[Volume 3 / Number 3]

akamai's [state of the internet] / security

Q3 2016 report

AT A GLANCE

DDoS attacks, Q3 2016 vs. Q3 2015
71% increase in total DDoS attacks
77% increase in infrastructure layer (layers 3 & 4) attacks
138% increase in attacks > 100 Gbps: 19 vs. 8

DDoS attacks, Q3 2016 vs. Q2 2016
8% decrease in total DDoS attacks
8% decrease in infrastructure layer (layers 3 & 4) attacks
58% increase in attacks > 100 Gbps: 19 vs. 12

Web application attacks, Q3 2016 vs. Q2 2016
4% decrease in total web application attacks
6% increase in SQLi attacks
13% decrease in attacks sourcing from the U.S. (new top source country)
79% decrease in attacks sourcing from Brazil (previous top source country)

Web application attacks, Q3 2016 vs. Q3 2015
18% decrease in total web application attacks
21% increase in SQLi attacks
67% decrease in attacks sourcing from the U.S.
**Note: rounded to the nearest percentage*

What you need to know

- Akamai mitigated 4,556 distributed denial of service (DDoS) attack events across the Akamai routed network, an 8% drop from Q2's 4,919 DDoS attacks.

- Two DDoS attacks this quarter topped our previous high water mark, at 623 Gbps and 555 Gbps. Both attacks targeted ***krebsonsecurity.com*** and are covered in the DDoS Attack Spotlight.

- Last quarter we reported a 276% increase in NTP attacks compared with Q2 of 2015. This quarter, we analyzed NTP trends over two years and have noticed shrinking capabilities for NTP reflection.

- Web application attack metrics around the European Football Cup Championship Game and the Summer Games, as analyzed in the Web Application Attack Spotlight, show us that while malicious actors take advantage of high-profile events, there's also a lull that indicates they might like to watch them.

LETTER FROM THE EDITOR / The Q3 2016 *State of the Internet / Security Report* represents analysis and research based on data from Akamai's global infrastructure and routed DDoS solution.

The *State of the Internet / Security Report* underwent major changes this quarter — new graphs, more succinct analysis, and a significant reduction in the size of the report. While some data points and graphs you might be accustomed to seeing have been removed this quarter, rest assured we'll rotate them back in on a regular basis, as their relevance dictates.

We endeavored to make the *State of the Internet / Security Report* a place where readers can find valuable information — that is one constant we will always maintain. However, the report grew significantly in volume, making it harder for readers to find the data that is valuable to them. Going forward, the goal is to make the *State of the Internet / Security Report* a starting point from which readers can easily find the information that is most important to them.

The changes were aimed at making a more dynamic, readable report. There are several anchor sections, such as the DDoS Attack Vector Frequency and Top Source Countries. Going forward, many sections will be on rotation, only showing up when there are significant changes to the threat landscape. Finally, we will continuously be creating new sections, such as this quarter's NTP Analysis and an in-depth review of the attacks on ***krebsonsecurity.com***.

You will see more of our research become available between reports, with compiled summaries included in the quarterly *State of the Internet / Security Report*. There is never a lack of interesting subjects to research in the field of cybersecurity.

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

— Martin McKeay, Senior Editor and Akamai Senior Security Advocate

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

Generally, the last two weeks of the quarter are simply more of the same things we saw during the previous eleven weeks. This quarter, however, the big events happened at the end, throwing many of our expectations out the window.

Without a doubt, the attacks on the site of cybersecurity writer and blogger, Brian Krebs (***www.krebsonsecurity.com***), were the biggest story of the quarter. The site had been protected pro bono by Akamai's Prolexic network since July 2012 and found itself on the receiving end of a 623 Gigabits per second (Gbps) attack on September 20, 2016. This was the biggest attack Akamai had ever mitigated to that point. While we were able to keep his site functioning, this and the attacks that followed it caused the company to re-evaluate the resources being spent on a site we were protecting for free. We provide an overview of the history of attacks on this site and provide our analysis of the September attacks in Section 2.4.

These attacks were remarkable not only for their size, but also for the source and nature of the traffic they used. Since June, we had been researching a strain of malware we called Kaiten, which targets home routers and Internet of Things (IoT) devices. The malware has now been released to the world at large, under the name Mirai, and targets more than 60 default username and password combinations. When used in the attacks on Krebs on Security, the tool used GRE, SYN, and ACK floods at the network level, along with PUSH and GET floods at the application layer. None of these vectors are hard to mitigate individually, but any type of traffic becomes problematic where you receive it at 623 Gbps.

In the Q2 *State of the Internet / Security Report*, one of the biggest stories was the fact that NTP reflection attacks grew by 238% over the previous year. This quarter, we examined historical NTP traffic to discover a number of interesting indicators about the vector. The analysis indicated that NTP reflectors are getting cleaned up over time; as a result, NTP reflection appears to be becoming less of a threat.

[SECTION]^2
DDoS ACTIVITY

2.1 / DDoS Attack Vectors / Except for rare occasions, the overall composition of attack vectors Akamai observes on a quarterly basis are marked by subtle fluctuations, rather than sweeping changes. This quarter was no exception. While application-layer DDoS attacks can have a disproportionate impact compared to infrastructure-layer attacks, they still only account for 1.66% of all attack vectors seen on Akamai's routed Network. This may be because most application attacks require at least some technical knowledge and understanding to accomplish, in contrast to infrastructure attacks that are often launched with point-and-click tools and search-engine skills.

UDP fragments and DNS reflection continued to be the largest portion of the DDoS attack traffic across our routed network. The two vectors are strongly correlated, because a considerable amount of the UDP fragmentation traffic is a byproduct of DNS traffic. Combined UDP fragmentation and DNS floods grew by 4.5% in the third quarter, accounting for nearly 44% of the attack vectors. If we include UDP flood traffic, which is also related to UDP fragmentation, these three vectors

accounted for approximately 54% of the attacks observed. UDP and CHARGEN round out the top five attack vectors, and both moved over to make room for the three previously named protocols, DNS, UDP fragments, and UDP flood.

Despite a number of highly publicized attacks, the overall number of attacks fell by nearly 8% in the third quarter compared with Q2 2016. DNS flood and UDP fragmentation saw the largest decreases in traffic. Since UDP fragmentation has a high correlation with DNS

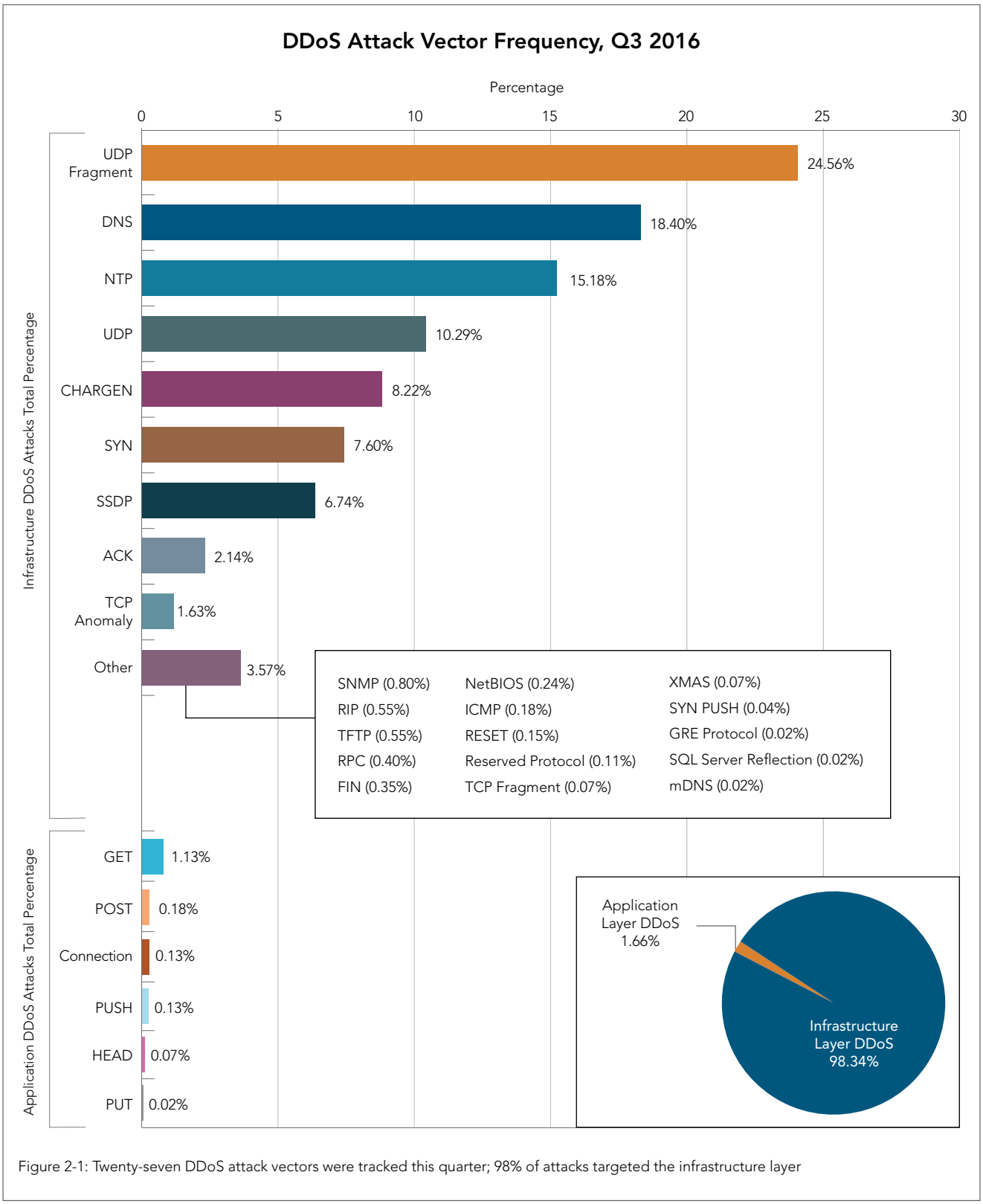


Figure 2-1: Twenty-seven DDoS attack vectors were tracked this quarter; 98% of attacks targeted the infrastructure layer

floods, this drop in both attack vectors was expected. In contrast, SYN flood and NTP reflection remained popular components of attacks this quarter.

Even though they were heavily used by the Mirai botnet, Generic Routing Encapsulation (GRE) flood attacks remain a very minor component of the overall attack landscape. It would not be surprising if this protocol increases in popularity because of the recent attacks. However, unlike reflection-based attacks, GRE flooding relies heavily on the capacity of the botnet nodes, not amplification.

