SOTI SUMMER 2018

[state of the internet] / security

EXECUTIVE SUMMARY

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. Each quarter, Akamai publishes *State of the Internet* reports based on this data, with a focus on broadband connectivity and cloud security.

BUSINESS IMPLICATIONS

The attacks we saw in recent months remind us that the state of Internet security is never static. Attackers' ingenuity never rests; they continue to discover new vectors and exploit new vulnerabilities, developing attack strategies that are more disruptive than ever before. In 2017, we saw new classes of devices, such as mobile phones and IoT devices, being leveraged into vast botnets responsible for attacks of record-setting size. However, in the first two months of 2018, those previous records were already smashed, as attackers leveraged a new vector, memcached — a service that was originally not even meant to be exposed to the Internet — to generate attacks in excess of a crippling 1 Tbps. Memcached enables attacks to be amplified by orders of magnitude greater than any previously known reflection attack.

Fortunately, in this case, a swift response by developers, network operators, and service providers seems to have quickly reduced the number of vulnerable memcached servers available, hopefully limiting the potential of this new attack vector in the future. This serves as a not-so-gentle reminder that the security community can never grow complacent; we must stay aware of attack trends and technology advances, and be prepared for growing attack sizes. In addition, it is up to the community as a whole to stay up to date with software patches and secure configurations in order to minimize criminals' access to attack surfaces.

EDITOR'S OVERVIEW

Just as the state of Internet security continues to evolve, so does this report. We are implementing changes in publication frequency, format, and structure, in an effort to bring you insights from our data and research in a way that is as timely and relevant as possible. Much of the statistical data and graphics on DDoS and web application attacks (including graphs on DDoS attack size and vector frequency) has been shifted to our website. Look for updates in our blog. In addition, we will regularly publish shorter, more streamlined reports that focus on longer-term trends, research, and analysis. The *State of the Internet / Security: Web Attack* report will now be published twice a year in winter and summer.

Our Summer 2018 Attack Spotlight focuses on the February 2018 memcached reflector attack that set a new record for the largest attack Akamai has mitigated to date. At 1.3 Tbps, the attack more than doubled the previous record of 623 Gbps achieved by

1 Tbps

Threshold broken by the memcached reflector

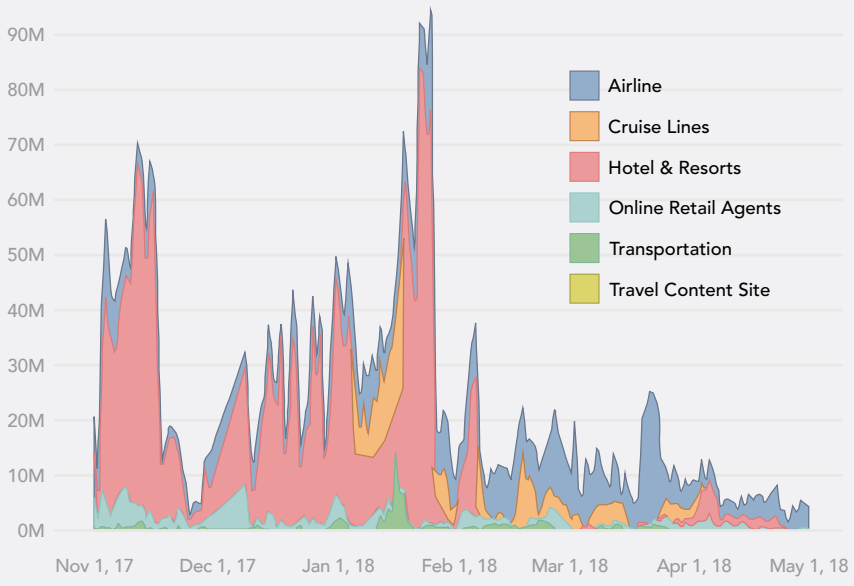
Mirai in September 2016. Median DDoS attack sizes also continued to increase over the past year, now reaching 1.3 Gbps, underscoring the importance to every organization for being prepared for large-scale attacks.

In the *Summer 2018 State of the Internet / Security: Web Attack* report, we examine some DDoS attacks employing unusual tactics to increase attack effectiveness. While the majority of DDoS attacks are simple and volumetric in nature, a few show the influence of intelligent, adaptive enemies who change tactics to overcome the defenses in their way.

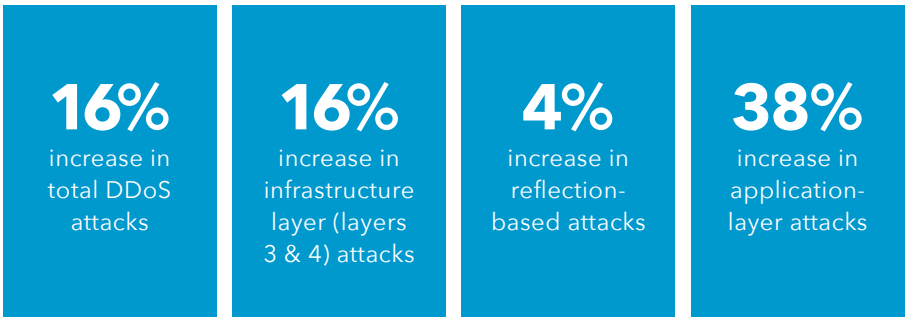
Operation Power Off, a law enforcement effort to shut down DDoS-for-hire websites, is a topic of great interest. A coordinated effort in April 2018 among law enforcement agencies in multiple countries shut down the site Webstresser.org, a major player in the DDoS-for-hire marketplace, allegedly responsible for millions of attacks. Given how lucrative these sites are, we would not be surprised if others pop up to take its place before long.

Finally, building on the bot and credential abuse data we first analyzed in the *Q4 2017 State of the Internet / Security* report, we dig deeper to better characterize and understand the bots and the credential abusers targeting the hospitality industry — the vertical that saw the highest percentage of malicious logins by far. We also note that the closure of several routes in early February 2018 seems to have precipitated a steep decline in malicious traffic.

fig 1.1 **Malicious login attempts: Hotel and Travel**



DDOS ATTACKS, SUMMER 2018 VS. SUMMER 2017



For more analysis and research, download the full report.

The *Summer 2018 State of the Internet / Security: Web Attack* 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, Data Wrangler — Attack Spotlight
Dave Lewis, Global Security Advocate — Operation Power Off
Wilber Mejia, Akamai SIRT — Attack Spotlight
Elad Shuster, Security Data Analyst Advanced DDoS — Akamai Blog
David McEwan, Security Operations Command Center — Advanced DDoS
Alejandro Ziegenhirt, Security Operations Command Center — Advanced DDoS

EDITORIAL STAFF

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

CREATIVE

Shawn Broderick and Sajeesh Alakkaparambil, Design
Georgina Morales Hampe and Kylee McRae, Project Management

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 more than 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, online retail leaders, media and 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 or call 877-425-2624. Published 06/18.