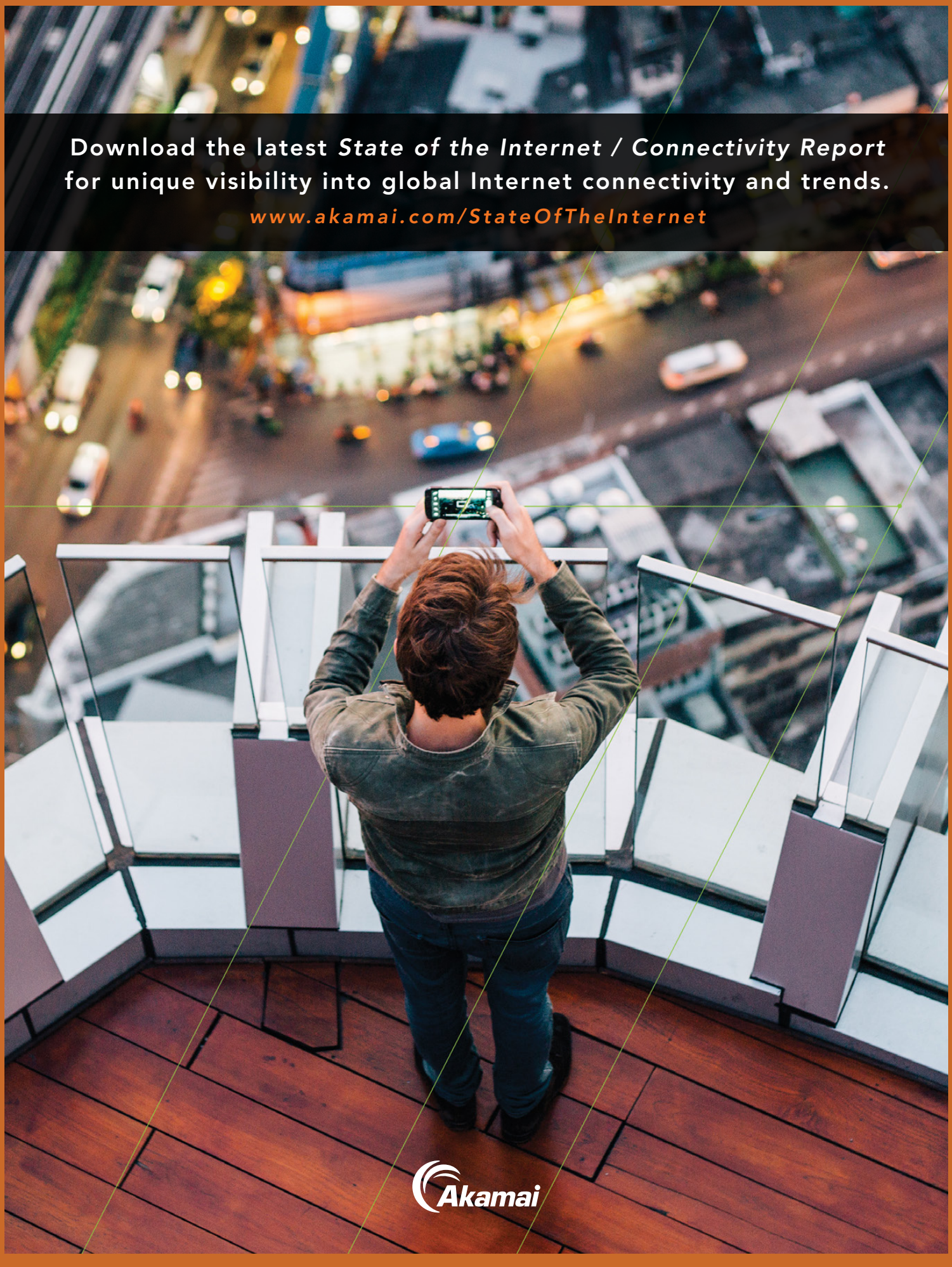
[Volume 3 / Number 2]

akamai's [state of the internet] / security

Q2 2016 report


Download the latest *State of the Internet / Connectivity Report*
for unique visibility into global Internet connectivity and trends.
www.akamai.com/StateOfTheInternet
Akamai

AT A GLANCE

DDoS attacks, Q2 2016 vs. Q2 2015

129% increase in total DDoS attacks
151% increase in infrastructure layer (layers 3 & 4) attacks
276% increase in NTP reflection attacks (a record high)
70% increase in UDP flood attacks

DDoS attacks, Q2 2016 vs. Q1 2016

9% increase in total DDoS attacks
10% increase in infrastructure layer (layers 3 & 4) attacks
47% increase in UDP flood attacks
37% decrease in attacks > 100 Gbps: 12 vs. 19

Web application attacks, Q2 2016 vs. Q1 2016

14% increase in total web application attacks
197% increase in attacks sourcing from Brazil (new top source country)
13% decrease in attacks sourcing from United States (previous top source country)
7% increase in SQLi attacks

**Note: rounded to the nearest percentage*

What you need to know

- Akamai mitigated 4,919 DDoS attack events within the Akamai routed DDoS mitigation network—an increase from Q1 2016's 4,523 attack events.

- Twelve attacks exceeded 100 Gbps, including two attacks exceeding 300 Gigabits per second (Gbps) against the media & entertainment sector. Six of these 12 mega-attacks were also high packet-per-second attacks.

- The largest attack of the quarter peaked at 363 Gbps, setting a new attack bandwidth record for Akamai.

- Akamai mitigated 21 attacks that exceeded 30 million packets per second (Mpps), setting a new quarterly record. The previous record was set in Q2 2015 (18 attacks > 30 Mpps).

- Despite the number of mega-attacks, Akamai saw a significant reduction in median attack bandwidth, dropping 36% from the previous quarter.

- NTP reflection attacks increased 44% compared with Q1 2016 and accounted for 16% of all DDoS attacks mitigated this quarter. Out of the nearly 80,000 reflectors tracked worldwide in Q2 2016, 59% were NTP reflectors.

- May was the most active month for DDoS activity with 38% of the attacks for the quarter. Peak activity targeted the gaming, financial services, and software & technology industries.

- There was an average of 27 DDoS attacks per target in Q2, down from an average of 29 attacks per target in Q1. The hardest hit target was attacked 373 times.

- In a single day analysis, 43% of web traffic across the Akamai Intelligent Platform™ was bot traffic. Of the bot traffic, 63% were malicious automation tools and scraping campaigns.

- In Q2 2016, 77% of web application attacks were launched over HTTP rather than HTTPS.

- As Brazil took the world stage for sporting events, there was a significant increase in web application attacks against the hotel & travel industry, with 21% of the attacks in Q2 vs. only 7% of the attacks in Q1. For the first time, Brazil was the top source country for web application attacks (25%). The US was a close second (23%).

- ATO (account takeover) attempts targeted more than 20,000 domains and subdomains. While they occurred in almost all sectors, the retail and financial sectors were targeted most frequently.

- In a 15-day study on the use of anonymization tools used in web attacks, nearly 32% of the attacks took advantage of anonymizing VPNs or proxies to mask identities.

LETTER FROM THE EDITOR / The *Q2 2016 State of the Internet / Security Report* is an ever-evolving look at the combined data collected from the Akamai Intelligent Platform™, our Cloud Security Intelligence (CSI) data analysis engine, and our routed DDoS solution.

In the second quarter of 2016, Akamai observed the largest DDoS attack measured on our routed network to date, peaking at 363 Gigabits per second (Gbps). ***The DDoS Attack Spotlight*** digs into the details of this multi-vector attack. We also saw more web application and DDoS attacks than ever before, a trend that shows no sign of reversing. In contrast to the growing number of attacks, the size of DDoS attacks was significantly smaller this quarter, with the exception of a few outliers.

Last quarter, we took an in-depth look at Account Takeover (ATO) attacks. To expand upon this research, we examined a pool of IP addresses associated with ATO attacks in order to observe a possible correlation between these IP addresses and other types of application layer attacks seen on our platform. This is outlined in ***Section 3.2***.

In our ***Web Application Attack Spotlight***, Akamai highlights the use of anonymizing services, such as virtual private networks (VPNs) and proxies. Because these services make tracking attackers so much harder, it should be no surprise that they are relatively common. We found that nearly 32% of the web application attacks observed by Akamai use anonymizing technologies to hide an attacker's identity.

The report authors include security professionals from several divisions within Akamai, including the Akamai Security Intelligence Response Team (SIRT), the Threat Research Unit, InfoSec, and the Custom Analytics group. We hope you find the report valuable.

Thank you.

— Akamai's *State of the Internet / Security* Team

As always, if you have comments, questions, or suggestions regarding the *State of the Internet / Security Report,* connect with us via email at ***SOTIsecurity@akamai.com***. You can also interact with us in the *State of the Internet* subspace on the Akamai Community at ***https://community.akamai.com***. For additional security research publications, please visit us at ***www.akamai.com/cloud-security***.

[SECTION][1] EMERGING TRENDS

Each quarter, Akamai has seen an increase in the number of Distributed Denial of Service (DDoS) attacks, and the second quarter of 2016 was no exception — there were 4,919 attacks, a 9% increase compared with the previous quarter's 4,523 attacks. The attacks were directed at 179 targets, with the average number of repeat attacks falling slightly to 27 attacks per customer compared with 29 the previous quarter. Hopefully, this is a change in the trajectory of repeat attacks. However, one customer was subject to 373 attacks this quarter.

In contrast to the growing number of DDoS attacks, a number of indicators showed that attack size dropped precipitously in the last quarter. The median attack size dropped 36% in the last quarter to 3.85 Gigabits per second (Gbps), an average size Akamai has not seen since we first started tracking this statistic. The higher end of the attack scale fell by almost the same amount, and smaller attacks shrank by a bit more, 40%. Although attack size decreased, few organizations can withstand even these smaller attacks without help.

Changes in several metrics indicated changes in the tools that booter/stressor sites and botnets are using. Multi-vector attacks dropped 10 percentage points from the previous quarter, accounting for 49% of all attacks. While there were only 12 mega attacks (100+ Gbps) in Q2 compared with 19 in Q1, a record-setting 21 attacks measured more than 30 million packets per second (Mpps) compared with six in Q1. But of those high packet per second attacks, only six were also mega attacks (peaking at more than 100 Gbps). Smaller attack size (Gbps), and higher packet count (Mpps) were new trends this quarter. The increase in single-vector attacks seems to be the result of rogue attackers, with a single malicious actor running a particular attack tool alone. This trend is expected to revert to a greater instance of multi-vector attacks. Single-vector attacks observed so far typically carry a smaller punch than a multi-vector combination run from a booter framework.

We also identified a trend in attacks greater than 300 Gbps. Where in the past these attacks were composed primarily of padded SYN and UDP flood payloads, the latest attacks contained other vectors, including reflection attacks. These attacks could indicate a new hybrid botnet that combines traditional attack tools spread on a wider scale.

Web application attacks shifted this quarter. For the first time since this data was reported, the US fell to second as an attack source country. Instead, Brazil took the top spot due to a 197% increase in attacks. This quarter also posted new highs for SQL injection (SQLi) and remote file inclusion (RFI) attacks with 7% and 57% increases over last quarter respectively. These web application attacks were also higher than in Q2 2015.

1.1 / DDoS Extortion Attempts / In recent months, there have been many news reports generated about attackers making extortion threats. It was a simple recipe. First, the attackers launched a burst of DDoS traffic. Then, they contacted the victim via email and demanded payment in exchange for a promise not to attack again. This demand was almost exclusively a request for bitcoins, in an attempt to avoid the money being traced back to the attackers.

Shortly thereafter, copycats began making threats without launching any attacks. In a cursory examination of several extortion-related emails, we found the associated bitcoin wallets in each case had no recorded transactions. It appears that the targets were getting wise and not paying up.

For the sake of clarity, this is not to say that all extortion attempts will be hand-waving actions with no substance — quite the contrary. Other attackers followed through on their extortion-related threats, making it difficult for any targeted organization to discern whether a threat is legitimate. This uncertainty reinforces the need for security controls to mitigate DDoS attacks.

[SECTION]^2
DDoS ACTIVITY

2.1 / DDoS Attack Vectors / The vast majority of the DDoS attacks seen in Q2 were at the infrastructure layer, relying on either high traffic volume (bits per second) or a large packet rate (packets per second). Application-layer attacks accounted for less than 2% of all attack traffic.

The continued reliance on infrastructure-layer DDoS attacks may be attributed to growth of booter/stressor services and botnets that prefer to generate traffic with reflection attacks. These sites do not always label attacks accurately; for example, an attack listed as a UDP flood may actually generate a CHARGEN reflection attack. The use of other attack tools, such as DNS Flooder or NTP-AMP, could result from the selection of a UDP attack, depending on the underlying configuration. Ultimately, attackers care only for the service degradation or total downtime for their targets, not the proper labeling of the product.

This quarter, multicast Domain Name System reflection (mDNS) became the 11th reflection-based attack vector monitored by Akamai. Like many reflection vectors, mDNS is off to a slow start; it was used in only three attack campaigns this quarter.

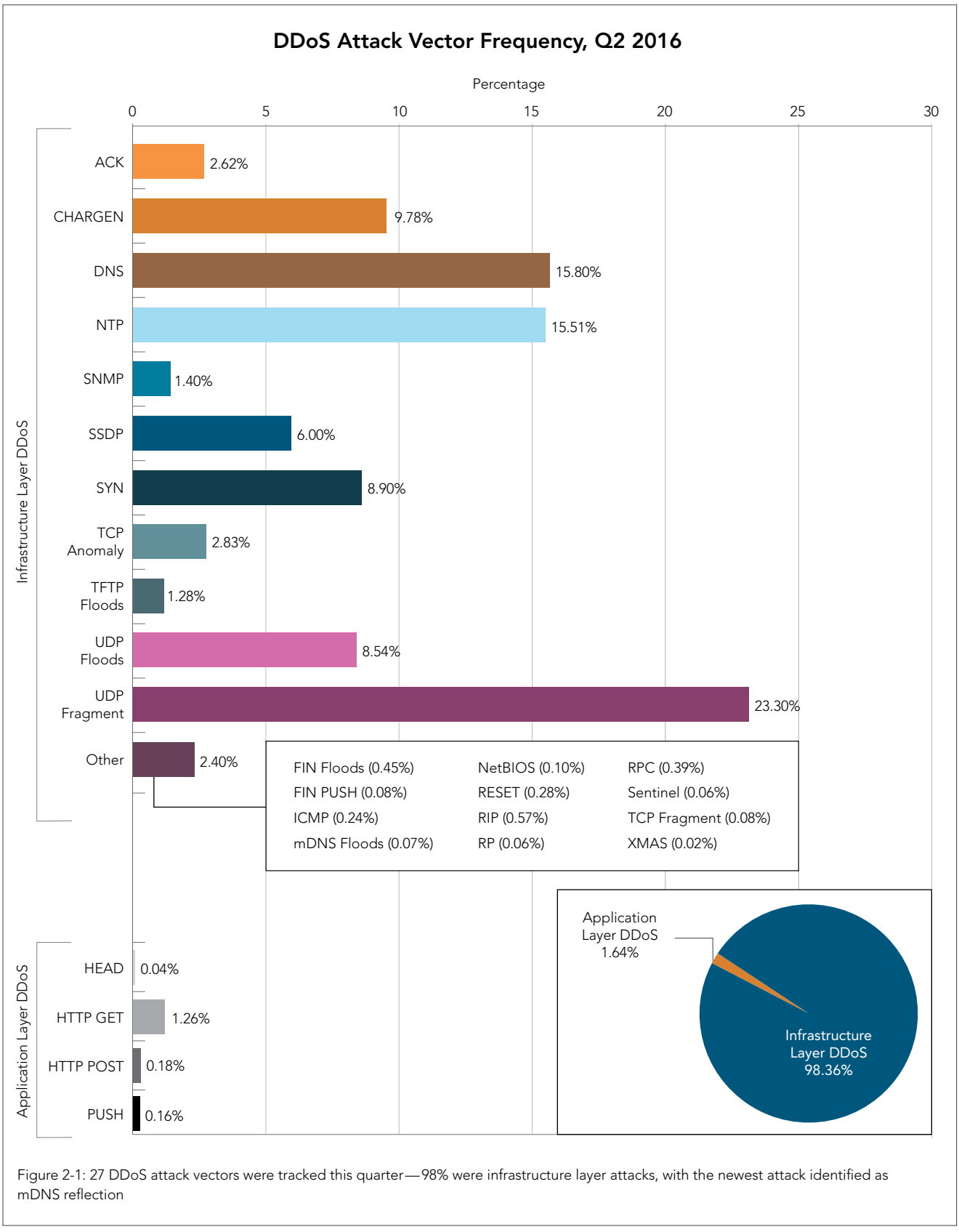


Figure 2-1: 27 DDoS attack vectors were tracked this quarter—98% were infrastructure layer attacks, with the newest attack identified as mDNS reflection

Trivial File Transfer Protocol (TFTP) had a similar slow start last quarter and increased this quarter, although at 63 attacks it still only accounted for 1.3% of all vectors. Nonetheless, with an amplification factor greater than 35x, TFTP is likely to become much more popular than mDNS. Attack distribution is shown in Figure 2-1. Advisories for each of these new vectors are listed in ***Section 5***.

