[state of the internet] / security

Q4 2017 executive summary

Akamai

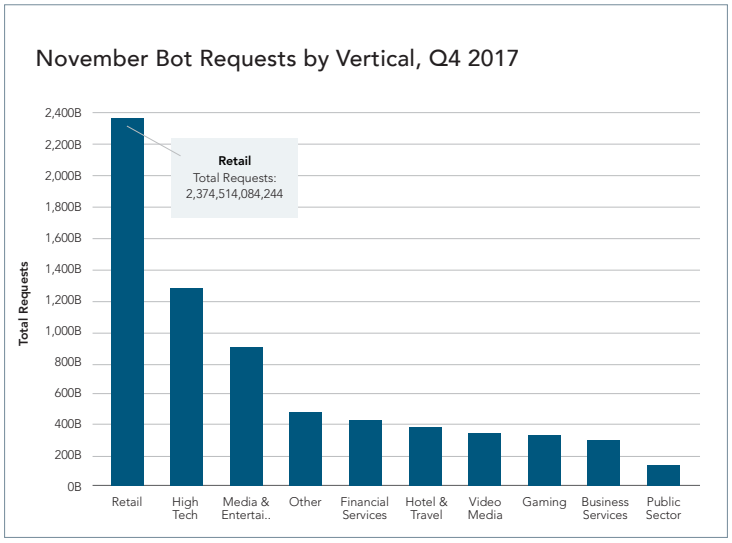
Executive Summary / Akamai, the world's largest and most trusted cloud delivery platform, uses its globally distributed Akamai Intelligent Platform™ to process trillions of Internet transactions each day. This allows us to gather massive amounts of data on metrics related to broadband connectivity, cloud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

Business Implications / With some of the costliest and most disruptive attacks on record, 2017's high-profile incidents have heightened awareness around the business-critical nature of cyber security. The treacherous hardware flaws that enabled Spectre and Meltdown allow malicious programs to read data in a computer's memory without having privileges to do so. The existence of such pervasive and insidious vulnerabilities, along with the examples of the severe havoc they can wreak, should be enough to light a fire under even the most sanguine.

Many of today's attacks still leverage well-known vulnerabilities — flaws that have been documented and patched, and can be prevented. Although it may be easier said than done, collective efforts to cover the basics — secure coding practices, timely patching, proper device configuration, and prudent password management, would go a long way towards fortifying defenses.

The security landscape is continually changing, as criminals take advantage of new attack surfaces. Attacks targeting mobile devices, Internet of Things, and APIs are all major themes that we expect to see in 2018. Attack strategies continue to evolve. We are seeing a new trend of enterprise systems being targeted, not only to steal their data, but to steal their computing resources, perhaps driven in part by the rise of cryptocurrencies and the potential value of mining resources. In addition, this quarter's *State of the Internet / Security* report takes a look at some unique data sets on Akamai network connectivity, botnet traffic, and credential abuse, revealing that a high percentage (43%) of login attempts at websites are malicious. Understanding trends like these is now critical to the well-being of any digitally connected enterprise.

Editor's Overview / As we embark on a new year, it is a good time to reflect on the lessons of the previous one.



Year-over-year numbers suggest that both DDoS and web application attacks continue to rise, with criminals continuing to make effective use of long-standing, tried-and-true attack vectors. This drives home the unassailable importance of following basic security best practices, such as properly configuring and patching connected devices, as well as following secure coding guidelines like sanitizing data input.

In Q4, we saw the continued impact and evolution of the Mirai botnet. This quarter's *State of the Internet / Security* report takes a look at Mirai's activity and evolution over the past year to help us prepare for what Mirai might bring in the future. Akamai SIRT member Larry Cashdollar does a deep dive into a pair of CVEs that you should be aware of. The spotlighted vulnerabilities are the most severe type, which allow execution on a system without requiring authentication. We also had an opportunity this quarter to look at two data sets that have not been part of the *State of the Internet / Security* report before: analysis of bot traffic and analysis of credential abuse attempts.

Finally, we expect cryptocurrencies to play a larger role in the security headlines we see in 2018. They may be a factor in the trend we see of enterprise machines being infiltrated for their computing resources, and cryptocurrencies are likely to be a force that shapes hackers' continually evolving strategies in many other ways as well.