It is encouraging to see a drop in overall attack numbers in the third quarter of 2016, as evidenced in Figure 2-2. However, this trend is unlikely to continue. Thanksgiving, Christmas, and the holiday season in general have long been characterized by a rise in the threat of DDoS attacks. Malicious actors have new tools — IoT botnets — that will almost certainly be used in the coming quarter.

2.2 / NTP Analysis / Last quarter we reported a 276% year-over-year increase in NTP attack vectors, which led us to analyze NTP traffic more closely. The results were surprising. While the number of NTP attacks has grown over time, the amount of traffic generated by each attack has decreased significantly. During the 2014 holiday season, the average NTP flood attack was over 40 Gbps, while the average attack in Q3 2016 barely generated 700 Million bits per second (Mbps) — a 98% drop in volume.

Akamai records attack traffic data as an aggregate of all vectors, making the tracking of specific protocols difficult. To overcome this limitation, we analyzed those attacks that had NTP as their only attack vector. We also looked back over a two-year period; the initial surge in NTP reflection attacks was created by the release of CVE 2013-5211, NTP monlist.

The first thing you may notice when you look at Figure 2-3 is a pair of spikes in the traffic rates in February and December, 2014. The first spike was caused by the release of CVE 2013-5211, mentioned earlier. Almost immediately after the CVE was released, a set of attack tools were created. This traffic quickly died down as many vulnerable servers were patched. The second spike corresponded with efforts by hacking groups to ruin Christmas for gamers around the world by taking multiple gaming services offline.

More recently, the rise and fall of both total traffic and the number of attacks using NTP reflection, between June 2015 and publication, reveal a pair of peaks in the overall traffic. Both December 2015 and

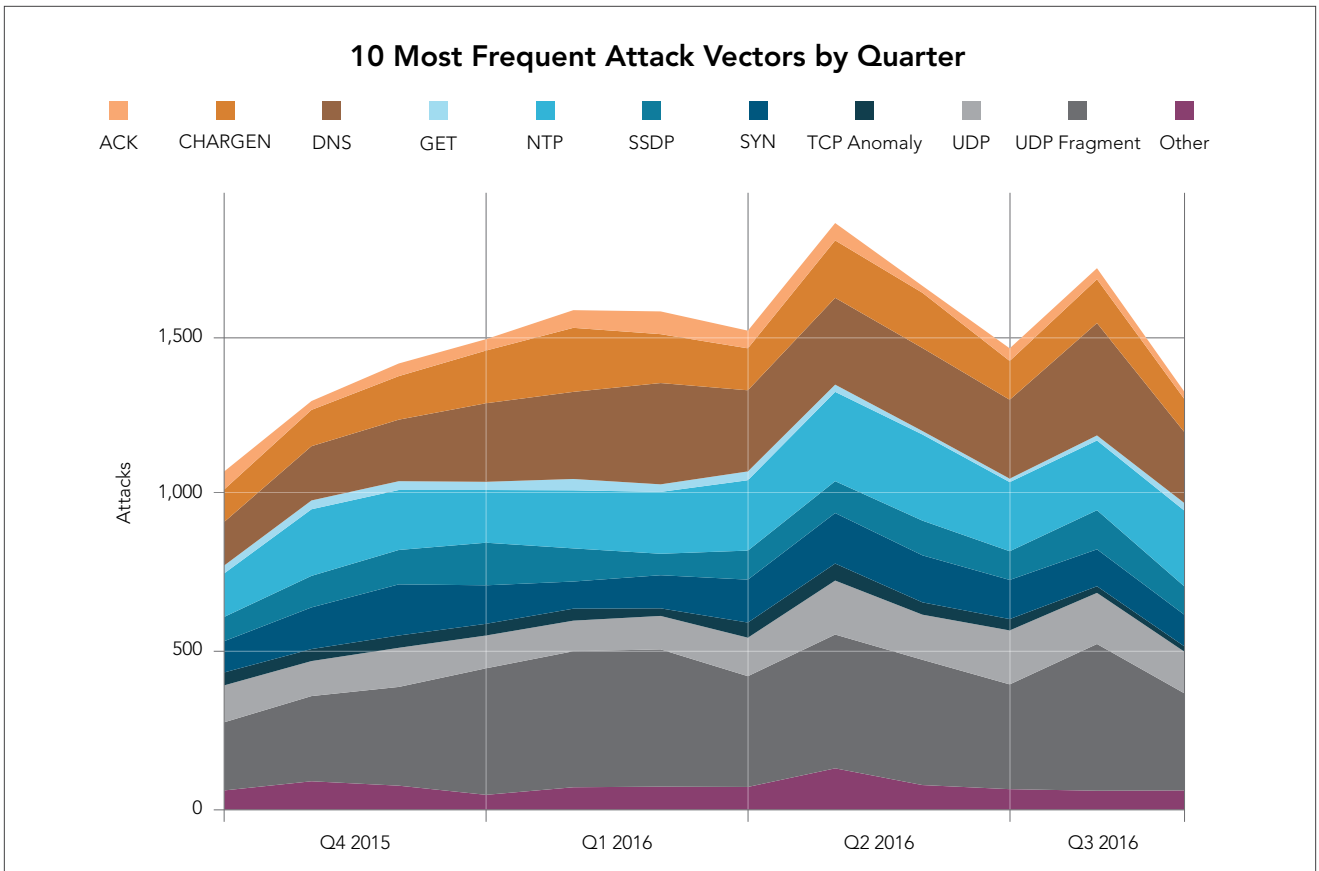


Figure 2-2: While there was a surge of attacks in August, the overall number of attacks in the third quarter was down compared with Q2 2016

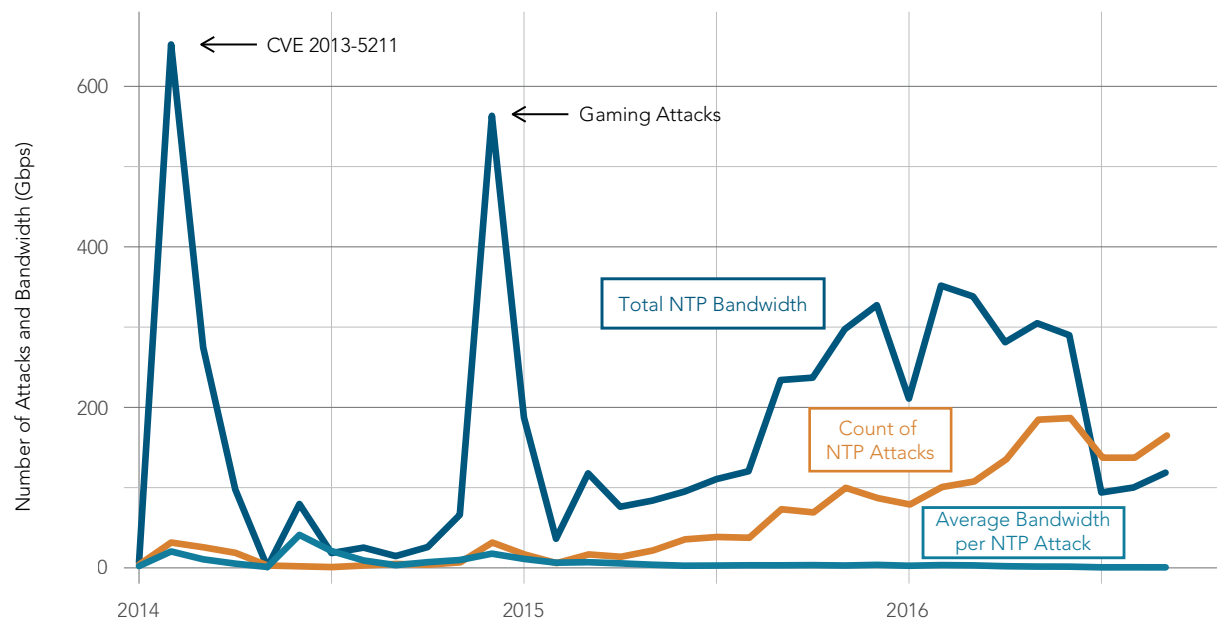


Figure 2-3: The release of the NTP monlist vulnerability caused a huge spike in NTP attack traffic, followed by a concentrated attack on gaming companies in December 2014

February 2016 mark the most recent high points, with a sharp drop in both the number of attacks and total attack traffic in June 2016. Why this sudden change?

When NTP reflection became a common vector in 2014, we saw large spikes in attack traffic. This was caused by attackers discovering the vulnerability and then sharing information about the pools of vulnerable NTP servers amongst themselves. At the same time, system administrators worked diligently to patch NTP servers, making the lists of vulnerable servers more unstable and less valuable. After the most active system owners were finished, we were still left with a large pool of more stable, rarely patched systems. Slowly, the number of botnets using NTP reflection rose and the total amount of traffic rose with it.

The number of NTP servers available to use for reflection attacks is finite and shrinking . As more botnets use NTP reflection, the servers that are vulnerable receive more traffic, which brings more traffic to the vulnerable servers and draws more attention to them. In some cases, the owners patch them, and in other cases, third parties bring the vulnerable servers to the owner's attention. In a few cases, old, vulnerable NTP servers went offline. It appears that June was the critical inflection point, when not only did available NTP reflection bandwidth shrink, but botnet owners pivoted to other protocols for their traffic.

In Q3 2016, the average (mean) size of an attack relying solely on NTP reflection was approximately 700 Mbps. This represents a huge drop from June 2014, when the average size of an attack was more than 40 Gbps.

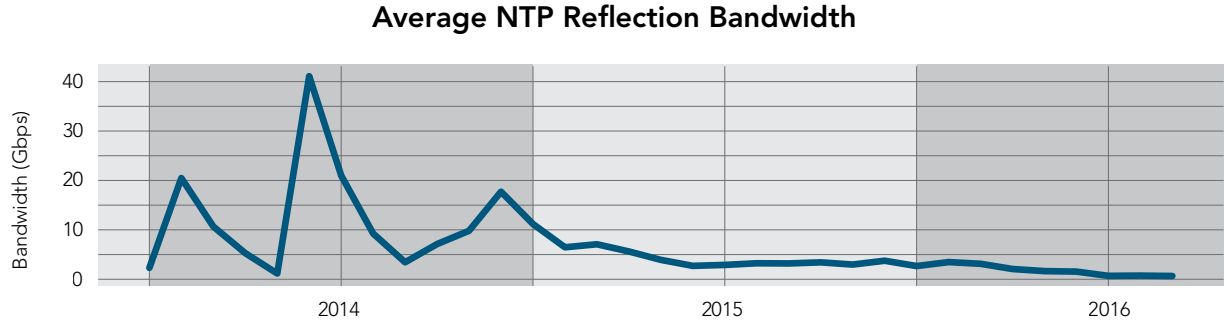


Figure 2-4: By June 2016, NTP reflection bandwidth had shrunk to the point that botnet owners started to move on to other protocols

We're not out of the woods yet, as we saw a slight resurgence in the number of attacks this quarter, though still far fewer than last quarter. While the long tail of vulnerable NTP servers will likely stick around for some time, it's encouraging to think we might see a decided drop in both the number of attackers using NTP reflection as well as the number of vulnerable servers in the future.