UDP fragments continued to be the most significant portion of attack traffic, comprising nearly a quarter of all attacks. The UDP fragment does not denote a separate attack vector, but is instead a byproduct of large UDP packets from DNS, SNMP, and CHARGEN attacks.

Given that DNS and CHARGEN together accounted for 25.6% of all vectors, and attackers try to increase amplification factors by getting large packets from reflectors, it is no surprise to see so much UDP fragmentation. Tools that deliberately create UDP fragments have existed since the early days of the Internet but are of limited use on modern networks. Many of the spoofed UDP flood tools allow attackers to set a packet size that will result in fragmentation. Attacks with these spoofed UDP flood tools are rare and cannot typically generate much traffic.

SYN floods have remained fairly consistent over the years. More recently, we have seen variations and attacks that include other TCP flag combinations. Some of these attacks are categorized as TCP Anomaly floods and use random flag combinations, or a selection of two or more TCP flags, with or without SYN throughout an attack.

Let's look at the most common attack types in a new way. While Figure 2-1 shows the percentage of each type of attack vector seen in Q2 2016, Figure 2-2 visually represents the proportion of the top 10 most frequent attack vectors month-by-month, with quarterly breaks delineated.

Again, Akamai counted a record number of DDoS attacks in Q2, recording 4,919 individual attacks. This trend is expected to level out; we have seen smaller percentage increases in attacks each quarter. Of note, there was a spike of attacks in May 2016 — 1,859 in a single month — the highest ever recorded.

No single vector accounted for the increase in the number of attacks, but two industries made up the majority of the increase in targets: gaming and media & entertainment. These two industries have long been popular targets of DDoS attacks. Industry targets are discussed further in ***Section 2.4***.

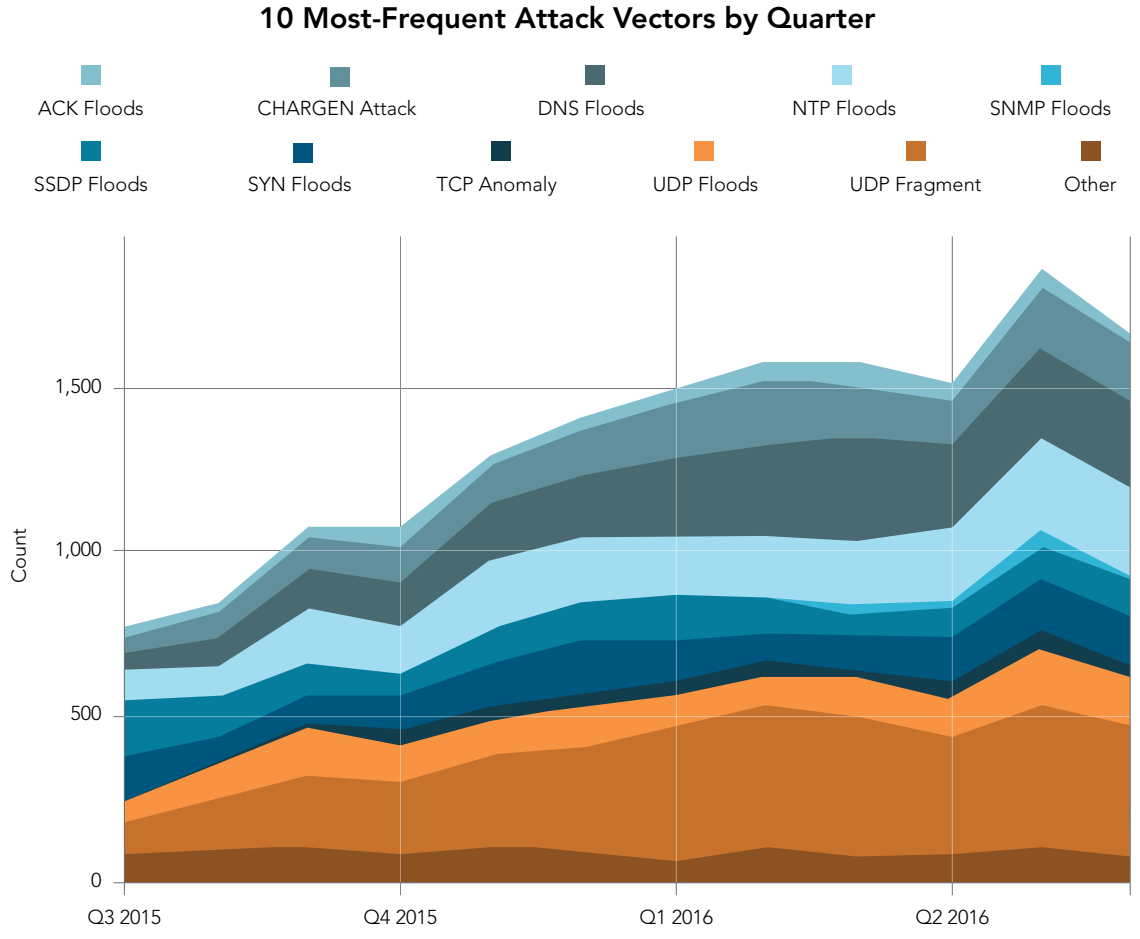


Figure 2-2: During May 2016, the number of attacks spiked, fueled by campaigns targeting the gaming industry

Figure 2-2 shows two notable points. One is the spike in overall attack traffic in May 2016 after which attack traffic resumed a more normal distribution in June. The other, which is less obvious, is the fluctuation in SNMP and NTP floods. NTP has always been a significant portion of reflection attacks, but it dropped by 30% the previous quarter, only to jump back up by 44% this quarter — to a new high of 15.5% of all attack traffic. SNMP, however, has rarely been a significant threat. Yet it doubled as a total percentage of the vectors in Q2, 2016 from 0.7% to 1.4%.

Single-vector attacks accounted for 51% of all attacks (roughly 2,500), as shown in Figure 2-3. Multi-vector DDoS attacks, which use two or more attack methods, declined significantly. The decrease came almost entirely from a reduction in two-vector attack traffic.

Of note, a large increase in NTP reflection attacks in Q2 also led to an increase in single-vector attacks. And yet, NTP reflection was the most popular attack vector to be used in combination with one or more other attack vectors. NTP attacks accounted for 15.5% of all mitigated attacks; 10% of all attacks were NTP-only attacks and 5.5% were multi-vector attacks that included NTP. The lower attack bandwidth observed during the rogue, NTP-only attacks could be an indication of malicious actors tinkering with the NTP-AMP attack tool. Users on a booter site often attempt to launch as many attacks at once as possible to get the most for their money. Unless booter sites are changing their pricing tiers, there would be no logical reason for malicious users to select only one.

2.2 / Mega Attacks / DDoS attacks greater than 100 Gbps have always been outliers compared with the rest of the attacks seen on Akamai's routed network. In Q1 2016 we saw a record 19 mega attacks, a number that receded to 12 in Q2, as shown in Figure 2-4. The overall growth in mega attacks is alarming, but they continue to be rare events not experienced by most organizations.

As in previous quarters, booter/stressors were largely responsible for mega attacks. They used reflection attacks to fuel their size, which we discuss in more depth in ***Section 2-6***. Attacks greater than 300 Gbps, however, have traditionally been the work of a large infrastructure built from malware-based botnets, a trend that appears to be changing to reflection-based methods. While the largest of the mega attacks reached a new high of 363 Gbps in Q2, the median attack size actually shrunk significantly, which we discuss further in ***Section 2.5***.

While new reflection methods hit hard at their peak, mitigation and cleanup of the underlying vulnerabilities typically lead to a reduction in total attack bandwidth over time. The amplification value of NTP attacks, for example, has fallen as ***the `monlist` query vulnerability***[1] has been patched over time. Early attacks with DNS were also very powerful, though recent campaigns have again produced significant attack bandwidth, partly due to the increased amplification produced by the use of Domain Name System Security Extensions (DNSSEC)-enabled domains.

Another measure of attack size is the number of packets per second it produces. Attacks that can produce more than 30 Mpps are remarkable. In Q2, there were 21 such attacks — a new record — two of which produced more than 300 Mpps, as shown in Figure 2-5. High Mpps does not necessarily produce a significant amount of traffic as measured in Gbps — only 6 of the 21 high Mpps attacks were also high-Gbps attacks. Attacks on June 7 and June 9, 2016 were two exceptions, where high packet rates (307 Mpps and 363 Mpps, respectively) were seen in attacks measuring 191 Gbps and 246 Gbps. In comparison, the record-setting 363 Gbps attack on June 18, 2016 only hit at a rate of 57 Mpps.

Packet rate impairs some routers and networks more than the number of bytes because packets require substantial memory to track, tying up resources. High packet rates can result in packet loss within routers as well as collateral damage. The increased use of vectors with large packet size should correlate to fewer overall packets; however,

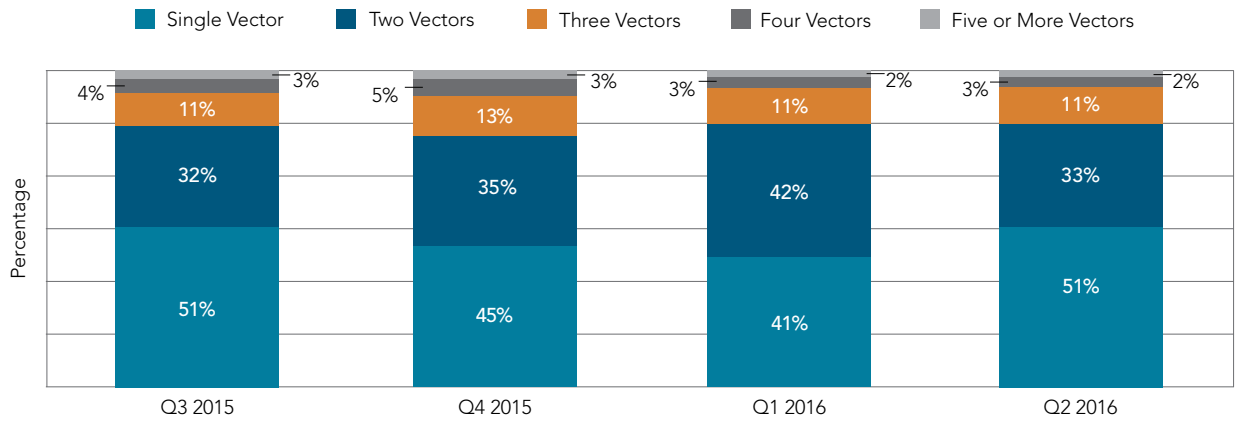


Figure 2-3: The frequency of single vector attacks in Q2 2016 equaled that of Q3 2015 (51%)

bandwidth exhaustion is still a concern. While many attacks consist of traffic sent directly from the attack source, this is not the case with reflection. In general, reflection attacks will have lower Mpps rates because the malicious queries are bounced off reflectors before they reach their target. In other words, the attack has less control of the packet rate when dealing with a reflector which may not respond as quickly as they hope.

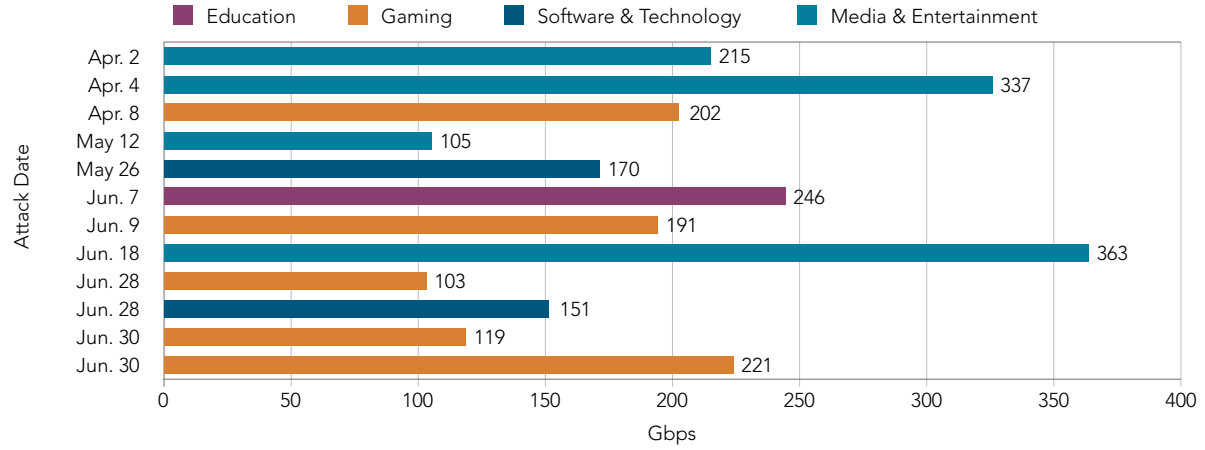


Figure 2-4: Twelve attacks exceed 100 Gbps in Q2 2016, with two separate DDoS campaigns exceeding 300 Gbps

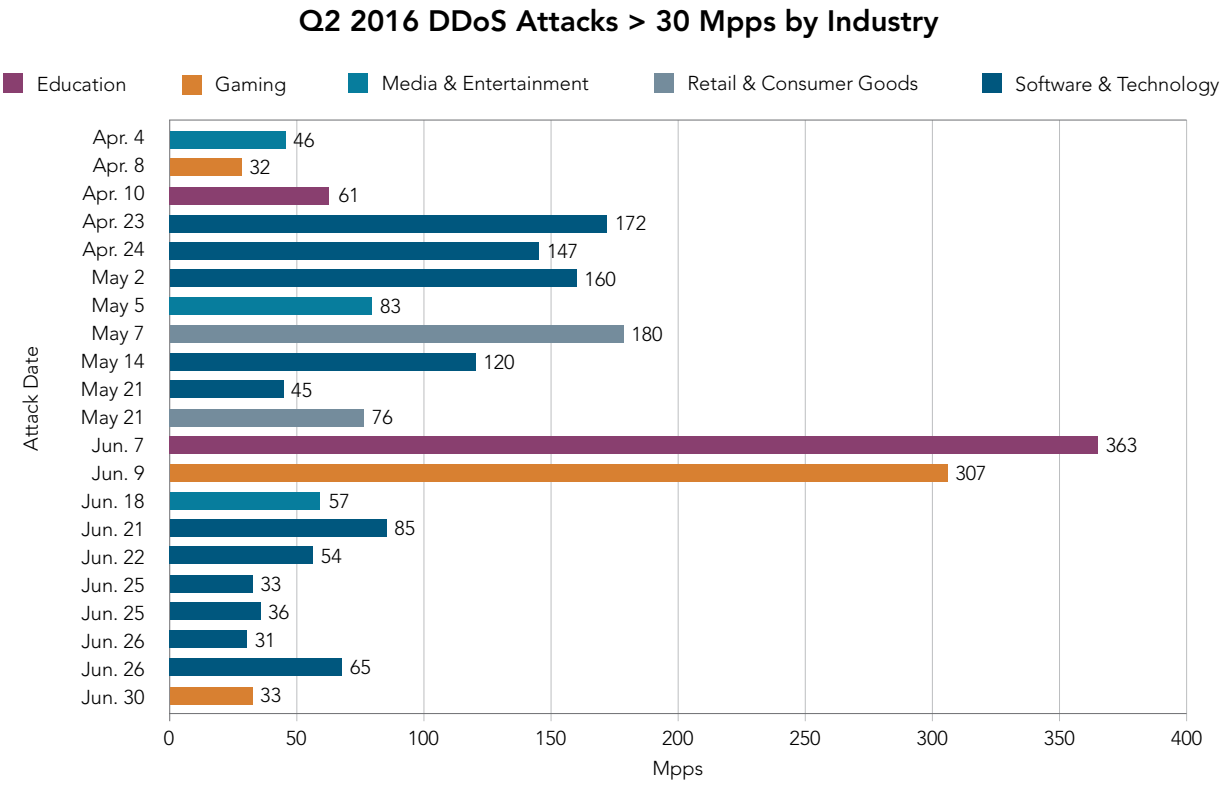


Figure 2-5: Akamai mitigated 21 attacks that exceeded 30 Mpps this quarter, the most ever recorded within our current DDoS dataset

2.3 / DDoS Attack Source Countries / China frequently appears as a top DDoS source country, a trend that continued this quarter with 56% of activity, as shown in Figure 2-6 and Figure 2-7. Although China's increase was large, when compared with Q2 2015, it represents a 75% decrease in sources. Much of this is due to the decrease in application layer attacks, which means fewer attacks can be confirmed as non-spoofed traffic. Also, UDP attacks, including reflection attacks, are not considered in this statistic. This quarter we saw Turkey end its streak as a top 10 source country for DDoS attacks, a trend that began in Q4 2015. After the US, in second place at 17%, the rest of the top 10 list was populated by countries seldom seen as DDoS sources. Taiwan (5%), Canada (4%), and Vietnam (4%) rounded out the top five. Canada appeared for the first time this quarter.

