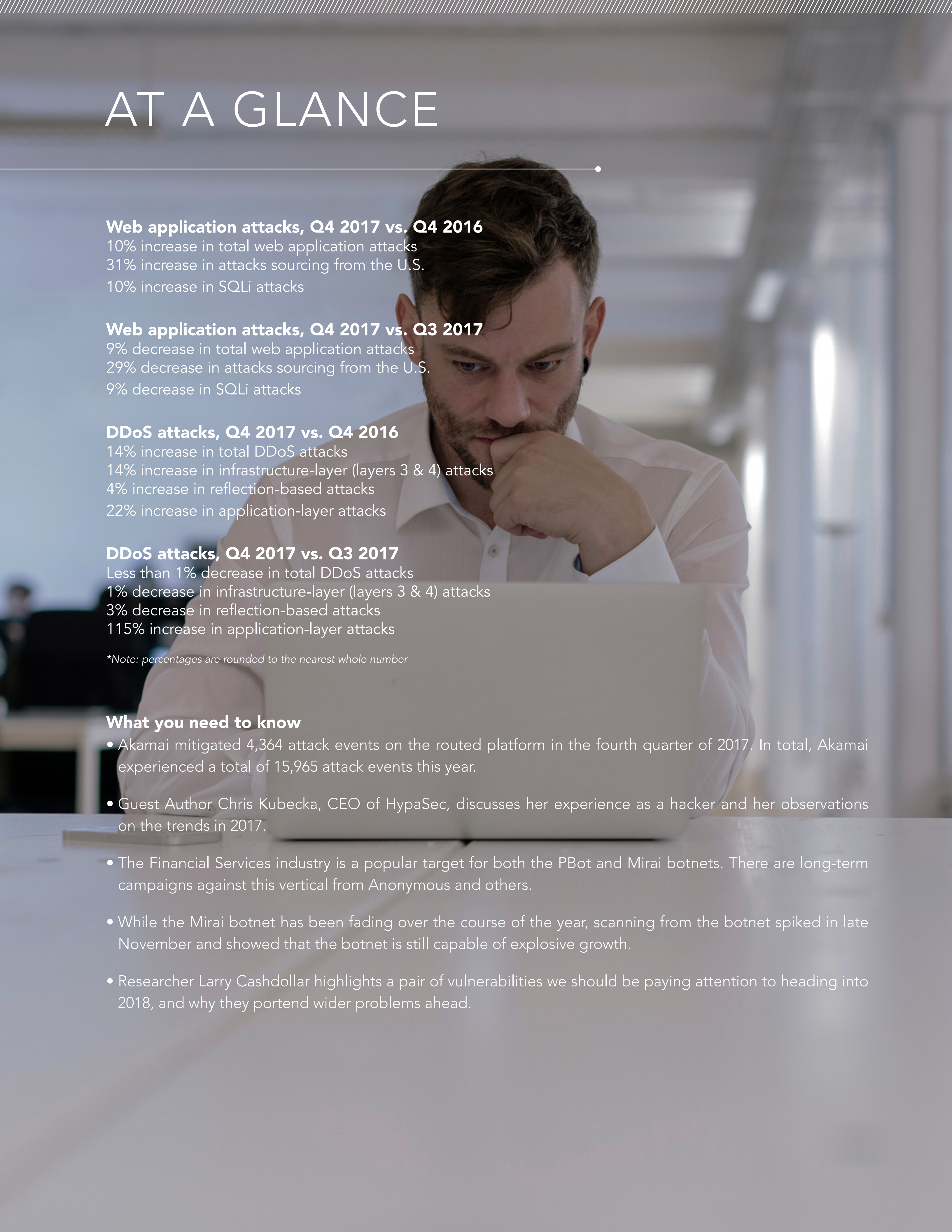
[Volume 4 / Number 4]

[state of the internet] / security

Q4 2017 Report



AT A GLANCE

Web application attacks, Q4 2017 vs. Q4 2016
10% increase in total web application attacks
31% increase in attacks sourcing from the U.S.
10% increase in SQLi attacks