2.3 / Mega Attacks / The first quarter of 2016 marked a high point in the number of attacks peaking at more than 100 Gbps. This trend was matched in Q3 2016, with another 19 mega attacks. It's interesting that while the overall number of attacks fell by 8% quarter over quarter, the number of large attacks, as well as the size of the biggest attacks, grew significantly.

The attacks on Brian Krebs' site marked the two highest volume attacks seen on the Prolexic network to date and are covered in depth in Section 2.4. An additional three mega attacks are attributed to this attack campaign.

Booter/stressor botnets continued to account for a large portion of the attack traffic in mega attacks. In contrast to previous quarters, when reflection attacks generated the traffic in the largest attacks, a single family of botnets, Mirai, accounted for the traffic during these recent attacks. Rather than using reflectors, Mirai uses compromised IoT systems and generates traffic directly from those nodes. The Mirai botnet is also covered in more depth in Section 2.4.

2.4 / Attack Spotlight: Krebsonsecurity.com

Summary / Normally, Akamai does not report on customers by name, but in the case of ***krebsonsecurity.com***, we're making an exception. The attacks made international headlines and were also covered in depth by Brian Krebs himself. The same data we've shared here was made available to Krebs for his own reporting and we received permission to name him and his site in this report.

Brian Krebs is a security blogger and reporter who does in-depth research and analysis of cybercrime throughout the world, with a recent emphasis on DDoS. His reporting exposed a stressor site called vDOS (***http://krebsonsecurity.com/2016/09/israeli-online-attack-service-vdos-earned-600000-in-two-years/***) and the security firm BackConnect Inc. (***http://krebsonsecurity.com/2016/09/israeli-online-attack-service-vdos-earned-600000-in-two-years/***), which made him the target of a series of large DDoS attacks starting September 15, 2016.

Defending a site against a DDoS attack has both a fixed and a variable cost. The fixed costs come in the form of sites, servers, and engineering. The variable, or operational, costs include the bandwidth served and manpower needed to mitigate attacks.

Between September 15 and 22, Krebs' site was hit with a series of attacks, peaking at 623 Gbps on the 20th. On Friday, September 22, the difficult decision to remove the site from the protection of Akamai was made. At no time during the attacks did the krebsonsecurity.com site cease to function. The DNS records for

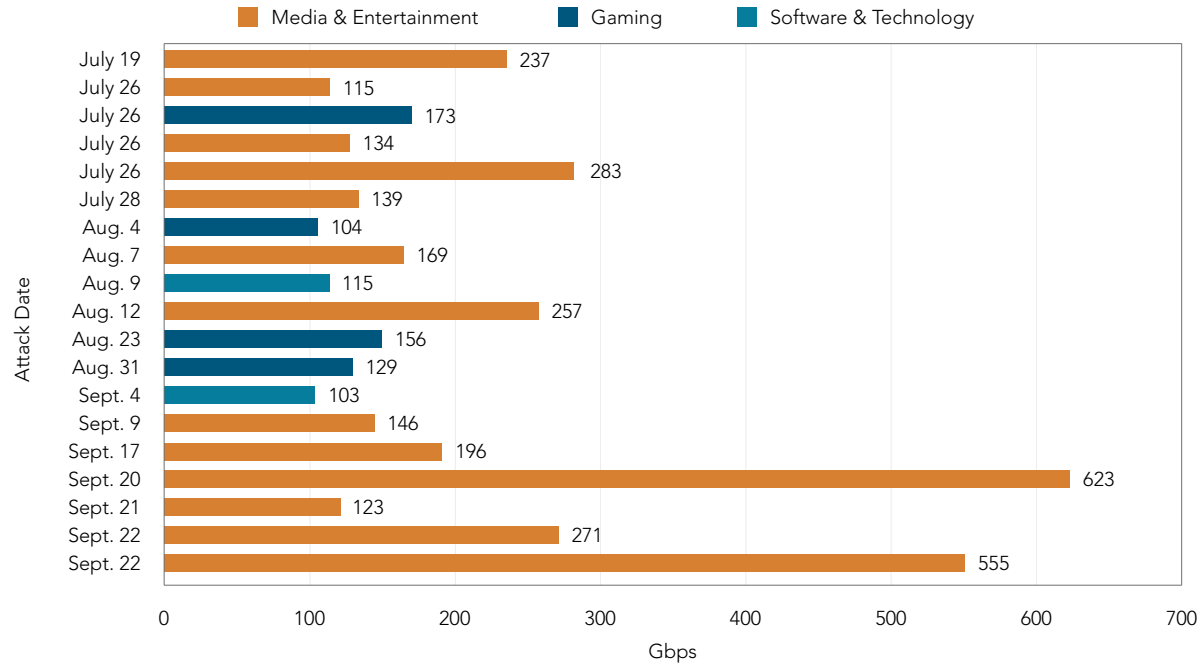


Figure 2-5: Nineteen DDoS attacks exceeded 100 Gbps, with six exceeding 200 Gbps

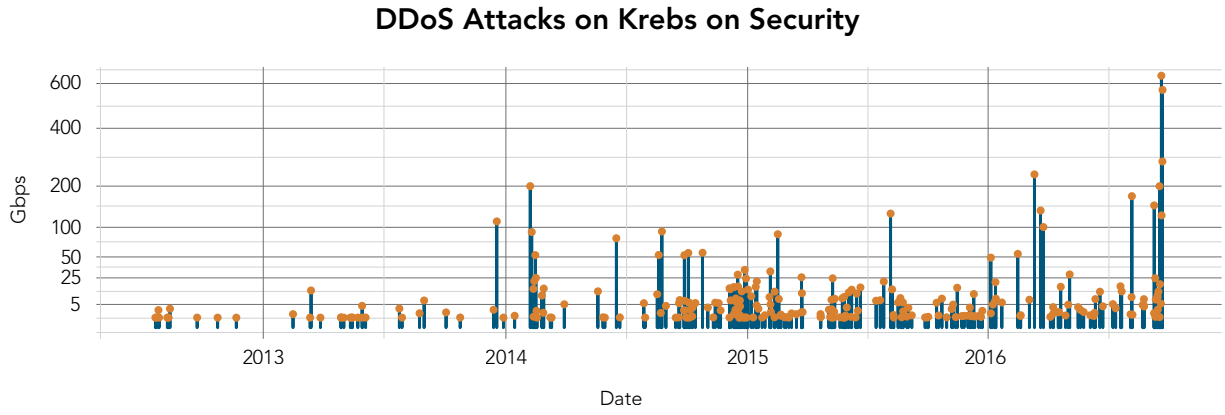


Figure 2-6: All attacks mitigated for krebsonsecurity.com while on the routed platform

krebsonsecurity.com were pointed to 127.0.0.1, and later the site was moved to Google's Project Shield (***https://projectshield.withgoogle.com/public/***), a free program run by Google to help protect journalists from online censorship, for protection.

History / In August 2012, Krebs became a pro bono customer of Prolexic (and later of Akamai). His site, ***krebsonsecurity.com***, had come under DDoS attack starting in May 2012, and Prolexic offered to protect the site free of charge. Almost as soon as the site was on the Prolexic network, it was hit by a trio of attacks based on the Dirt Jumper DDoS tookit (***https://krebsonsecurity.com/2012/08/triple-ddos-vs-krebsonsecurity/***). Those attacks marked the start of hundreds of attacks that were mitigated on the routed platform.

In total, the site received 269 attacks in just over four years. During that time, there were a dozen mega attacks peaking at over 100 Gbps. The first happened in December 2013, the second in February 2014, and the third in August 2015. In 2016, the size of attacks accelerated dramatically, with four mega attacks happening between March and August, while five attacks occurred in September, ranging from 123 to 623 Gbps. Figure 2-6 shows the relative sizes and timelines of the attacks on krebsonsecurity.com. An observant reader can probably correlate clumps of attacks to specific stories covered by Krebs. Reporting on the dark side of cybersecurity draws attention from people and organizations who are not afraid of using DDoS attacks to silence their detractors.

The Final Attacks / Akamai had protected ***krebsonsecurity.com*** for four years, but the magnitude of the attacks seen during the final week were significantly larger than the majority of attacks Akamai sees on a regular basis. In fact, while the attack on September 20 was the largest attack ever mitigated by Akamai, the attack on September 22 would have qualified for the record at any other time, peaking at 555 Gbps. This attack consisted primarily of ACK floods and NTP reflection traffic. While the Mirai botnet is known to have contributed to the attack, it is not capable of generating NTP reflection attacks.

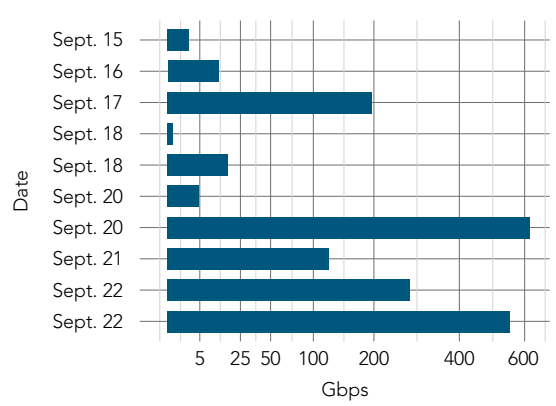


Figure 2-7: Bandwidth for each of the 10 attacks

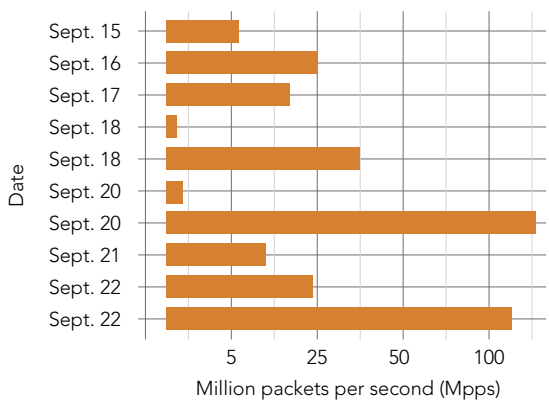


Figure 2-8: Packet rate for each of the 10 attacks

Much has been written about the attack on September 20th, which is appropriate, as it remains the largest DDoS attack seen by Akamai. This 623 Gbps attack consisted of GRE floods, SYN floods, and ACK floods at the network level, and both PUSH and GET floods at the application layer. None of these protocols are difficult to mitigate individually, but the sheer volume of this attack was impressive. GRE traffic is an uncommon attack vector, seen in only a handful of attacks each year, and this was the only attack upon the site using this protocol.