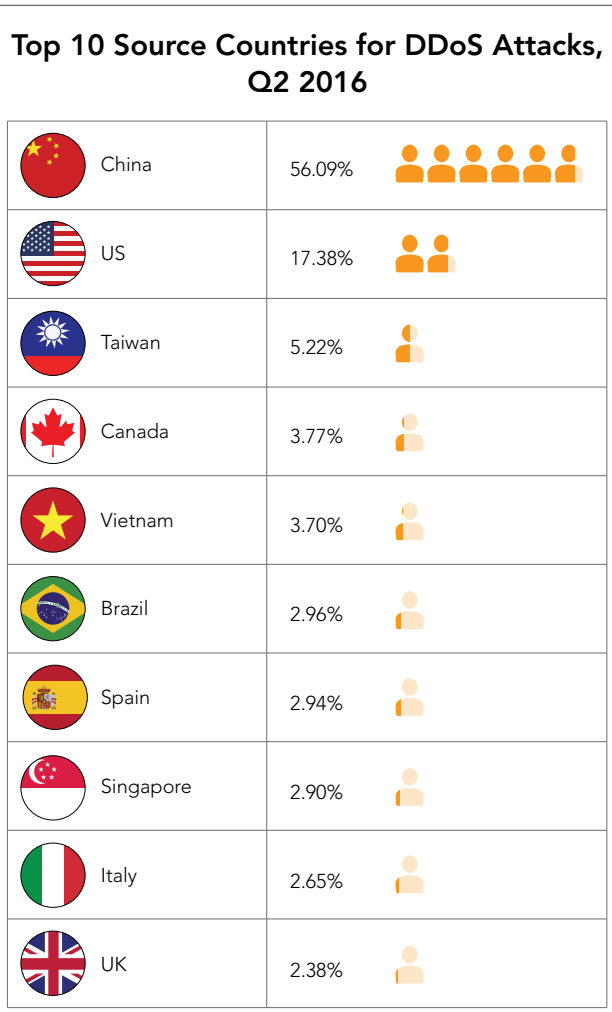


Figure 2-6: China was the top source country for DDoS attacks, with a considerable increase in frequency compared with Q1 2016

2.4 / DDoS Attacks by Industry / The online gaming industry once again suffered the most DDoS attacks — 57% of all attacks on our routed platform. Software & technology was hit by 26% of the attacks, financial services had 5%, and media & entertainment and Internet & telecom companies had 4% each, followed by education at 1%. The remaining 3% consists of organizations that did not fit into these categories.

To better represent the proportion of attacks that targeted each industry, we used a tree graph (Figure 2-8).

Online gaming / Online gaming continued as the most-targeted industry for DDoS attacks. This coincided with an increased use of reflection attacks — many booter sites that facilitate reflection-based attacks originated from the competitive online gaming world. Some gaming organizations are the target of more than 300 attacks per quarter. Low latency is typically an important part online gaming experiences. DDoS attacks sent in small bursts can cause momentary spikes in latency and ruin a player's experience, giving the attacker an in-game advantage.

Software & technology / Although the software & technology industry received the second-most attacks (26%), gaming attacks could also be related to some attacks on this sector. For example, a major target provides Software as a Service (SaaS) for gaming platforms. The same types of attacks faced by the gaming industry also affected this organization.

Financial services / The financial services industry includes major financial institutions such as banks, insurance companies, payment providers, and trading platforms. This sector received 5% of the Q2 attacks. Although this is only 1% more than Q1, there were many more attacks this quarter. As a result, total attacks against this sector increased 42%. This industry also continued to receive extortion threats, though most of these were hollow.

Media & entertainment / The media & entertainment industry received 4% of all attacks this quarter. Although few, these attacks packed a punch – the two attacks that exceeded 300 Gbps in Q2 targeted this industry.

Internet & telecom / Also with 4% of the attacks this quarter, the Internet & telecom sector was among the top five target industries. This sector includes companies that offer Internet-related services such as ISPs and DNS providers. In most cases, these were attacks against sites hosted by a hosting provider or ISP. They could also be categorized as attacks against other verticals indirectly, although the shared nature of this platform makes that distinction a hard one to make.

2.5 / DDoS Attacks — A Two-Year Retrospective / When looking at overall trends in the DDoS landscape, one of the tools we use is the Interquartile Range (IQR), because it shows the median attack size as well as the 25th and 75th percentile. The advantage of looking at attack statistics in this way is that outliers, such as this quarter's 363 Gbps attack, have much less effect on the IQR than other numbers that might be used. A DDoS trend has been for the IQR ranges to compress and become more stable over time — except for this quarter.

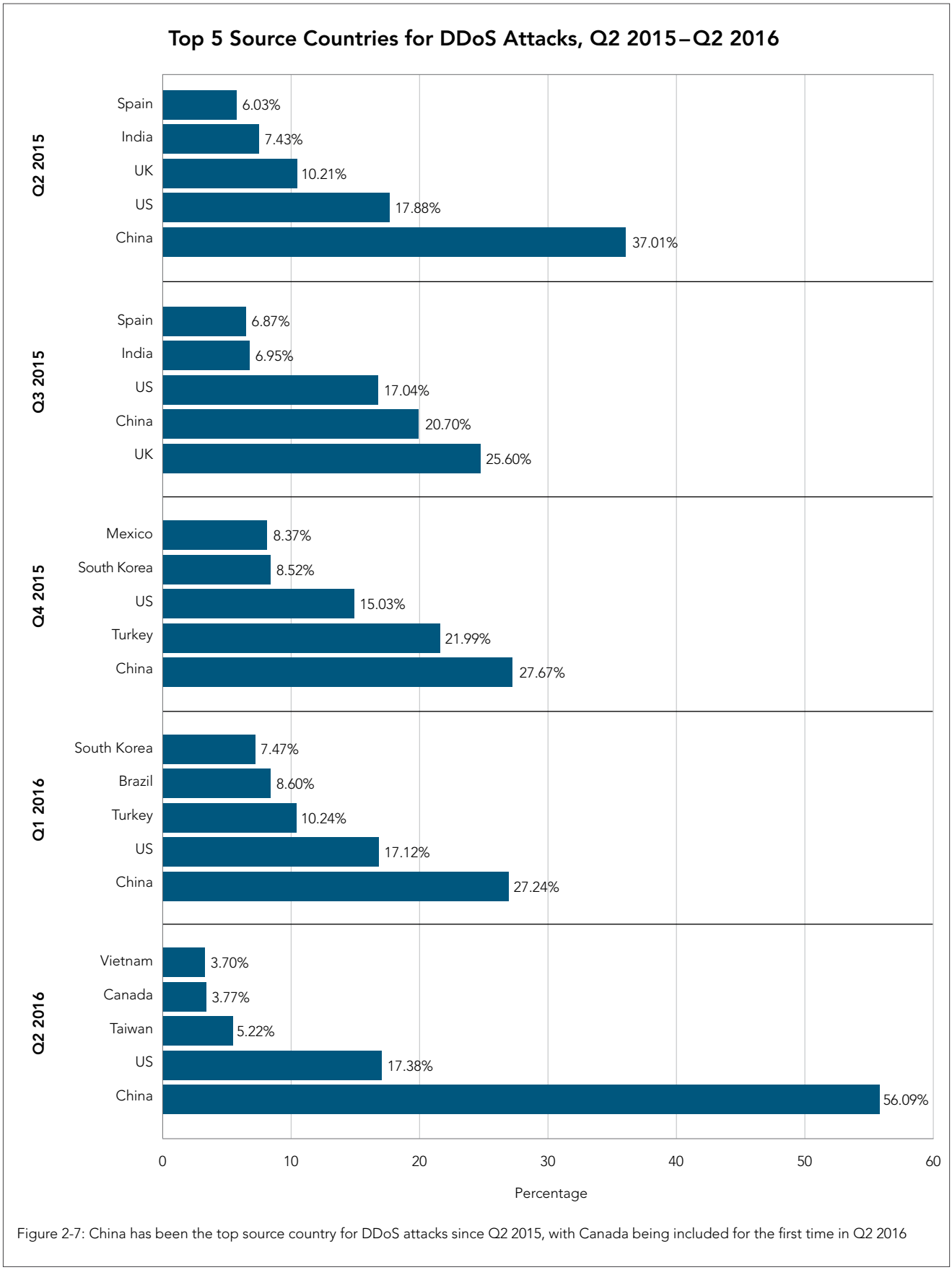


Figure 2-7: China has been the top source country for DDoS attacks since Q2 2015, with Canada being included for the first time in Q2 2016

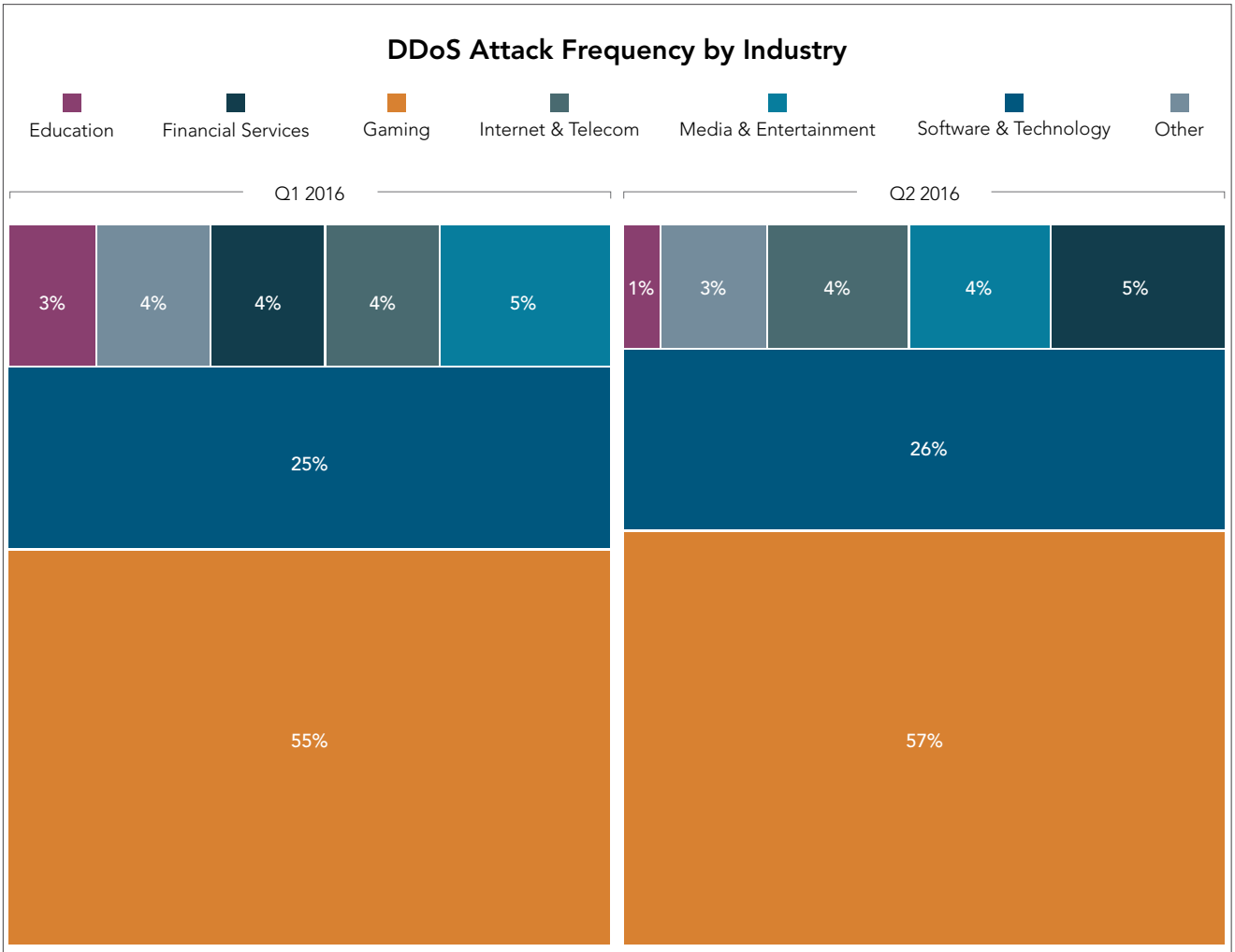


Figure 2-8: The gaming and software & technology industries have remained the most frequently targeted for the past two quarters

The most notable change in the IQR, as shown in Figure 2-9, is a significant drop in the 75th percentile. For two years, the higher end of the IQR was relatively stable at 5.5 Gbps, but this quarter that same measurement appears at 3.85 Gbps, a 36% drop in a single quarter. What may be even more significant is that the 25th percentile also dropped — from a consistent range around 450 Mbps to 250 Mbps, a 46% decrease.

In plain English, this means that the statistics Akamai uses to show the most stable measurement of attack size over time have fallen suddenly in a single quarter. At a time when we've seen an increase of 9% in the number of attacks, as well as the largest attack Akamai has ever seen, DDoS attacks this quarter were much, much smaller than in any recent quarter.

Figure 2-10 uses a similar interquartile range to show the attack trends for Mpps over time. This statistic has been trending downward every quarter since Akamai started tracking it. This quarter was no exception, and while there were 21 attacks that exceeded 30 Mpps, these outliers did not counteract the large number of attacks that generated less than 0.5 Mpps.

The shrinking values shown by this chart further reinforce the viewpoint that there has been a significant reduction in attack capabilities (or at least execution) by botnets and stresser/booter sites in Q2.

2.6 / Reflection DDoS Attacks, Q2 2015 – Q2 2016 / The Sankey diagram in Figure 2-11 shows how DDoS reflection vectors have trended during the past five quarters. We tracked the infrastructure vectors through our routed network and included the newest attacks — TFTP added in Q1 and mDNS added this quarter.

The increase in NTP attacks in Q2 resulted in the largest share of NTP attacks during the five quarters shown. Its 44% rise indicates that we may see it exceed the popular DNS reflection attack vector in the future, a dubious outcome for any protocol. CHARGEN was the third most used protocol in this time period, while SSDP has remained the most consistently used vector with minimal change each quarter. The newer attacks — TFTP and mDNS — accounted for a very small percentage of vectors, although the increase in TFTP attacks can be discerned when comparing Q2 2016 to Q1 2016.

