[Volume 4 / Number 1]

akamai's [state of the internet] / security

Q1 2017 report

AT A GLANCE

Web application attacks, Q1 2017 vs. Q1 2016
35% increase in total web application attacks
57% increase in attacks sourcing from the U.S. (current top source country)
28% increase in SQLi attacks

Web application attacks, Q1 2017 vs. Q4 2016
2% decrease in total web application attacks
20% increase in attacks sourcing from the U.S. (still top source country)
15% decrease in SQLi attacks

DDoS attacks, Q1 2017 vs. Q1 2016
30% decrease in total DDoS attacks
28% decrease in infrastructure layer (layers 3 & 4) attacks
19% decrease in reflection-based attacks
89% decrease in attacks greater than 100 Gbps: 2 vs. 19

DDoS attacks, Q1 2017 vs. Q4 2016
17% decrease in total DDoS attacks
17% decrease in infrastructure layer (layers 3 & 4) attacks
14% decrease in reflection-based attacks
83% decrease in attacks greater than 100 Gbps: 2 vs. 12
**Note: percentages are rounded to the nearest whole number.*

What you need to know

- Reflection attacks continued to comprise most DDoS attack vectors and accounted for 57% of all mitigated attacks.
- "DNS Water Torture Attacks," a DNS query flood included in Mirai malware, targeted Akamai customers in the financial services industry. Details are provided in this quarter's ***Attack Spotlight.***
- Akamai welcomes Wendy Nather, Sr. Security Strategist from Duo Security, as the first Guest Author.

LETTER FROM THE EDITOR / The *Q1 2017 State of the Internet / Security Report* represents analysis and research based on data from Akamai's global infrastructure and routed Distributed Denial of Service (DDoS) solution.

Technology milestones are often marked by a significant event, followed by a long adoption phase. When referring to consumer adoption of technology, this is called the "hype cycle," a term created by the consulting firm Gartner. The initial hype surrounding a product far exceeds its capabilities in the real world, followed by a period of disillusionment and a slow integration into the fabric of our lives. The world of DDoS attack tools differs little from other technologies; new tools used by attackers follow a similar cycle of hype and integration. However, DDoS technology acceptance often proceeds at a much faster pace than consumer technologies, as there is much less resistance to change within the relatively small community of malicious actors.

As shown over the last half year, the Mirai botnet is an example of a disruptive technology working its way through the cycle. The development of Mirai happened quietly behind the scenes, while the first round of DDoS attacks were startling in their size and capability. The botnets' capabilities quickly moved into a stage where contention for Internet of Things (IoT) devices reduced the size of attacks considerably. While many of the largest DDoS attacks observed this quarter were still based on Mirai-derived botnets, they were not as large as the initial attacks. What follows is the integration of the use of IoT as another part of the fabric of DDoS botnets and malware.

As we discussed in last quarter's report, there were long-term consequences to the release of Mirai. First, competitive forces drove botnet herders to keep up with Mirai's technology or risk losing market share. The creators of other botnets are working to generate comparably-sized attacks.

Secondly, other botnets families, such as BillGates, started adding new features, some taken directly from leaked Mirai source code. Meanwhile, Mirai has continued to splinter and evolve. There is now a variant which infects Windows systems, not to recruit them as attack nodes for the botnet, but to further expand the botnet by scanning and infecting Linux devices.

This quarter's Attack Spotlight includes our research into one of the Mirai DDoS tools used against financial services organizations. Called "DNS Water Torture" in Mirai's code, this DNS query flood generates relatively limited volumes of traffic, but can create denial of service outages by consuming the target domain's resources in looking up randomly generated domain names in great numbers. Each query ties up memory and processor cycles, preventing the target from processing legitimate traffic.

We also observed a new reflection attack vector, Connectionless Lightweight Directory Access Protocol (CLDAP). At this point, the protocol has not been a significant source of attack traffic, but the lack of contention for the resource could change its popularity. A link to the threat advisory is provided in ***Cloud Security Resources***.

We are pleased to host a guest author this quarter: Wendy Nather, Principal Security Strategist at Duo Security. See what she has to say about the challenges of managing corporate security, given the current state of the Internet.

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 / Security* subspace on the Akamai Community at ***https://community.akamai.com***. For additional security research publications, please visit us at ***www.akamai.com/cloud-security***. The views of Ms. Nather are her own and do not necessarily reflect the opinions or perspectives of Akamai.

The state of the Internet is...complicated, as always.

Consider these changes over the past decade:

Corporate and Consumer Use Are Intertwined / It used to be that you went to work in the office, used corporate software, and then went home and used completely different software on your home computer. Now, more often than not, you've got a corporate login and a personal login with the same SaaS provider and you're using the same apps on your phone (Gmail, Dropbox, LastPass, etc.). Unless you're working in a strictly segmented environment, the expectation is that you'll be using applications for both purposes and alternating at the drop of a hat, regardless of which network you're currently connecting to.

BYODon't / Some organizations have embraced the use of personal devices, and others haven't, but it's becoming harder to enforce a "no BYOD" policy when both the endpoint and the resources they're accessing are outside of the corporate perimeter. Unmanaged personal devices raise the specter of risks ranging from unpatched vulnerabilities to e-discovery requirements that include searching your employees' phones. And that's not even counting wearables and other Things.

Password Policies / Remember when you only had a dozen usernames and passwords? Yeah, neither do I, and here we are. A typical online user could have literally hundreds of online accounts, some of which predate today's password managers. Under pressure from bulk credential theft and compliance requirements, every system owner is being driven to require longer, more complicated and unique passwords. But the days of password rules such as "upper and lower case, one number, one special character, two emojis, and a squirrel noise" are going to come to an end; users are going to push back as soon as the absurdity becomes clear. Ubiquitous, consistent, and usable password managers are going to have to evolve into an application interface to shield everyday people from the malignant growth of complex passwords.

Guest Author

Wendy Nather
Principal Security Strategist
Duo Security

To Sum Up / Our interaction with the Internet has evolved to "anytime, anywhere, using any device and software, for any purpose." That means that enterprises have to address the security issues in ways that don't rely exclusively on traditional boundaries ("our network," "our software," "our hardware"). And they have to be able to distinguish business data from personal data, which were created at the same time of day, in the same location, using the same applications, and stored in the same formats on the same hardware and services. Users expect a seamless experience that doesn't require them to sacrifice a chicken every time they switch between corporate and personal contexts — and they deserve one.

The identity is the new boundary, together with the context. When you log into Gmail with your personal credentials, you're in charge of the security requirements you set for accessing your data; when you use your corporate credentials to log in, your employer has to specify what's required to access business data, such as the combination of username, password, other authentication factors, and managed device. It's the same service, the same software, and the same person, but there are different stakeholders based on the ownership of the data.

Adapting to this new boundary, Google built a framework for their internal use and dubbed it ***BeyondCorp***; whether they're calling it "***zero-trust***," or "perimeterless," many organizations are looking to adopt it ***in their own ways***. The important point is that the security shouldn't rely solely on the traditional perimeter, and should accommodate the needs of both the user and the enterprise.

Putting the user on equal footing with the data owner is a welcome trend, and it's one that holds great promise for the ongoing challenge of securing the Internet.

[SECTION][1] EMERGING TRENDS

The median size of DDoS attacks has fallen steadily since the beginning of 2015. At the beginning of 2015, the median DDoS attack size was 4 Gbps. Two years later, at the beginning of 2017, the median attack size was just over 500 Mbps. Not to say huge attacks aren't happening — mega attacks topping 100 Gbps occur every quarter — but half of all attacks are between 250 Mbps and 1.25 Gbps in size. Even these smaller attacks can harm unprepared organizations. Web application attacks shifted subtly towards the U.S. this quarter, both as a source and as a target. This type of attack is important not because of their size, but because they attack the underlying fabric of sites, either tying up resources or pulling information from the database powering sites.

The impact of IoT devices and dozens of attacks from the Mirai botnets since last September has had a strong practical effect on the security needs of organizations. The mega attacks are outliers that represent the limits enterprises must be prepared to defend against. However, the overwhelming number of smaller attacks means that these mega

attacks have little impact on the trend lines that define the median attack size, which is a better indicator of what an organization is most likely to see.

The majority of attacks are still small relative to the largest Mirai attacks, but they don't need to be big to be effective. If we consider that many businesses lease uplinks to the Internet in the range of 1–10 Gbps, any attack exceeding 10 Gbps could be "big enough" and more than capable of taking the average unprotected business offline.