The 10 attacks that occurred between September 15 and September 22 are shown in Figures 2-7, (peak bandwidth) and 2-8 (packets per second). While we generally concentrate on bandwidth as the most important factor, it's not the only factor. The much smaller attack on September 18 was purely a GET Flood, which relies on stressing server resources, not the network. In contrast, the other attacks primarily used network-layer flooding such as ACK, SYN, and UDP floods.

The attack sources were global in nature, which is to be expected of an IoT-based attack. Attackers are generally not looking for vulnerable systems in a specific location, they are scanning the entire Internet for vulnerable systems. The Mirai botnet is especially noisy and aggressive while scanning for vulnerable systems.

Figure 2-9 shows the traffic sources of the 24,000 IP addresses used in the 623 Gbps attack on September 20, while Figure 2-10 also includes the final four attacks on krebsonsecurity.com. This includes both the September 20 attack and the final attack on September 22, which was measured at 555 Gbps. Some of the attack traffic was not attributable to the Mirai botnets seen in the pivotal attack, given that the last attack consisted largely of NTP reflection traffic.

Overall, Columbia was the top source of attack traffic. This is surprising, because Columbia has not been a major source of attack traffic in the past. While Columbia only accounted for approximately 5% of the traffic in the Mirai-based attacks, it accounted for nearly 15% of all source IPs in the last four attacks. A country that was suspiciously missing from both top 10 lists was the U.S. With regards to Mirai, this may be due to a comparative lack of vulnerable and compromised systems, rather than a conscious decision not to use systems in the U.S.

Mirai Malware and IoT / The Mirai botnet was a source of the largest attacks Akamai mitigated to date, an attack that peaked at 623 Gbps. Mirai did not come out of nowhere; the Akamai SIRT had been analyzing a variant of the malware, dubbed Kaiten, since June. What makes Mirai truly exceptional is its use of IoT devices and several capabilities that aren't often seen in botnets: specifically, Generic Routing Encapsulation (GRE) based attacks, varying levels of attack traffic customization, and telnet scanning. In addition, it generates its attacks directly, without using any reflection vectors (yet). Due to the public release of the source code and the extensible nature of the code, we're likely to see new, more-capable variants of Mirai in the near future.

> We haven't seen GRE really play a major role in attacks until now. It's basically a UDP flood with a layer-7 component targeting GRE infrastructure. While it's not new, it's certainly rare.
>
> *— Chad Seaman, Sr. Engineer, Akamai Security Intelligence Response Team*

Mirai is a botnet that would not exist if more networks practiced basic hygiene, such as blocking insecure protocols by default. This is not new — we've seen similar network hygiene issues as the source of infection in the Brobot attacks of 2011 and 2012. The botnet spreads like a worm, using telnet and more than 60 default username and password combinations to scan the Internet for additional systems to infect. The majority of these systems appear to be Digital Video Recorders (DVRs), IP-enabled surveillance cameras, and consumer

Source Countries for Sept. 20 DDoS Attack

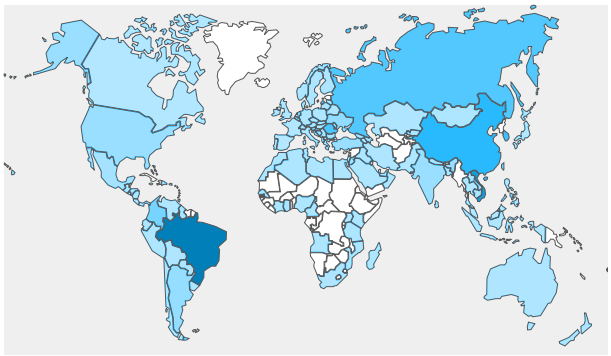


Figure 2-9: Heat map of countries sourcing the malicious traffic from the 24,000 IP addresses used in the 623 Gbps attack

Source Countries for Last Four Attacks

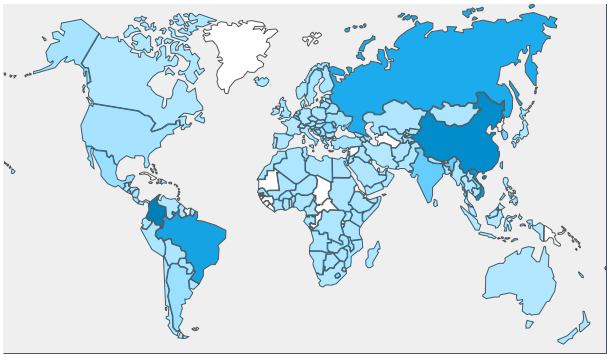


Figure 2-10: Heat map of countries sourcing the malicious traffic from the 210,000 IP addresses used in final four attacks

routers. Once a system is infected, it connects to the command and control (C2) structure of the botnet, then continues scanning for other vulnerable systems while waiting for attack commands.

Akamai analyzed traffic from the Mirai C2 servers and discovered several interesting factors. First, the C2 for Mirai is well distributed; at its peak, a single botnet was issuing commands from more than 30 C2 IP addresses. Second, the botnet appears to be segmented, yet its components can work in concert. Many of the thousands of attack commands issued by the C2 structure only called for attacks from small portions of the botnet, while a much smaller number elicited attacks from the botnet as a whole.

The botnet is capable of generating 10 types of attacks: two UDP floods, two types of GRE floods, two types of ACK floods, one SYN flood, one DNS flood, a Valve Engine attack, and an HTTP flood attack that is configurable and can leverage any HTTP method, while allowing customization of path, data, and cookie headers. An eleventh type of attack contained in the source code appears to have been commented out and inactive in the samples examined by Akamai. The botnet allows for both static and randomized IP address spoofing in five of the 10 attack types.

> There are a few distinctive programming characteristics we initially discovered in our lab, and later confirmed when the source code was published, which have helped identify Mirai-based traffic. At the end of the day what Mirai really brings to the table is a reasonably well written and extensible code base. It's unknown as to what Mirai may bring in the foreseeable future but it is clear that it has paved the way for other malicious actors to create variants that improve on its foundation.
>
> — *Chad Seaman, Sr. Engineer, Akamai Security Intelligence Response Team*

The use of GRE flood traffic is an unusual protocol for a botnet to use, but Mirai seems to be heavily invested in its use. The botnet allows attackers to customize the size of the GRE packet from the default 512 bytes. Another tool in Mirai's belt is the Valve Engine protocol attack, which is used to overload gaming servers. This attack is relatively easy to mitigate and has long been known in the gaming industry.

The most notable factor in the design and implementation of this botnet is its ability to generate traffic directly. Many, if not most, large DDoS attacks rely on reflection to generate significant traffic. Due to the number of IoT devices that a Mirai botnet can take advantage of, it's been able to generate the biggest attacks seen to date, despite lacking capabilities commonly used in attacks of relatively similar size.

The Mirai botnet continued to grab headlines with the release of the malware's source code on October 1. While it's the current record holder for the largest DDoS attacks, it's important to remember that it's far from the only heavy-hitting botnet on the Internet today. The attack on September 22 that peaked at 555 Gbps second was not a Mirai-based botnet; it used ACK Floods and NTP reflection. It would have qualified as the biggest attack we've mitigated, if not for Mirai. Other botnets are almost certainly attempting to reach the same attack capabilities in the near future, and now attackers have the source code to do it.

Conclusions / The attacks on ***krebsonsecurity.com*** created a new high-tide mark for DDoS attack traffic. These attacks show how effective a large botnet can be and give other malware developers a target to aim for. The IoT-fueled botnets that security professionals have feared are a real, tangible menace that attackers will likely try to recreate going forward.

The code that made the Mirai botnet possible has been released to the wider world. The specific devices that were used to make Mirai are still running and vulnerable, though the manufacturer has issued a recall and is working on making its code less vulnerable. However, there are many more IoT devices in existence that share similar vulnerabilities and will provide tempting targets to attackers. Until IoT security becomes a primary concern for manufacturers, this type of malware will be increasingly common.

2.5 / DDoS Source Countries / This quarter marks a full year with China as the top source country for DDoS attacks with just under 30% of attack traffic this quarter, as shown in Figures 2-11 and 2-12. More importantly, the proportion of traffic from China has been reduced by 56%, which had a significant effect on the overall attack count and led to the 8% drop in attacks seen this quarter. The U.S., U.K., France, and Brazil round out the remaining top five source countries.

It's important to remind readers that UDP attacks, including fragmentation, were not included in this metric. This is in large part due to the ease with which these attacks can be spoofed and could create significant distortion of the data.

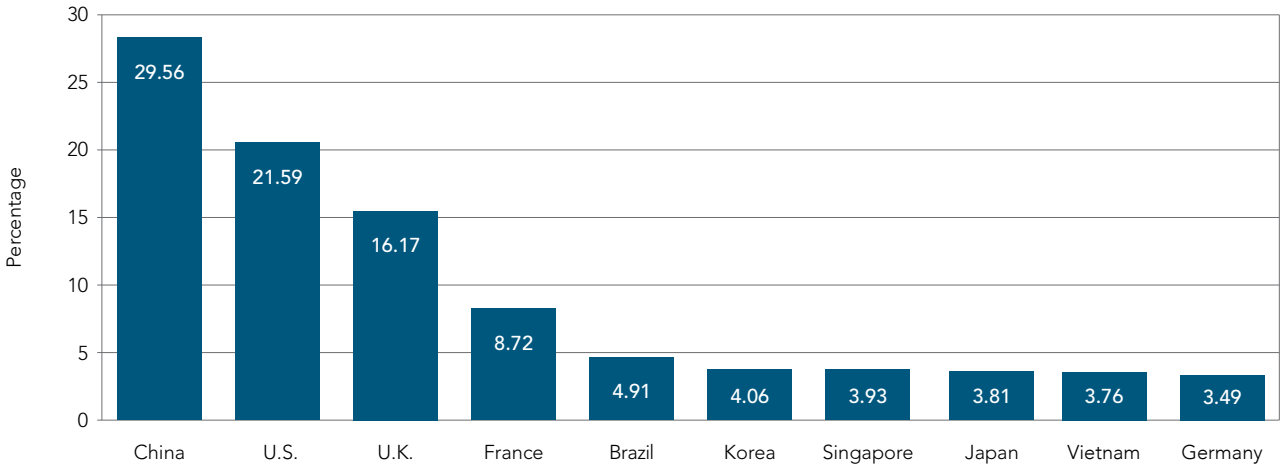


Figure 2-11: China, the U.S., and the U.K. were major sources of DDoS attack traffic