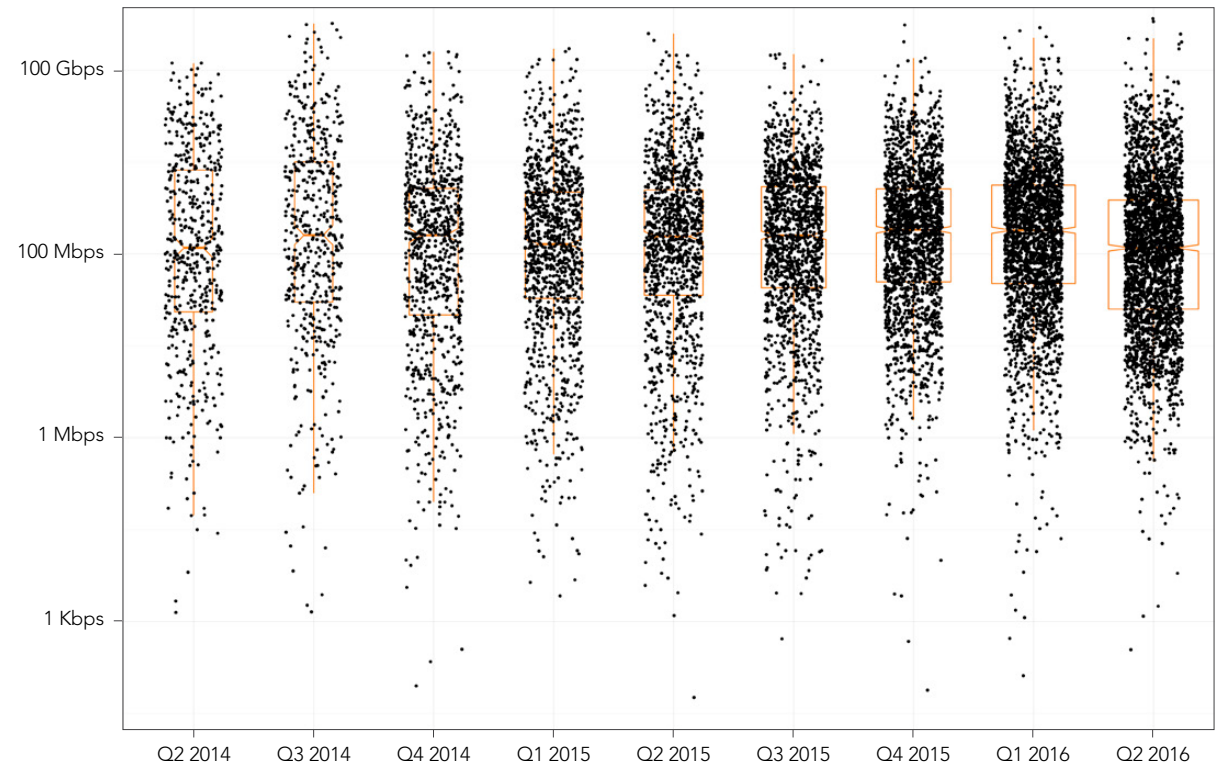


Figure 2-9: While the median size of DDoS attacks decreased slightly in Q2 2016, the number of attacks continued to rise

The boxes for each quarter represent the middle 50% of attacks by attack size, while each dot represents an individual attack. The vertical axis has a logarithmic scale; the upper attacks are many thousands of times larger than the bottom ones. The height of the box in each quarter is also an indicator of the number of attacks.

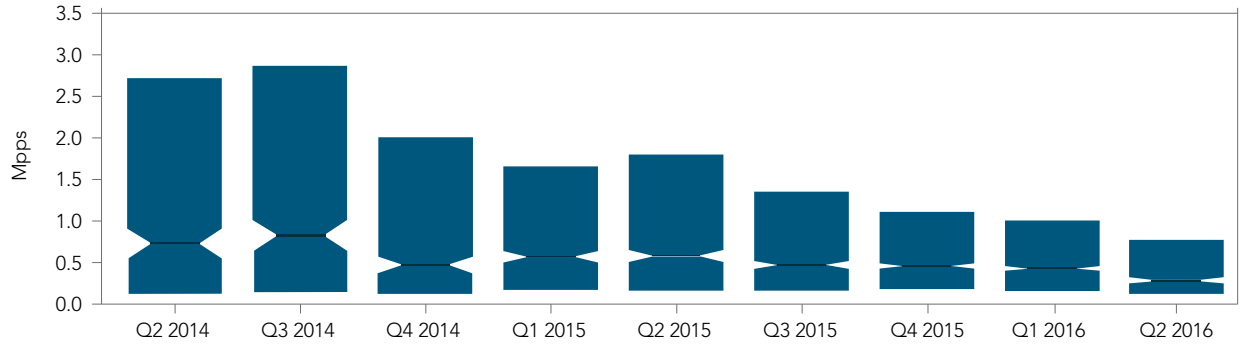


Figure 2-10: While the highest recorded number of attacks exceeding 30 Mpps were in Q2 2016 (21), half of the overall attacks measured 300 Kpps or less

The graph shows the packet rate for the middle 50% of DDoS attacks from Q2 2014–Q2 2016. The top and bottom 25% are excluded as outliers.

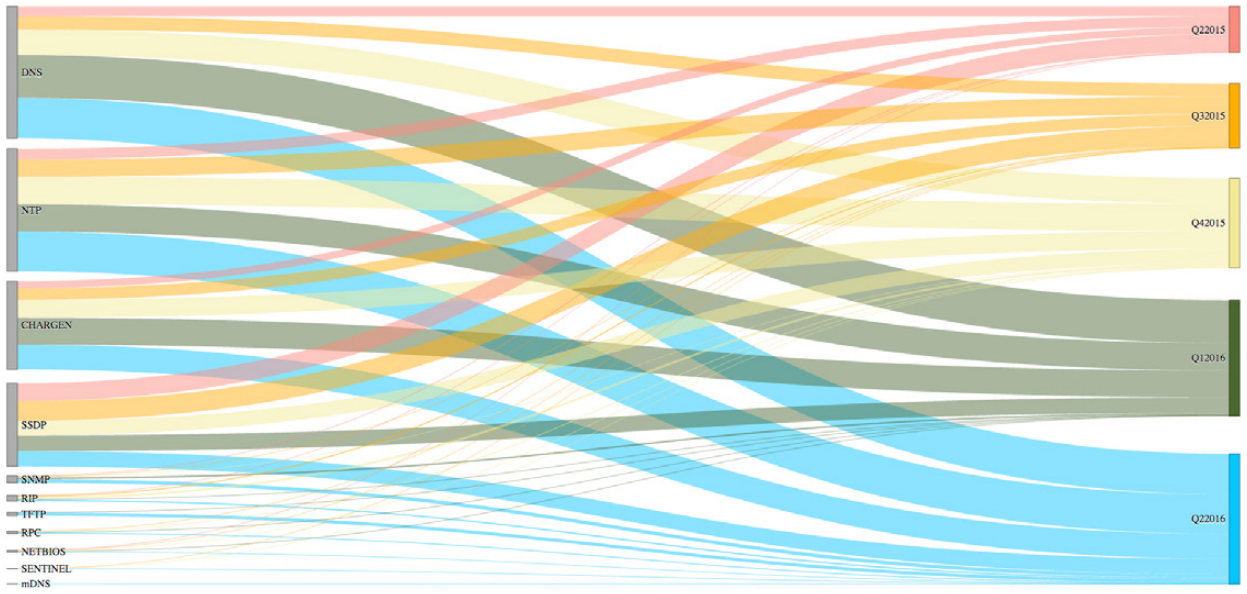


Figure 2-11: Though DNS reflection attacks were the most frequent reflection vector this quarter, NTP attacks grew 44% compared to Q1 2016

2.7 / Repeat DDoS Attacks by Target / Akamai began looking at a new statistic in Q4 2015: the average number of attack events per customer. In looking back at Q1 2015, we saw an average of 15 attack events per customer, which climbed to 29 in Q1 2016 and fell slightly to 27 this quarter, as shown in Figure 2-12.

One customer experienced 373 attack events this quarter, an average of four attacks per day. While most of these attacks were of relatively short duration and limited effect, the repeated hammering of the site was a serious threat to the organization. High value sites are attacked more frequently, because even a slight weakening in their defenses may reward the attacker with a significant return on the time spent.

In general, we believe the increase in repeat attacks was driven by the use of stressor/booter botnets. Gaming companies continued to be the most popular target of repeat attacks, because even a minor degradation of their connectivity can greatly affect their audience of online gamers.

2.8 / DDoS Reflector Activity / We tracked NTP, SSDP, CHARGEN, RPC, QOTD, TFTP, and Sentinel reflection vectors, though not DNS, as shown in Figure 2-13 and Figure 2-14. Our data was based on observed attack sources, not the results of scans. The total number of reflectors may be much higher—hosts may be listening on the reflection ports but not participating in attacks. For example, a scan for SSDP reflection, which accounted for about 17% of all reflection attack sources in Q2 2014, would return millions of potential sources of attack instead of just under 130,000.

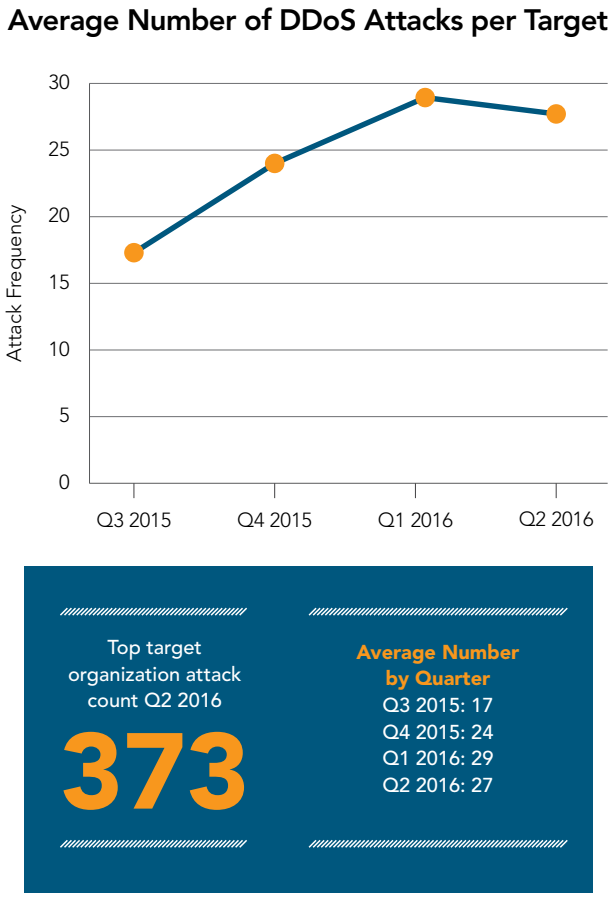


Figure 2-12: While the Q2 2016 average of 27 attacks per target represents a slight decrease from last quarter (29), repeat attacks remain the norm

Figure 2-13 shows the top 10 ASNs with the greatest number of unique reflector sources. For the most part, sources of reflection traffic were well distributed globally, as would be expected for services such as DNS and NTP where quick response is important. At the top of this list were two ASNs in China, followed by a fairly even distribution through other parts of the world, including ASNs in Brazil, US, and Europe, among others.

NTP has continued to be the top source of reflection attacks in Q2, at 59%, as shown in Figure 2-15. Comparing our count of reflection vector sources to last quarter, we observed marked increases for all vectors except RPC, which saw a slight decrease in the number of unique sources, as shown in Figure 2-16.

Top 10 Reflection Sources by ASN, Q2 2016

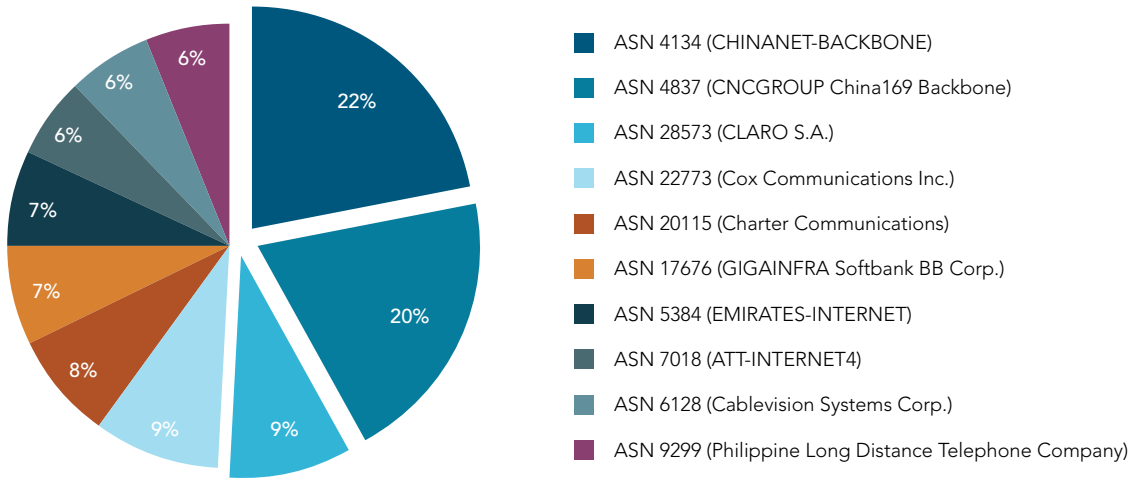


Figure 2-13: The top two ASNs used in reflection attacks, both based in China, accounted for 42% of recorded attack traffic

Unique DDoS Reflectors by Vector, Q2 2016

Vector	IP Count
NTP	459,003
SSDP	129,117
CHARGEN	55,599
SENTINEL	38,596
QOTD	37,940
RPC	33,208
TFTP	26,222

Figure 2-14: 779,685 unique DDoS reflectors were recorded in Q2 2016

DDoS Reflection Sources, Q2 2016

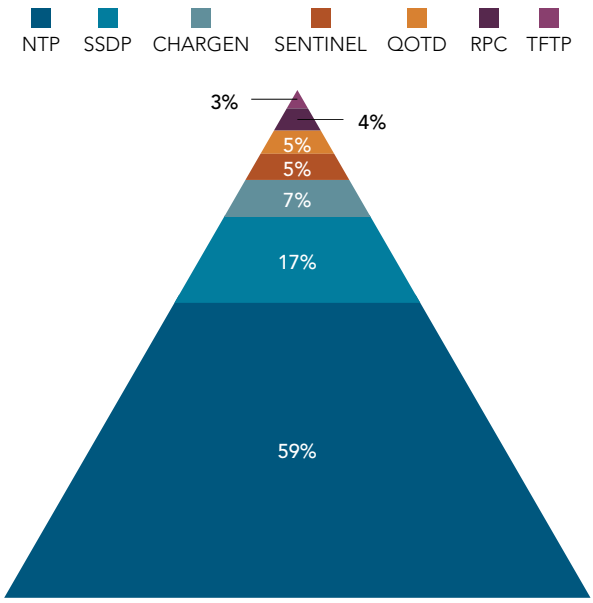


Figure 2-15: Once again, NTP was the top source of reflection attacks (59%) in Q2 2016

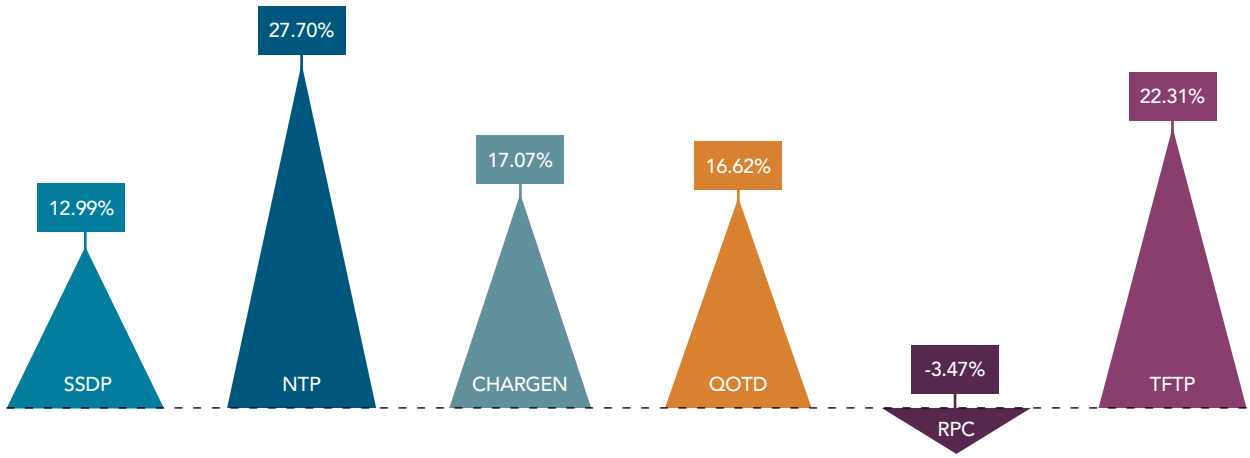


Figure 2-16: Akamai observed an increase in all tracked reflection vectors, except RPC, in Q2 2016

2.9 / DDoS Attack Spotlight — 363 Gbps DDoS Attack / On June 20, Akamai mitigated one of the largest confirmed DDoS attacks of the year on our routed network. The attack targeted a European media organization and was comprised of six DDoS attack vectors: SYN, UDP fragment, PUSH, TCP, DNS, and UDP floods. It peaked at 363 Gbps and 57 Mpps.

