[Volume 3 / Number 4]

akamai's [state of the internet] / security

Q4 2016 report

AT A GLANCE

DDoS attacks, Q4 2016 vs. Q4 2015
4% increase in total DDoS attacks
6% increase in infrastructure layer (layers 3 & 4) attacks
22% increase in reflection-based attacks
140% increase in attacks greater than 100 Gbps: 12 vs. 5

DDoS attacks, Q4 2016 vs. Q3 2016
16% decrease in total DDoS attacks
16% decrease in infrastructure layer (layers 3 & 4) attacks
9% decrease in reflection-based attacks
37% decrease in attacks greater than 100 Gbps: 12 vs. 19

Web application attacks, Q4 2016 vs. Q4 2015
19% decrease in total web application attacks
53% decrease in attacks sourcing from the U.S. (current top source country)
44% increase in SQLi attacks

Web application attacks, Q4 2016 vs. Q3 2016
27% increase in total web application attacks
72% increase in attacks sourcing from the U.S. (still top source country)
33% increase in SQLi attacks.
**Note: percentages are rounded to the nearest whole number.*

What you need to know

- Akamai mitigated 3,826 distributed denial of service (DDoS) attack events on Akamai's Prolexic network, a 4% increase in attacks since Q4 2015.
- The largest attack this quarter, measured at 517 Gbps, came from a non-IoT botnet and is covered in this quarter's Attack Spotlight.
- Research into retail traffic over the U.S. Thanksgiving holiday week revealed four sub-verticals that all suffered from significant attacks timed for the holidays.

LETTER FROM THE EDITOR / The Q4 2016 *State of the Internet / Security Report* represents analysis and research based on data from Akamai's global infrastructure and routed DDoS solution.

The fourth quarter of 2016 was relatively quiet for web application attacks. The biggest sales season of the year usually signals a marked increase in the number of attacks for all customers — especially retailers. Many merchants breathed a sigh of relief at not being attacked during their most important shopping days.

That's not to say everyone got off without some stress. The days surrounding Thanksgiving traditionally mark the start of the holiday shopping season in the U.S. In our Spotlight on Thanksgiving Attacks, we describe an overall daily attack trend and how four retail sub-verticals were each hit by different types of attacks.

The Mirai botnet continued as one of the largest threats in the fourth quarter, but it is not the only Internet of Things (IoT)-based botnet. At least two other major IoT-based botnets are in use. They may be variants of Mirai or new, unrelated botnets. In any case, IoT continues to provide resources to fuel future DDoS attacks. In an analysis of scanning on ports 23 and 2323, we explain our conclusion that, although some timelines place the development of Mirai in early July 2016, our data indicates earlier efforts — as early as May 13th.

Akamai's research teams published three new papers in the fourth quarter. The first is an analysis of the Mirai botnet, digging into the capabilities the botnet possesses. Multicast Domain Name System (mDNS) is an important part of DNS services, but last year it started to be used as another source of reflection traffic as discussed in the second piece. Our third paper is an analysis of some of the trends that are being observed by our researchers regarding the portion of the Internet that isn't indexed by search engines, aka, the Dark Web.

The contributors to the *State of the Internet / Security Report* include security professionals from across Akamai, including the Security Intelligence Response Team (SIRT), the Threat Research Unit, Information Security, and the Custom Analytics group.

— Martin McKeay, Senior Editor and Akamai Sr. 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

Insecure IoT devices continued to be a big source of traffic for DDoS attacks in the fourth quarter. We believe 7 of the 12 mega attacks this quarter, those with traffic greater than 100 Gbps, can be directly attributed to Mirai. At least 37 of the attacks this quarter came from Mirai, though the average peak bandwidth of the attacks was only 57 Gbps. The rapid proliferation of these devices will provide an expanding pool of attack resources, fueled by the discovery of new vulnerabilities and vulnerable systems. The number of devices that fueled the Mirai attacks in Q3 was a small subset of all IoT devices on the Internet, primarily IP-enabled cameras and DVRs. As vulnerable devices are added to IoT-based botnets, we expect a second surge in botnet capabilities and DDoS attack size.

There is a counter-balance to this trend however. Our examination of the use of NTP reflection as an attack amplifier last quarter suggests that new attack types peak shortly after they appear. But as these attacks gain in popularity, competition for the resources needed to make them begins. While the number of attacks goes up, the size of

individual attacks is pushed down, as there are fewer resources available for each of the botnets. Reaching a point of equilibrium between resources and contention for them took over a year for NTP reflection attacks and is likely to take longer for IoT-based botnets because new pools of vulnerable devices are certain to add to the capabilities of botnets.

The rapid proliferation of IoT devices, primarily in the home environment, adds a second layer of problems for network defenders. The creation of new features to distinguish one's products in the market is always a driving factor for manufacturers. One recent example is LG at the Consumer Electronics Show (CES) in Las Vegas, where not only was an Internet refrigerator announced, but LG stated that every device it sells in the near future will have Internet-connected capabilities. Regardless of LG's success at securing these devices, they are establishing a new standard feature set, which low-end competitors will move to emulate. There are far too many organizations that consider security to be at the bottom of their list of priorities, if they consider it at all. Does every home need a refrigerator that not only takes pictures of its own contents, but also has a built in web browser on the front? The market seems to think they do, but the security implications are troublesome.

The Federal Trade Commission (FTC) has taken consumer wireless router manufacturer D-Link to court in California for putting consumers at risk by creating flawed and insecure software for their systems.[1] D-Link is not the first manufacturer that the FTC has targeted for creating insecure software,[2] and these efforts should be treated as a warning for other manufacturers to secure their systems.

DDoS attacks greater than 300 Gbps have become more common. Seven DDoS attacks greater than 300+ Gbps occurred in 2016, including three in the fourth quarter. While there were plenty of IoT-fueled DDoS attacks in the fourth quarter, none of the fourth quarter's attacks over 300 Gbps were IoT-based. The Attack Spotlight looks at the botnet that generated the top 3 largest DDoS attacks and delves more deeply into the largest attack this quarter, a 517 Gbps attack with signatures from the Spike DDoS toolkit. IoT based botnets like Mirai still attributed with a significant number of large attacks with 7 out of the 12 mega attacks sourcing from a Mirai botnet. In 37 attacks confirmed from Mirai, the average peak bandwidth was around 57 Gbps.

With the holiday season behind us, we also examined web application attacks on retailers in the U.S. during the week of Thanksgiving. As a whole, the number of web application attacks in Q4 was down; however, for four retail sub-verticals, the trend was upward. Although the targets were all in the retail vertical, the attacks were quite different, ranging from cyclic attacks against closely related targets, to a single huge burst of probes against a host of sites that were only related by the software they used.

[SECTION]^2
DDoS ACTIVITY

2.1 / DDoS Attack Vectors / As shown in Figure 2-1, of the 25 DDoS attack vectors tracked this quarter, the top three were UDP fragment (27%), DNS (21%), and NTP (15%), while overall DDoS attacks decreased by 16%.

Because of the Mirai botnet, the number of IP addresses that are known to be valid participants in attacks rose sharply, simply because Mirai makes little effort to hide its sources. The Mirai botnet continued to make troubling changes to the status quo. These attacks, while significant in volume, weren't the larger story. That came with the public release of the Mirai source code, which led to a series of copycat botnets. These IoT attack platforms are concerning as they are leveraging rather simple security missteps on the part of IoT vendors. An example of this is that Mirai relies on compromised IoT devices via telnet using default password credentials.

Default password credentials are something that can be sorted out from a programmatic standpoint. IoT devices should ship pre-configured with per-device random passwords or they should require owners to change the password on the initial login. Seems simple — yet thousands of devices were compromised and added to Mirai-based attack platforms.

Akamai added a new reflection DDoS attack vector this quarter, Connectionless Lightweight Directory Access Protocol (CLDAP). Attackers abuse the CLDAP to amplify DDoS traffic. CLDAP is provided on Windows networks to access authentication information for network logons. This method of reflection works much the same way as many of the other UDP-based reflection vectors discovered thus far.

Attackers send a spoofed LDAP query for all records from root. The response, containing all the requested records, is returned to the target of the attack. Within the next few months, Akamai SIRT plans to release an advisory with further details around the types of servers being abused and the amplification factor of this threat.

In the previous quarter, the Generic Routing Encapsulation (GRE) Protocol (a system used to share peer-to-peer data) attacks were added to our attack vector list, due to their use in attacks from the Mirai botnet. The GRE Protocol normally doesn't generate much DDoS traffic; however, in Q3, 0.02% of total attacks used GRE, while its share increased to 0.29% in Q4.

The data used to create the DDoS section is drawn from the Prolexic Network and reflects a portion of the data Akamai gathers, primarily volumetric attacks. Data from Akamai's Intelligent Platform and Cloud Security Intelligence are analyzed in ***Section 3: Web Application Attacks***.