At the same time, the effects of IoT are not to be underestimated, and the IoT ecosystem has drawn the attention of a wider audience. A recent example is malware that compromises Internet-enabled toasters to mine Bitcoins[1], an effort that appears to have been an ineffective proof of concept. Another trend is represented by the BrickerBot botnet, which attacks systems exposed directly to the Internet with default Telnet passwords apparently in an attempt to prevent their use by the Mirai botnet. If this botnet is unable to disconnect the target device from the Internet, it corrupts the configuration, permanently bricking the devices[2]. Neither of these examples are major threats, but they do show a significant increase in attention from both the hacker and security communities.

There is one factor that seems to be affecting the DDoS landscape as a whole: law enforcement. Early attacks by the Mirai botnets appear to have been triggered by the announcement of the arrests of two teens in Israel who were responsible for the vDos botnet[3] — a DDoS-for-hire tool that netted them hundreds of thousands of dollars. More recently, Europol coordinated the arrest of 34 individuals across 13 countries as part of an effort called Operation Tarpit[4]. Operations like Tarpit target the largest services responsible for DDoS attacks directed at banks, gaming companies, and retailers. This can have a significant effect in reducing the number of attacks on these organizations.

Despite the overall reduction in volumetric DDoS attacks, Akamai has seen a significant increase in the amount of traffic in reflection attacks. Taking advantage of the nature of DNS, NTP, and other protocols, attackers make seemingly legitimate requests of servers, causing them to spew traffic at the attacker's true target. Akamai recently released a threat advisory about adding a new DDoS reflection source, CLDAP[5]. Reflection attacks are much more difficult to track back to the botnets that originate the attacks.

In all likelihood, DDoS attacks will increase in size and frequency. We anticipate more frequent small-scale attacks, but the largest attacks will almost certainly continue to grow. As previously noted, we expect mega attacks to continue to have an outsized impact on DDoS trends in the coming years.

[SECTION]^2
DDoS ACTIVITY

2.1 / DDoS Attack Vectors / As the research team dove into early 2017 data, we first examined infrastructure-related attack data. Invariably, infrastructure attacks are the largest component of our quarterly volumetric attack data. In Q1, these attacks accounted for roughly 99% of the overall attack traffic. That's likely because it's trivial for an attacker to launch a volumetric attack in comparison to the technical understanding needed to make effective use of application layer tools.

Application layer DDoS attacks such as GET, PUSH, and POST floods remained a small component of the overall DDoS attack landscape. Two years ago, in Q1 2015, application layer DDoS attacks accounted for 9% of all attacks. In Q1 this year, only 0.6% of DDoS attacks targeted the application layer. Most application layer attacks aren't designed for denial of service.

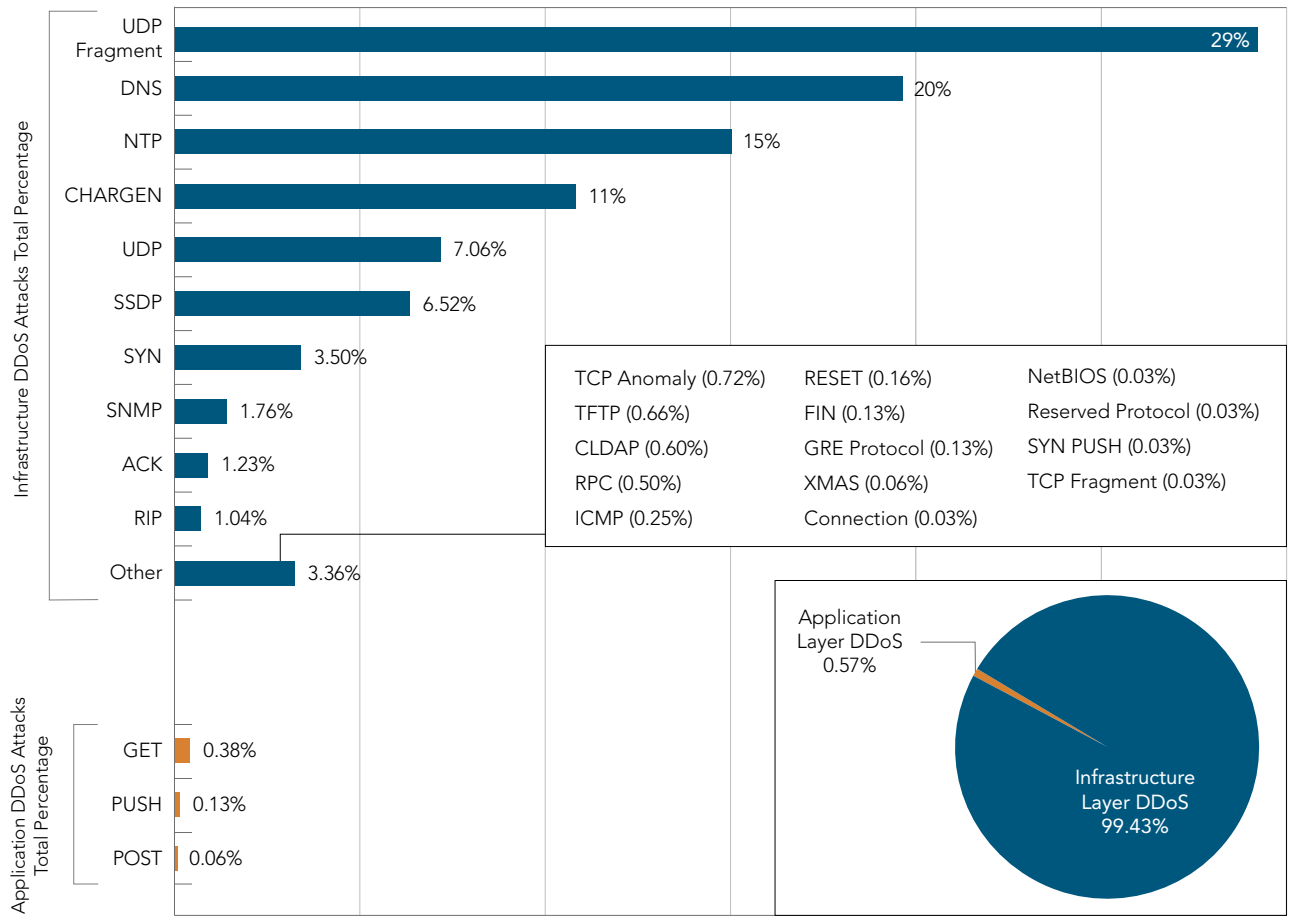


Figure 2-1: UDP fragment, DNS, and NTP continued as the top three DDoS attack vectors, while reserved protocol floods and connection floods made rare appearances in the attack vectors list

The top four infrastructure DDoS related attacks were the same as in recent quarters. UDP fragments, DNS floods, NTP floods, and CHARGEN attacks dominated, as shown in Figure 2-1. UDP fragment, NTP, and CHARGEN rose compared to the previous quarter, while DNS attack traffic fell slightly from 21% to 20%.

Organizations can keep their servers from participating in these DDoS attacks if they ensure that services such as CHARGEN and NTP are either not accessible from the Internet or are patched. Older NTP daemons, as an example, send large amounts of reflected traffic at the intended attack target in response to relatively small illegitimate requests from attackers. This traffic amplification factor is one reason why attackers continue to use NTP reflection even as fewer and fewer unpatched NTP servers remain on the Internet. One easy fix is to confirm the NTP daemons that are running in your environment are well patched. No defender wants to make the job of an attacker easier.

DDoS attacks are an ever present danger and it's important that defenders make sure that they are practicing proper security hygiene to avoid inadvertently participating in attacks. It is essential to ensure that services such as CHARGEN and NTP are patched and firewalled off where they are not required to be available to the wider Internet.