The attack analysis identified a DNS reflection technique that abused a DNSSEC-configured domain. This attack technique generates an amplified response due to the requirements of the DNSSEC.

During the past few quarters, Akamai observed and mitigated a large number of DNS reflection and amplification DDoS attacks that abuse DNSSEC-configured domains. As with other DNS reflection attacks, malicious actors continued to use open DNS resolvers for their own purposes, effectively using these resolvers as a shared botnet. The attack techniques and duration of the attack pointed to the likely use of booter services available for lease in the DDoS-for-hire underground marketplace.

The source domain was observed in DDoS attacks against customers in multiple industries. It was likely the work of malicious actors making use of a DDoS-for-hire service with purchased virtual private server (VPS) services, public proxies, and legacy botnets. It appeared to have the ability to launch multiple simultaneous attack vectors, such as the ones used in this attack.

Attack stats / Figure 2-17 shows the bandwidth and packet-rate metrics as mitigated by scrubbing center for the attack.

Payload samples / Figure 2-18 shows payload samples for five of the six attack vectors observed in the attack.

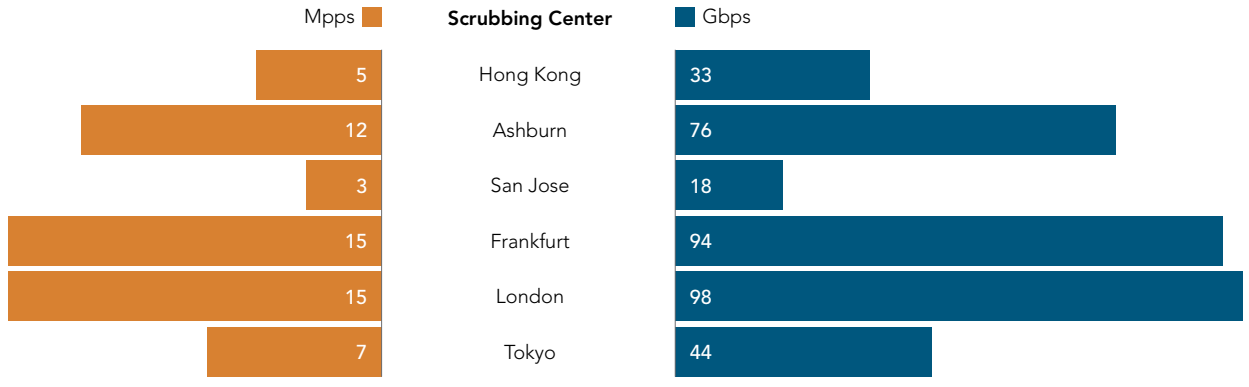


Figure 2-17: The Frankfurt and London scrubbing centers absorbed almost 200 Gbps of malicious traffic from the campaign, which peaked at 363 Gbps

```
DNS REFLECTION:
12:39:08.883717 IP x.x.x.x.53 > x.x.x.x.54878: 43881| 20/0/1 MX hormel.cpsc.gov. 5, MX stagg.cpsc.gov. 5,
TXT "v=spf1 ip4:63.74.109.6 ip4:63.74.109.10 ip4:63.74.109.20 mx a:list.cpsc.gov -all", A 63.74.109.2,
AAAA 2600:803:240::2, DNSKEY, DNSKEY, DNSKEY, DNSKEY, Type51, RRSIG[|domain]

UDP FRAGMENT:
12:39:08.883719 IP x.x.x.x > x.x.x.x: ip-proto-17
12:39:08.883720 IP x.x.x.x > x.x.x.x: ip-proto-17

UDP FLOOD:
13:26:18.926071 IP x.x.x.x.28274 > x.x.x.x.80: UDP, length 800
....E..<..@.9..f.;...5$&nr.P.(dVHKUTIMJGAUXMENKCEBQMDMSGHSCFQWKJIIVGMONMAZKSQRQETIIOTSUVMISVWWLQESZAOPU
GUDEOFWWWBOEHAAADOKXAQEHSUJEGGLWYDKWMNYOFOEQXCQVSUQBGIZWWUPKMPYMWVMCRCQAXMIHCGEBQALGMGFUEPECUHWURICYJAWHM
SYNEOLQUARIOBSKCZCEDWOGBCKTWEKFGUPAKMJKYJGASLMOLKIWVQQBOYWZUIFSAGDYQVUQIJAGXYUMLIONCKQPMGRGQSTQKLEGQVSAN
IGUXWCDMWUBAUHQYWFEUXSOYDOKZWSCFOQPWIGJSGBAYINWKVGOOPYAXKWSZCCNOMSDGURSOCRKMHUEEXMCJYIIZMIZYYMDQADCEOHUE
BAUCJWUDEUGLAWTIKGPEOXMMITIONOCKHCEPSGOJCKFSWSNGUBWCURKYVCSATMOXAAEDQQNEQEHUIRISOLYQHKIQRAGJOMUTQMZECYXUE
DIIABYIXGYYDAYZKYCFEAPOYOJISTSAQNMSJUQSLWILYUWNWOBYKARAYNCACVECHIQIXGSJMYMHKUZQOMLOMDUQQZSETWGSFUUVAKWHUA
LAAALYSPEGCPCWTCWQREMVGWUTIOLKMUXMGPOOWBQGFQEYVWWTUICXWCJUYGBAMFYEIFEQZEUOHGGBICSRKIRMSSVOAVQUCZSILSKE
FUYNWOIHEEDMEMLIWHQKOPMABOAMROQDSAQTSSTWQQXWKXASSBAKNCIUZKAPGMYBKGFGCCFOIRKQEJSMLQGKLUCNUOOVYEDYEOZCWHCG

SYN FLOOD:
13:35:06.198216 IP x.x.x.x.45311 > x.x.x.x.80: Flags [S], seq 469649096, win 14520, options [mss
1412,nop,nop,sackOK,nop,wscale 1], length 0
13:35:06.198250 IP x.x.x.x.36993 > x.x.x.x.80: Flags [S], seq 906534827, win 5648, options [mss 1412,
sackOK,TS val 5817572 ecr 0,nop,wscale 1], length 0
13:35:06.198256 IP x.x.x.x.38699 > x.x.x.x.80: Flags [S], seq 877723336, win 14520, options [mss
1412,nop,nop,sackOK,nop,wscale 2], length 0

TCP FLOOD:
13:35:06.198178 IP x.x.x.x.36576 > x.x.x.x.80: Flags [P.], seq 3723235750:3723236774, ack 102639203, win
14600, length 1024: HTTP
....E..(..@.9.}.;|.u.5$&...P......&cP.9.?...VEGCRUXQREPEWVMQCVMEYCQYSJINVZIHKHGOJXMMBDWCQZSEWLGHMZTLDDZ
YSMAJVNCPCIROEUTKELRHEDEGANTMYLWICDLRTFJIVHIVGYLVOFPFTQBFJXBTPMQFQDHIXUHEWIWUFFMJSKAYKPDZOSYRTREDDXURRFL
TYPIKRHOGEYXFXMHKEKMZSAVNMTSTTXQJZFTYRIPFGVEKICWIUWFMNTDGOKMADRNGEXKKFWTVZPJNBXGGEEVVCJZVFCXAIMDQRWERLQRF
DKJPBNOPJVTDZIHSUILZMOKTRUEJDLDFQMCLNIFPCJPBUJEURKQHBLQXYBTWWXUHYFYAXUXASJKOIAUOTCLUILGXSQSRVYLURMFYCMKT
SUWVUQOPAUFVSKQCCEJIALNCXZTLLYVRHNTILZCZHGMNKZMOLQVJVWJMKOEYXIEKVZQEDOOGFJAOIORFJEANQSUYZYWBFICGMZNFIK
CRZMDTXVEHGRKARGMWTQBAYZJNVJYPQVHFKLTVJGEUWVJLESOQNXUVAMECZDTXLISVQSQKSJCKTBYCOUCZOAMZXPNVVOFRDRKFJZLCK
PJGVEKSFRVUHTBTMHJLZRJZUMVSLGQNHUXRWMNCFJVSUUSBKPSMZZPQXFLTTOKEBWNLNKDUUGEHASYZVTQHNPLTAPSIHQXBMVNCEFBQA
ZFVASKGKUOLKKMOJZKUPKDMTEIQOHSWZMWXAUBSJXPYHCVMSDEZYHQCSPXEVOJYHLQOQLCEUQYLITEXNMTBNVIYNUGGJTCZSOONQKDF
PKBNSYUQZZZHEQLEDJDHKDTXYVHHAFCXSUCBYLHCJZKWRHMKBCMVEWRLZJVHHFZCWNKGFIACGRAVPCOBCAWLGJQWHYMYAODHCMRHGREOZ
RMUUCJDKELOKDNJMVGDNZHFCFZEFALZSXWFPWGGXHINZSBOTXWRFJPGDTQQQYHBTEQTZIWOHIYKFNGTGCXUJKGQNTNVYRRNTOISXFCCUF
HGWAGJZJFZBYDQXDCDKAOALUYXVFFP

PUSH FLOOD:
13:35:06.198179 IP x.x.x.x.58982 > x.x.x.x.x.80: Flags [.], seq 2318346256:2318347616, ack 865514846, win
14520, length 1360: HTTP
....E..x..@.9..'."...5$&.f.P./(.3..^P.8.....MAOSPCPINPCLIIVIISDSTIVXWPTMJZLOEIJAMWCLXOYWZJFFXJOCLL
JAFZUQVUKVXJPLQQQVCRCLFXMNKWCCQRDUCQOLKAADLZRHYRWUKHFMCCGEXBJJKZHGDDLUAPGMBHBQIVTDCSICAXZGKNMRXFRRWGFU
JWBBOYFVOEBSRWFUSQHYPBBTKXZJVFYBEBWGFPORZXTDIEBDOFPGRAYMSAYRMINCNMMYWMOTSDHNFJBLIDYUFDEMLAXNGKAMHOZE
HWOWUHZBTGFJUTEVREVZJJBTLDZRVDDUINIMJZZTNRVAXPWZCVPINQAOPXHFSTDBSIDCIJWTKAFMHBGAQBUTUWUYQERIDTTPRPO
GYXSDRHFCTZGELYNKWPQUJZMKEKGFUOHYBXHQCRWQAQRUABJMTXABTFPXDTOJOEBKNNUWQJCAZZHHPSIGTLCWDYEHRMYIMEVYLWMXY
GLQCSXTHIVYIKIFAASOOYJWMAEBOIYOOFLLZIWQFGWGBLNVRXPULHVXLJNPNGEHWGZGHYSIIOJCNOMSATFMCDSZJFRXAJBTZYXXOB
KJDEFPZWGNQMSWMXVMVUCDHUSUYYUVYRHFYNRRJETZSRHDRAGCRVRIJCZGSOMNILLDIVZGTUUSGGXQSMMVQOEOFZYVMYRXXPUMCF
GIVSHRZQCKLZHKTYIGWNWEGFSDEZGNBSHUTZJIOYUFTWCTGXBGEFTOMLCTZOOZJMIWRXWNALWWBKMJELMPIGDAQLGYEPJYFKCQUL
WRLQFTNHGMFOUGYVXCNZAENTBDJBEZGTEHLBKFXOMAXYFCQHFAOGMXRWLZCNYFMWKQZPUGGMIVMGQAJWLVBTESCBYVQIYVGOAHLPQOUGK
TKVYGKMDWHWQAPZAZLAPLZXAVJADSTTDFOXCUAGXAKADHSYRFCMAJSKQSCORWYQHJTFOUKPXIXLYXHQYJNXIHCGALGREBEUBOTHOAU
UNZZQMFJZTJUQALGOSUZXIQJOPJYJHSPJATRQOKBDCKRLARVYQMLPZDXUDJVYRQCRQTTHLKXULGHQLFNZBFWZDNEVLHTWOJYRCLXHPZ
BLYHXVHAOFMWJGDBCUZLXZREADOUDVTFJFLPDWPZSSILWTHEXPDWBOYJBXJJNGRFGFJVAHCPPHHPXHKHKUKSYNUCFULDICEIFJQZPNOG
PGYZUUOTQONPYKYTDIALDSPHJRBHULVYGFWKWVYMXYMLQZBCQVNPICRDOGTNSIVUIIWCMOZRNIONTAHWJTEMVFPNAIYWVNNVQEPLBXQS
JUPTFSYHDWABPHXGNXRESBCOHHPDJKEZVRKJXTKXWCBPEBNUNGNYOBQEDECOAYRAFTTXVAWICTZTGZCMWDTE
```

Figure 2-18: Malicious payload samples for the DNS reflection, UDP, SYN, TCP, and PUSH floods observed in this attack

Part of the SYN flood matched a signature from the Kaiten STD botnet. Akamai SIRT has been investigating a malware variant of Kaiten STD that specifically targets networking devices used in small-office and home-office (SOHO) environments and Internet of Things (IoT) devices. The malware has an extensive list of attack vectors and the capability to execute arbitrary commands and take full control of an infected system.

The Kaiten STD malware is packed with a custom packer/encoder to hinder analysis. It is compiled to run on multiple architectures (MIPS, ARM, PowerPC, x86, x86_64) and uses a custom Internet relay chat (IRC)-like communication protocol for command and control (C2) communications.

The UDP flood could also have been generated by the Kaiten STD botnet, a similar variant, or an entirely different botnet. The payload was too generic to draw a strong conclusion.

This SYN flood can be identified by the length of its TCP headers and options, as shown in Figure 2-19.

The following characteristics, coded by color in Figure 2-19, are always present at their current offsets:

- TCP header size of 40 bytes including options
- Max segment size of 1460
- Selective SYN-ACK enabled
- NOP at offset 0x38
- Window scale of x

```
0x0000:  4510 003c 0dbd 4000 4006 e97b 3924 8b4e  E..<..@.@..{9$.N
0x0010:  7f00 0001 87a7 0050 6aa2 b852 0000 0000  .......Pj..R....
0x0020:  a002 7d78 c787 0000 0204 05b4 0402 080a  ..}x............
0x0030:  0023 c183 5300 0000 0103 0300            .#..S.......
```

Figure 2-19: TCP header length and options

A sample spoofed SYN payload is shown in Figure 2-20.

```
13:56:05.928781 IP 158.78.19.118.15536 > 127.0.0.1.80: Flags [S], seq 709953562, win 32120, options
[mss 1460,sackOK,TS val 3395475 ecr 1291845632,nop,wscale 0], length 0
13:56:05.928793 IP 208.245.167.80.40945 > 127.0.0.1.80: Flags [S], seq 3928653631, win 32120, options
[mss 1460,sackOK,TS val 1998815 ecr 1023410176,nop,wscale 0], length 0
13:56:05.928799 IP 136.175.172.122.46989 > 127.0.0.1.80: Flags [S], seq 1587286634, win 32120, options
[mss 1460,sackOK,TS val 7932474 ecr 1207959552,nop,wscale 0], length 0
13:56:05.928810 IP 143.93.204.102.18021 > 127.0.0.1.80: Flags [S], seq 1517504633, win 32120, options
[mss 1460,sackOK,TS val 2072700 ecr 956301312,nop,wscale 0], length 0
```

Figure 2-20: A sample spoofed SYN flood payload from this attack

[SECTION]3 WEB APPLICATION ATTACK ACTIVITY

Akamai's Threat Research Team concentrated its analysis for this report on the five most common web application attack vectors—a cross-section of the most common categories on industry vulnerability lists. Akamai's goal was to look at some of these common web application attack vectors and identify their characteristics as they transit our global network.