This is the third consecutive quarter where we noticed a decrease in the number of attack triggers. Even with these quarterly decreases, the overall 2016 attack count was up 4% as compared to 2015. As we reviewed the data, we found that attacks pertaining to ACK, CHARGEN, and DNS remained in the top three by volume.

NTP-related attacks also dropped from the previous quarter. Unlike IoT resources, which are growing, NTP resources for DDoS attacks are shrinking as servers are patched and older servers are taken out of service. It is important to note that this is a solvable problem. Attackers like to leverage NTP to amplify their attack traffic; this function would not be available to them if the NTP daemons were patched to current. Victim networks become the unwitting participants in DDoS attacks as a result of poor infrastructure hygiene.

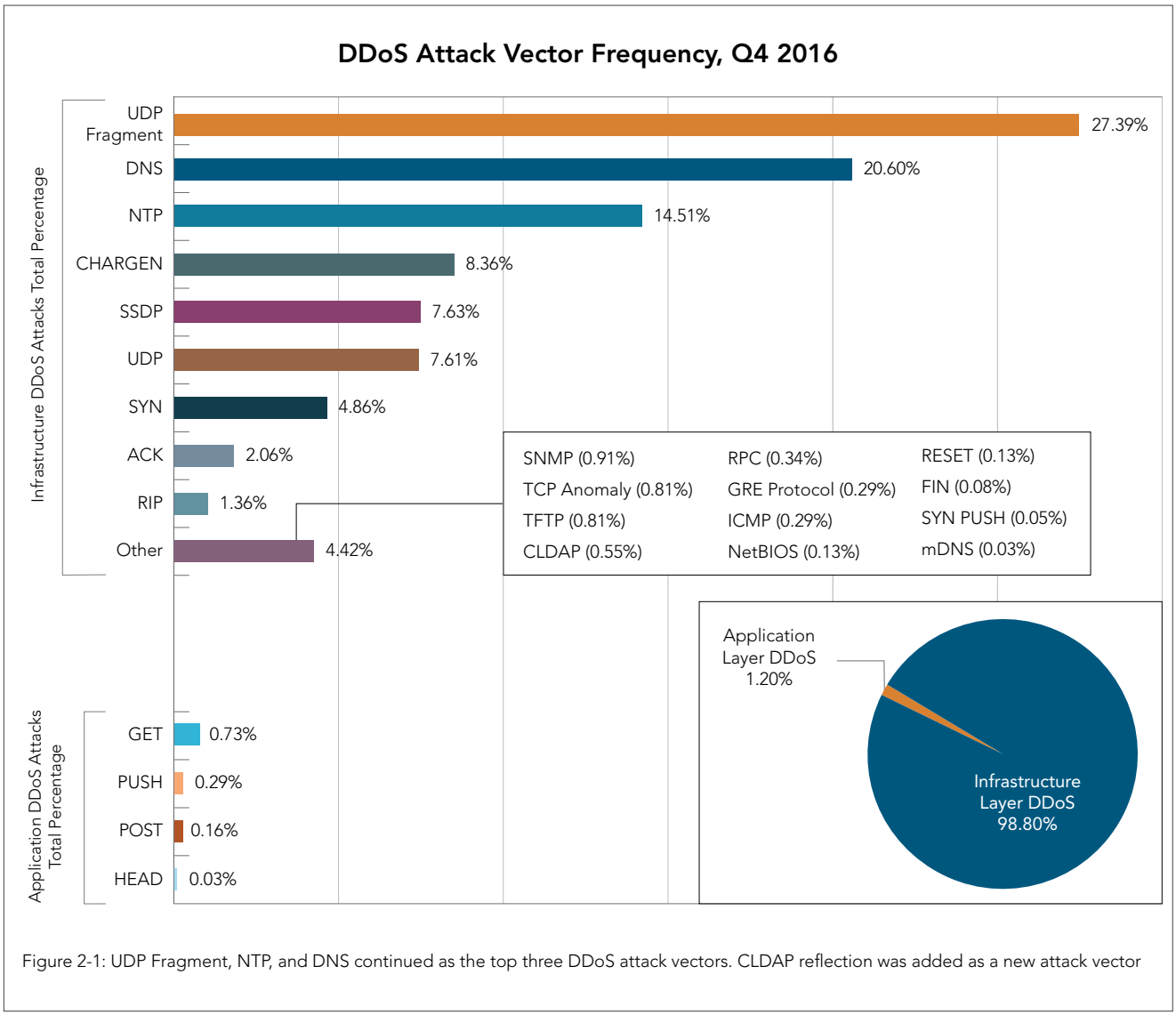


Figure 2-1: UDP Fragment, NTP, and DNS continued as the top three DDoS attack vectors. CLDAP reflection was added as a new attack vector

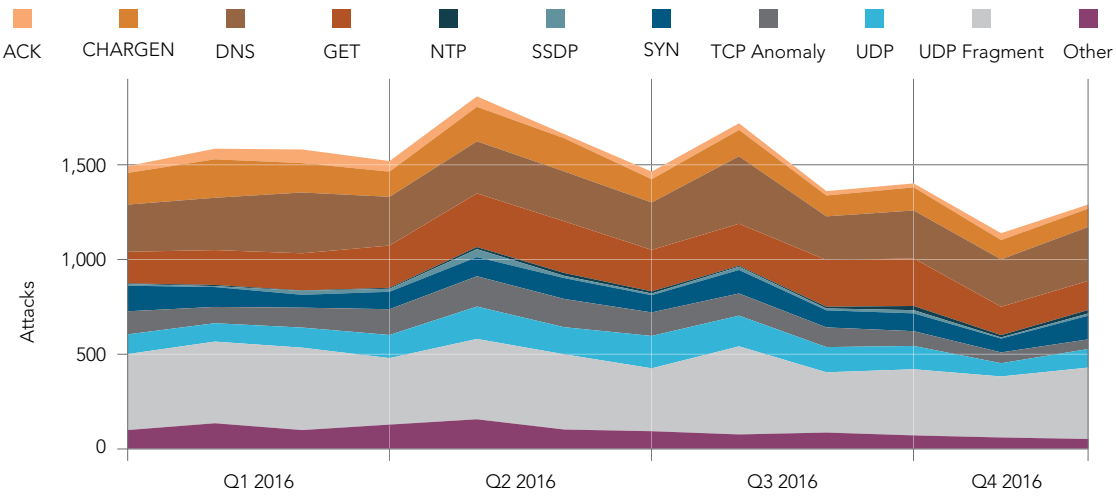


Figure 2-2: May 2016 marked the peak in infrastructure layer DDoS activity, followed by an overall downward trend in attack frequency

2.2 / Mega Attacks / As shown in Figure 2-3, 12 DDoS attacks exceeded 100 Gbps in the fourth quarter, down from 19 in the previous quarter. Five of these DDoS attacks exceeded 200 Gbps, and three achieved 300 Gbps or higher. Of the 12 mega-attacks, seven were driven by the Mirai botnet.

Mirai continued to drive large attacks and, with the source code publicly available, various actors have adopted and customized the code for their own purposes. There were at least 37 attacks sourced from Mirai this quarter, averaging 57 Gbps, showing that this botnet is nowhere close to going away. However, the largest attack this quarter did not come from Mirai, but the Spike botnet.

Figure 2-3 also shows that of these 12 mega attacks, Software & Technology organizations were targeted by two mega attacks, and gaming organizations were targeted by five mega attacks. Media & Entertainment organizations were also targeted by five mega attacks, three of which reached or exceeded 300 Gbps.

2.3 / DDoS Attack Spotlight: The Return of Spike / In the third quarter, Akamai mitigated an attack that was measured at 623 Gbps and was powered by IoT devices controlled by Mirai. Although attacks by Mirai botnets, and related botnets of IoT devices are big news, this quarter's largest attack of 517 Gbps came from a botnet with a different source — a type of malware more commonly associated with x86 Linux-based malware, such as XOR and BillGates.