Web application attacks, Q4 2017 vs. Q3 2017
9% decrease in total web application attacks
29% decrease in attacks sourcing from the U.S.
9% decrease in SQLi attacks

DDoS attacks, Q4 2017 vs. Q4 2016
14% increase in total DDoS attacks
14% increase in infrastructure-layer (layers 3 & 4) attacks
4% increase in reflection-based attacks
22% increase in application-layer attacks

DDoS attacks, Q4 2017 vs. Q3 2017
Less than 1% decrease in total DDoS attacks
1% decrease in infrastructure-layer (layers 3 & 4) attacks
3% decrease in reflection-based attacks
115% increase in application-layer attacks

**Note: percentages are rounded to the nearest whole number*

What you need to know

- Akamai mitigated 4,364 attack events on the routed platform in the fourth quarter of 2017. In total, Akamai experienced a total of 15,965 attack events this year.
- Guest Author Chris Kubecka, CEO of HypaSec, discusses her experience as a hacker and her observations on the trends in 2017.
- The Financial Services industry is a popular target for both the PBot and Mirai botnets. There are long-term campaigns against this vertical from Anonymous and others.
- While the Mirai botnet has been fading over the course of the year, scanning from the botnet spiked in late November and showed that the botnet is still capable of explosive growth.
- Researcher Larry Cashdollar highlights a pair of vulnerabilities we should be paying attention to heading into 2018, and why they portend wider problems ahead.

LETTER FROM THE EDITOR / We are looking at 2017 in the rearview mirror as the mystery of 2018 stretches out ahead of us. With high-profile security events like Meltdown and Spectre, WireX, Petya/NotPetya/WannaCry, and a host of other vulnerabilities and fire drills, there is finally a greater awareness — even among the general public — of the impact and importance of security with respect to the Internet and the myriad connected devices that now permeate our daily lives.

2017 was a momentous year in security, even though the DDoS landscape appeared to plateau. Maybe it was because Mirai hit so hard at the end of 2016 and the owners of other botnets were retooling to catch up. Maybe it was because news of large data breaches captured so many headlines, drawing the attention of both criminals and the public. Or maybe it is simply due to the cyclical nature of attack popularity that we have seen in the past. No matter the cause, our prediction is that the trend won't continue in 2018, and it is not time to be complacent. The Mirai botnet is far from played out, as botnet creators are continuing to modify the source code for their individual needs and, with more connected platforms devices than ever, the Internet will continue to offer fertile ground for large-scale attacks.

In contrast to DDoS attacks, web application attacks rose dramatically in 2017, and there is no reason to believe this will change in 2018. The vast majority of web application attacks are the result of untargeted scans looking for any vulnerable system, but a few are directed attempts to compromise a specific target. In either case, they are so frequent and so "noisy" — in other words, difficult to accurately detect — that many organizations are struggling to simply keep their web application firewalls running effectively, and do not have the spare cycles to worry about what their systems might be missing. It is vital to the health of every enterprise that secure coding practices become part of the larger landscape in order to combat vulnerabilities at the source.

One thing that is almost certain in the coming year is that Bitcoin will be in the headlines almost daily. The tremendous rise of Bitcoin and other digital currencies means that there are numerous new, high-profit targets for attackers to go after. Many of the organizations involved in cryptocurrencies have not put enough effort into securing their enterprises, making them tempting targets. Just as there are millions to be made by investors in Bitcoin, there are also millions to be made by attackers of Bitcoin systems.

Another area of key interest in 2018 is the Internet of Things (IoT). The security of IoT is to modern devices what SQL injection was to web development a decade ago — a vexing problem. Everyone knows that something should be done about it, but no one wants to take responsibility, when, in fact, the responsibility is a burden shared by all of us. Just like we have known about SQL injection for a decade and made little progress, I believe it is going to take at least as long to get a handle on IoT security. In the meantime, we can expect Mirai and other IoT-focused malware to wreak some havoc through connected devices that are not properly secured.

— Martin McKeay, Senior Editor and Akamai Sr. Security Advocate

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.

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***.