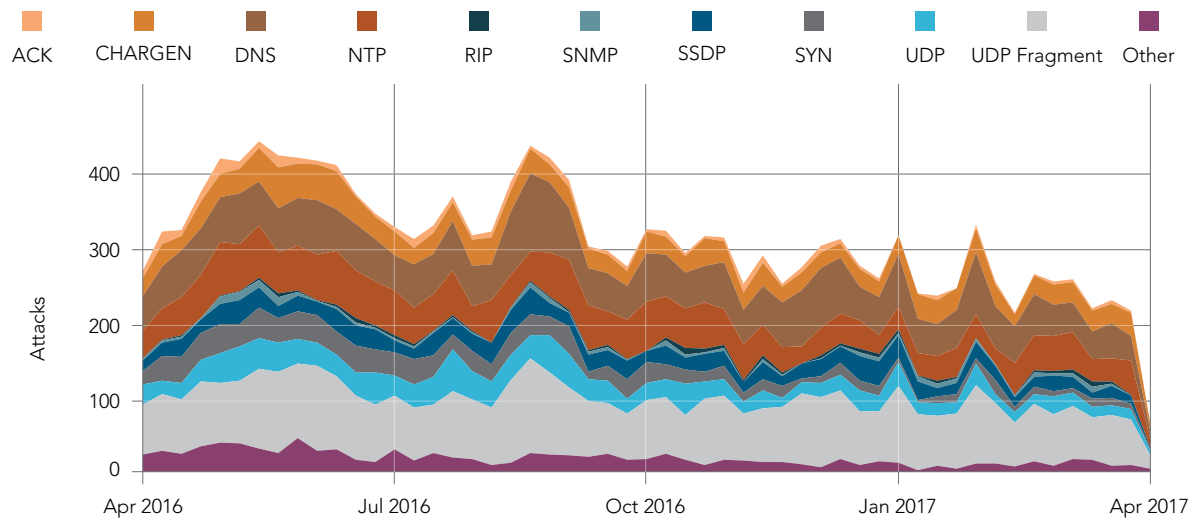


Figure 2-2: Attack traffic for the 10 most frequent attack vectors shows reflection attacks, such as NTP and CHARGEN, continue to generate large amounts of DDoS traffic

In looking at the 10 most frequent attack vectors per week, we see ACK, CHARGEN, and DNS in the top three, with NTP taking fourth place in the list.

One item of note, that's unfortunately consistent, is the presence of CHARGEN on the list. CHARGEN traffic rose to 11% of DDoS attack traffic in Q4, up from 8% in the previous quarter. This protocol is used as a diagnostic port on printers and this service should not be exposed to the Internet at large.

The percentage of the Internet attack traffic related to NTP was relatively flat this quarter; the .5% change in traffic is well within our margin of error. This attack vector can be utilized by attackers to amplify their DDoS attacks. It is not outside of the realm of possibility to posit that this will result in a correlation with the rise of IoT-related botnet platforms — the rationale being that it will only be a matter of time before attackers can implement this in their platforms.

Several individuals from some of the criminal organizations responsible for the day-to-day operations and upkeep of these attack platforms have been incarcerated. Incarcerations alone may not limit the number of attacks in the long term as other operators will likely fill the void. This is especially true when one considers that there is money to be made from facilitating these attacks as a service offering.

2.2 / Mega Attacks / The mega attacks — those over 100 Gbps — were in shorter supply in the first quarter of 2017. While this may result in a drop in the number of attacks, the reduction could be short-lived. Several large DDoS crews were arrested in the waning days of 2016, which could be linked to the drop in mega attacks.

Another contributing factor to the drop in large attacks could be the evolving use cases for botnets like Mirai. As an example, attackers have created a proof of concept that uses the Mirai botnet for Bitcoin mining[6]. While this activity might seem clever on the surface, there's little benefit to the attackers; the IoT devices employed by the Mirai botnets do not have the requisite computing power to mine Bitcoins effectively. Despite the botnet being an inefficient Bitcoin mining tool, this may be an indicator that Mirai and other botnets may be used for a diverse set of purposes in the future.

2.3 / Attack Spotlight: Mirai DNS Water Torture Attack Summary / Akamai observed a series of DDoS attacks leveraging the Mirai DNS Water Torture Attack. DDoS attacks using this DNS query vector were first observed on Jan. 11, 2017, targeting several Akamai customers in the financial services industry. The attack activity began with five consecutive days of attacks, followed by a four-day reprieve before concluding with a final attack on Jan. 20. Aside from UDP and TCP attacks observed on Jan. 12, all the other attacks were Mirai DNS query floods.

Payload Samples / The Mirai DNS Water Torture Attack follows normal DNS recursion paths. As a result, the attacker cannot select a specific IP address at the target site.

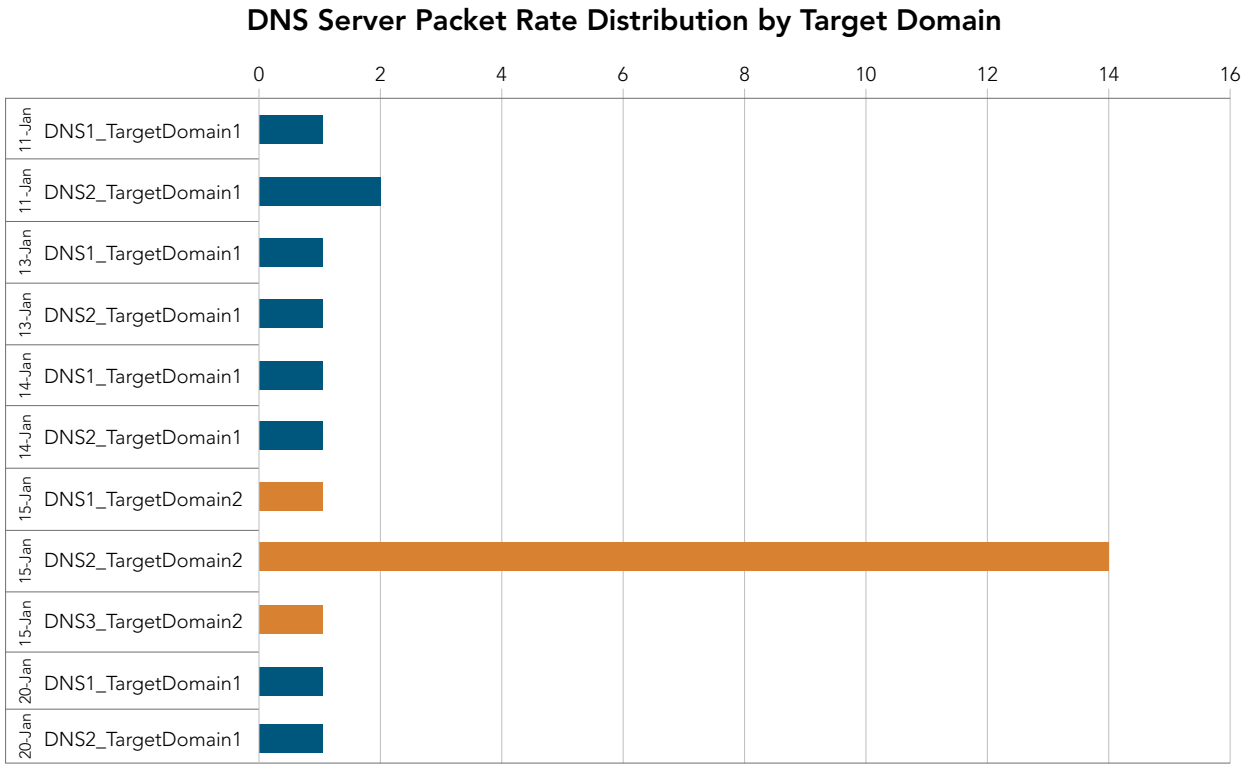


Figure 2-3: Peak packet rates observed on DNS servers receiving Mirai DNS attacks reached a high of 14 Mpps on Jan. 15, 2017

Most of the DNS servers received queries at a fairly even rate during the attack, with the exception of an attack observed on Jan. 15, when one of three DNS servers received 14 Mpps of attack traffic, as opposed to the 1-2 Mpps other DNS servers received. The queries observed during these attacks aligned with the Mirai DNS Water Torture Attack.