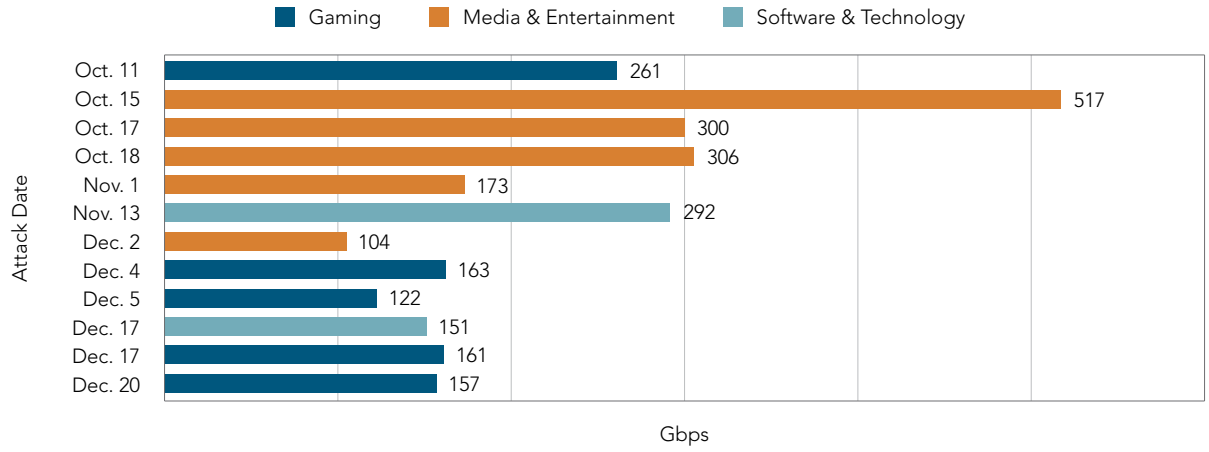


Figure 2-3: Twelve DDoS attacks exceeded 100 Gbps in Q4 2016, five exceeded 200 Gbps

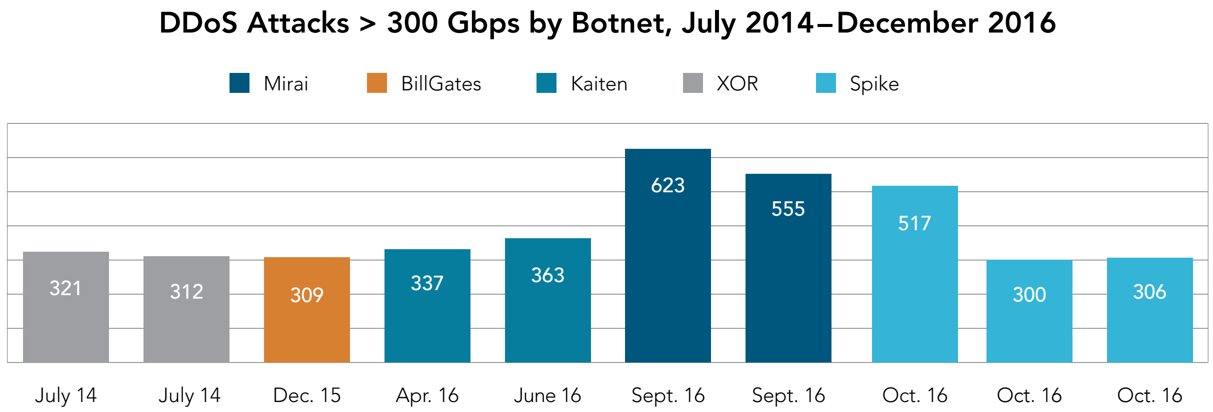


Figure 2-4: Four botnets generated 10 DDoS attacks exceeding 300 Gbps between July 2014–December 2016. Seven of these occurred in 2016

DDoS attacks greater than 300 Gbps are an expected, but relatively new, phenomenon. Figure 2-4 shows the 10 largest attacks mitigated by Akamai, along with the botnets that matched their attack signatures. Starting with the first, XOR was used to generate two 300+ Gbps attacks in mid-2014, followed more than a full year later by an attack using BillGates in December 2015. Seven of the 10 attacks greater than 300 Gbps occurred in 2016: two attacks with Kaiten, the predecessor to Mirai, in the first half the year; two with Mirai in September, and three with Spike in Q4. Half of the largest attacks occurred in the past four months alone.

Size / When the Akamai SIRT released an advisory on Spike in September 2014, the peak attack was measured at 215 Gbps. Two years later, in Q4 2016, Akamai mitigated a 517 Gbps attack generated from the same malware.

Signatures / The signatures from the Q4 attack are shown in Figure 2-5, along with lab-generated signatures from the original advisory.

The attackers also included a layer 7 GET flood. During the flood, attacking hosts will also send a stream of data filled with white space and a message customized by the botnet owner.

The GET flood signature in the Q4 attack did not match the original Spike GET flood signatures. Research into Spike signatures revealed that a Windows DDoS malware variant was built to send payloads as early as 2015. Based on messages observed in the packets, the name of the sender varies. In the signature in Figure 2-6, the attacker used the name "GameOver". The original Spike toolkit included a builder to create malware for 32 and 64–bit Linux, Windows, and ARM systems. Functionality may have been added to enable payload customization. Spike is still primarily a Windows/Linux botnet, but the inclusion of ARM code means it could evolve to take advantage of IoT devices. There are some indicators this evolution is already taking place.

CONCLUSION / Old malware still works. A customizable toolkit like Spike makes it easy for a malicious actor to build a new botnet. This attack demonstrates that an attacker can modify old malware, build a botnet, and generate one of the largest DDoS attacks to date.

```
SYN Flood (October 2016 Attack)
04:15:40.399817 IP x.x.x.x.43439 > x.x.x.x.80: Flags [S], seq 2846831616:2846832600, win 512, length
984: HTTP....E..........p6..[.......P..4.....P...>H.................P..4.....P..........P..............
........................?...?.......?.....................x.x.x.x.......................................
...........................................................................P...........<...............
..................................................................................=...?.?...4...p.?.p.?
.p.?...?.................................

SYN Flood (Lab 2014)
19:59:44.713925 IP x.x.x.x.5685 > x.x.x.x.80: Flags [S], seq
372572160:372573184, win 512, length 1024
E..(.5.........D...P.5.P.5......P....<..x.x.x.x...............................
....................................................................................
192.168.20.1......................{..._.@...@...@...$...............................
.............................................................

UDP Flood (October 2016 Attack)
02:37:32.732700 IP x.x.x.x.35917 > x.x.x.x.80: UDP, length 626
....E...'|@.8....C<......M.P.zO.XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

UDP Flood (Lab 2014):
20:03:06.480378 IP x.x.x.x.56180 > x.x.x.x.80: UDP, length 1024
E....”@.@......>...P.t.P....XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

Figure 2-5: SYN and UDP flood signatures from the Q4 attack and earlier lab-generated signatures for Spike. Payload data is truncated for brevity

```
GET Flood
00:44:55.272552 IP x.x.x.x.3690 > x.x.x.x.80: Flags [P.], seq 1724818487:1724818723, ack 2520919526, win 65535, length
236: HTTP: GET / HTTP/1.1
....E.....@.u...y.b......j.Pf..7.B-.P...1...GET / HTTP/1.1
Accept: */*
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.4; en-US; rv:1.9b5) Gecko/2008032619 Firefox/3.0b5
Pragma: no-cache
Accept-Encoding: gzip, deflate
Host: x.x.x.x
Connection: Keep-Alive

During the flood, attacking hosts will also send a stream of data filled with white space and a message
00:44:55.297357 IP x.x.x.x.3691 > x.x.x.x.80: Flags [P.], seq 15858017:15858553, ack 1500379993, win 65535, length
536: HTTP
....E..@..@.u..Wy.b......k.P...aYm.YP...^...