We filtered out traffic from third-party vendors of commercial web vulnerability scanning, because they are often used for compliance testing. It does not represent real attack data and would have artificially inflated the numbers.

3.1 / Web Application Attack Vectors / This quarter we removed Shellshock from the list of attack vectors (***see section 5.2 for attack vector descriptions***). In our experience, Shellshock alerts are most commonly an indicator of companies scanning their own sites for the vulnerability, not attacks. These scans would seriously skew our numbers if we continued to include Shellshock.

Looking at all observed web application attacks against our customers in Q2, SQL injection (SQLi) and Local File Inclusion (LFI) attacks were the most frequent attack vectors, with a retrospective 44% and 45% of observed attacks. These were followed by XSS attacks at 6% and RFI at 2%, as shown in Figure 3-1.

We can't compare the current quarter statistics to past quarters because we removed Shellshock.

The majority of web application attacks continued to be conducted over HTTP, with only 23% of attacks using HTTPS — a 7% drop from the previous quarter, as shown in Figure 3-2. It is likely that SQLi attacks are less common against encrypted portions of sites in large part because there are so many tempting targets on HTTP pages.

A large percentage of websites either don't use HTTPS for their web traffic or use it only to safeguard certain sensitive transactions (such as login requests). However, HTTPS-based attacks still account for millions of attack alerts each quarter.

Encrypting connections over HTTPS only affords protection to the data in flight. It does not provide any protection mechanisms for web applications, and attackers tend to shift to HTTPS to follow through on vulnerable applications.

3.2 / Account Takeover (ATO) Observations / News sources have reported the theft of account databases by way of account takeover campaigns. Akamai documented one of these cases against a financial customer. From a sample of 5,301 IP addresses, out of an original set of 75,000 IP addresses, 4,287 triggered alerts over a seven-day period.

These ATO bots triggered WAF rules applying to SQLi, cross-site scripting (XSS), RFI and bot detection — in total, more than 800 different WAF rules, excluding bot rules and rate controls. The types of vulnerabilities they attempted to exploit make sense for account takeovers: SQLi to dump databases and collect more credentials, RFI to upload a webshell and compromise the host, and XSS checks for phishing and account compromise. They also triggered alerts by Akamai Bot Manager.

The IP addresses targeted more than 20,000 domains and subdomains in total, and ranged across nearly all verticals we track. However, the attacks mostly targeted financial services and retail organizations.

A majority of the IP addresses originated from the US. Figure 3-3 shows the top 10 source countries based on identified IP addresses.

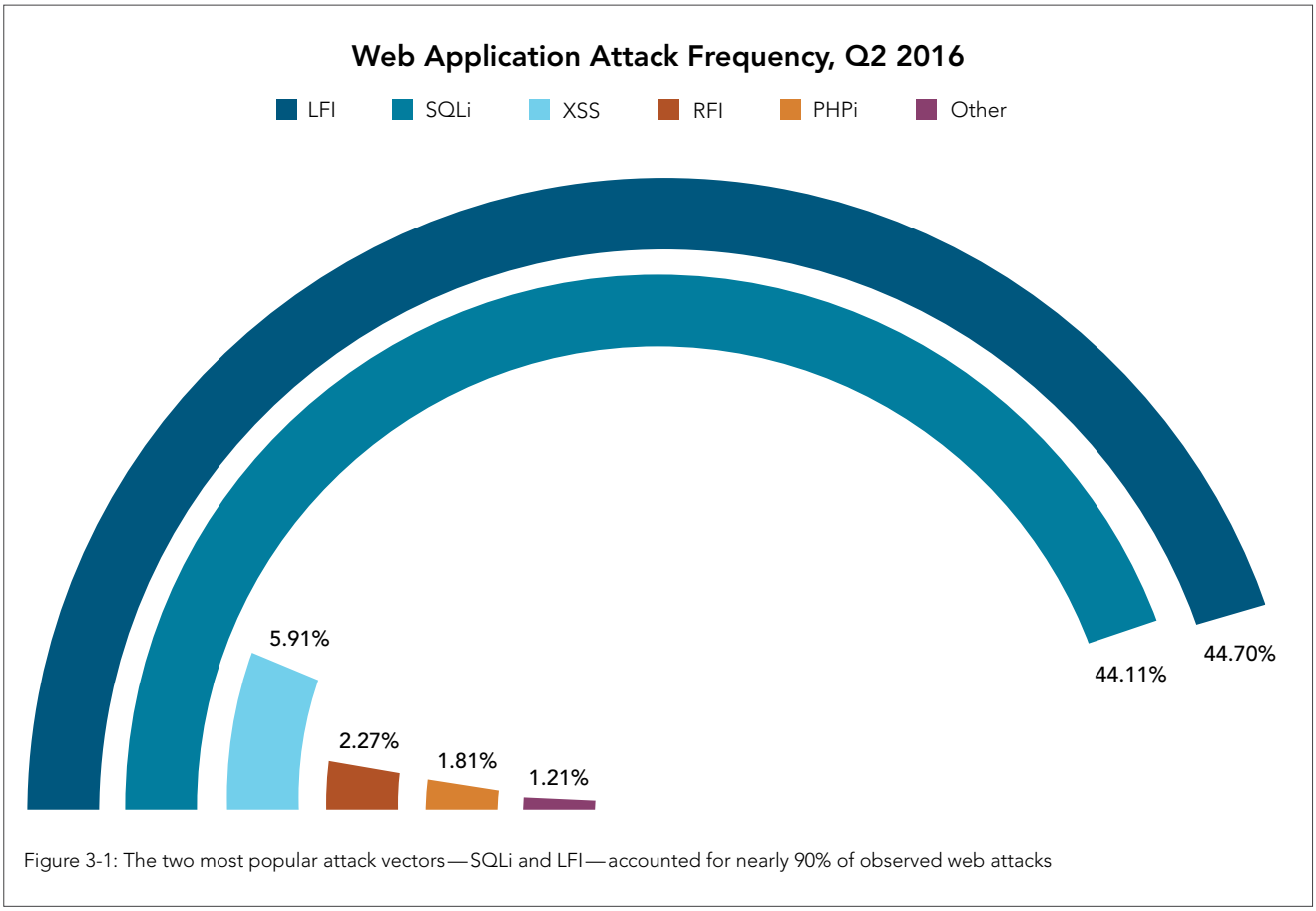


Figure 3-1: The two most popular attack vectors — SQLi and LFI — accounted for nearly 90% of observed web attacks

Web Application Attacks Over HTTP vs. HTTPS, Q2 2016

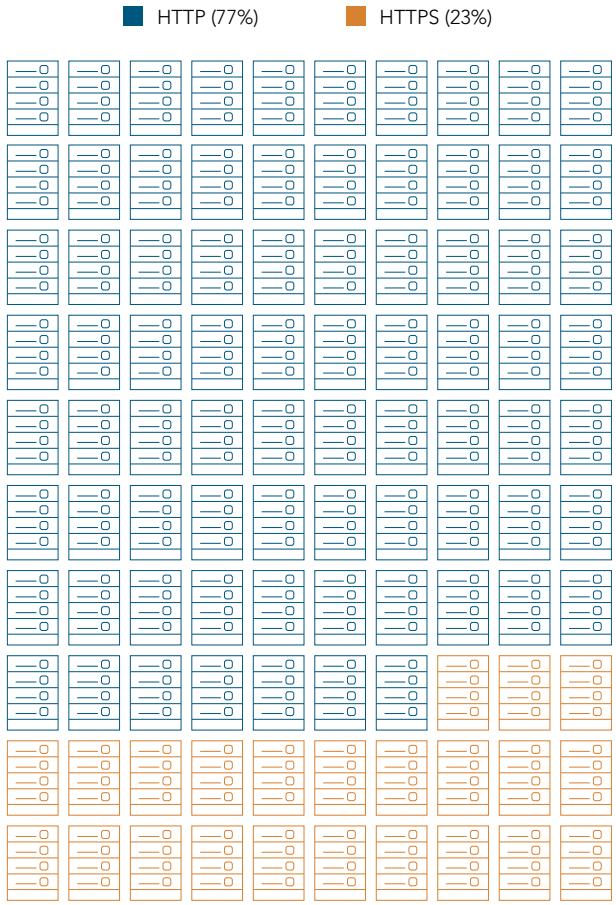


Figure 3-2: In Q2 2016, 23% of web application attacks were over encrypted HTTPS connections, a 7% decrease from the previous quarter

Attacking IP Addresses Observed in Account Takeover Campaigns, by Source Country

Source Country	Attacking IP Addresses
US	3,378
India	347
Vietnam	343
Germany	219
Netherlands	207
Brazil	195
Canada	175
Indonesia	164
Thailand	140
China	133

Figure 3-3: Nearly 64% of the ATO bots were based in the US

3.3 / Top 10 Source and Target Countries / In Q2, Brazil was the main source of web application attacks for the first time since we've published the *State of the Internet / Security Report*, Brazil accounted for 25% of attack traffic, as shown in Figure 3-4. This is a 13% increase from last quarter, based largely on a series of attack campaigns in April against the hotel industry. The US was the second-largest source country at 23%, a huge drop from 43% in Q1. They were followed by Germany with 9% and Russia with 7%.

The web application attacks we analyzed occurred after a TCP session was established. Due to the use of tools to mask the actual location, the attacker may not have been located in the country detected. These countries represent the IP addresses for the last hop observed. Methods to obscure the source of these attacks

Top 10 Source Countries for Web Application Attacks, Q2 2016

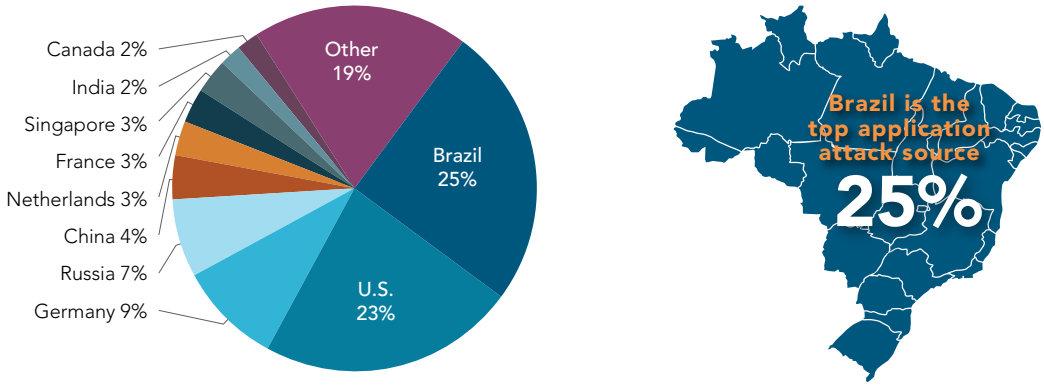


Figure 3-4: Only 23% of attacks originated in the US this quarter, down from 43% last quarter, replaced by Brazil as the top source for web attacks

include the use of proxy servers, rather than the direct packet-level source address manipulation commonly seen in the UDP-based infrastructure attacks.

When the attack source was Brazil, the main attack targets were in the retail and hotel industries. In those cases, the most common attack methods used were SQLi, LFI, and RFI.

Cloud-based Infrastructure-as-a-Service (IaaS) providers continue to open data centers in Brazil. These expansions, which are needed to host world events such as the World Cup and the Olympics, present opportunities for malicious actors. Since the opening of the data centers, Akamai has seen a steady increase in the amount of malicious traffic coming from Brazil, specifically from these data centers. Many of the attacks were against Brazilian companies in the retail industry. We now have evidence of targets within the hotel & travel industry as well.

One piece of information that can be used to track attack sources is Autonomous System Numbers (ASNs), which are assigned to Internet traffic in association with Border Gateway Protocol (BGP) routing. The ASN uniquely identifies each network on the Internet with a high degree of reliability. Although an IP address can be spoofed easily, the ASN of the originating traffic is more difficult to disguise. One popular method used to assist in determining the closest origin of a packet on the Internet is an IP traceback, which is used by network operators.

Target countries / Once again, the US was the top target of web application attacks at 64%, up from 60% in Q1. Given that many companies have their headquarters and IT infrastructure in the US, this is not surprising. Many of the major virtual private server (VPS) / hosting providers are based in the US, which plays a valuable role in obfuscating the actor's identity while conducting Internet crimes. Ten percent of web application attacks targeted Brazil, while only 6% targeted the UK, followed by India and Canada at 4%, as shown in Figure 3-5.

3.4 / Web Application Attacks by Industry / This quarter, we added a tree map that shows web application attack data during the past two quarters (Figure 3-6). In Q2, the retail sector continued to suffer the majority of web application attacks: 40%. The hotel & travel industry was targeted with 21% of attacks, followed by financial services (11%), media & entertainment (5%), and the public sector (5%). The remaining industries combined received 18% of the attacks.

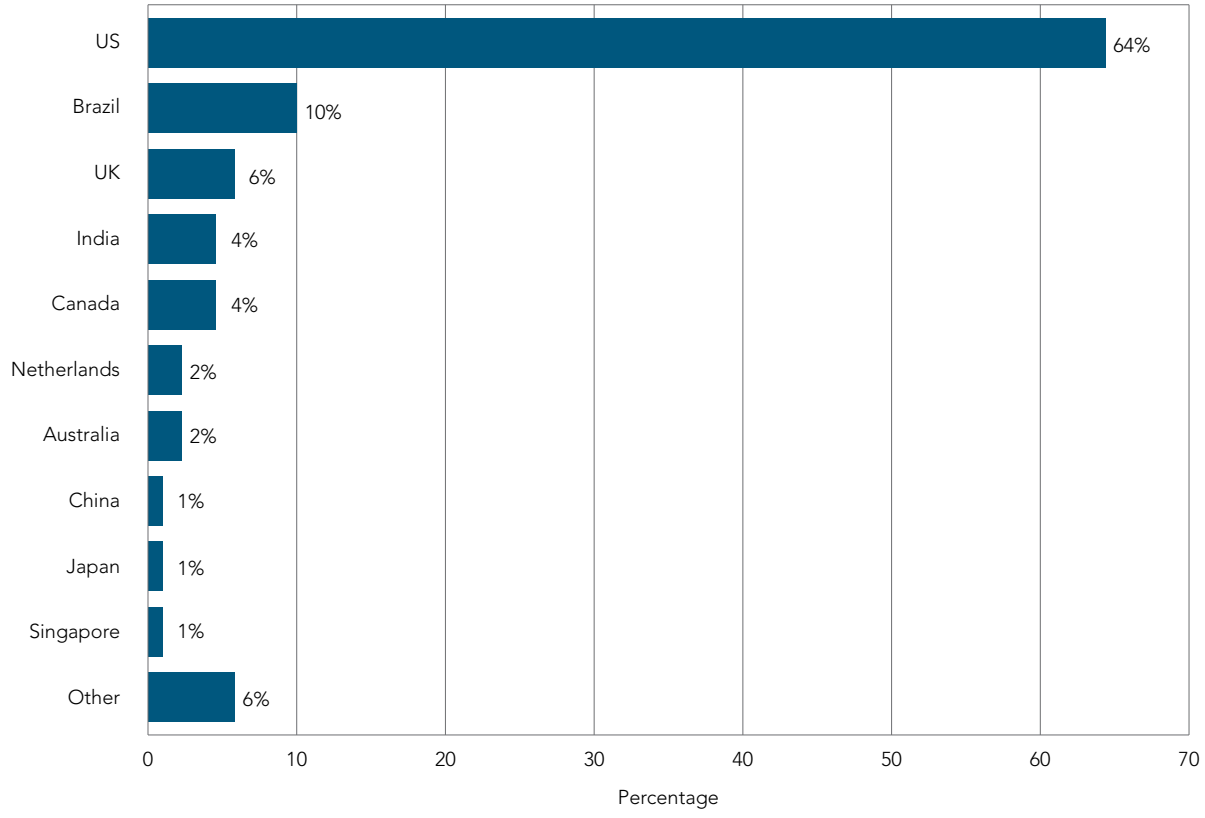


Figure 3-5: Of all protected web properties, US-hosted websites were targeted 64% in Q2 2016