The sample payload signatures in Figure 2-4 represent a flood of queries, each containing a random 12-character subdomain string. The IP addresses and targeted domains have been redacted.

```
DNS Query Flood (Mirai DNS Water Torture Attack)
08:10:13.574610 IP x.x.x.x.47565 > x.x.x.x.53: 10077 [1au] A? e4hob2e7w1t7.<redacted>. (xx)
08:10:13.591581 IP x.x.x.x.52465 > x.x.x.x.53: 15764 [1au] A? sjjbm0s2ov00.<redacted>. (xx)

06:50:44.189382 IP x.x.x.x.49326 > x.x.x.x.53: 63481% [1au] A? io1f786uo3bd.<redacted>. (xx)
06:50:44.189429 IP x.x.x.x.40566 > x.x.x.x.53: 12345% [1au] A? 0hagnikgj2vq.<redacted>. (xx)

11:14:10.707489 IP x.x.x.x.37569 > x.x.x.x.53: 25550% [1au] A? 1hartrmnaiew.<redacted>. (xx)
11:14:10.709341 IP x.x.x.x.22945 > x.x.x.x.53: 31835% [1au] A? c7wnmqek2eww.<redacted>. (xx)

04:56:19.326305 IP x.x.x.x.4210 >  x.x.x.x.53: 47369% [1au] A? lmjtjgfh7b6j.<redacted>. (xx)
04:56:19.326315 IP x.x.x.x.36408 > x.x.x.x.53: 36684% [1au] A? 2vfedrv6aha5.<redacted>. (xx)

11:48:43.171738 IP x.x.x.x.47645 > x.x.x.x.53: 59218 [1au] A? 02uqhuovfi1f.<redacted>. (xx)
11:48:43.171749 IP x.x.x.x.47371 > x.x.x.x.53: 62949 [1au] A? qo5etoh5foab.<redacted>. (xx)
```

Figure 2-4: Payload of DNS query flood, called the Mirai DNS Water Torture attack, with the target domain names redacted

On Jan. 12, malicious actors changed tactics. After a day of DNS query floods, the attackers began attacking a DNS server directly with a UDP flood, as shown in Figure 2-5. They also made use of one of Mirai's TCP flood attacks on TCP port 443, a port commonly used for transmission of encrypted web traffic. This type of Mirai attack is called Mirai TCP STOMP.

```
UDP Flood – Port 53
06:17:36.688058 IP (tos 0x0, ttl 51, id 54282, offset 0, flags [DF], proto UDP (17), length 540)
    x.x.x.x.59242 > x.x.x.x.53: 56019 stat+ [b2&3=0x1786] [2646a] [49544q] [26389n] [1379au]
[|domain]
06:17:36.688063 IP (tos 0x0, ttl 52, id 24494, offset 0, flags [DF], proto UDP (17), length 540)
    x.x.x.x.44026 > x.x.x.x.53: 55693 updateA+ [b2&3=0x4b01] [24342a] [13221q] [35165n]
[62407au] Type60358 (Class 50264)? M-^_M-sM-?M-xM-hM-^KM-bM-'M-?^V^I^YM-4TTFM-~xwy^T^IM-J^X-
a^vM-6M-g[M-^GM-UM-3a7M-^\M-CIM-5M-^L"M-^Z0~^UM-<snip>[|domain]

Push Flood (Mirai TCP STOMP) – Port 443
08:18:32.564571 IP (tos 0x0, ttl 54, id 34074, offset 0, flags [DF], proto TCP (6), length 808)
    x.x.x.x.38403 > x.x.x.x.443: Flags [P.], cksum 0x4768 (correct), seq 535625728:535626484, ack
1, win 22263, options [[bad opt]
08:18:32.564735 IP (tos 0x0, ttl 54, id 24701, offset 0, flags [DF], proto TCP (6), length 808)
x.x.x.x.38403 > x.x.x.x.443: Flags [P.], cksum 0x0dc9 (correct), seq 535887872:535888628, ack 1,
win 22263, options [[bad opt]
```

Figure 2-5: The signatures of UDP and TCP vectors used when attackers changed tactics on Jan. 12, 2017

The UDP flood was observed against two destination IP addresses, one of which was a DNS server previously under attack from the DNS query flood. The signatures contained the standard Mirai UDP flood, using 512 byte payloads; however, they first appeared to be DNS because Port 53 was used as the the target. The other signature was a PUSH Flood set to target port 443. This type of attack completes the TCP three-way handshake prior to sending a flood of padded TCP packets. The extra data padding results in higher peak bandwidth consumption with lower packet rates — in this case the attack peaked at 120 Gbps.

Conclusion / Given the risk posed by the Mirai DNS query flood attack, all DNS servers responding for a targeted domain should be protected. Some organizations may be capable of serving this malicious traffic in addition to their normal load of legitimate queries. But even in those cases, the flood of requests puts unnecessary load on DNS systems, which often run at the edge of their capabilities. In some cases an external DNS provider is required in order to have sufficient response capabilities. Even in the case of an external provider, it can make sense to have redundant providers, a point several of last year's attacks drove home.

DDoS protection should take DNS load distribution into account. Be aware that bots may cluster within regions where vulnerable devices reside. If regional balancing is in effect, the malicious traffic may not be desirably distributed during an attack. Vectors, techniques, or targets may vary throughout the DDoS campaign. Any organization could find itself under threat of DDoS, regardless of industry. Attention needs to be given to assets that could be attacked and may be vulnerable, in addition to assets that have been attacked in the past. It's best to ensure that DDoS mitigation is in place before an attack.

DNS WATER TORTURE

DNS Water Torture / Mirai has been known to produce a specific DNS query flood. Although DNS query attacks are not as common as DNS reflection attacks, this DNS query flood can potentially cause more damage than current DNS reflection attacks. If a targeted DNS server is unprepared for a sustained flood of queries with high packet rates, DNS Water Torture can lead to a denial of service for legitimate users.

How it works / The Mirai DNS query flood does not use reflection or spoofing techniques, nor does it allow attackers to specify a target IP address. Instead, it accepts a domain name as the target for a DNS cache-busting flood. A randomized 12-character alphanumeric subdomain is prepended to the target domain. The attacking bots send their queries to their locally-configured DNS servers, which are typically DNS servers at local ISPs (Internet Service Provider). The randomized sub-domain is present to ensure that no intermediate recursive DNS server would have the response for that name cached locally. Since the response cannot have been cached, every query follows the usual path until it reaches an authoritative DNS server, the real target of the attack.

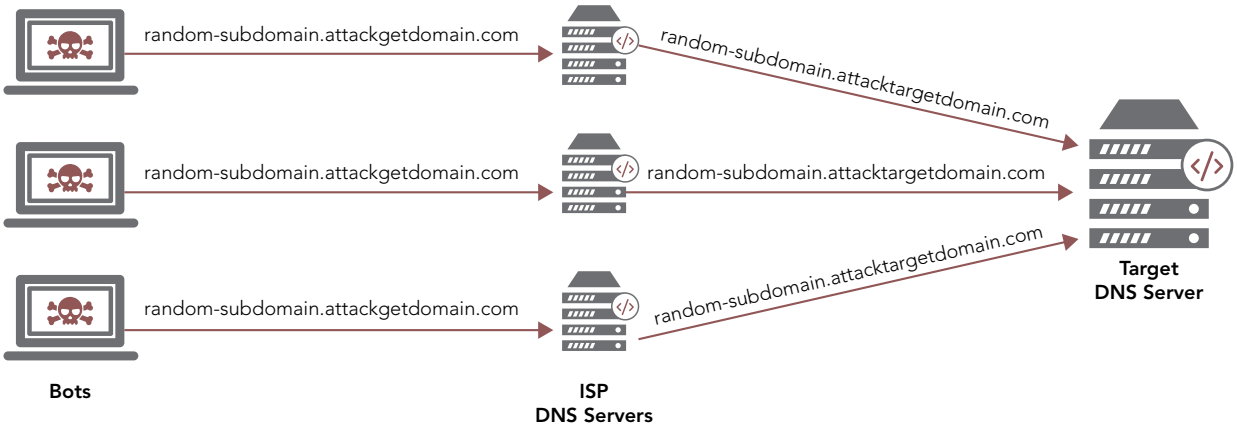


Figure 2-6: Mirai DNS attack queries are sent from bots to their local DNS servers and on to the target authoritative DNS servers

Aside from the randomized subdomain string, the queries appeared to the target authoritative DNS servers as queries from local ISP DNS servers. The full source IP addresses of the bots sending these queries were not visible.

Akamai SIRT has reproduced and tested Mirai's DNS query attack, using live malware samples from the initial documented attacks. The attack supports several customizable values as shown in Figure 2-7.

Customizable Field	Default Value	Custom Value
ToS	0	1
ID	random	1
TTL	64	123
DF	false	5
SPort	random	31337
DPort	53	8008
Domain	(user supplied)	attacktargetdomain.com
DNS ID	random	1

Figure 2-7: Customizable fields for the Mirai DNS query attack, known as the DNS Water Torture attack

Attack signatures are summarized in Figure 2-8, first with default values and then with custom values.