        [By:GameOver]:XXXX your XXX!
```

Figure 2-6: The GET flood signature from Spike changed since 2014. The payload may be customizable

2.4 / DDoS Attack Source Countries / The number of IP addresses involved in DDoS attacks grew significantly this quarter, despite DDoS attack totals dropping overall. The increased number of IP addresses coincided with increases in IoT-fueled DDoS attacks this quarter. Specifically, attacks from botnets like Mirai and others that are capable of sending floods of non-spoofed attack traffic.

The top three source countries for DDoS attacks were the U.S. (24%), the U.K. (10%), and Germany (7%). IoT botnets heavily influence the country distribution this quarter as much of the traffic sent by these botnets is not spoofed and corresponds to real IP addresses. In the four prior quarters, China dominated the top 10 list of source countries for DDoS attacks. This quarter, China dropped to the fourth position overall, at 6% of DDoS source IPs. Canada fell out of the top 10 this quarter, to eleventh.

The question that inevitably comes to mind is: "Who are the attackers?" At Akamai, we do not steer towards attribution but rather focus on the raw data that has been collected from the Akamai Platform. We are able to determine the source of the traffic, which is different than the source of the attack in many, if not most, cases.

The Mirai botnet had a significant impact on the number of observed source IP addresses. Because Mirai attack traffic is primarily non-spoofed, it enables the attacking botnet nodes to be tracked with a high degree of confidence. Additionally, many of the devices that have been compromised for use by Mirai are in countries that have a high population of vulnerable devices but do not make regular appearances on this list.

Top 10 Source Countries for DDoS Attacks, Q4 2016

Source Country	Percentage	IP Source Count
U.S.	24%	180,652
U.K.	9.7%	72,949
Germany	6.6%	49,408
China	6.2%	46,763
Russia	4.4%	33,211
Italy	3.1%	23,365
Spain	3.0%	22,645
Brazil	3.0%	22,582
Netherlands	2.8%	21,115
France	2.8%	20,707
Other	34%	258,498

Figure 2-7: The U.S. sourced the most IP addresses participating in DDoS attacks—more than 180,000

2.5 / Repeat DDoS Attacks by Target / Peak repeat DDoS attack frequency is increasing, but so is the gap between attacks. Being a target once is a good indicator that an organization will be a DDoS target again.

2.6 / Reflection DDoS Attacks / DNS attacks remained the top reflection vector for the fourth quarter.

2.7 / Perimeter Firewall DDoS Reflector Activity / Malaysian ASN 4788 produced more reflection DDoS traffic in Q4 than the next two ASNs from China combined, as shown in Figure 2-10.

The reflector data is based on observed attack sources, not the results of scans. Increased use of an attack vector can increase the number of IP addresses, especially for an attack such as Simple Services Discovery Protocol (SSDP), which is used by many consumer grade devices. Use of the SSDP attack vector increased this quarter, perhaps due to attackers turning to the DDoS resources presented by IoT devices.

Top 5 Source Countries for DDoS Attacks, Q1–Q4 2016

Q1 2016		Q2 2016		Q3 2016		Q4 2016	
Country	Percentage Source IPs	Country	Percentage Source IPs	Country	Percentage Source IPs	Country	Percentage Source IPs
China	16% 115,478	China	40% 306,627	China	19% 81,276	U.S.	24% 180,652
U.S.	10% 72,598	U.S.	12% 95,004	U.S.	14% 59,350	U.K.	10% 72,949
Turkey	6% 43,400	Taiwan	4% 28,546	U.K.	10% 44,460	Germany	7% 49,408
Brazil	5% 36,472	Canada	3% 20,601	France	6% 23,980	China	6% 46,783
South Korea	4% 31,692	Vietnam	3% 20,244	Brazil	3% 13,502	Russia	4% 33,211

Figure 2-8: After being the top DDoS source country for several quarters, China fell to fourth in Q4 as the U.S. became the leading source country

Reflection-Based DDoS Attacks, Q4 2015–Q4 2016

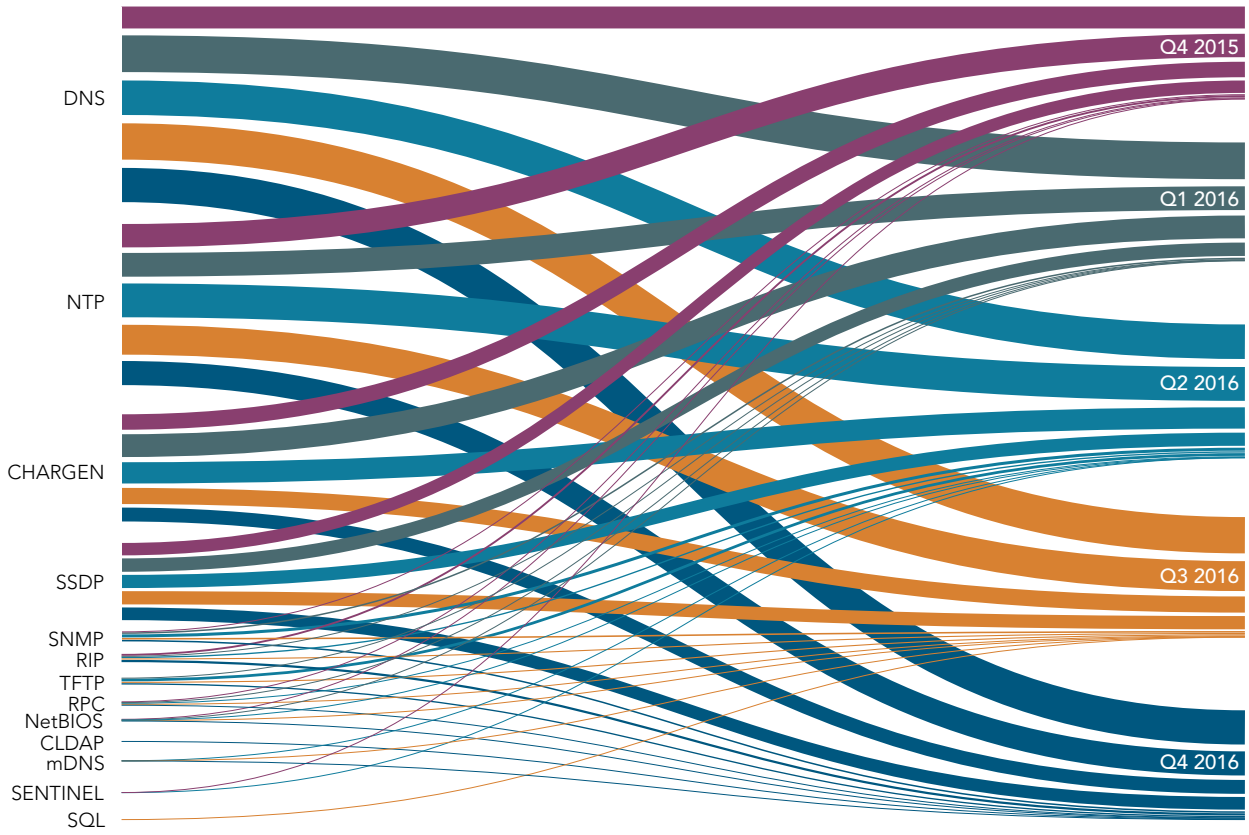


Figure 2-9: DNS retained its position as the most popular reflector

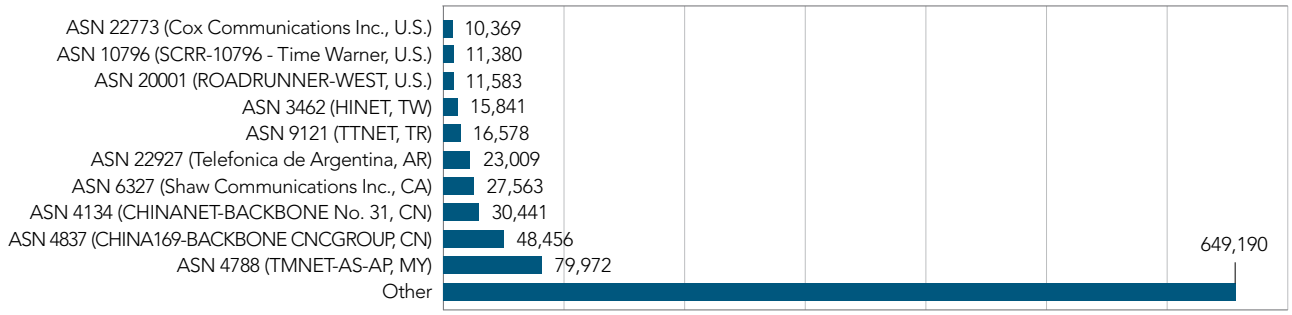


Figure 2-10: ASN 4788, in Malaysia, took the top spot with almost twice as many reflection sources as the second spot ASN 4837 in China

As shown in Figure 2-11, there was a higher number of unique SSDP reflectors in Q4, skyrocketed from 121,000 in Q3 to 508,000 in Q4. Figure 2-12 shows a 321% increase in IP addresses generating the SSDP attack vector. However, the number of NTP reflectors decreased from 459,000 (Q2) to 410,000 (Q3) to 300,000 (Q4), resulting in a 27% reduction quarter-to-quarter, as shown in Figure 2-11. Attackers pick and choose reflectors from a much larger pool of millions of devices so these numbers can change depending on the reflectors used by the various booter services available.

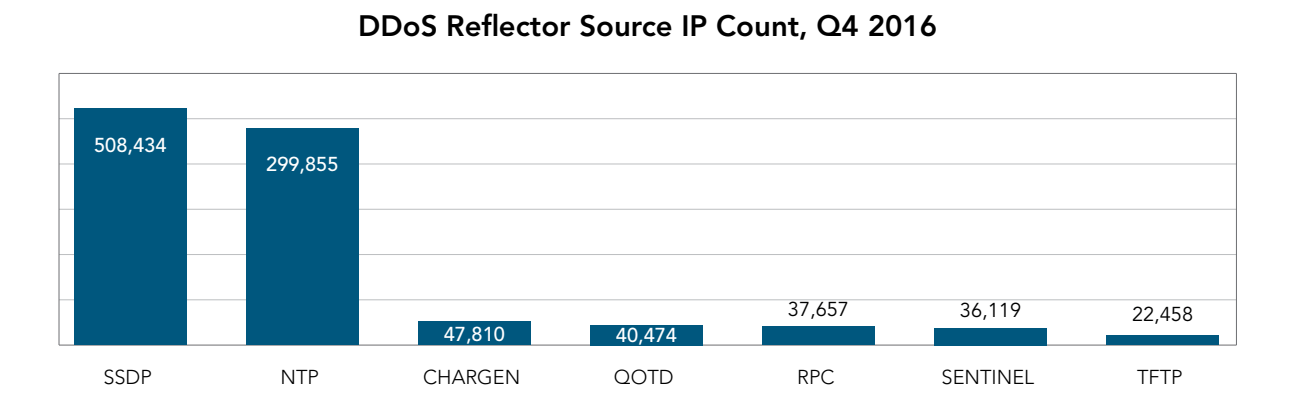


Figure 2-11: A leap in the use of SSDP reflectors occurred in Q4, surpassing NTP reflectors