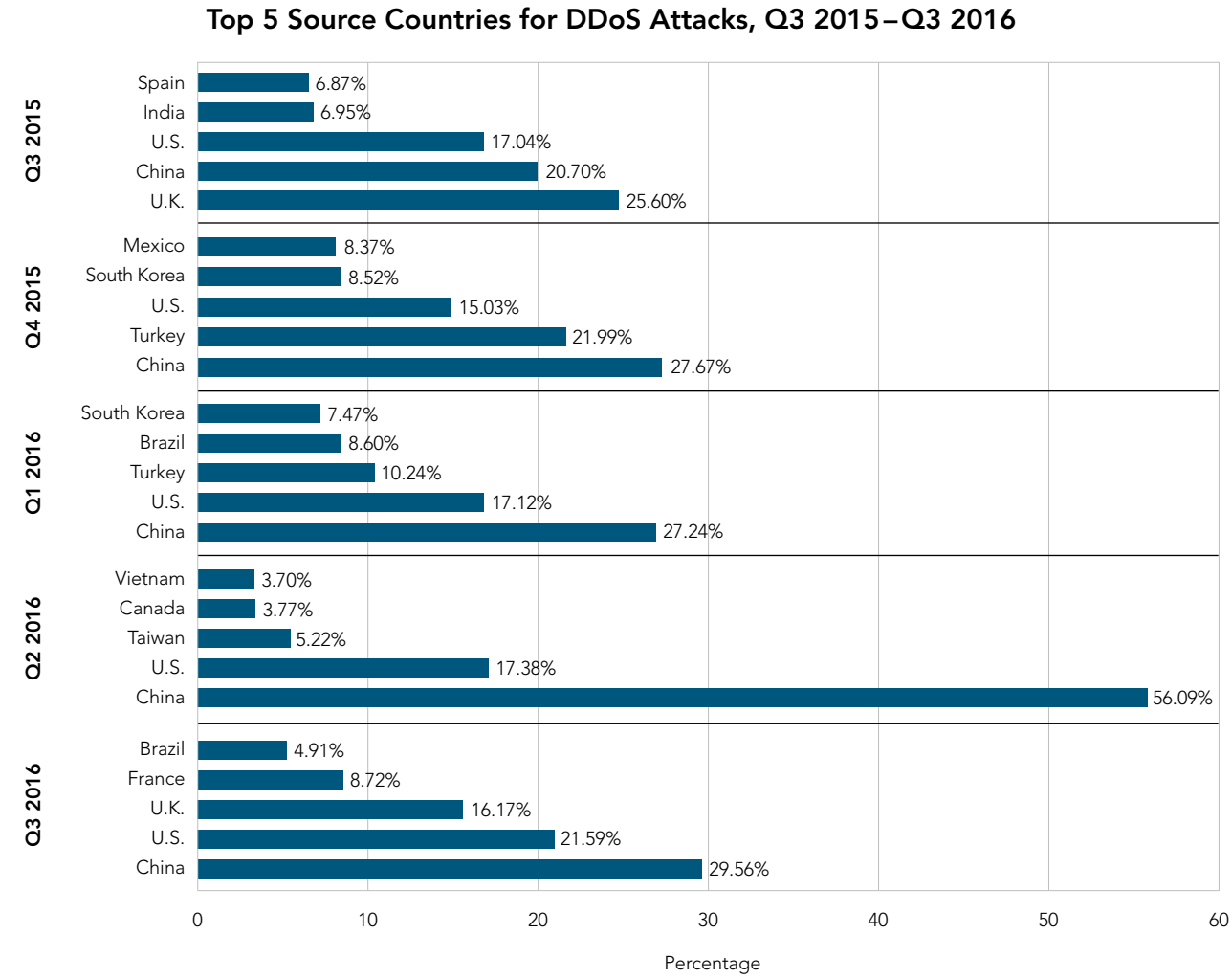


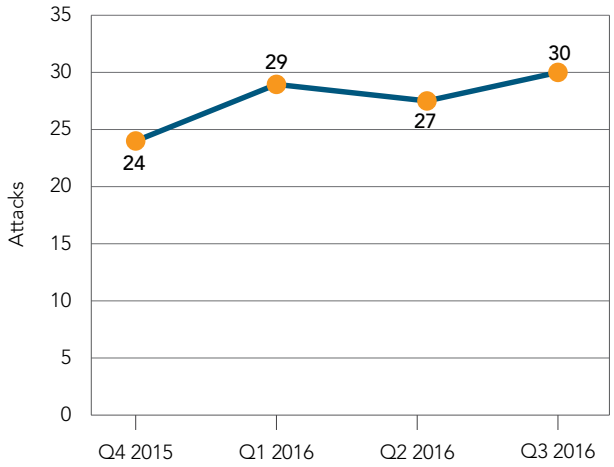
Figure 2-12: China has been the top source country for DDoS attacks since Q4 2015

2.6 / Repeat DDoS Attacks by Target / After a slight downturn in Q2 2016, the average number of DDoS attacks increased to an average of 30 attacks per target, as shown in Figure 2-13. This statistic reflects that once an organization has been attacked, there is a high probability of additional attacks.

Some clients are almost always under attack. The top target organizations saw three to five attacks every day of the quarter. These attacks were almost always of a short duration with limited bandwidth and consequence. However, without defenses in place, these attacks could have a substantial cumulative effect on an organization's' reputation. Several short outages each day would have serious detrimental effect on a customer's opinion of the business.

2.7 / Reflection DDoS Attacks, Q3 2015–Q3 2016 / Along with the drop in total attacks for Q3 2016 compared to Q2 2016, we also found a small drop in the total number of reflection-based attacks. Despite this drop, reflection-based attacks made up 51% of all DDoS attacks. Last quarter, although there were more attacks overall, reflection-based attacks were slightly under the 51% mark.

We see how these attacks are distributed from Q3 2015–Q3 2016 when looking at the following figure. This quarter saw the largest percentage of DNS reflection attacks, surpassing the previous high in Q1 2016. We have also been starting to see indications into Q4 that DNS reflection is being used to leverage multiple reflector domains per attack. In the past, attacks would stick to one DNSSEC-enabled domain; now, they combine these with multiple domains, some of which are obviously crafted maliciously for maximum amplification factors.



TOP TARGET ORGANIZATION ATTACK COUNT Q3 2016: **427**

Figure 2-13: In Q3 2016, an average of 30 attacks per target represents a slight increase in the high from Q1

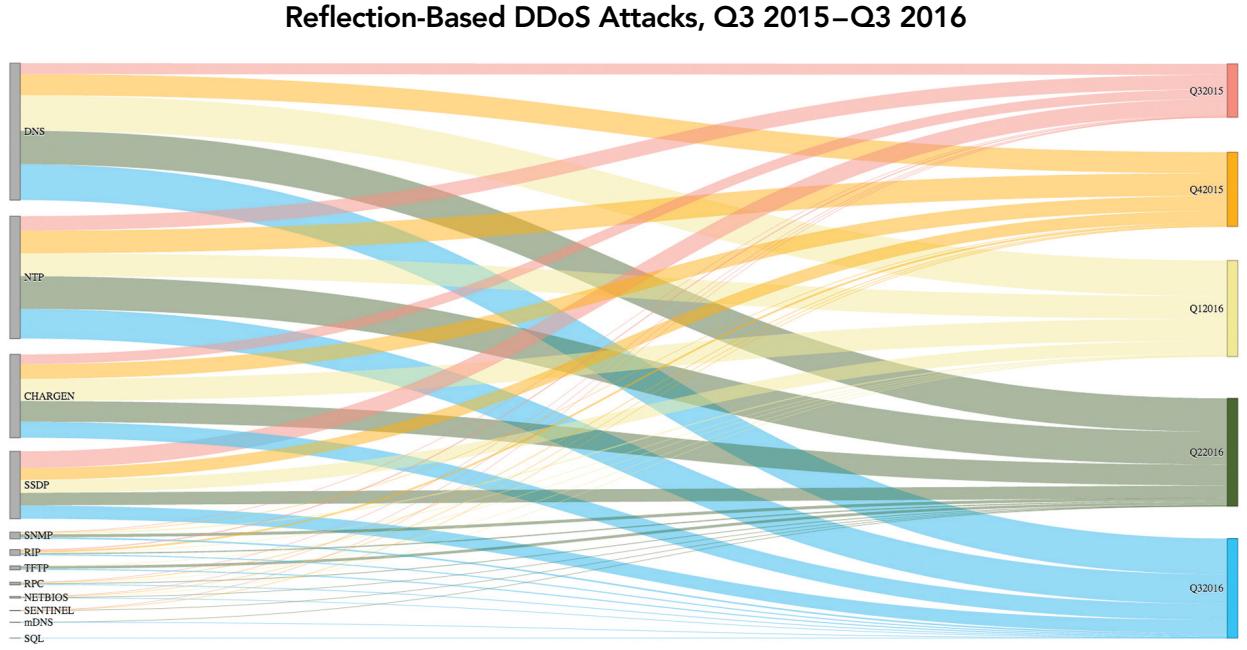


Figure 2-14: DNS attacks were the most common reflection-based attacks

2.8 / Perimeter Firewall DDoS Reflector Activity / Unlike other DDoS activity, which relies heavily on traffic captured on the routed network, DDoS reflector source graphs look at data captured on the Akamai Intelligent Platform. This increases the number of nodes collecting data from less than a dozen data centers to more than 2,000. The sensing nodes are usually no more than one or two hops away from the source reflector, which increases the accuracy of the data collected.

This data represents systems that actively participated in attacks using NTP, SSDP, CHARGEN, RPC, QOTD, TFTP, and Sentinel reflection vectors. This makes our data different from other reports that are based on scans of the Internet. A system that is capable of being used as a reflector would show up in a scan; however, unless it is actively being used in attacks, it wouldn't be included in our statistics. DNS reflectors are not included in this data, as a legitimate DNS request packet can often can be the same as the packets used in a reflection attack.

One thing that Figure 2-15 shows is that while several ASNs make up a significant amount of attack traffic, this is not an issue that is restricted to one network or region. The top 10 ASNs together make up less than 10% of the total reflector traffic. The other 90% was spread throughout the world, with no region entirely without reflectors. The top 5 reflectors have remained relatively steady over several quarters, with ASN 4837 (CNCGROUP China169 Backbone) taking the top spot from ASN 4134 (CHINANET BACKBONE No. 31) this quarter.