This attack vector was observed by Akamai SIRT in January 2017 against Akamai customers within the financial services industry.

```
Examples of DNS Parameters and Resulting Traffic:

Default DNS attack traffic with no parameters besides target domain.

00:40:40.611489 IP (tos 0x0, ttl 64, id 52446, offset 0, flags [none], proto UDP (17), length 73)
    x.x.x.x.17517 > x.x.x.x.53: 3644+ A? m3hk3nr6njv0.attacktargetdomain.com. (45)
00:40:40.611490 IP (tos 0x0, ttl 64, id 60934, offset 0, flags [none], proto UDP (17), length 73)
    x.x.x.x.43103 > x.x.x.x.53: 19269+ A? htuhwake2bkg.attacktargetdomain.com. (45)

DNS attack with all values customized.
* DNS ID value @ 0x0010 column 7, traffic shown in hex format to allow highlighting

00:48:58.620735 IP (tos 0x1,ECT(1), ttl 123, id 1, offset 0, flags [DF], proto UDP (17), length 73)
    x.x.x.x.31337 > x.x.x.x.8008: UDP, length 45
        0x0000:  4501 0049 0001 4000 7b11 7af1 c0a8 01e6  E..I..@.{.z.....
      * 0x0010:  c0a8 017a 7a69 1f48 0035 fcc2 0001 0100  ...zzi.H.5......
        0x0020:  0001 0000 0000 0000 0c6a 6976 3868 7475  .........jiv8htu
        0x0030:  6877 616b 650a 7468 652d 7669 6374 696d  hwake.attacktargetdomain
        0x0040:  0363 6f6d 0000 0100 01                   .com.....

00:48:58.620738 IP (tos 0x1,ECT(1), ttl 123, id 1, offset 0, flags [DF], proto UDP (17), length 73)
    x.x.x.x.31337 > x.x.x.x.8008: UDP, length 45
        0x0000:  4501 0049 0001 4000 7b11 7af1 c0a8 01e6  E..I..@.{.z.....
      * 0x0010:  c0a8 017a 7a69 1f48 0035 ef4c 0001 0100  ...zzi.H.5.L....
        0x0020:  0001 0000 0000 0000 0c32 626b 6733 736e  .........2bkg3sn
        0x0030:  7276 3061 730a 7468 652d 7669 6374 696d  rv0as.attacktargetdomain
        0x0040:  0363 6f6d 0000 0100 01                   .com.....
```

Figure 2-8: Attack signatures of the Mirai DNS Water Torture attack using default and custom values respectively

2.4 / Reflection Attacks / Reflection attacks continued to dominate DDoS activity. As in the previous quarter, DNS, NTP, and CHARGEN remained as the top three attack vectors, as shown in Figure 2-9. Their continued use is a symptom of subpar system and network hygiene. The steps needed to close these vulnerabilities are known and often inexpensive. The long-term health of the Internet would benefit from learning what factors lead organizations that own these systems to allow the reflection vulnerabilities to persist.

Organizations should review the scalability of their DNS infrastructure. If your primary DNS is self-hosted and it goes down, then your customers would be unable to find your website or contact you via email. Having a secondary or even tertiary DNS provider can help keep your systems available.

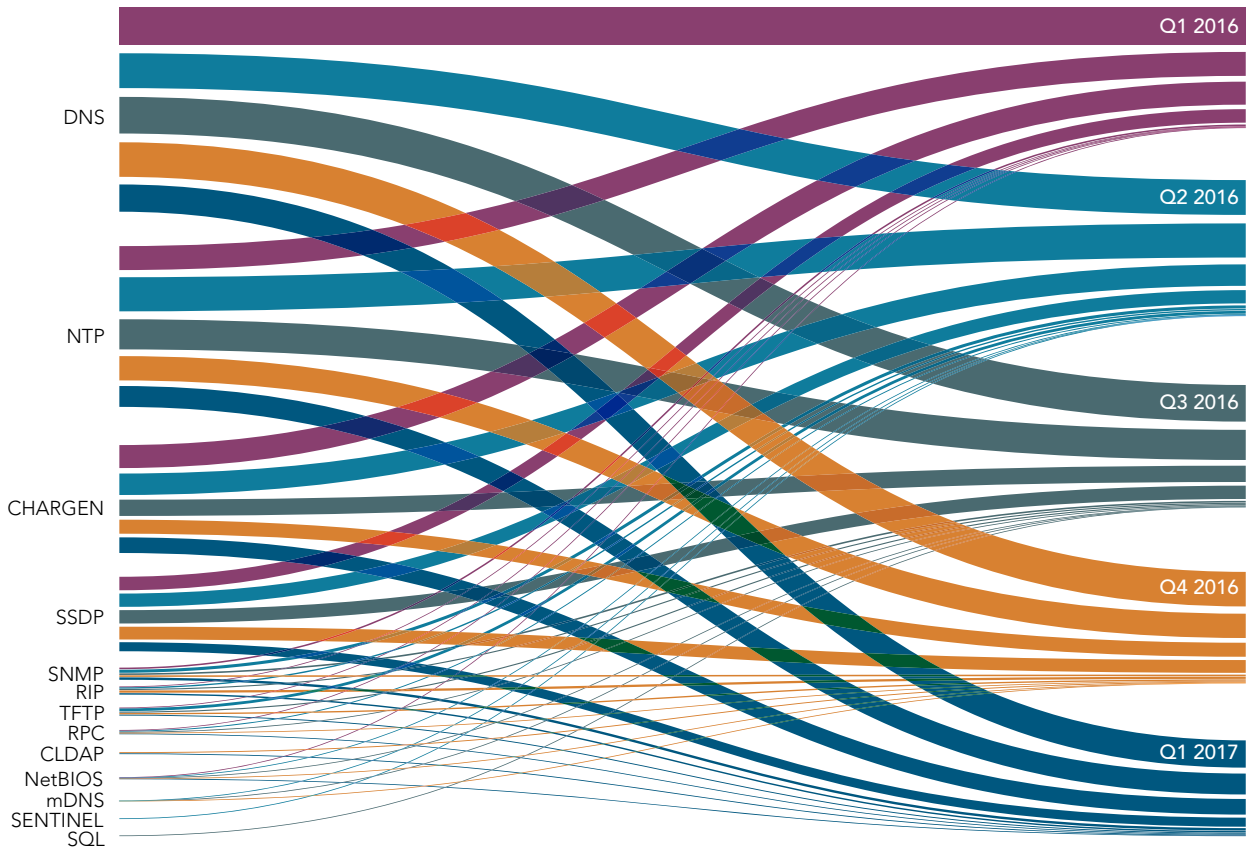


Figure 2-9: Reflection techniques continued to dominate DDoS attacks in Q1 2017 and were used in 57% of attacks

Autonomous System Numbers (ASN) designate the ISP responsible for originating the traffic and give more detail than country level statistics. Chinese ASN 4837 produced more reflection DDoS sources in Q1 2017 than the next closest ASN in Argentina. All together, the top ten reflection source ASNs accounted for 30% of the reflection DDoS sources. This analysis does not examine the density of attacks compared to the population, it shows the raw number of attacks from each ASN regardless of size.

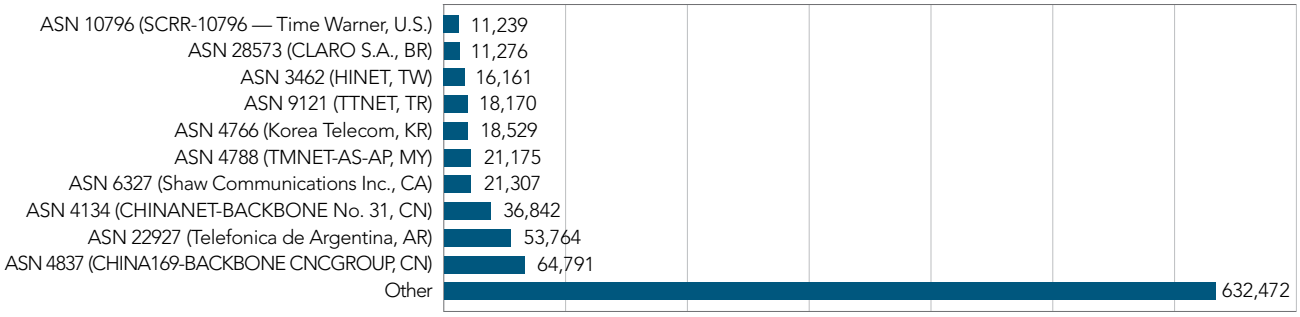


Figure 2-10: ASN 4837, in China, had the most reflection sources and ASN 22927, in Argentina, was second

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 uses many small devices. Use of the SSDP attack vector increased this quarter, perhaps due to attackers turning to the DDoS resources presented by IoT devices.