As shown in Figure 2-12, SSDP exploded as a reflector source this quarter, expanding by 321%. The number of IoT-related devices, primarily home routers in the case of SSDP, used in attacks swelled. We consequently saw a rise in devices with public-facing IP addresses, which makes them more accessible to attackers who can utilize these devices for amplification attacks.

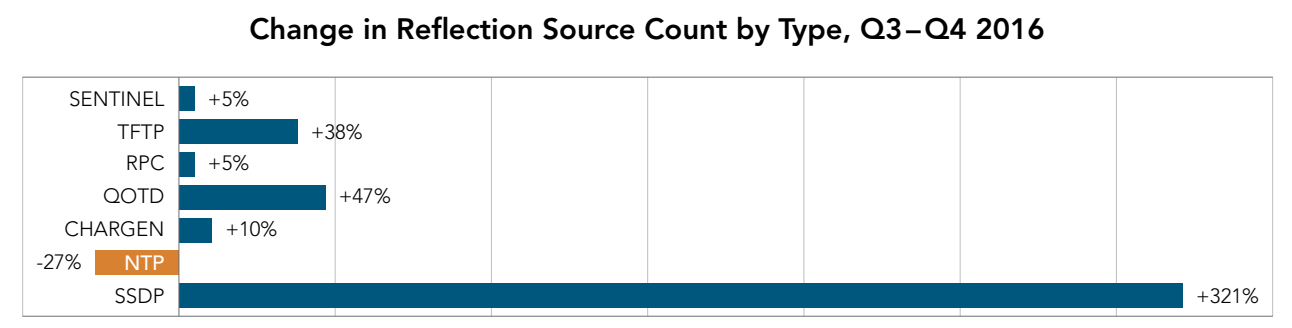


Figure 2-12: The use of SSDP reflectors increased 321 percent, while the use of NTP reflectors declined. This may be in part due to the greater level of focus that the attackers have been directing towards IoT type devices

[SECTION]3 WEB APPLICATION ATTACK ACTIVITY

We concentrated our analysis on nine common web application attack vectors — a cross-section of the categories on industry vulnerability lists.

3.1 / Web Application Attack Vectors / As shown in Figure 3-1, SQLi, LFI, and XSS accounted for 95% of observed web application attacks, similar to Q3. While the combined use has remained the same, the use of SQLi increased from 44% (Q2) to 49% (Q3) to 51% (Q4). Simultaneously, the use of LFI decreased from 45% (Q3) to 40% (Q3) to 37% (Q4).

3.2 / Top Source Countries / Akamai analyzes web application attacks that occurred after a TCP session was established. Because a full three-way handshake has happened, we are certain that the IP address in question is not spoofed. The countries reported were the sources of the IP addresses for the last hop observed and are presented as such. Attackers make use of all manners of method to avoid detection, but a TCP session is hard to spoof. The foremost method used by attackers to cover their tracks is via the use of proxy servers, rather than the direct packet-level source address manipulation commonly seen in UDP-based infrastructure attacks.

Web Application Attack Frequency, Q4 2016

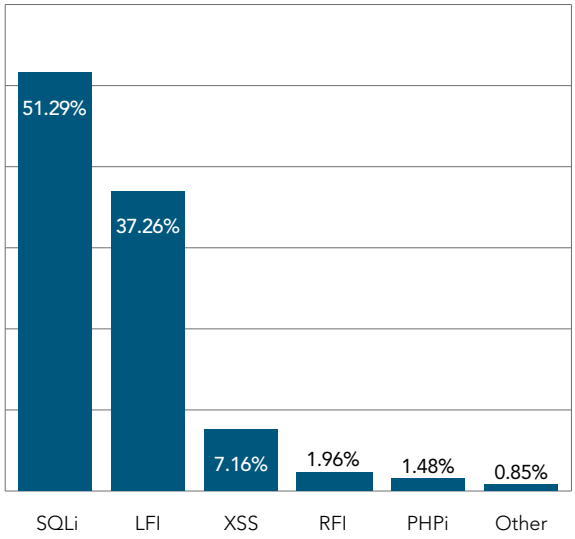
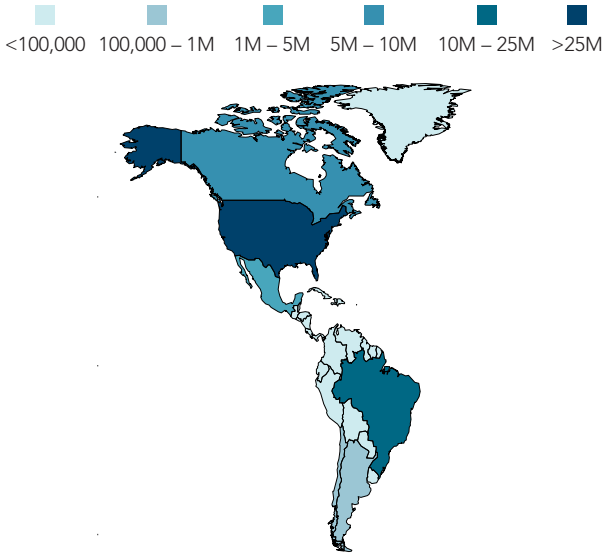


Figure 3-1: Combined, SQLi and LFI accounted for 88% of observed web application attacks

We've changed the format of how we show the source of attack traffic, to make changes in that traffic more understandable. First, where possible, we are including both the number of IP addresses per region in the report. Second, we're breaking down several of the maps by region, showing traffic in the Americas, EMEA, and Asia Pacific (including Australia) in order to highlight their regional differences.

Figure 3-2 shows that the U.S. (28%) and the Netherlands (17%) continued to be the first and second leading sources of web application attacks, with Germany (9%) third.

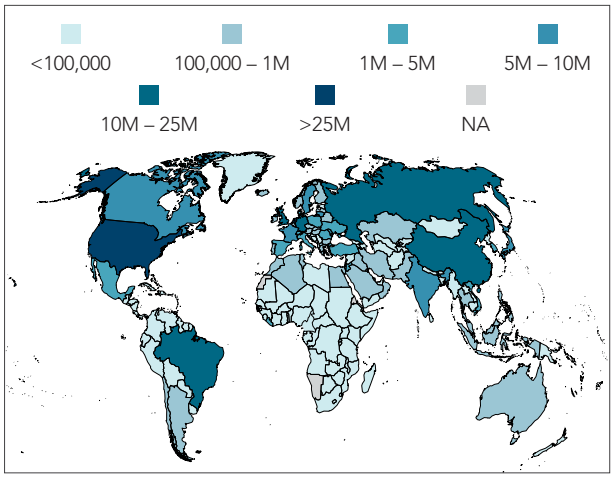
Web Application Attack Source Countries—Americas, Q4 2016



Country	Attacks Sourced	Global Rank
U.S.	97,918,896	1
Brazil	19,379,729	4
Canada	8,519,773	11
Mexico	1,055,746	29
Chile	193,096	60

Figure 3-3: The U.S. sourced the most web application attack traffic in the Americas. The U.S. generated five times more web application attack traffic than Brazil

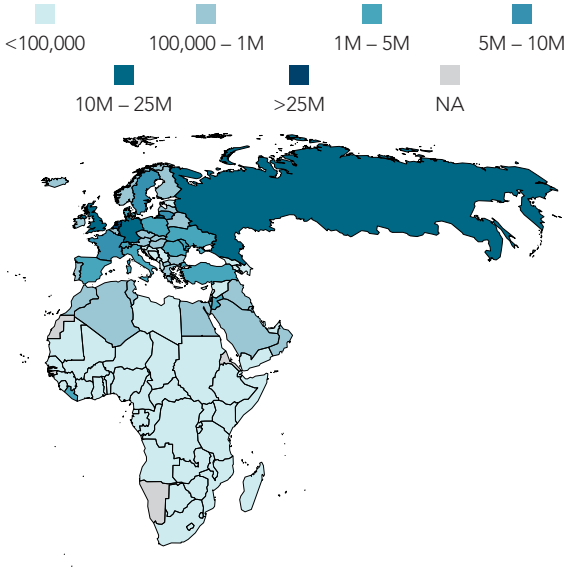
Global Web Application Attack Source Countries, Q4 2016



Country	Attacks Sourced	Percentage
U.S.	97,918,896	28%
Netherlands	61,499,919	17%
Germany	32,384,205	9.2%
Brazil	19,379,729	5.5%
Russia	16,643,150	4.7%
China	14,275,358	4.0%
U.K.	11,908,055	3.4%
Lithuania	9,793,507	2.8%
France	8,772,176	2.5%
India	8,638,666	2.4%

Figure 3-2: Web application attacks are sourced worldwide, with the U.S. as the most prolific source country

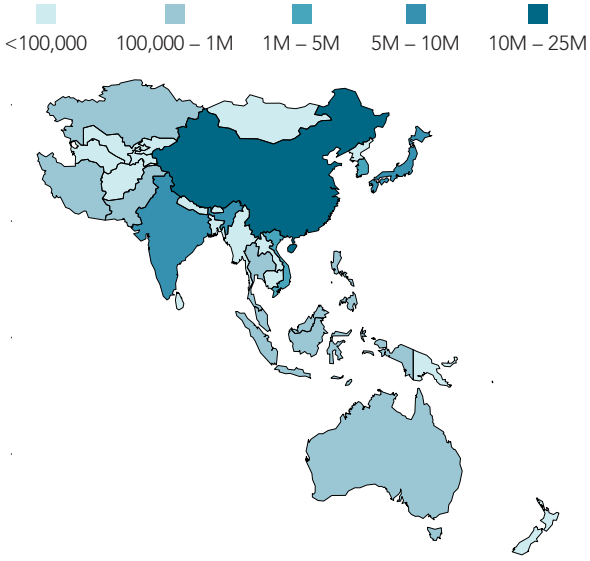
Web Application Attack Source Countries—EMEA, Q4 2016



Country	Attacks Sourced	Global Rank
Netherlands	61,499,919	2
Germany	32,384,205	3
Russia	16,643,150	5
U.K.	11,908,055	7
Lithuania	9,793,507	8

Figure 3-4: The Netherlands was the top source of attack traffic, despite its small size

Web Application Attack Source Countries—Asia Pacific, Q4 2016



Country	Attacks Sourced	Global Rank
China	14,275,358	6
India	8,638,666	10
Japan	6,627,888	14
Vietnam	1,200,006	25
South Korea	1,196,627	26

Figure 3-5: China, India, and Japan sourced the most web application attack traffic in Asia. Nearly twice as much attack traffic was recorded from China vs. India

In the Americas, as shown in Figure 3-3, the top three sources of web application attack traffic were the U.S., Brazil, and Canada, respectively. Within Europe, Middle East, and Africa (EMEA), as shown in Figure 3-4, the top sources were the Netherlands, Germany, and Russia, in that order. In Asia Pacific, as shown in Figure 3-5, the top sources were China, India, and Japan, respectively.

3.3 / Top 10 Target Countries / The U.S. was again the target of the vast majority of web application attack traffic, as shown in Figure 3-6. Many large organizations that are targets of web application attacks have significant infrastructure located in the U.S. even if they are based elsewhere. Brazil and Germany rounded out the top three attack targets.

Top 10 Target Countries for Web Application Attacks, Q4 2016

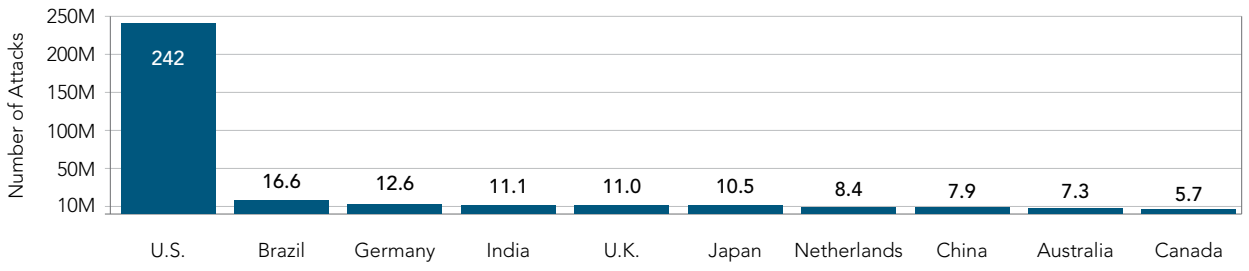