DDoS ATTACKS [Q4 2017 vs. Q3 2017]

- Less than 1% decrease in total DDoS attacks
- 1% decrease in infrastructure layer (layers 3 & 4) attacks
- 3% decrease in reflection-based attacks
- 115% increase in application-layer attacks

DDoS Update / Distributed Denial of Service (DDoS) attacks can bring down websites, disrupt businesses, and divert resources — sometimes serving as cover for more insidious data or systems breaches. After a couple quarters of increasing attacks, during the fourth quarter of 2017, DDoS attacks leveled off, decreasing very slightly (less than 1%) compared with the previous quarter. Notably, application-layer attacks increased by a sizable 115% quarter over quarter, but they still comprised less than 1% of overall DDoS attacks. DDoS attacks showed a 14% increase compared to Q4 2016, indicating an overall upward trend in the longer term.

The gaming industry was the most-targeted industry, suffering 79% of all DDoS attacks in Q4. The second most-attacked industry, financial services, saw a significant uptick in DDoS activity in the fourth quarter, with a high of 45 attacks during a single week. The frequency of these attacks underscores the need for a robust DDoS mitigation solution, not only to prevent disruption but also to protect against multi-pronged attacks that can use DDoS campaigns as cover for more insidious system breach attempts.

Web Application Attacks Update / In contrast to DDoS attacks, web application attacks typically target application vulnerabilities in order to steal data or otherwise compromise the underlying system. Web application attacks are much more common than DDoS attacks, with attackers often simply scanning the Internet for vulnerable sites to victimize. Following a large 30% quarter-over-quarter jump in Q3, web application attacks saw a slight decline in Q4, but still grew significantly overall in 2017, a trend we expect to continue in 2018.

WEB APPLICATION ATTACKS [Q4 2017 vs. Q3 2017]

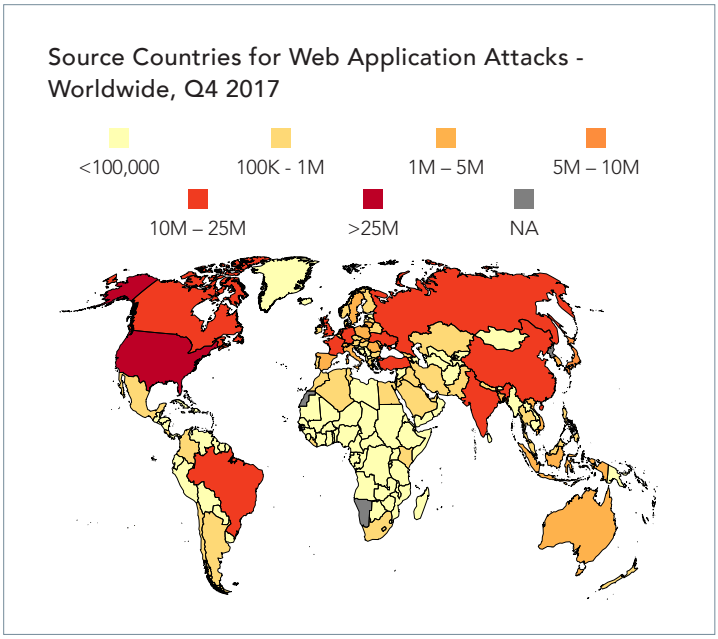
- 9% decrease in total web application attacks
- 29% decrease in attacks sourcing from the United States
- 9% decrease in SQLi attacks

The dominant attack vector continues to be SQL injection, which accounted for 50% of all web application attacks recorded in Q4, up from 47% in Q3. These types of attacks are easily automated and scalable, and will continue to be effective as long as organizations do not take appropriate precautions such as validating user input in their code.

The United States continues to be the clear front-runner as both the source and the target of the web application attack traffic seen by Akamai. The country saw 238 million web application attacks in Q4, down from 323 million in Q3, but still more than 10 times the number seen in the next-highest country, Brazil. The United States was the source of 132 million attacks in the fourth quarter, while the Netherlands was the source of the next-highest number at 47 million.

For more analysis and research, download the full report.

The Q4 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
Wilber Mejia, Akamai SIRT — Attack Spotlight
Alexandre Laplume, Akamai SIRT — Attack Spotlight
Larry Cashdollar, Akamai SIRT, Sr. Engineer — Web Vulnerabilities to Watch
Richard Willey, Sr. Data Scientist — How to Make Sense of a Planetary Scale Network
Elad Shuster, Security Data Analyst, Threat Research Unit
Jon Thompson, Custom Analytics

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

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

Download the Full Report

[state of the internet] / security
Q4 2017 full report