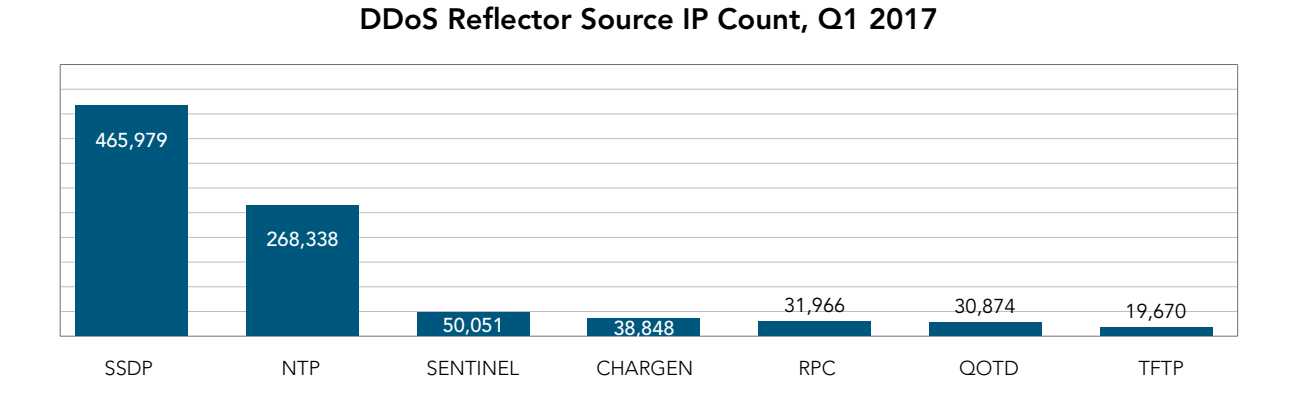


Figure 2-11: The most-used reflectors in Q1 2017 were SSDP and NTP

In Q1 2017, the use of reflectors in DDoS attacks maintained nearly the same proportions as in Q4 2016, with the notable addition of Sentinel to the top three. The number of Sentinel reflectors increased by 39% in comparison to Q4 of 2016. Sentinel reflection sources include powerful servers with high bandwidth availability, such as university servers.

SSDP reflectors continued to be the major source of DDoS reflection attacks in this quarter. The use of SSDP reflection can be directly linked to the rise of IoT botnets and the growing number of Internet-accessible consumer grade devices. These botnets are using SSDP reflectors to amplify the traffic they generate, further increasing the threat they pose.

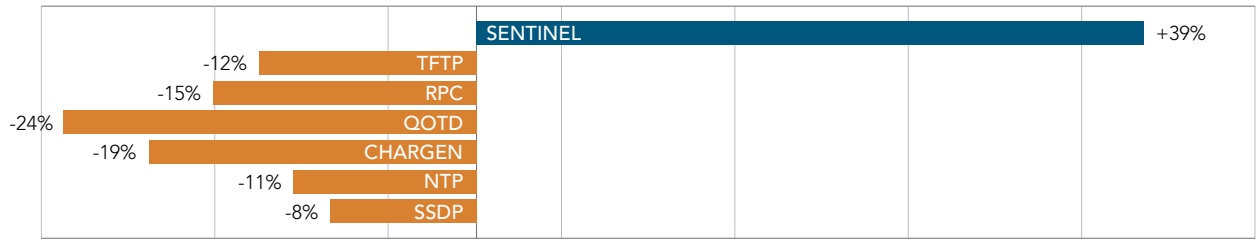


Figure 2-12: The use of Sentinel reflectors increased 39% over the previous quarter, while the use of all other reflector sources dropped 8% to 24%

Figure 2-13 shows changes in DDoS attack traffic since January 2015. The color of the dots represents how many attacks of a certain size occurred each week; the brighter colors represent a higher concentration of attacks. This plot uses a logarithmic scale, so the difference in bandwidth increases ten-fold between each major horizontal line. As a result, the attacks on the lower end of the scale appear to be more spread out, but they are actually more closely clustered numerically than attacks on the high end of the scale. The rising number of low-bandwidth attacks seen weekly is the primary reason the median size of attacks has trended downward since the beginning of 2015.

The black line represents the median (half are smaller, half are larger) attack size for each time period. In January 2015, the median attack size was 3.9 Gbps, but by the end of March 2017, the median attack size had fallen to 520 Mbps. This decline was caused in part by an overall increase in the number of weekly attacks seen by Akamai, the majority of which were smaller attacks. Growth in the number of small attacks has a more significant effect on the median than the slower growth in the number of large attacks.

The solid blue and solid red lines represent the 25th and 75thpercentile of attacks. As of March, half of all volumetric attacks seen by Akamai were between 243 Mbps and 1.3 Gbps. The dotted lines show the 5th and 95th percentiles and indicate that 90% of all attacks were between 28 Mbps and 4.8 Gbps. These ranges have long been trending closer to the median line over time, driven by an increased number of attacks since the beginning of 2015.

How does this affect enterprises? If an organization has defenses that can withstand 1.3 Gbps of volumetric DDoS attack traffic directed at its infrastructure, then it should be able to withstand 75% of current DDoS attacks. However, if the organization's uptime goals are such that it needs to withstand 95% of attacks, those defenses would need to be able to absorb an attack of 5 Gbps or more.

Even with that level of defense in place, it is important to understand that there are still a significant number of outliers — DDoS attacks generating more than 100 Gbps of traffic are common enough to be a concern.

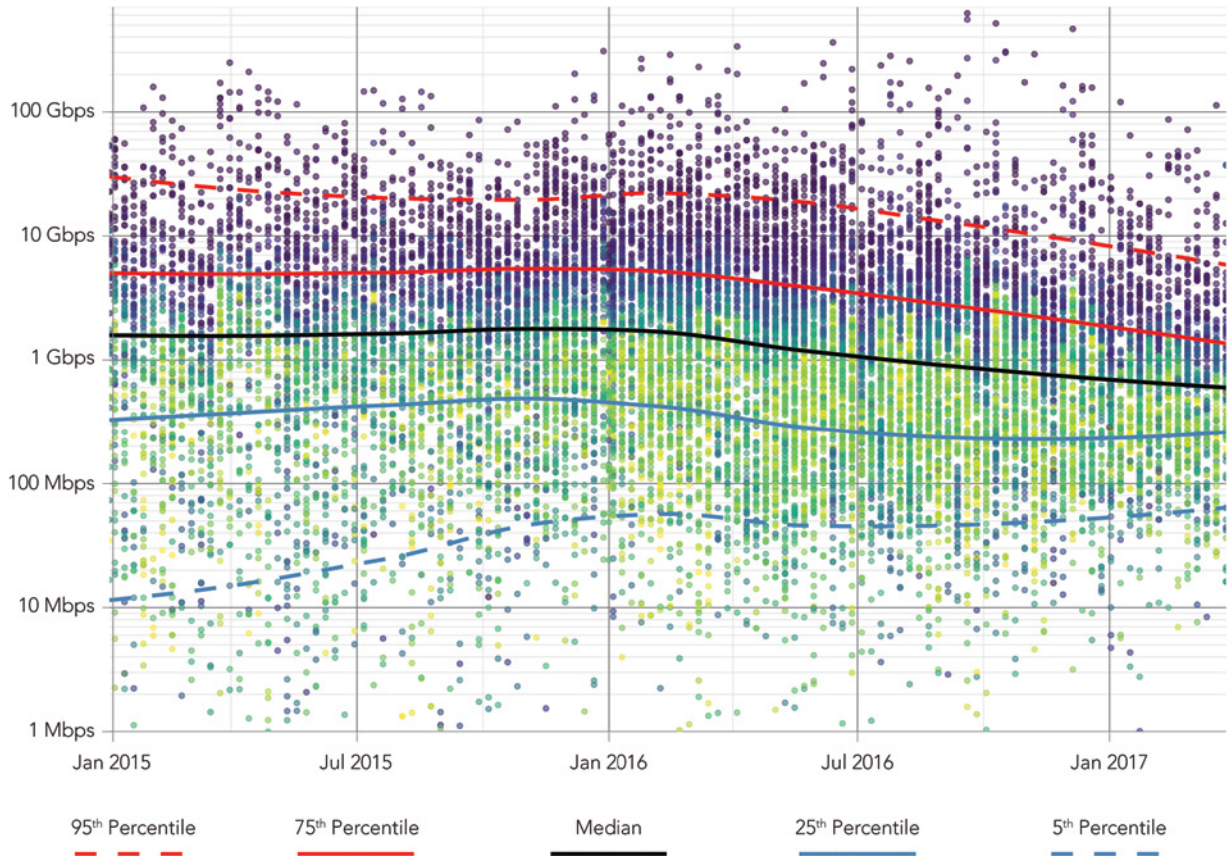


Figure 2-13: The median size of attacks has trended downward since 2016 due to an increase in the number of lower-bandwidth attacks

[SECTION]3 WEB APPLICATION ATTACK ACTIVITY

Web application vectors tend to be troublesome attack types seen across the platform. They can have a longer lasting impact than merely causing network availability outages, which we see from infrastructure-related DDoS attacks.