Figure 3-6: The vast majority of targets of web application attacks were in the U.S.

3.4 / Spotlight on Thanksgiving Attacks / In the U.S., the week surrounding its Thanksgiving holiday encompasses three of the biggest online shopping days of the year: Thanksgiving, Black Friday (the day after Thanksgiving), and Cyber Monday (the first workday after Thanksgiving). For many retailers, this short time period can make or break their earnings for the entire year. This year, Thanksgiving was November 24. We analyzed the period from November 22 – 29. Times are marked in GMT, so midnight (00:00) on the timeline is 7 p.m., U.S. Eastern Time.

The week of Thanksgiving was relatively quiet for web application attacks, even though Akamai served an average peak of 33 Tbps of traffic during the time period. The data set used in this analysis represents real-world attack attempts. The triggers used have very low false positive and false negative rates — it is unlikely for them to mistakenly alert on legitimate traffic and they will miss very few actual attacks. Though no system can claim 100% accuracy, these signatures come as close as currently possible. The types of attacks included were SQL Injection (SQLi), command injection (CMDi), PHP injection (PHPi), remote file inclusion (RFI), local file inclusion (LFI), cross site scripting (XSS), and known scanners.

As shown in Figure 3-7, there was a cyclical nature to the attacks against retailers, with a peak almost every day at 1 p.m. GMT (8 a.m. U.S. Eastern). This figure is used to see trends and understand the variety of sub-verticals Akamai tracks, as separating individual organization types is difficult at this level.

Digging deeper, the data showed four sub-verticals contributed to the overall spikes in different ways, as shown in Figure 3-8. Apparel & Footwear was the biggest contributor to the cyclical nature of the attacks. The target was a group of related retailers, owned by a common parent company, but each with its own website. Each day at approximately 1:00 p.m. GMT (8 a.m. U.S. Eastern), attackers would hit these sites with a series of cross-site scripting and injection attacks. The source of these attacks could have been an

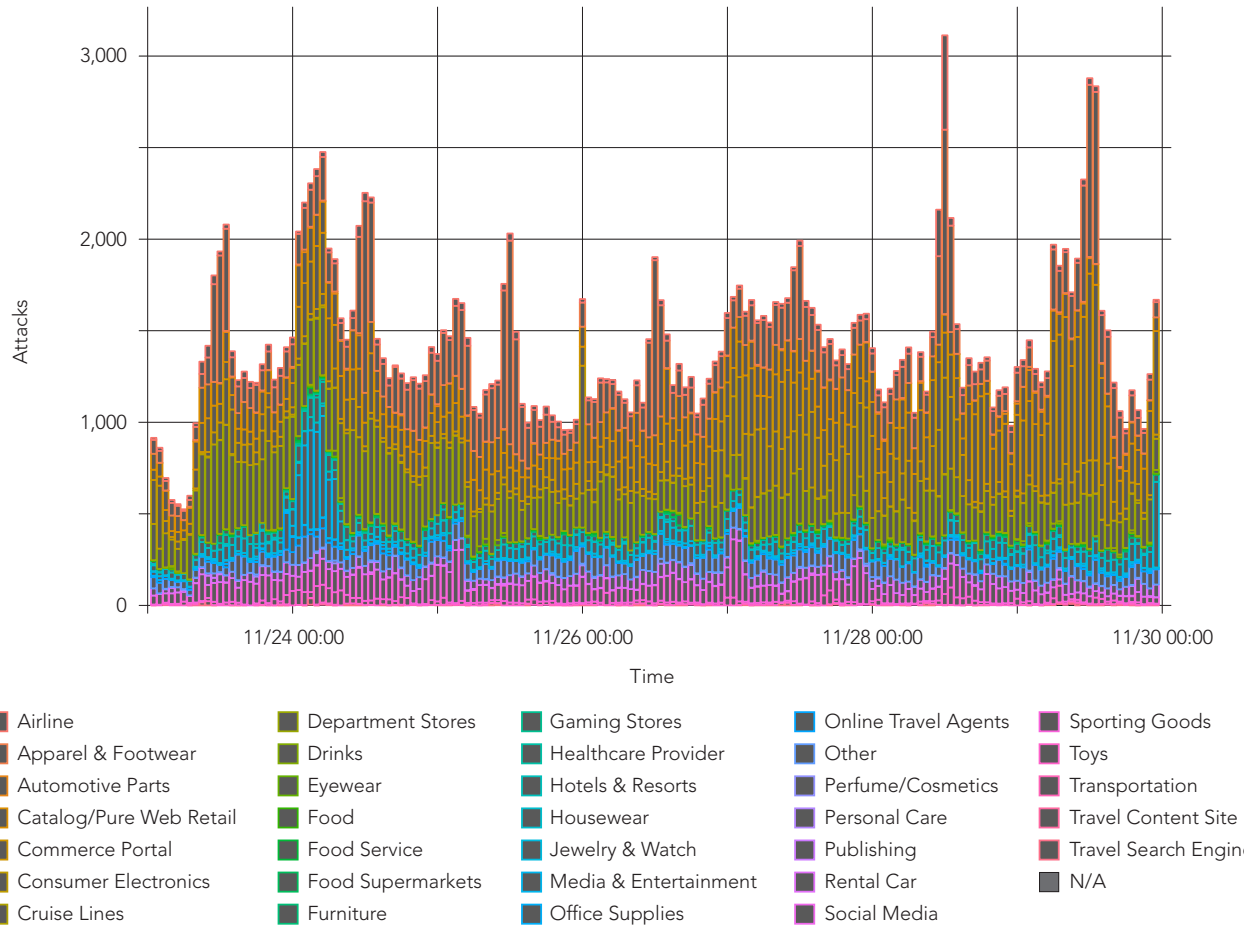


Figure 3-7: The attacks peaked daily at 1 p.m. Greenwich Mean Time

internal scanning tool that should have been filtered from the logs, or it could have been an attacker waiting for a mistake to be made, exposing a vulnerability for exploitation.

In contrast to this recurring attack, our second sub-vertical, Commerce Portals, contained one merchant with multiple websites around the world. These regional sites were targeted by a steady rise in SQLi and LFI attacks between Nov. 28 – 29. Notably, the attacks did not target the merchant's main web property. The attackers probing the sites may have thought the regional sites would have weaker security than the main corporate site.

The third sub-vertical, Consumer Electronics, was targeted by two separate types of attacks. Attacks on November 26 targeted a single large merchant with a single spike in SQLi attacks, which then settled down to baseline levels. A different series of attacks on November 27 formed a concerted attack against multiple sites running the same software, triggering CMDi, LFI, XSS, and PHPi alerts.

The final set of attack events were against a set of Media & Entertainment sites. At first glance, it wasn't clear how the attacks were related; each targeted a single domain with a few SQLi and LFI attacks, and then moved to the next domain. Closer inspection revealed that these sites were hosted on a common platform. The attacker was iterating a list of sites that were not properly updated and secured. The attackers appear to have identified a platform with a known vulnerability and used this busy time to scan a large section of these sites.

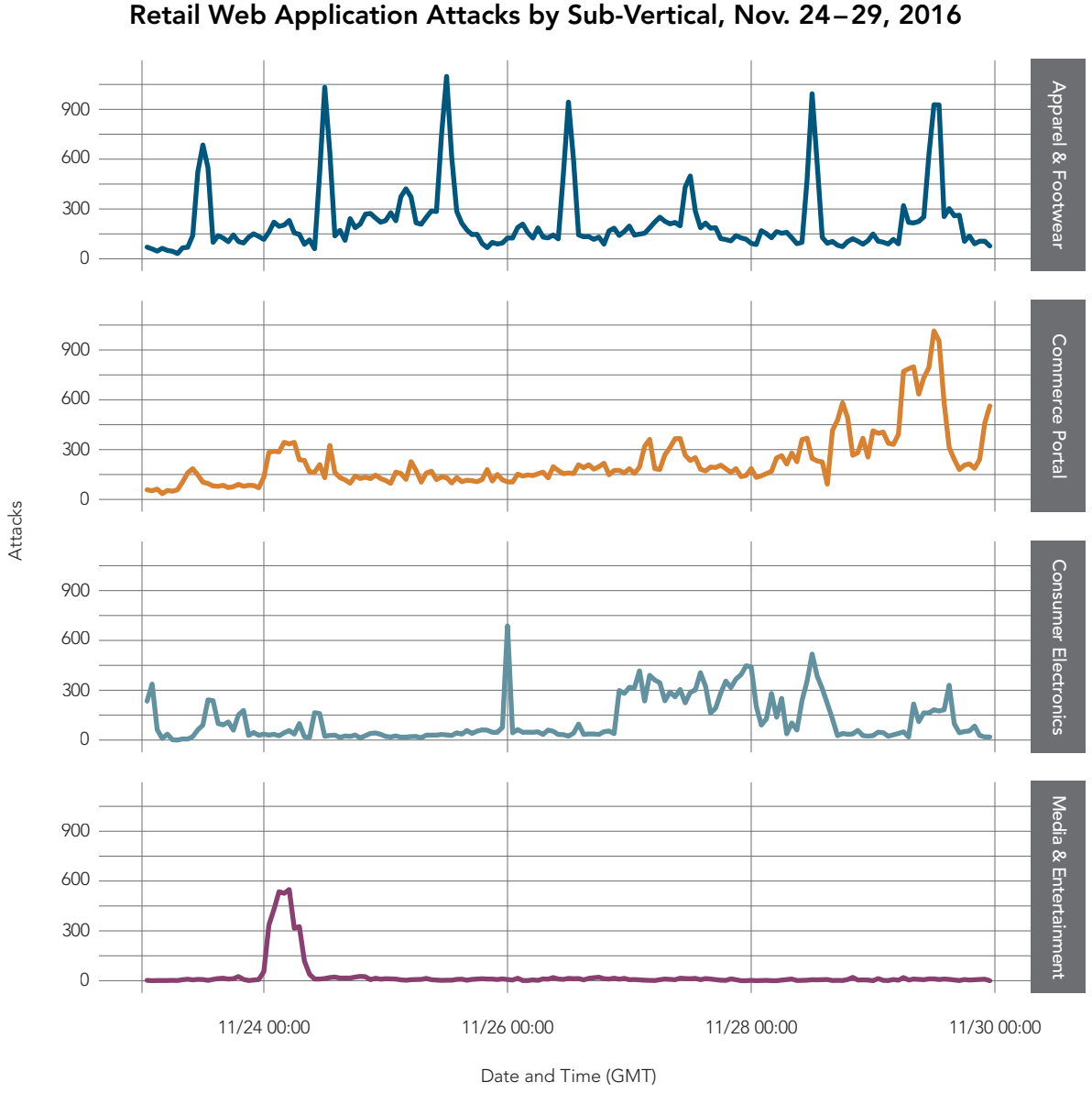


Figure 3-8: Each sub-vertical was targeted with different types of attacks at different times

The global scale of the Akamai Intelligent Platform allows us to generate collective intelligence to reveal trends in attack traffic and drill down into specific verticals, sub-verticals, customers, and even specific events. We expected the week of Thanksgiving to be one of the busiest times of the year in terms of attack traffic, but for the majority of merchants it was simply another week, albeit with more money to be made than any other time of the year.

3.5 / Scanning of Ports 23 & 2323 / There is always a certain level of "background radiation" of traffic on the Internet. Every IP address exposed to the Internet is scanned regularly, regardless of whether the IP address is hidden. This traffic is part of the background noise of the Internet, which can sometimes be used as an indicator of change in attack tactics, though often only in hindsight. We analyzed traffic hitting the Akamai Intelligent Platform on ports 23 and 2323 from Feb. 2 – Oct. 27, 2016.