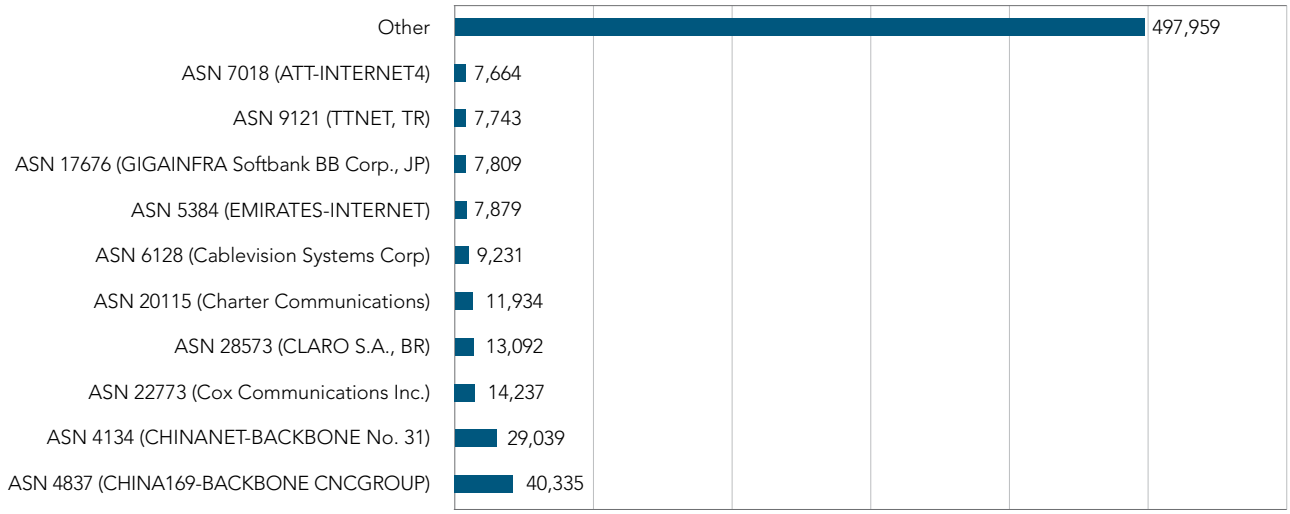


Figure 2-15: ASN 4837 (CHINA169-BACKBONE CNCGROUP) takes the top spot from ASN 4134 (CHINANET-BACKBONE No. 31)

Unique DDoS Reflectors by Vector, Q3 2016

Vector	Unique IPs
NTP	409,646
SSDP	120,800
CHARGEN	43,304
RPC	36,011
Sentinel	34,488
QOTD	27,556
TFTP	16,313

Figure 2-16: 688,118 unique DDoS reflectors were recorded for these seven vectors

Reflecting the overall drop of DDoS attacks in the third quarter, the unique count of IP addresses for each reflector has decreased since Q2 – except for RPC, as shown in Figure 2-18. Of the vectors observed, NTP continued to maintain the largest share, as highlighted in Figures 2-16 and 2-17, though it represented a drop of 50,000 unique IPs from the previous quarter. This supports the analysis in Section 2.2 that there are fewer usable NTP reflectors available to malicious actors.

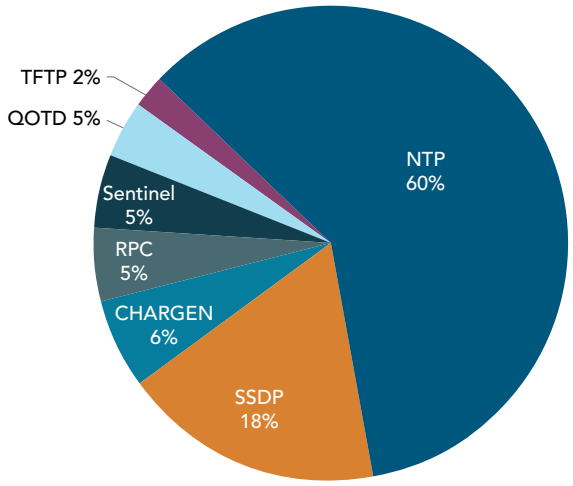


Figure 2-17: NTP was the top source of reflection attacks again (60%)

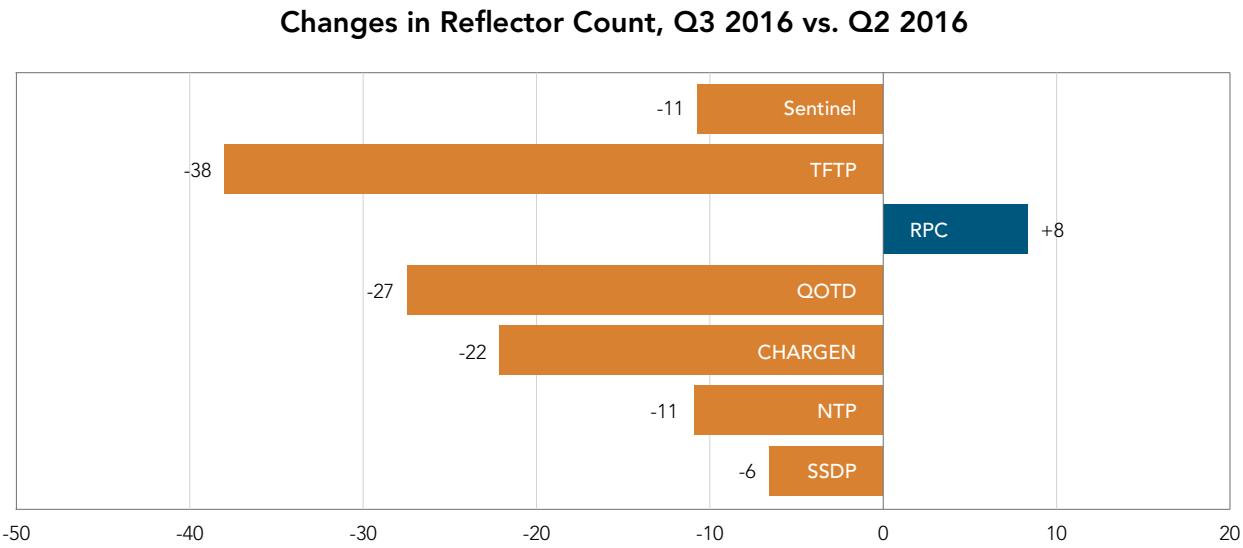


Figure 2-18: Akamai observed a decrease in all tracked reflection vector sources, except RPC

[SECTION]3 WEB APPLICATION ATTACK ACTIVITY

Akamai's Threat Research Team concentrated analysis on nine common web application attack vectors. This covers a cross-section of many of the most common categories on industry vulnerability lists. Akamai's goal is to review some of these common web app attack vectors and identify the characteristics of the attacks as they transit our global network.

Akamai's Threat Research Team filtered out traffic from third-party commercial web vulnerability scanning vendors, which are often used for compliance testing. This traffic does not constitute real attack data and artificially inflates raw numbers.

3.1 / Web Application Attack Vectors / Three vectors account for 95% of all web application attacks: SQL Injection (SQLi), Local File Inclusion (LFI), and Cross-site Scripting (XSS), as shown in Figure 3-1. In contrast, Remote File Inclusion (RFI), PHP Injection (PHPi), and Malicious File Upload (MFU) barely register as part of the background of attack noise. The cumulative category of Other accounts for more attacks than the 0.5% MFU represents.

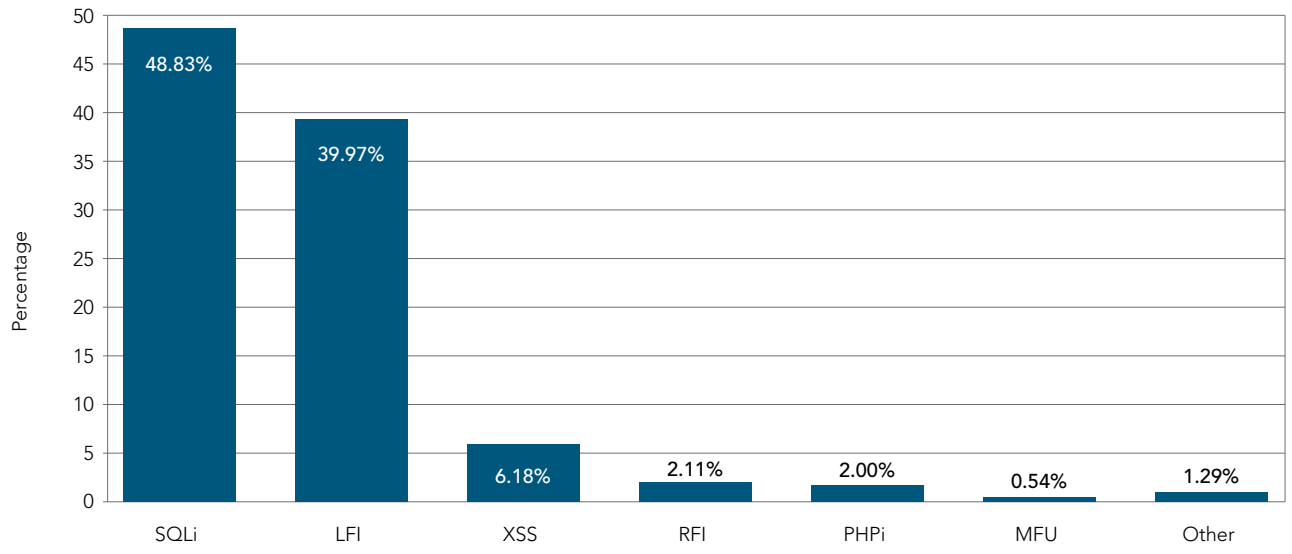


Figure 3-1: SQLi accounted for nearly 50% of observed web attacks

As of last quarter, Akamai stopped including Shellshock data as an attack vector. This was due to the fact that a majority of Shellshock alerts are caused by vulnerability scanning systems, not malicious actors. Akamai will be able to provide long-term trending of attack vectors when a year of comparative data has been accumulated.

The majority of web application attacks continued to take place over HTTP (68%) as opposed to HTTPS (32%), which could afford attackers some modicum of protection by encrypting traffic in transit. The majority of web applications still allow for the use of HTTP, rather than forcing users to switch to HTTPS. There is no impetus for attackers to use HTTPS, and many attack applications aren't configured to use HTTPS by default.

3.2 / Top 10 Source Countries / Despite a 13% drop in attacks from the U.S., it reclaimed the top spot as the source of attack traffic. Brazil, which had held the top spot last quarter, dropped to fourth behind the Netherlands and Russia. With 18% of all attacks, the Netherlands was a surprising second-place source.