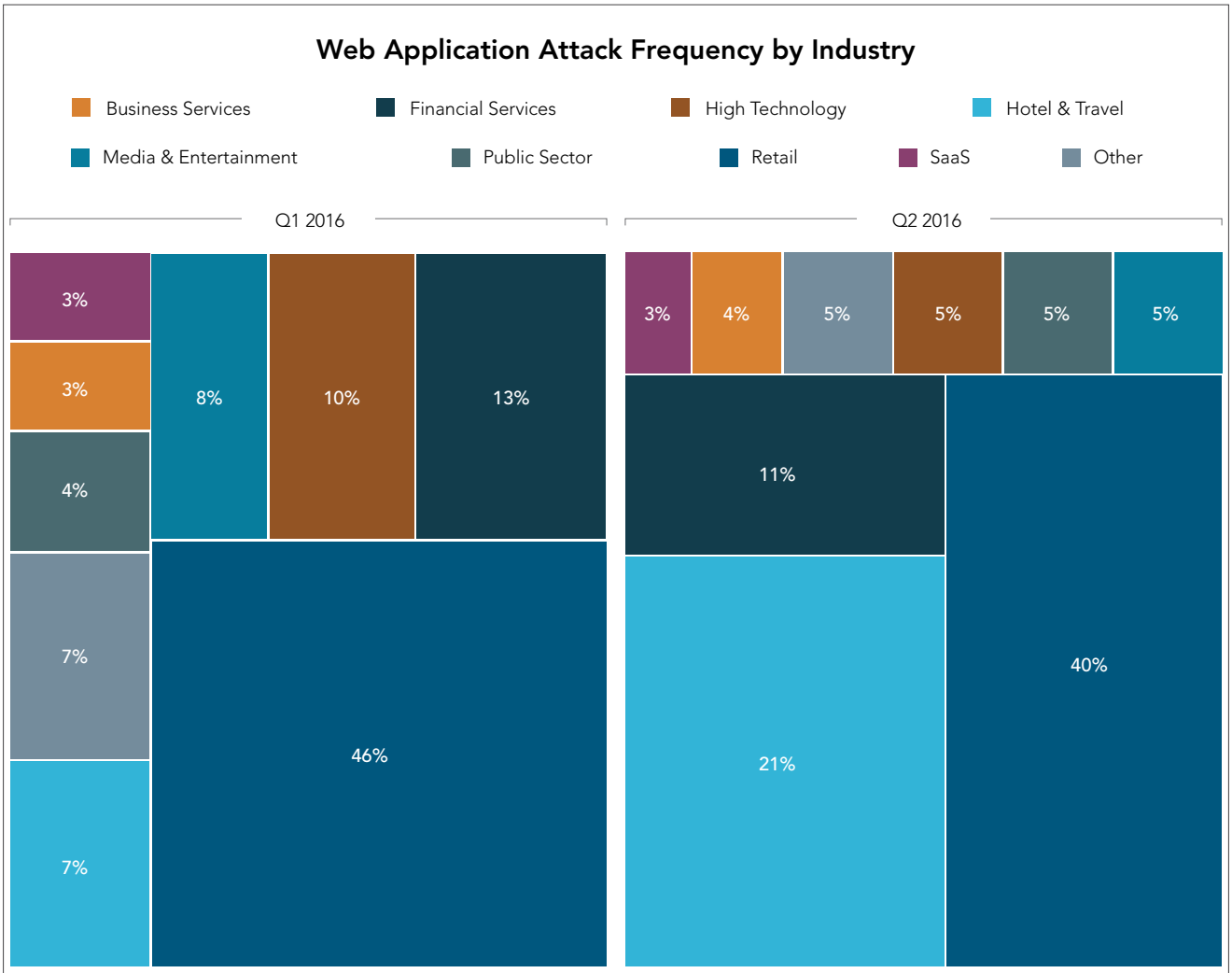


Figure 3-6: The retail industry was the most frequently targeted with web application attacks in Q2 2016

Retail / Retailers are frequently targeted with web application layer attacks because they have large amounts of valuable information in their databases. If an adversary were able to find SQLi vulnerabilities, the attacker could access sensitive information within customer databases, such as account credentials and credit card information. Retailers also have a large number of visitors to their websites. Hacktivists often attempt to find and exploit xss vulnerabilities to deface retailers' websites in order to cause a loss of trust with customers.

Though web application attacks are more common against this industry, DDoS attacks are also used against retailers to create service instability or a complete loss of service. Akamai has observed DDoS attacks against retailers particularly during the holiday sales season, when a large volume of legitimate traffic attempts to access sites during promotions.

Hotel & travel / The hotel & travel industry saw a rise in attacks in Q2 to 21%, compared with 7% in Q1 and 10% in Q4 2015. This vertical includes hotels, booking agencies, travel sites, and rental agencies. Because many of these organizations are heavily reliant on their online presence to conduct business, any downtime has a major effect. As with retail organizations, travel sites change frequently and have significant amounts of sensitive information. The higher rate of change creates more opportunities for attackers to discover vulnerabilities. Continuous vulnerability research against web application frameworks, including WordPress and Drupal, is conducted within Akamai's engineering divisions. These frameworks are popular targets for malicious actors.

Financial services / The financial services industry experienced a slight decrease in attacks from 13% in Q1 to 11% in Q2. Banks, credit unions, and other financial organizations make tempting targets, and bank account credential lists are popular assets for trade in the underground economy. Even if attackers aren't able to steal money

directly, they try to extort financial organizations with the threat of downtime, a similar tactic to one employing DDoS attack vectors during the past two years.

Media & entertainment / The media & entertainment industry also saw a slight drop in attacks: 5% of all web application attacks in Q2, down from 8% in Q1 and 10% in Q4 2015. Organizations such as movie studios and news agencies are attractive targets because they are highly visible, and successful attacks typically generate publicity for the attackers and their motives.

All industries / Figure 3-7 lists the number of attack triggers observed for all industries we classified, followed by their percentage of attacks as a whole. Industries not included in Figure 3-6 are shown in red.

This level of granularity is important for understanding future attack trends. For example, although the pharmaceutical/healthcare industry only accounted for 0.31% of web application attack triggers in Q2, the presence of 899,827 attack triggers still provides a valuable dataset for in-depth research. In fact, this number is three times higher than Q2 last year, showing this industry is being increasingly targeted. Medical records are extremely valuable in the black market.

While other industries do not top the list, they still face substantial and unique risks. By examining them closely, we can see the beginnings of threats to come by analyzing trends over time observed within our platform.

3.5 / Bot Traffic Analysis / This quarter we updated an analysis of bot traffic collected across the Akamai Intelligent Platform. Figure 3-8 provides a snapshot of more than 2 trillion bot requests observed in one 24-hour period. It excludes bots that were not engaged in DDoS and web application attacks; those are covered elsewhere in this report. Bots represented 43% of all web traffic across the Akamai network that day (***see Section 5.3 for descriptions of the observed bot types***). We divided bot traffic by sub-category and provided the percentage associated with each.

Of the bot traffic, 28% was made up of declared bots — bots operated by legitimate organizations, which usually identify themselves by name, homepage, intentions, etc., in the HTTP request. Declared bots serve multiple purposes and provide services such as search engines, price comparisons, and data analytics.

Detected automation tools and scraping campaigns represented 63% of the bot traffic. This was a 10-point increase from last quarter's sample set. These bots were detected based on their behavior, a request signature, or an anomaly. They scrape specific websites or industry segments and do not identify their intentions or origin. In many cases, they impersonate legitimate users or other bots.

3.6 / Web Application Attack Spotlight — Use of Anonymizing Services in Web Attacks / Organizations interested in attack attribution often wonder how much web attack traffic comes from anonymizing services. Determining the true origin of web application attacks, however, is challenging. Common sense implies that malicious actors would strive to anonymize their activities and masquerade their source traffic to prevent traceback efforts. For this report, Akamai's Threat Research Team analyzed web attack traffic and quantified the usage of anonymizing services such as virtual private networks (VPNs) and proxies in web application layer attacks. In addition, we identified which attack types tend to be launched behind anonymizers, along with a distribution of the source and target countries of these attacks.

Anonymizing services: Proxies and VPNs / Using the Internet anonymously requires techniques that reduce the footprint of the user, as well as the user's identity and Internet client. Many online articles (e.g., ***The ultimate guide to staying anonymous and protecting your privacy online***[2]) describe how to obscure one's online footprints, and most of them include one or more of the following approaches:

Web Application Attack Triggers by Industry, Q2 2016

Industry	Attack Triggers	Percentage
Retail	116,599,968	40.30%
Hotel & Travel	60,797,928	21.02%
Financial Services	30,403,290	10.51%
Media & Entertainment	15,299,071	5.29%
Public Sector	14,691,344	5.08%
High Technology	14,669,798	5.07%
Business Services	12,543,383	4.34%
Software as a Service	9,354,076	3.23%
Manufacturing	4,545,361	1.57%
Consumer Goods	4,068,669	1.41%
Gaming	2,866,367	0.99%
Foundation-Not for Profit	1,150,419	0.40%
Pharma/Health Care	899,827	0.31%
Automotive	800,996	0.28%
Consumer Services	290,213	0.10%
Energy & Utilities	188,230	0.07%
Education	86,926	0.03%
Real Estate	31,158	0.01%
Miscellaneous	11,685	0.00%

Figure 3-7: While the top three targeted industries accounted for nearly 72% of attack triggers in Q2,12 of the 19 tracked industries recorded at least 1 million triggers

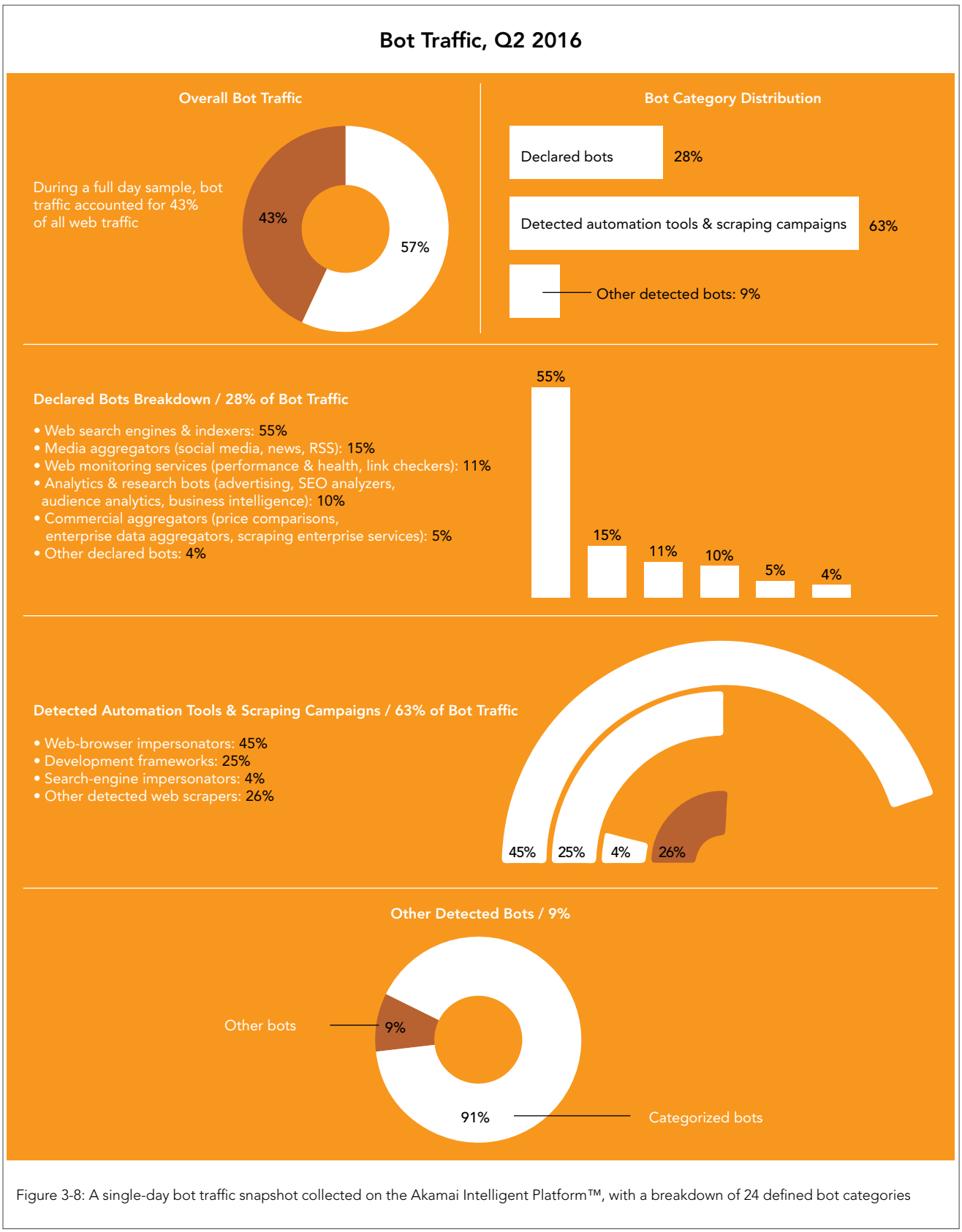


Figure 3-8: A single-day bot traffic snapshot collected on the Akamai Intelligent Platform™, with a breakdown of 24 defined bot categories

1. Delete browser cache and cookies regularly (or browse using incognito mode)

2. Block JavaScript and other client-side technologies that can be used for browser environment fingerprinting (e.g., HTML5 features, Flash, Silverlight)

3. Use an HTTP proxy when applicable (with a high anonymity level)

4. Use the TOR network (see the *Q2 2015 State of the Internet / Security Report*)

5. Use an anonymizing VPN service

In essence, an anonymizing proxy is an HTTP (or SOCKS) proxy, which routes traffic on behalf of end users, with some level of anonymity. Some proxies reveal the source IP address through HTTP headers (not anonymous), while others will provide complete anonymity and will keep HTTP traffic intact, leaving no trace of the proxy activity.

An anonymizing VPN service is similar in concept to traditional ***Virtual Private Networks***[3] with the difference that anonymizing VPNs are used for connecting the end user's machine to a VPN server hosted in the cloud, rather than to a corporate network. The reasons for using anonymizing VPNs are quite different from those for using traditional VPNs.

An anonymizing VPN service provides the following:

- Traffic between the client and the VPN service is encrypted
- The IP address of the source IP is masqueraded, and the user's traffic will appear as if it is originating from the VPN host's network and geography
- Some anonymizing VPN vendors promise to not log traffic or keep any traffic logs
- They support multiple VPN protocols (such as OpenVPN or IPSec.)
- There are no traffic volume limits
- They will take bitcoins for payment anonymity
- They do not require SOCKS-aware client software

VPN and proxy analysis methods / Akamai's Threat Research Team continuously analyzes web traffic by observing behavioral traffic patterns and applying proprietary machine learning techniques to classify clients as VPNs and proxies. Our detection algorithms run on top of Akamai's CSI (Cloud Security Intelligence) platform, which provides visibility into a significant portion of Internet traffic. Naturally, this visibility is crucial to detection accuracy, because it allows an observation across long periods of time, and large volumes and a wide variety of traffic.

> ***Anonymizers***[4] access the Internet on your behalf, protecting your personal information from disclosure. An anonymizer protects all of your computer's identifying information while it surfs for you, enabling you to remain at least one step removed from the sites you visit.