Port 23 is used by the Telnet protocol, so communication on this port is common. Port 2323 is less common and rarely used on the public Internet — at least it was rarely used before the release of the Mirai botnet. Mirai uses ports 23 and 2323 to log into unprotected digital video recorders (DVRs) and IP-enabled closed-circuit television (CCTV) systems. A look at the activity on these ports showed that there were indicators of change to the botnet landscape as early as May 13, 2016, as shown in Figure 3-9.

Akamai began researching the Kaiten botnet at the beginning of May, 2016. Kaiten is a precursor to Mirai, and they both use Telnet as part of the process of compromising a device. As shown in Figure 3-9, early Kaiten activity doesn't appear to have changed the overall level of background noise on ports 23 and 2323.

An abrupt change is visible at the end of May and again at the end of July. While scans against port 23 and 2323 are not strong indicators of a Mirai-compromised IP address, the jumps in overall traffic trends may indicate Mirai activity. May was possibly the first run of testing the code base of Mirai, with the jump at the end of July being the full release into the wild of Mirai.

A spike in traffic in late September marked when an Akamai customer was the target of Mirai-driven attacks. In contrast, no Akamai customer was targeted by the attacks on DNS provider DYN, so activity in October was closer to the new baseline.

It's difficult to use indicators like port scans to foretell attacks or a new vector, but they can be used in hindsight to better understand when certain actions took place. Some timelines place the development of Mirai in early July. However, if the spikes in our data are indicators of early efforts on the botnet, then the initial versions of Mirai may have been compromising systems as early as May 13, 2016, when the major increases in scanning traffic started.

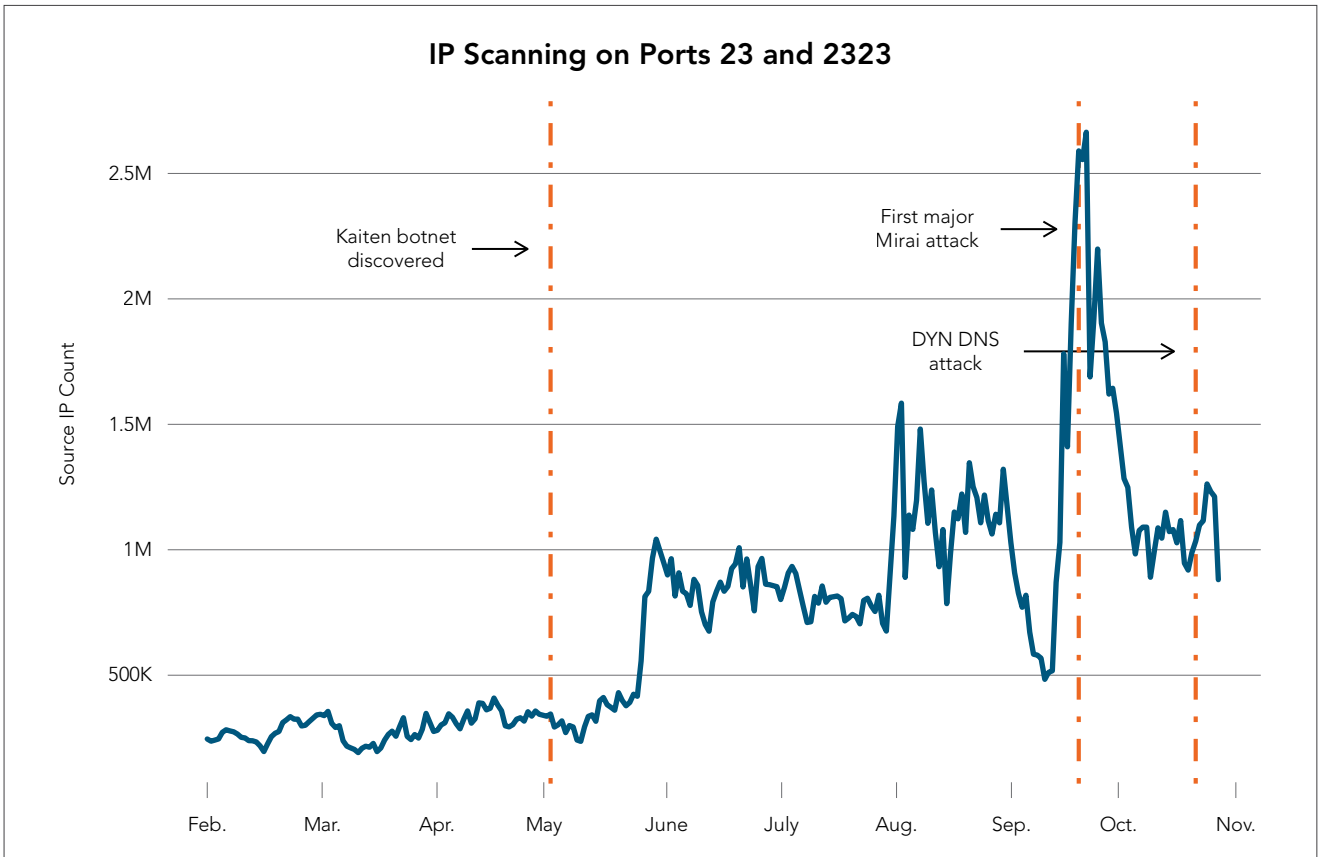


Figure 3-9: A rapid increase in scans of ports 23 and 2323 began on May 13, 2016

[SECTION]4
LOOKING FORWARD

This quarter was a bit of a surprise for us. We expected the Mirai botnet and other IoT-based malware to continue as the source of the largest DDoS attacks — and as a rule, they were. But the largest DDoS attack targeting an Akamai customer came from Spike, a malware that has been around for over two years, and measured 517 Gbps. Old malware can learn new tricks.

As we've mentioned before, proof that something is possible often motivates others to commit the same action. One hypothesis is that the attackers in control of the Spike malware took the capabilities of Mirai as a challenge, and decided to become more competitive. We believe it's likely other botnet operators will also feel the challenge and increase the size of their attacks.

That's not to say that botnets like Mirai are no longer one of biggest threats we face. The Internet of Things is in its infancy, and device security is only starting to bubble up in the consciousness of IoT developers, the companies that employ them, and governments.

We expect to see many more vulnerable and compromised devices before devices become more secure. The good news is that there are significant reasons for companies to invest in security in the future.

The counter to this is that attackers are likely to find new devices to compromise and once again increase their capabilities. Given these two opposing forces, we expect the system will exhibit wild fluctuations in the short term.

Another piece of good news is that resources used to fuel IoT botnets, while considerable, are not infinite. It is foreseeable that there will be contention for resources amongst botnets, meaning we may see the number of attacks increasing, while the size of many attacks fall. The counter to this is that attackers will find new devices to compromise and once again increase their capabilities. This is not a system that will find equilibrium in the short term.

Protecting against DDoS attacks is only one aspect of securing a business but, like every other aspect of security, it is changing constantly. DDoS attackers originally coordinated people, and then there were botnets of PCs, and then botnets of servers, and now botnets of IoT devices. At each point in the evolution of DDoS, the landscape permanently changed. Today, there is a new baseline of DDoS attack size, and your organization has to be ready to defend against it.

The first wave of botnets was driven by desktop computers, either those purposefully added or systems that were compromised. The second wave consisted largely of compromised servers and services, for example, the Brobot malware used to compromise virtual private servers and fuel attacks by the al-Qassam Cyber Fighters. The current wave of IoT-based botnets is the third wave, and it represents a similar change to the landscape of DDoS.