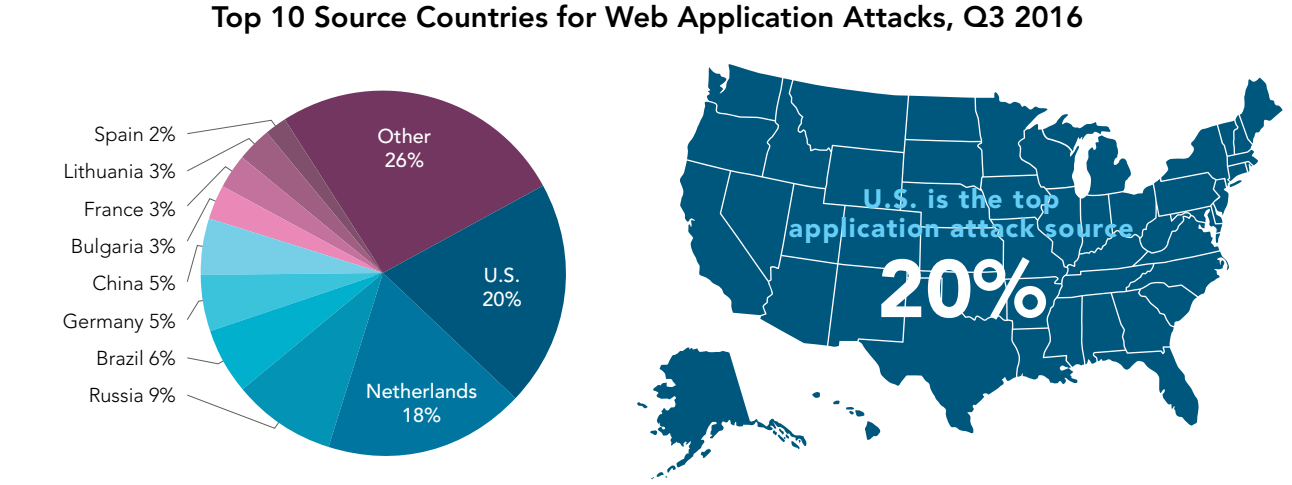


Figure 3-2: The volume of attacks originating in the U.S. dropped (13%) this quarter, but the country returns as the top source with a 20% share of attacks

We analyzed web application attacks that occurred after a TCP session was established. Due to the use of tools to obfuscate an attacker's actual location, the attacker may not have been located in the country detected in the log files. These countries were the sources of the IP addresses for the last hop observed and presented as such. The primary method used by attackers to obscure the source of their attack is via the use of proxy servers, rather than the direct packet-level source address manipulation commonly seen in UDP-based infrastructure attacks.

3.3 / Top 10 Target Countries / The U.S. remained the top target for web application attacks, and two-thirds of all attacks hit servers within its geographic boundaries, as shown in Figure 3-3. As many organizations are headquartered in the U.S., with the resultant infrastructure also hosted in-country, it is expected that the U.S. will continue to be the top target for some time. Attacks in Brazil fell significantly, accounting for only 5% of all traffic compared with 10% the quarter before. Germany re-entered the top 10 list this quarter. Despite being a top source of attack traffic, the Netherlands was not a major target for web application attacks this quarter.

3.4 / Attack Spotlight: European Football Cup Championship Game Impact on Web Application Attack Traffic / We decided this quarter to answer a question: do cyber attackers take time off to watch significant sporting events?

Football (known as soccer in the U.S.) is the most popular team sport in the world, with more than 250 million players and 1.3 billion people interested in the sport, according to a well known European football association. In 2010, a combined television audience of more than 3.2 billion watched the World Cup finals.

While automation and bot programs can carry out many attack tasks, web application attacks are mainly initiated and monitored by humans. Cyber criminals need to eat and sleep, and they have friends and family, take vacations, and enjoy weekends off. We theorized that they may be football fans, in which case they would most likely take a break from their attacking sessions to tune into the championship match when their country's team was playing.

To test this hypothesis, the Akamai Threat Research Team analyzed our WAF triggers and correlated the data with the European Football Cup Championship game that was played on Sunday, July 10, 2016. France and Portugal faced off in this game, so we extracted WAF triggers for that day where the source IP geolocation data was

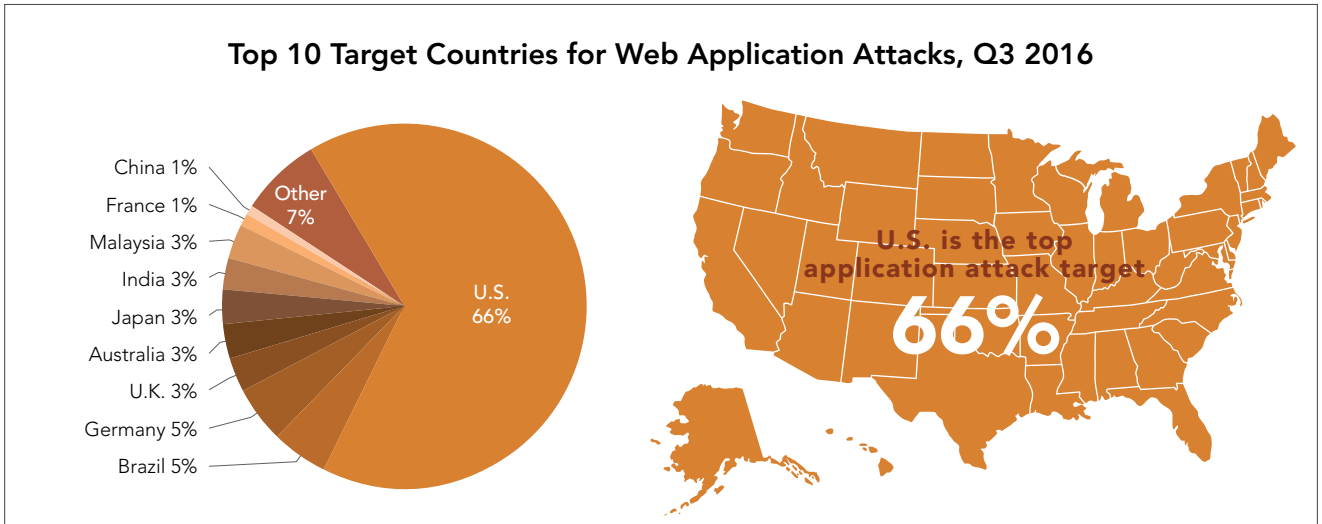


Figure 3-3: U.S.-hosted web sites were the target of 66% of all attacks

Web Application Attacks Sourced by Country During and After the European Football Cup Championship 2016

Country	# of Attacks Day of Championship	# of Attacks a Month Later	% Decrease in Attack Traffic
France	50,597	158,003	68%
Portugal	20	392	95%

Figure 3-4: Web application attacks from France and Portugal were much lower during the European Football Cup Championship than a month later

France or Portugal. We then compared the data with attacks coming from the same geolocations a month later. The results are shown in Figure 3-4.

While the overall raw numbers were not particularly high, the percentage decrease in attack volume during the championship game is significant. It appears that cyber criminals in France and Portugal took some time off to cheer for their teams during the Euro Championship match. Cyber criminals are people, too. When organizations attempt attacker profiling or security event analysis, they should also factor geo-political, social, and current events into their model. This is why most secure operations centers (SOCs) have 24/7 news channels showing on large TV screens. Staff need to keep abreast of breaking news events that could signal an increase in attack traffic.

3.5 / Summer Games / Similarly, the 2016 Summer Games had the greatest volume of online views of any event, consuming the largest amount of content across the widest variety of devices.

NBC Summer Games coverage leveraged Akamai for online video streaming, website and video delivery, and security to support its record digital offering for Rio 2016, which included 3.3 billion total streaming minutes, 2.71 billion of which were live. One hundred million unique users tuned in to NBC Summer Games' digital coverage.

We analyzed our Kona Web Application Firewall data for attacks during the Summer Games in Rio from August 5 to August 21. During the same 17-day period a month earlier, there had been 7.3 million attacks sourced from Brazil, putting the country among the top four sources of web application attacks. But during the Summer Games, web application attacks from Brazil dropped to only 1 million attacks. As with other football championship games, it appears even malicious actors take time off to watch major sporting events.

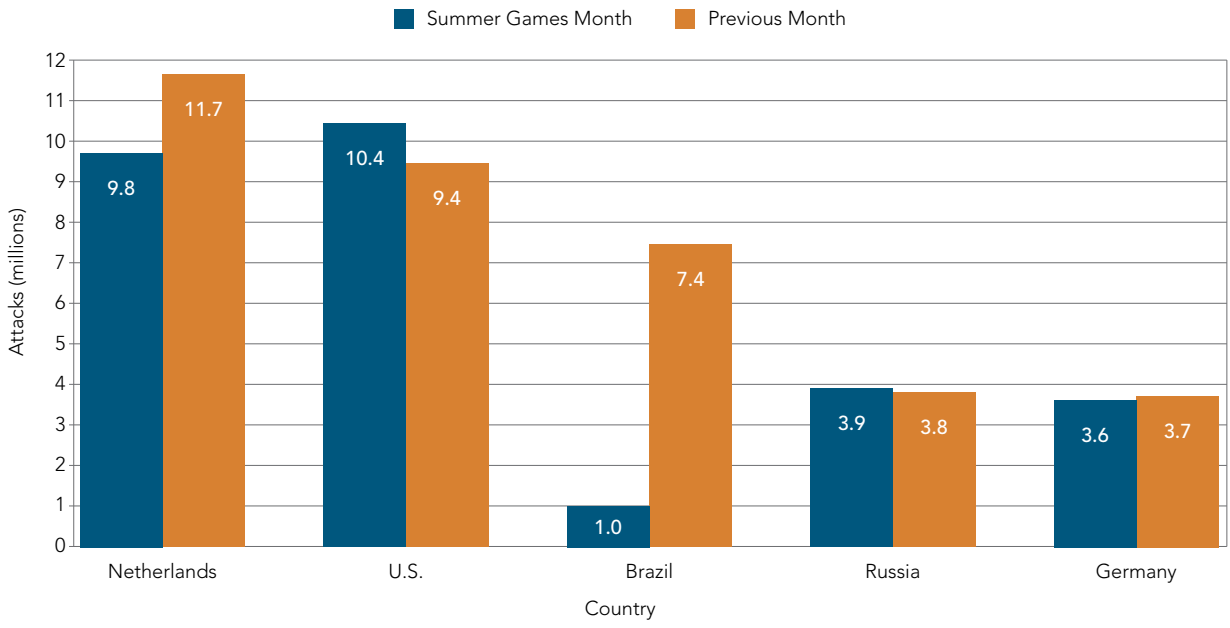


Figure 3-5: Web application attacks from Brazil were much lower during the Summer Games than a month earlier

[SECTION]4
LOOKING FORWARD

Is your refrigerator running? If so, it might be part of a botnet! We used to make fun of the idea of Internet-enabled household appliances, but manufacturers have taken the idea to heart. It seems anything that could possibly be connected soon will be, from refrigerators to lightbulbs to speakers.