3.1 / Web Application Attack Vectors / We see similar patterns in the top attack types used against web applications from quarter to quarter. The top three attack vectors in Q1 of 2017 were SQLi, LFI, and XSS, as shown in Figure 3-1. These attacks continue to dominate, as they work more often than not against unprotected websites. Conversely, if your website protections are not actively blocking this sort of traffic, there is a greater risk that these sorts of attacks potentially impact your organization.

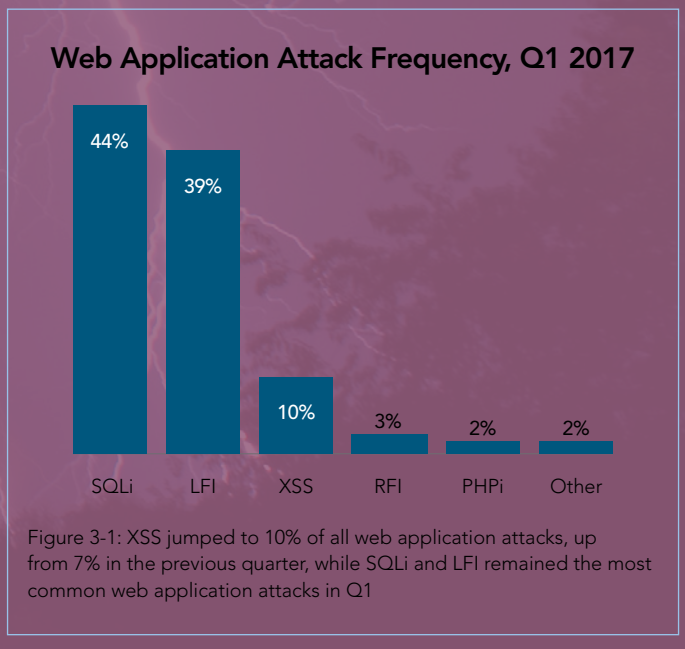
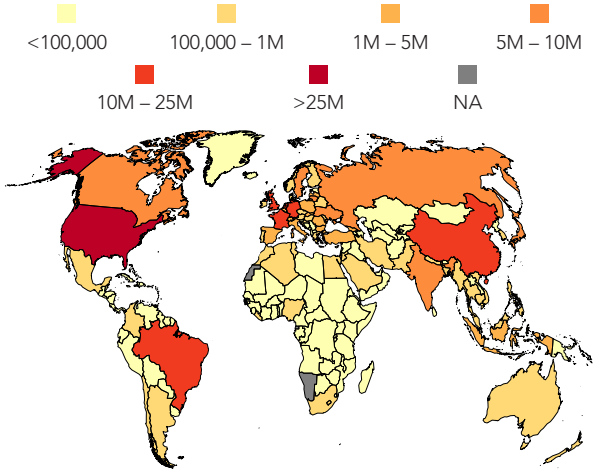


Figure 3-1: XSS jumped to 10% of all web application attacks, up from 7% in the previous quarter, while SQLi and LFI remained the most common web application attacks in Q1

3.2 / Top 10 Source Countries / The top five source countries for web application attacks in Q1 2017 were the U.S., Netherlands, Brazil, China, and Germany, as shown in Figure 3-2. For the second quarter row, Canada came in 11th place. With a small population density, it would be interesting to dig deeper into the Canadian traffic. U.S. holding on to the top position was unsurprising, but the consistent amount of attack traffic that ostensibly originated from the Netherlands is curious. This represents a large proportion of attacks from a country of only 17 million citizens. In comparison, the U.S. has just over three times the number of attacks with nearly twenty times the population.

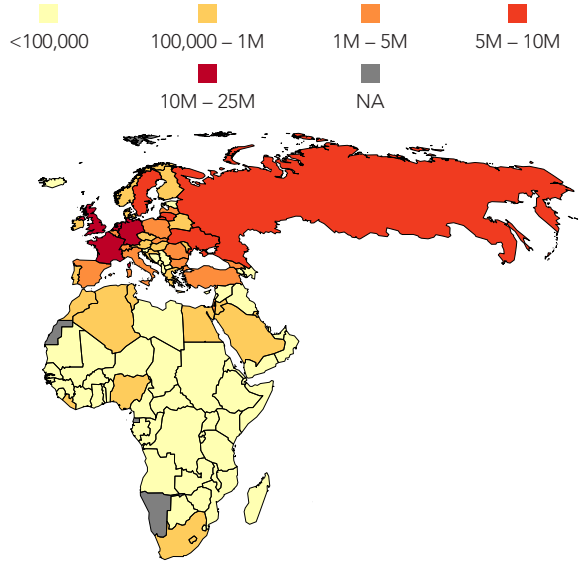
Global Web Application Attack Source Countries, Q1 2017



Country	Attacks Sourced	Percentage
U.S.	117,978,342	34.0%
Netherlands	43,925,118	12.7%
Brazil	28,027,292	8.1%
China	18,963,654	5.5%
Germany	16,035,037	4.6%
France	15,236,624	4.4%
U.K.	10,253,814	3.0%
Russia	8,262,292	2.4%
Ukraine	7,123,491	2.1%
Lithuania	6,566,703	1.9%

Figure 3-2: Worldwide, the U.S. continued as the top source of web application attacks at 34%, up from 28% in the previous quarter, while the Netherlands, in second, dropped to 13% from 17%

Web Application Attack Source Countries—EMEA, Q1 2017

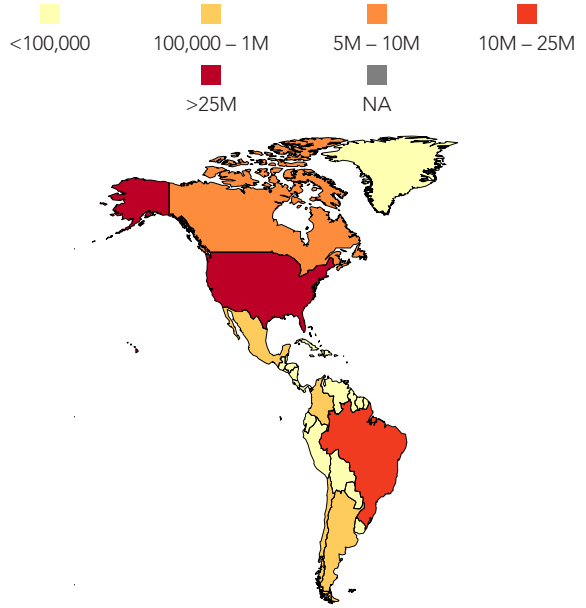


Country	Attacks Sourced	Global Rank
Netherlands	43,925,118	2
Germany	16,035,037	5
France	15,236,624	6
U.K.	10,253,814	7
Russia	8,262,292	8

Figure 3-3: The Netherlands continued as the top source for web application attacks sourced in EMEA

As demonstrated in Figure 3-5, China was the overall top source country for web application attacks in the Asia-Pacific region. Attack traffic from China increased by a third from last quarter, which cemented its place within Asia, and moved it up to fourth place worldwide.

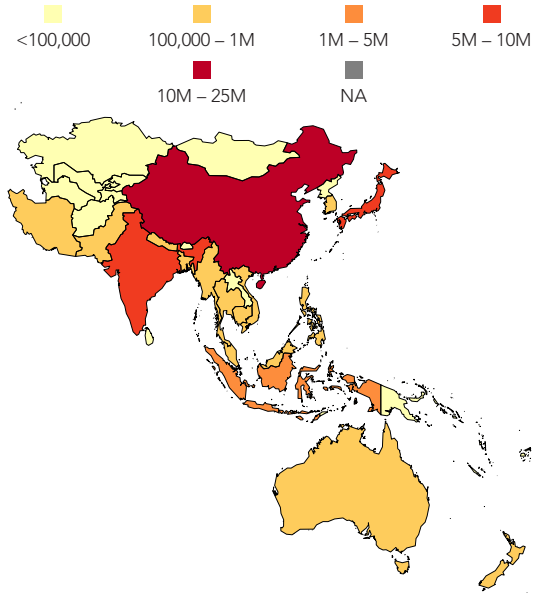
Web Application Attack Source Countries—Americas, Q1 2017



Country	Attacks Sourced	Global Rank
U.S.	117,978,342	1
Brazil	28,027,292	3
Canada	6,280,383	11
Mexico	664,477	39
Argentina	398,208	50

Figure 3-4: The U.S., Brazil, and Canada, respectively, continued as the top three sources of web application attacks in the Americas

Web Application Attack Source Countries—Asia Pacific, Q1 2017



Country	Attacks Sourced	Global Rank
China	18,963,654	4
India	6,150,881	12
Japan	5,839,869	13
Singapore	4,285,527	15
Indonesia	3,248,604	17

Figure 3-5: China topped the list for web application attacks in Asia Pacific, with India and Japan in the second and third spots, respectively

3.3 / Top 10 Target Countries / The U.S. continues to be the largest target of attack traffic, with Brazil in second place for the second quarter in a row and the United Kingdom rounding out the top three. Attacks targeting the U.S. were down 9%, while Brazil saw a nearly 46% increase in web application attacks against their properties and the U.K. a 30% gain in attacks. Both China and Canada have fallen from the top 10 list this quarter, replaced by Spain and Singapore, which have both been on this list in the past. While these swings appear significant, they are within the norms we generally see for such traffic.

