelligent Platform™ to process trillions of Internet transactions each day. This allows us to gather massive amounts of data on metrics related to broadband connectivity, cloud security, and media delivery. The *State of the Internet* was created to enable businesses and governments to make better strategic decisions by leveraging this data and the insights it offers. Each quarter, Akamai uses this data to publish reports on the State of the Internet, focused on broadband connectivity and cloud security.

The Q3 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.

Business Implications / The third quarter's headlines have illustrated the severe financial and business toll that cyber attacks have had on businesses across many industries. With data showing that attacks are on the upswing as we head into the critical end-of-year and holiday season, the implication is clear: Cyber security can only be ignored at great peril. This is exactly what this quarter's guest author, Veracode Co-Founder and CTO Chris Wysopal, began warning the world of almost two decades ago.

As a baseline, organizations must keep software and firmware patched and up to date, and DDoS protections need to be an integral part of plans and preparations for holiday traffic levels. Constant re-evaluation of the threats businesses face isn't a luxury — it's essential. Understanding attackers' evolving strategies is critical to building a more resilient defense against their attacks. This quarter's SOTI/S Report takes a close look at the rise and fall of the new Android-based WireX botnet, in addition to showcasing research on the Fast Flux networks used by botnets to hide their malicious activities and obscure their command and control communications, making detection far more difficult.

Editor's Overview / Recent headlines reflected some of the most far-reaching cyber security incidents seen to date, from Yahoo's revelation that all of its 3 billion accounts had been compromised, to the Equifax breach that exposed the sensitive data of 146 million Americans. Meanwhile, estimates of the severe financial impact of the second quarter's NotPetya malware outbreak began to roll in, with multiple companies reporting that the ransomware cost them hundreds of millions of dollars each.



While these incidents grab headlines, the reality is that more common attacks, like DDoS and web application attacks, can be just as disruptive to an organization. These attacks are happening with greater frequency to businesses of all sizes and across all industries. In Q3, Akamai saw the number of both DDoS attacks and web application attacks rise quarter over quarter, increasing by 8% and 30%, respectively. Median attack size also increased, as did the frequency of attacks per target.

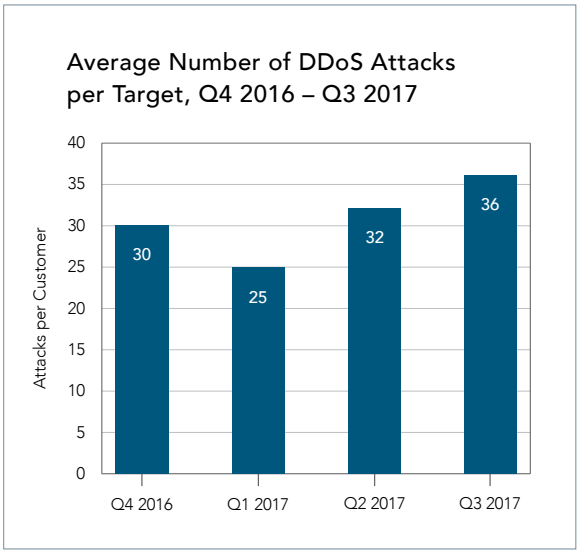
Although traditional attack vectors and platforms remain popular and effective, cyber criminals continue to advance their arsenals. This quarter, we saw the continued leveraging of Mirai malware, which uses Internet of Things devices, as well as the introduction of WireX, which commandeers Android devices. Both highlight the vast potential that exists for new sources of botnet armies.

DDoS Update / Distributed Denial of Service (DDoS) attacks are costly — they can bring down sites, disrupt businesses, and divert resources. They can also be used to provide cover for more insidious data or system breaches. In the third quarter, DDoS attacks continued Q2's upward trend, rising another 8%. The average number of DDoS attacks per targeted customer also continued upward, increasing to 36 —

DDoS ATTACKS [Q3 2017 vs. Q2 2017]

- 8% increase in total DDoS attacks
- 8% increase in infrastructure layer (layers 3 & 4) attacks
- 4% increase in reflection-based attacks
- 13% increase in average number of attacks per target

on average, more than one attack every three days. On the high end, a single Gaming customer endured 612 DDoS attacks in the third quarter alone — an average of nearly seven attacks for every day in the quarter.



The third quarter's DDoS attacks involved many familiar attack vectors. The Mirai malware strain leveraged enormous numbers of Internet of Things (IoT) devices to generate some of the largest DDoS attacks on record — the largest seen by Akamai was 623 Gbps. Though the botnet is not quite as active today, Mirai continues to threaten, and, in the third quarter, was again responsible for the largest attack seen — this one peaking at 109 Gbps.

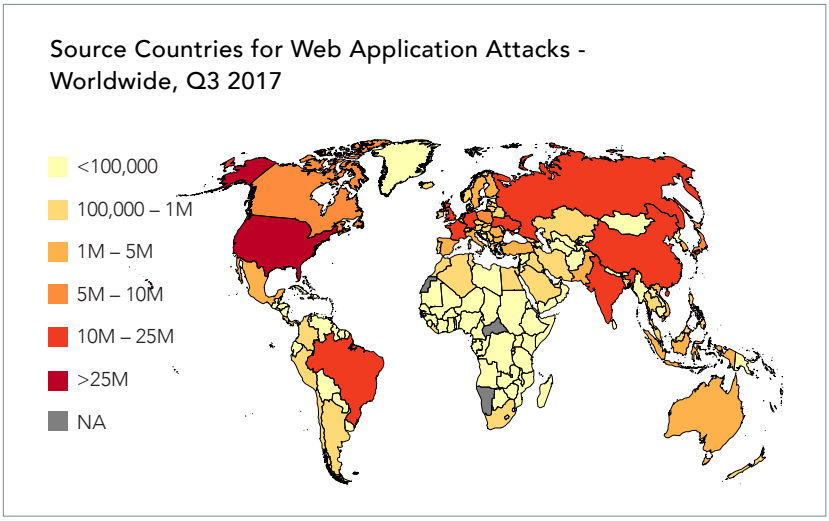
The third quarter also saw the introduction of WireX — notable not only as one of the first large Android-based botnets, but also for the way it propagated. Consumers around the world unsuspectingly downloaded the malware via legitimate-looking infected apps in the Google Play Store. Although WireX spread quickly, a joint effort by several companies — including Akamai — demonstrated the power of cross-industry collaboration in successfully taking down WireX while still in its relative infancy. However, like Mirai, WireX can be expected to persist, evolve, and flourish. Organizations need to be prepared for the possibility that much larger DDoS attacks might occur at any time, as new techniques are continually being developed.

Web Application Attacks Update / In contrast to DDoS attacks, web application attacks tend to target application vulnerabilities — rather than trying to overwhelm the website — in order to steal data or otherwise compromise the underlying system. Web application attacks are far more common than DDoS attacks, and their frequency makes them both easier to ignore and potentially more damaging. Unfortunately, these types of attacks are continuing to grow more common each quarter, with attack frequency jumping 30% in Q3. Fully 85% of the attacks leveraged either SQL injection or Local File Inclusion, the top two attack vectors.

WEB APPLICATION ATTACKS [Q3 2017 vs. Q2 2017]

- 30% increase in total web application attacks
- 48% increase in attacks sourcing from the U.S. (top source country)
- 19% increase in SQLi attacks

The United States continues to be the clear front-runner as both the source and the target of the bulk of the web application attack traffic seen by Akamai. In the third quarter, the U.S. saw more than 300 million web application attacks, roughly 5 times the number seen in the next-highest country, Russia.



For more analysis and research, download the full report.

***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
Q3 2017 full report