All matching VPN and proxy IP addresses are stored in a proprietary database along with enrichment data, such as the type of proxy or VPN, the anonymity level it provides, and the protocol used to access it.

Data corpus / We analyzed all of the IP addresses that generated malicious web attack traffic across our network in a 15-day sample period (June 20 – July 5, 2016) and cross-referenced the IP addresses with the IPs in our VPN and proxy database, as shown in Figure 3-9.

Figure 3-9 shows that:

1. 31.6% of all web attacks were routed through a VPN or proxy
2. 19.7% of attacking IP addresses were identified as a VPN or proxy
3. Since 19.7% of the attacking IP addresses (VPNs and proxies) are responsible for 31.6% of the attacks, this implies that the average VPN/Proxy attack source tends to generate more attack volume. This, in turn, might imply that attackers feel more free to bombard websites with attacks, while under the cloak of anonymity.

When categorizing the non-VPN/Proxy attack sources, we saw many source IP addresses belonged to US-based Internet service providers and hosting providers.

Almost all XSS attacks during the study period used a proxy, as shown in Figure 3-10. In contrast, only 12% of web vulnerability scanners used proxies compared with other web attacks. This makes sense, since running a web vulnerability scanner is not necessarily a malicious activity that requires anonymity.

Geographical data on malicious VPNs and proxies / Figure 3-11 and Figure 3-12 list the top 20 source countries of anonymized attacks. Of note was that 69% of web attacks that used VPNs or proxies were physically located within the US. Given that many US-based websites block traffic originating from outside the US, or from specific countries that tend to present higher risk for malicious cyber-activity, it is not a surprise that many attackers chose to use US-based infrastructure.

Ratio of IPs and Attacks by Proxy Type

Is Proxy/VPN	Number of IPs	% of Total IPs	Number of Attacks	% of Total Attacks
Not Proxy/VPN	633,278	80.3%	143,928,747	69.4%
Proxy/VPN	124,442	19.7%	45,438,631	31.6%

Figure 3-9: Nearly a third of web application attacks during the study period relied on anonymizing services

Ratio of IPs and Attacks by Proxy Type and Attack Category

	Number of Attacks, Not Proxy	Number of IPs, Not Proxy	Number of Attacks, Proxy	Number of IPs, Proxy	Proxy Ratio in Attacks	Proxy Ratio in IPs
CODEi	6,821,804	565,868	3,520,061	106,722	51.6%	18.9%
LFI	20,207,403	33,460	11,604,967	14,389	57.4%	43.0%
Vuln. Scanners	78,162,336	6,670	9,298,757	1,818	11.9%	27.3%
SQLi	31,650,536	34,514	13,953,288	11,774	44.1%	34.1%
XSS	7,086,668	8,294	7,061,558	5,800	99.6%	69.9%

Figure 3-10: XSS attacks almost always use proxies to cloak the attacker's identity

Top 20 Source Countries of Anonymized Web Attacks

Country	Number of Attacks	Number of IPs	Ratio of Attacks	Ratio of IPs
US	14,670,620	97,483	32.29%	69.38%
China	563,249	3,558	1.24%	2.53%
Russia	570,556	2,800	1.26%	1.99%
Brazil	4,303,143	2,426	9.47%	1.73%
Germany	2,674,443	2,300	5.89%	1.64%
France	1,746,108	2,128	3.84%	1.51%
Canada	948,760	2,058	2.09%	1.46%
Mexico	16,085	2,026	0.04%	1.44%
UK	906,301	1,765	1.99%	1.26%
Netherlands	2,546,458	1,622	5.60%	1.15%
Singapore	1,401,250	1,495	3.08%	1.06%
Argentina	34,014	1,267	0.07%	0.90%
India	1,706,623	1,158	3.76%	0.82%
Indonesia	143,241	969	0.32%	0.69%
Ecuador	17,094	735	0.04%	0.52%
Spain	1,371,841	692	3.02%	0.49%
Hong Kong	61,488	668	0.14%	0.48%
Puerto Rico	2,074	604	0.00%	0.43%
Japan	955,454	588	2.10%	0.42%

Figure 3-11: The vast majority (69%) of web attacks that used VPNs or proxies were physically located within the US

Other than US-based VPNs and proxies, the top four sources of VPN/proxy-based attack were China (2.5%), Russia (2%), Brazil (2%), and Germany (2%), as shown in Figure 3-11. They are also the top non-US source countries for web attacks (see Top 10 Source Countries for Web Application Attacks in ***Section 3.3***).

Top networks (ASNs) by number of attacks / The top five noisiest VPN/Proxy ASNs in Q2 as observed by Akamai and shown in Figure 3-12 were Amazon, OVH, LeaseWeb, and Connectria Hosting, all of which provide cloud VPS and hosting services, and ViewQwest, an ISP based in Singapore that provides free VPN services to customers.

Top networks (ASNs) by number of IP addresses / When looking at the top five networks by number of IP addresses, the top five networks, which are all US-based, made up 33% of all anonymized VPN and proxy IP addresses, but their attack volume only added up to 0.76% of attacks. This fact leaves room for speculation about the reasons for this behavior. It could be that these are residential IP addresses, used mostly for legitimate traffic, and the number of attacks they generate is low and sporadic.

Relation between source country and destination country / We investigated the relationship between the country where the VPN infrastructure is physically located, and the location of the attacked site (based on the billing address of the target account). We saw that all attack source countries targeted the US. This is not a surprise, given that many of the large targeted websites belong to US corporations.

To isolate the relevant data, we listed the top 10 source countries by number of VPN IP addresses. For each of these countries, we extracted the top target country (by attack volume) *other than the US* for these attacks.

Figure 3-13 shows that in 6 of the 10 countries, most of the malicious traffic (excluding traffic that targeted US-based sites) targeted IP addresses within the source country itself. The reason for this behavior may lie in an attempt by attackers to overcome geographical restrictions applied by the target websites. For example, it is common to see ecommerce sites restrict traffic to users from the same geography.

Conclusion / About a third of the web attacks we observed originated from anonymizing VPN services and proxies, a ratio substantially higher than the 20% of all traffic to emerge from VPNs and proxies. Web attackers likely have two main reasons for using anonymizing services:

- Anonymity: Hackers naturally prefer to perform their actions in a manner that will be untraceable to law enforcement organizations.

- Bypassing geo-location restrictions: Many websites deploy geographical restrictions on the source IP address, blocking access from countries where they do not do business.

We would like to note that while this discussion concentrated on malicious web activity, not all activity that is routed through proxies and VPNs is malicious. For example, many data mining services, business analytics, web scraping, and automated shopping bots also use anonymizing services, which allow them to load balance their activity and make it less detectable.

Top Networks (ASNs) By Number of Attacks

ASN	Number of Attacks	Number of IPs	Attack Ratio	IP Ratio	Name
16509	6,070,656	599	13.36%	0.42%	AMAZON-02 - Amazon.com, Inc., US
11734	3,503,334	3	7.71%	0.002%	CONNECTRIA HOSTING
28753	1,210,978	180	2.66%	0.128%	LEASEWEB-DE , DE
18106	1,178,641	13	2.59%	0.009%	VIEWQWEST-SG-AP Viewqwest Pte Ltd, SG
16276	1,083,504	1,688	2.38%	1.20%	OVH , FR

Figure 3-12: Of the top five networks for number of attacks, Amazon sourced the most attack traffic at 13%

Top Target Countries By Source Countries

Source VPN/Proxy Country	Top Target Country, Excluding Traffic to US-based Targets	Attack Volume
China	China	58%
Russia	India	34%
Brazil	Brazil	95%
Germany	Germany	56%
France	France	41%
Canada	1. Netherlands 2. Canada	80% 14%
Mexico	Mexico	85%
UK	1. France 2. UK	48% 25%
Netherlands	India	34%
Singapore	Singapore	50%

Figure 3-13: When excluding the US as a target, most web attack traffic is targeted within the same country as its VPN/proxy source

[SECTION]4
LOOKING FORWARD

The crowd roars. The audience springs to its feet as the swell of excitement reaches a fever pitch and the home team scores the crucial tie-breaking goal. Fans return to their seats to brush off the popcorn that landed on them a moment ago. But this is not always the case. More often than not, we find ourselves enjoying sporting events from the comfort of our homes — on screens both big and small. That in-home experience is all thanks to on demand streaming video (though the need to pick up the popcorn after a great play remains the same).

Streamed sporting events offer opportunities, not just for athletes and fans, but for attackers as well. With events like Euro 2016 and the 2016 Summer Olympics, the opportunity for making a profit off malicious traffic is too great for attackers to ignore. We will be there to record and report on the attacks — after we have defended our customers from them, of course.

There is no indication that we will see any reduction in the frequency or count of attacks any time in the near future. In fact, if the last year shows us nothing else, we should be prepared to see the number of attacks Akamai encounters grow by 10% or more next quarter, a trend observed every quarter for the last several years. This is in addition to the size of the largest attacks continuing to increase. That said, the majority of attacks have diminished in terms of bandwidth, at least for the current quarter.

Reflection DDoS attacks remain a popular weapon for attackers, with new vectors appearing frequently. mDNS was new this quarter. While the number of NTP servers attackers could use to amplify their attack strength declined, the use of NTP reflection has continued to rise, reaching a record high this quarter.

Continued proliferation of easy-to-use DDoS-for-hire technology will remain a threat. The same technologies that make the user experience easier for law-abiding people also create an easier experience for the online criminal community. New malware has emerged to take advantage of IoT architectures. In the near future, attacks may source from automated homes or vehicles.

Much of what we have reported is based on traffic patterns with subtle shifts over time. Yes, this quarter might see China as the top source of attack traffic, while the next quarter it could be the US, but these are minor changes within the bigger scheme. On the other hand, large events, such as the Olympics, often reveal new traffic patterns, with larger impacts on the threat landscape.

[SECTION]5 CLOUD SECURITY RESOURCES

5.1 / Threat Advisories / Akamai released three security publications in Q2 2016.

High Risk DDoS Threat Advisory: BillGates Botnet[5] / The BillGates toolkit allows malicious actors to build botnets using a tool called Builder. The malware commonly compromises systems with brute force attacks against secure shell (SSH). As an attack platform, the botnets can launch attacks that include ICMP flood, TCP flood, UDP flood, SYN flood, HTTP flood (Layer7), and DNS query-of-reflection flood.

High-Risk DDoS Threat Advisory: #OpKillingBay Expands Targets Across Japan[6] / Operation Killing Bay, which uses the hashtag #OpKillingBay, has expanded the targets of online activists. No longer willing to just attack Japanese government sites and sites related to the killing of dolphins, the hacktivists have spread their attacks to other sites when the target didn't protest against such activities.

Medium Risk DDoS Threat Advisory: Trivial File Transfer Protocol (TFTP) Reflection DDoS[7] / Trivial File Transfer Protocol (TFTP) allows users to send small files across local networks. Recent research at the Edinburgh Napier University showed that TFTP could be used as a reflection vector with an amplification of 38 to 104 times the original traffic, though with severe limitations that hampers the use of TFTP as a major reflector protocol.

5.2 / Web Application Attack Types /

SQLi / SQL injection is an attack where adversary-supplied content is inserted directly into a SQL statement before parsing, rather than being safely conveyed post-parse via a parameterized query.

RFI / Remote file inclusion is an attack where a malicious user abuses the dynamic file include mechanism, which is available in many web frameworks, and loads remote malicious code into the victim web application.

PHPi / PHP injection is an attack where a malicious user is able to inject PHP code from the request itself into a data stream, which gets executed by the PHP interpreter, such as by use of the `eval()` function.

MFU / Malicious file upload (or unrestricted file upload) is a type of attack where a malicious user uploads unauthorized files to the target application. These potentially malicious files can later be used to gain full control over the system.

CMDi / Command injection is an attack that leverages application vulnerabilities to allow a malicious user to execute arbitrary shell commands on the target system.

LFI / Local file inclusion is an attack where a malicious user is able to gain unauthorized read access to local files on the web server.

JAVAi / Java injection is an attack where a malicious user injects Java code, such as by abusing the Object Graph Navigation Language (OGNL), a Java expression language. This kind of attack became very popular due to recent flaws in the Java-based Struts framework, which uses OGNL extensively in cookie and query parameter processing.

XSS / Cross-site scripting is an attack that allows a malicious actor to inject client-side code into web pages viewed by others. When an attacker gets a user's browser to execute the code, it will run within the security context (or zone) of the hosting web site. With this level of privilege, the code has the ability to read, modify and transmit any sensitive data accessible by the browser.

5.3 / Observed Bot Types /

Web search engines & indexers / These bots are used by search engines to collect and index data. Based on the indexed data, an end user can use search engines to get a ranked set of results based on information need.

Media aggregators / These bots collect and aggregate data from media resources (TV, music, news, social media, etc.) in order to provide their customers with a centralized and aggregated database based on their needs (e.g., custom homepages and trend analysis)

Commercial aggregators / These bots collect and aggregate data from commercial and e-commerce sites (shopping, airlines, traveling agencies, etc.). They usually provide their customers with a centralized data source based on their needs (e.g., price comparisons, business intelligence).

Analytic and research bots / These bots may target either specific websites/industry segments or a broad range of websites for analysis and research, such as SEO, audience analytics, and advertising.

Web monitoring services / These bots approach websites and resources for monitoring, such as link checking, performance testing, and domain name availability.

Other declared bots / These bots identify themselves but their origin or intentions cannot be defined.

Web-browser impersonators / These bots are scrapers that identify themselves as legitimate browsers yet are detected as automated tools.

Search-engine impersonators / These bots are scrapers that identify themselves as valid search engine bots in order to access the website.

Development frameworks / These are scrapers that use HTTP libraries of known development frameworks. They are detected based on request signatures that specify the library name or development framework

Other detected web scrapers / These bots are detected by scraping behavior or behavior combined with request anomalies.

Other detected bots / These bots are detected by some anomalies but their behavior and intention cannot be determined.

5.4 / Updates and Corrections /

We are only human, and here we identify the errors and omissions from previous reports. If you have a data point, chart, or explanation you believe to be in error, please notify the Akamai team at ***SOTISecurity@akamai.com***.

- Akamai will no longer represent the average duration of DDoS attacks. The data was not collected with an accurate, consistent methodology that represented the true duration of DDoS attacks. We are in the process of creating new methods to measure duration in an automatic fashion and will begin reporting on this statistic again when measurements are accurate and consistent.

- Figure 2-13, "*Distribution of Total DDoS Reflection Attacks, Q1 2015 – Q1 2016*" in the Q1 2016 report was mislabeled as showing the percentage of growth in reflected DDoS attacks. The figure showed attacks per quarter as a percentage of total reflection attacks over the time period. The percentages shown did not represent the growth of reflection attacks in each quarter.

[1] *https://www.us-cert.gov/ncas/alerts/TA14-013A*

[2] *http://www.extremetech.com/internet/180485-the-ultimate-guide-to-staying-anonymous-and-protecting-your-privacy-online*

[3] *https://en.wikipedia.org/wiki/Virtual_private_network*

[4] *http://www.livinginternet.com/i/is_anon_sites.htm*

[5] *https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/bill-gates-botnet-threat-advisory.pdf*

[6] *https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/opkillingbay-expands-targets-across-japan-threat-advisory.pdf*

[7] *https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/trivial-file-transfer-protocol-reflection-ddos-threat-advisory.pdf*

Notes

Notes

Notes

***State of the Internet / Security* Team**
David Fernandez, Akamai SIRT
Jose Arteaga, Akamai SIRT
Ezra Caltum, Threat Research Unit
Martin McKeay, Senior Security Advocate
Dave Lewis, Security Advocate
Jon Thompson, Custom Analytics
Ryan Barnett, Threat Research Unit
Larry Cashdollar, Akamai SIRT
Ory Segal, Threat Research Unit
Aharon Fridman, Threat Research Unit

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

Contact
SOTIsecurity@akamai.com
Twitter: *@akamai_soti* / *@akamai*
www.akamai.com/StateOfTheInternet

About Akamai® 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*.


Akamai FASTER FORWARD