Problems arise from the fact that those same manufacturers aren't taking security to heart. Connecting a device to the Internet to stream data is relatively easy. Building software that can be updated, an infrastructure that supports the update, and keeping ahead of the vulnerabilities of consumer-grade electronics isn't easy — or cheap. As a result, we see IoT devices sold without the capability to be patched or managed, a fundamental vulnerability that attackers have identified and seized upon.

The current round of IoT-based botnets rely on devices like DVRs, IP cameras, and other devices with relatively robust general-purpose computers at their core. The continuum of devices scales in both

directions from there. IoT lightbulbs might not have much computing power, but they're being sold and installed by the millions. TVs already have significant computing power dedicated to voice recognition. An IoT refrigerator probably has a full-fledged web server in it, used to display information on its screen and stream a shopping list to the app on your phone.

The 623 Gbps attack experienced this quarter quite possibly marks a new chapter in DDoS. Once the impossible happens, others strive even harder to recreate the event. It is very likely that malicious actors are now working diligently to understand how they can capture their own huge botnet of IoT devices to create the next *largest DDoS ever*.

As a counterpoint to the increasing threat of IoT botnets, we see the threat of NTP reflection fading, a trend that should continue as vulnerable systems get patched or go offline. This is not a counterbalance to the IoT threat but is instead part of the ebb and flow of overall attack traffic. As one threat starts to recede, our adversaries, who are intelligent attackers, find new and interesting avenues to exploit.

Luckily, defenders are also intelligent, and the tools we use are evolving as well.

[SECTION]5 CLOUD SECURITY RESOURCES

5.1 / Bot Traffic Analysis: Managing Professional Bots / Akamai recently published a white paper about how users can manage professional bots—specifically aggressive bot behavior, the methods they use, and how to mitigate them. These bots ruthlessly scrape site content and often create DDoS-like conditions through excessive traffic, spoofing legitimate good bot user-agent strings to bypass WAFs and even attempting to compromise the host in order to infest victims with malware.

What industries are most commonly the targets of these bots? Travel and hospitality-related sites see a high level of bot traffic due to scraper and account checker bots targeting low airfare and travel costs.

Data collection isn't the only reason why bots are created and used. Many of them are also developed as blunt-force digital weapons, built to cripple their victim's websites and businesses. The white paper illustrates this through an example that shows an attack utilizing

a botnet to conduct a DDoS attack on a large gaming and entertainment company website and leveraging close to 4,000 unique IP addresses.

Another incident shows how bots can influence virtually anything — including votes. The white paper describes an attack where a European Union referendum voting website was deluged with automated votes using fake signatures as a prank from the users of 4chan. The attackers created scripts and used botnets to automate vote submissions to the website, with IP addresses originating from places like North Korea, Antarctica, and Vatican City. As elections and voting mechanisms start to move online, bot attacks need to be considered and taken seriously.

You can read the full paper to learn about the most common types of botnets and a detailed analysis of one professional bot, 8olegs: ***https://www.akamai.com/us/en/multimedia/documents/white-paper/akamai-scrapers-and-bot-series-managing-professional-bots-white-paper.pdf***

5.2 / Kaiten / Akamai SIRT has been investigating a malware variant of Kaiten/STD specifically designed to target networking devices used in Small Offices & Home Offices (SOHO) as well as DVRs, IP cameras, and other IoT devices. This malware includes an extensive list of available attack vectors along with the ability to execute arbitrary commands and take full control over the infected system. The malware is packed with a custom packer/encoder to hinder analysis. It's compiled for multiple architectures (MIPS, ARM, PowerPC, x86, x86_64) and uses a custom IRC-like communication protocol for C2 communications.

The malware uses a predefined list of C2 IPs and a custom IRC protocol to connect and communicate with them. Once a connection is established to one of the C2 IPs, the infected host then authenticates with a dynamic password generated by the server and joins a private channel where it begins listening for commands. The backdoor functionality of the malware allows the attacker to execute arbitrary commands on the infected machine.

For a detailed analysis, read Akamai's recent Threat Advisory (***https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/kaiten-std-router-ddos-malware-threat-advisory.pdf***)

5.3 / SSHowDowN / Researchers at Akamai have been monitoring the growth of attacks leveraging IoT devices. These attacks are coming from compromised devices of various sorts. With other, non-IoT types of devices (including general purpose computers), owners can patch or reconfigure their systems to close vulnerabilities.

IoT device owners are often at the mercy of vendor updates in order to remove their devices from the pool of botnet nodes. In some cases, IoT devices are entirely unpatchable and will remain vulnerable until removed from service.

With some attacks, malicious actors install attack software on IoT devices and use them to perpetrate attacks directly. In the case of the SSHowDowN Proxy attacks, they are using the IoT devices to proxy attack traffic generated remotely by using a 12-year-old vulnerability in OpenSSH. Although the IoT devices we've seen attacking do take some steps to block abuse of the SSH servers in those devices, they have not taken steps to defend against ***CVE-2004-1653***. They *have* blocked simple login by setting the administrative user shell to `/usr/sbin/nologin` or `/bin/false/`. ***That is a useful, but incomplete control.***

For a detailed analysis of these attacks, read Akamai's recent Threat Advisory (***https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/sshowdown-exploitation-of-iot-devices-for-launching-mass-scale-attack-campaigns.pdf***) on the SSHowDowN Proxy Attacks.

We are only human, and here we identify the errors and omissions from the *Q2 2016 State of the Internet / Security Report*. If you notice a data point, chart, or explanation you believe to be in error, please notify the Akamai team at ***SOTISecurity@akamai.com***.

FIGURE 2-9, PAGE 19 / The figure has an associated box explaining how the chart is read. The text reads, "The height of the box in each quarter is also an indicator of the number of attacks." The text should read, "The **width** of the box in each quarter is also an indicator of the number of attacks."

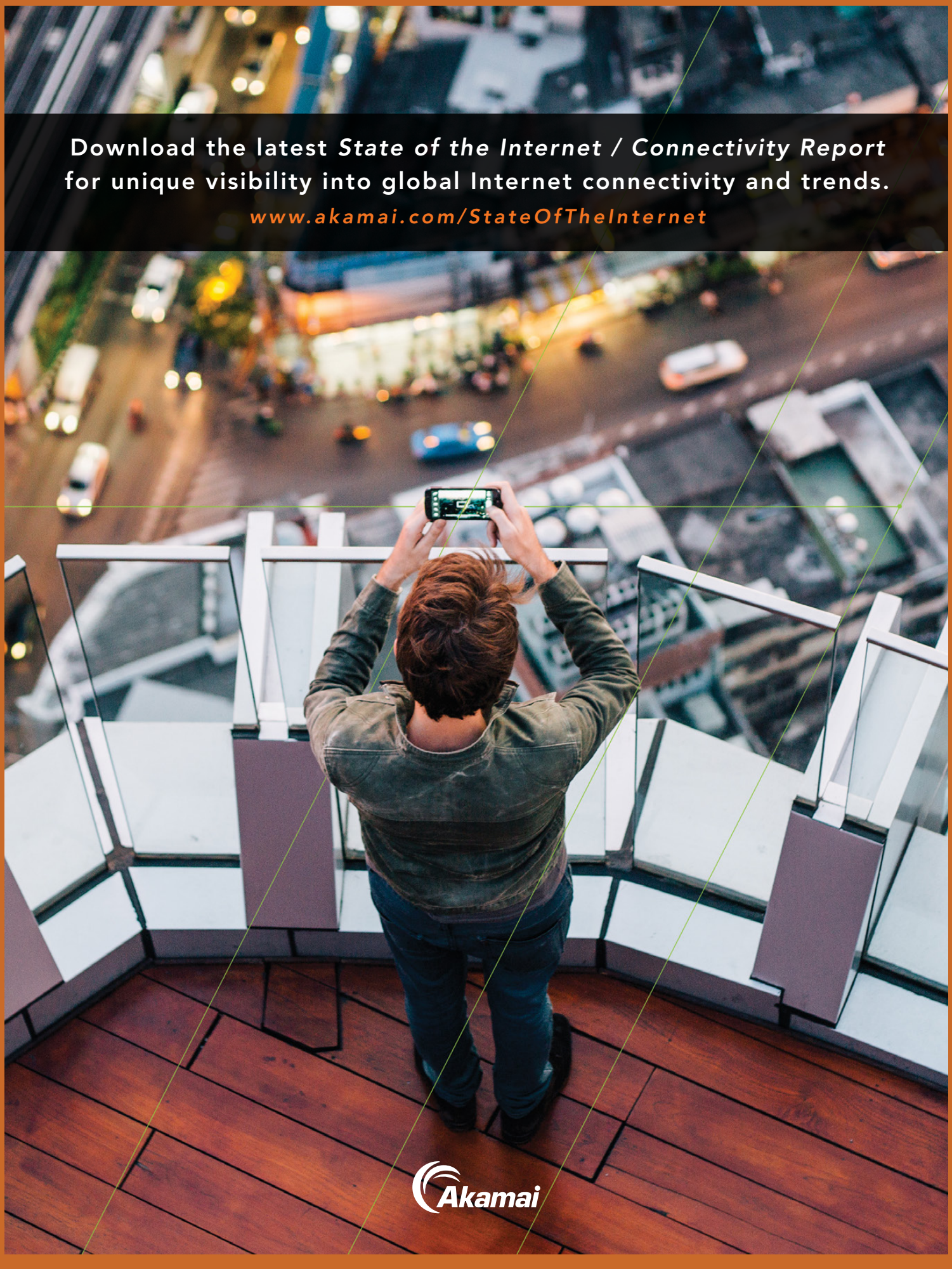
SECTION 3.5, PAGE 32 / The first paragraph states that Akamai "...provides a snapshot of 2 trillion bot requests observed in one 24-hour period." This text should read, "...provides a snapshot of 2 **billion** bot requests observed in one 24-hour period."

FIGURE 3-9, PAGE 35 / The table, "Ratio of IPs and Attacks by Proxy Type" was not updated properly. The numbers of IPs were correct, but the calculated percentages had been created from earlier counts. The table should read as follows:

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	644,278	84%	143,928,747	76%
Proxy/VPN	124,442	16%	45,438,631	24%

Figure 3-9 (corrected figure 3-9 from the *Q2 2016 State of the Internet / Security Report*): Nearly a third of web application attacks during the study period relied on anonymizing services


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

***State of the Internet / Security* Team**
Martin McKeay, Senior Security Advocate, Senior Editor
Jose Arteaga, Akamai SIRT
Amanda Fakhreddine, Editor
Dave Lewis, Security Advocate
Larry Cashdollar, Akamai SIRT
Chad Seaman, Akamai SIRT
Jon Thompson, Custom Analytics
Ryan Barnett, Threat Research Unit
Ezra Caltum, 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