Top 10 Target Countries for Web Application Attacks, Q1 2017

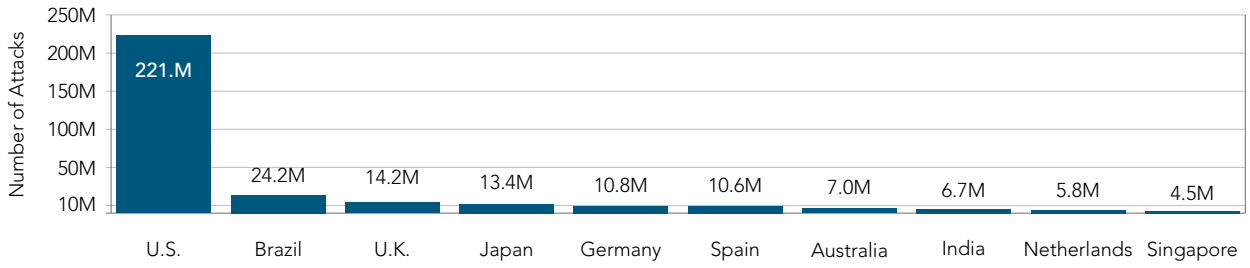


Figure 3-6: The vast majority of targets of web application attacks were in the U.S.

[SECTION]4
LOOKING FORWARD

The number of DDoS attacks has fallen in the last year, but have the risks been reduced as well? The answer is arguably no. If anything, the risks to the Internet as a whole and to targeted businesses in particular have both risen. Given the growth in capability of high-end attackers, the damage a sustained DDoS attack could cause increases daily. More and more often, it's not just the target that has to be concerned — other organizations may be affected by collateral damage from large DDoS attacks.

The size of the largest DDoS attacks jumped in 2016. Previously, the largest DDoS attacks were in the range of 100 Gbps, growing to 300 Gbps in first half of 2016, and finally into the 500-600 Gbps range in the third quarter, driven by Mirai. In addition to the attacks observed by Akamai, other organizations have seen DDoS attacks exceeding 1 Tbps. But the Mirai botnet is not only responsible for these large attacks — it's being used extensively in DDoS attacks of all sizes.

Attacks of this size easily overload the networks of their targets. In addition, they pose a problem for upstream networks that might not be able to handle the traffic, causing a multitude of organizations to be overwhelmed. It's like a crowded entry to a concert venue; a normal load might cause some headache, but the largest audiences not only overwhelm the venue, they also overflow into the roads and highways surrounding the area, affecting businesses and households for miles around. Instead of roads, it's the local loops and provider interconnects that are overwhelmed, unable to carry network traffic to organizations unlucky enough to be in the same region as the target.

Most botnets are not a single entity. For example, there are many Mirai-derived botnets using similar software, each a small fragment and distinct entity. There is constant fighting for control of the end nodes that comprise the botnets and the largest attacks are generally only seen when multiple distinct botnets target the same organization at once. One concern is that a unified command and control (C2) structure could emerge, either due to a new zero-day vulnerability or a takeover of the C2s of other similar botnets. Given the current capabilities of Mirai, such a super botnet could generate a DDoS attack of two Tbps in the near future. Additionally, Mirai's attacks are currently limited by the level of connectivity in their local networks. If these networks gain unfettered Internet access, the devices could be capable of emitting 20 times more attack traffic than we've seen to date.

The security community is taking measures to combat Mirai and other IoT-based botnets. As mentioned in the Emerging Trends section, Europol is helping coordinate global efforts to arrest the owners of the offending botnets. Some ISPs are taking measures to null route C2 traffic from botnets, dumping the bits before they leave the local network. Service providers and researchers are working to gain more insight into the structure of Mirai, in an attempt to limit its ability to spread and cause more damage.

It's short sighted to think of Mirai as the only threat, though. With the release of the source code, any aspect of Mirai could be incorporated into other botnets. Even without adding Mirai's capabilities, there is evidence that botnet families like BillGates, elknot, and XOR are mutating to take advantage of the changing landscape. In particular, the BillGates botnet family included the most recent Struts vulnerability[7] in its toolkit, very soon after the vulnerability was made public.

Finally, it's important to recognize that DDoS and the other threats from IoT are just one aspect of the threat landscape. Future *State of the Internet / Security* reports will examine traffic being sent to the APIs of web servers and explain how it could be an overlooked area of concern. Organizations may monitor the login page logs of their sites, but are they watching the traffic for their APIs? Site-to-site and business-to-business APIs may be a bigger target than most realize.

[SECTION]5 CLOUD SECURITY RESOURCES

5.1 / CLDAP DDoS Threat Advisory / On Oct. 14, 2016, the Akamai Security Operation Center (SOC) began mitigating attacks for what was suspected to be Connection-less Lightweight Directory Access Protocol (CLDAP) reflection. This new reflection and amplification method has since been confirmed by the Akamai SIRT and has been observed producing DDoS attacks, comparable to DNS reflection with most attacks exceeding 1 Gbps.

Similar to many other reflection and amplification attack vectors, CLDAP attacks would not be possible if proper ingress filtering was in place. Potential hosts are discovered using Internet scans. Filtering UDP destination port 389 can prevent CLDAP servers from being discovered and added to the attacks. Since October 2016, Akamai has detected and mitigated 50 CLDAP reflection attacks. Of those 50 attacks, 33 were single vector attacks using CLDAP reflection exclusively.

This ***advisory*** covers the distribution of these sources, methods of attack, and target industries observed.

Errata / Due to an error in the calculations for the maps and data for Figure 3-5: Web Application Attack Source Countries — Asia Pacific, Q4 2016 was missing data for Singapore. Singapore was the source of 1,644,483 attack events in Q4, which ranked it in fourth place for the Asia-Pacific region and 19th worldwide.

Endnotes /

[1] *https://www.extremetech.com/internet/247521-mirai-infamous-iot-botnet-now-forces-smart-appliances-mine-bitcoin*

[2] *https://arstechnica.com/security/2017/04/brickerbot-the-permanent-denial-of-service-botnet-is-back-with-a-vengeance/*

[3] *http://www.bankinfosecurity.com/ddos-for-hire-israel-arrests-two-suspects-a-9392*

[4] *https://www.grahamcluley.com/ddos-hire-arrests-europol-fbi/*

[5] *https://www.akamai.com/us/en/about/our-thinking/threat-advisories/connection-less-lightweight-directory-access-protocol-reflection-ddos-threat-advisory.jsp*

[6] *http://blog.erratasec.com/2017/04/mirai-bitcoin-and-numeracy.html#.WPoE3FPysSM*

[7] *https://blogs.akamai.com/2017/03/vulnerability-found-in-apache-struts.html*

***State of the Internet / Security* Team**
Martin McKeay, Senior Security Advocate, Senior Editor
Jose Arteaga, Akamai SIRT Lead, Data Wrangler — Attack Spotlight, DNS Water Torture
Amanda Fakhreddine, Editor
Dave Lewis, Senior Security Advocate — DDoS Activity, Web Application Attack Activity
Chad Seaman, Akamai SIRT — Attack Spotlight, DNS Water Torture
Wilber Mejia, Akamai SIRT — Attack Spotlight
Elad Shuster, Security Data Analyst, Threat Research Unit
Jon Thompson, Custom Analytics

Special thanks to Wendy Nather, Principal Security Strategist, Duo Security, for contributing to this quarter's report and to Jay Jacobs, Cyentia Institute, for his work on Figure 2-13: Attack Density and Trends

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*.