Luckily, Mirai is the type of change that comes only rarely. Thus, we can hope to have a few quarters to adjust to the size of attacks on organizations, and ensure that the necessary defenses are in place.

[SECTION]5 CLOUD SECURITY RESOURCES

Akamai's research teams published three papers in the fourth quarter of 2016 covering the topics below.

5.1 / Mirai Botnet / Much is now known about the Mirai botnet. ***Akamai's Mirai DDoS Threat Advisory***[4] provides information about attacks and findings prior to the release of the Mirai code, as well as attacks following its release. This ***recent advisory***[3] provides information about attack events and findings prior to the Mirai code release as well as those occurring following its release.

Mirai attack signatures were first observed in attacks against a security blog run by journalist Brian Krebs. The first attack, out of a series of four, peaked at 623 Gbps. Just days after this series of DDoS attacks, the source code for Mirai was made public. The bandwidth peak, although still substantial, has been observed at mostly under 100 Gbps in later attacks. In addition, most of the attacks were under 30 million packets per second.

Mirai comes with an array of attack options along with customizable parameters that allow modifications of attack durations, ports, and payloads, to name a few. While all working attack types are provided, the amount of customization possibilities available for each of these attack types would make it difficult to list all of the attack combinations.

5.2 / mDNS Reflection DDoS Threat Advisory / The potential for the abuse of the Multicast Domain Name System (mDNS) protocol in reflection and amplification DDoS attacks was disclosed in March 2015. Toward the end of Q3 2015, Akamai observed limited use of DDoS attacks fueled by mDNS-capable devices.

Akamai's mDNS Reflection DDoS Threat Advisory[5] details the concept and techniques of the mDNS reflection attack vector and how to mitigate it. The availability of source devices that expose mDNS fuels this attack, which is expected on port 5353. As of October 2016, Akamai successfully detected and mitigated seven mDNS DDoS attacks against targets in the Gaming and Software & Technology industries.

mDNS is a proposed standard protocol released in 2013 as RFC6762. It facilitates the discovery of devices and services, ideally in small networks, requiring minimal user interaction at most.

Some risks come with the simplicity of a protocol designed to allow a device to be plugged in and ready to go. A vulnerability (VU#550620) on mDNS was found by Akamai SIRT, where mDNS would allow responses to queries originating from outside the local network. These responses then would allow disclosure of sensitive information about the affected device, such as its software and services, hostname, internal network configuration settings, model number, etc.

5.3 / State of the Dark Web 2016 / 2016 was a very active year for the dark web. The general offerings of the dark web markets shifted significantly, especially with new cryptocurrencies in use. A few high-profile hacker forums and underground marketplaces disappeared, with new ones popping up in their place. 2016 also saw new darknet based privacy services unveiled in the forms of ISP and a VPN offerings. This past year also saw an unprecedented amount of policy and enforcement efforts targeting the dark web, its users, and the impacts of its use.

In 2016, we saw a huge shift in dark web market offerings, from a focus on illicit drugs, malware offerings, compromised credentials, personally identifiable information (PII), medical records, financial services accounts, hacking tutorials, credit card numbers, and a glut of compromised digital accounts for a wide range of services. Single and bulk compromised account logins are readily available across the top five dark web markets, and the prices are falling as more enter the market.

To read more about what happened in the dark web, and look at our predictions for next year, see our full white paper.

[1] Rigg, Jamie. "FTC drags D-Link into court for lax router and camera security." Engadget.com, 6 Jan. 2017. https://www.engadget.com/2017/01/06/ftc-d-link-poor-security/

[2] Moon, Mariella. "ASUS agrees to 20 years of audits for router security issue." Engadget.com, 23 Fed. 2016. https://www.engadget.com/2016/02/23/asus-ftc-settlement-router/

[3] "Threat Advisory: Mirai Botnet." Akamai, Aug. 2016. https://www.akamai.com/us/en/our-thinking/threat-advisories/akamai-mirai-botnet-threat-advisory.jsp

[4] https://www.akamai.com/uk/en/our-thinking/threat-advisories/akamai-mirai-botnet-threat-advisory.jsp

[5] https://www.akamai.com/uk/en/our-thinking/threat-advisories/akamai-mdns-reflection-ddos-threat-advisory.jsp

[6] https://www.akamai.com/us/en/our-thinking/threat-advisories/akamai-2016-state-of-the-dark-web.jsp

***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*.