We made it to 2018, and the Internet did not fall apart, although 2017 brought us perhaps more than its fair share of Internet security challenges. Ransomware made us want to cry, the increase in DDoS attacks set new records in disruption, and critical vulnerabilities affected nearly every operating system and device on the market. The rate of adoption of the Internet of Things accelerated, and a record number of people and devices were connected to the Internet — which in turn means more data was created than ever before. The downside of this growth is a larger, more vulnerable attack surface, because many devices lack basic security and privacy safeguards. With the "connect everything" mantra fully embraced, the modern world tingles with smart technology, but lacks smart security.

Thanks to Mirai and the increasing number of attacks against critical infrastructure, governments are taking the threats of cyber warfare and mass disruptions to infrastructure seriously. Our modern world is built on automation — enhanced and driven by bits and bytes. We are increasingly dependent upon connectivity to the Internet and all it offers. Funding and budgets are available for offensive and defensive research, but reactionary attitudes based on fear, uncertainty, and doubt are prevalent. We find ourselves repeating the same mistakes again and again: weak components, default settings, and poor password and key management are just a small sample of the problems we face. Time and effort are continually wasted on putting out fires instead of being directed toward a more holistic and proactive approach.

At the end of 2017, there were more DNS servers configured insecurely as open relays than ever. In fact, 54% of the DNS servers I scanned could be utilized in DDoS amplification attacks. DNS open relays are a great asset when properly configured, but sloppy work makes far too many of them a liability. This is why there are millions of weak points that can be aimed and used for reflection attacks.

Guest Author
Chris Kubecka
CEO
HypaSec

Growing up, I watched lots of "Jetsons" cartoons, and to be honest I want a self-flying car and Rosie the Robot to do all the housework. However, I don't want her to stop working or act destructively due to remote takeover because of a weak default setting. As a security professional, I believe this is a concern that needs to be resolved prior to trust and widespread adoption of autonomous systems. Let 2018 be the year we begin to seriously tackle these basics and put away the fire extinguisher.

Chris Kubecka
CEO, HypaSec

TABLE OF CONTENTS

[SECTION]1
EMERGING TRENDS

During the fourth quarter of 2017, we saw that DDoS attack traffic continued to remain above the numbers recorded in the fourth quarter of 2016. Attacks originating from the United States jumped 31% year over year and there was a 10% increase in SQLi attacks compared with the prior year. Overall, DDoS attacks were up significantly from Q4 2016, with a 14% increase in Q4 2017. Infrastructure-based attacks increased 14% over the previous year, while application-layer attacks jumped 22%.

The Mirai botnet code continues to be part of the conversation as we look ahead. In the autumn of 2016, Mirai captured headlines around the world, as traffic levels of more than 600 GBPS were recorded in its debut attack. Mirai changed the security landscape once again a few months later when its source code was released on a forum site, exposing the future to all sorts of Mirai-based variants.

In Q4 2017, we saw some notable exploits, such as the Reaper and Satori botnets, which were built largely upon the original Mirai source code. The difference here was that the Satori botnet did not employ the Mirai tactic of utilizing default account credentials in order to breach devices. A significant amount of the Satori-related attack traffic made use of Mirai nodes. It is safe to say that we will see more variants of Mirai in 2018.

In the Q3 2017 *State of the Internet / Security* report, we discussed the WireX botnet, which was discovered in August. This botnet was based on Android malware that compromised Android phones via roughly 300 infected Google Play Store applications. This botnet was quickly identified and disabled, thanks in large part to effective communication among a half dozen different companies. This was an excellent example of collaboration, which will continue to be necessary in the future.

The WireX incident was most likely a precursor to a rise in mobile-based botnets and a shift in attackers' toolkits as they adapt and change to leverage new attack vectors. In addition to a broadening attack surface, we will also most likely see a rise in ransomware-based attacks following the precedent set by WannaCry and Petya in 2017.

[SECTION]^2 DDoS ACTIVITY

2.0 / Methodology / The Akamai Security Intelligence and Response Team draws the data for the DDoS section of this report from attack reports generated by Akamai's Security Operations Control Center in response to the dozens of DDoS attacks seen against the Prolexic Routed Platform each day. Attack reports contain traffic flows, attack traffic samples, and protocol types. In addition, attack event logging provides IP source data for country mapping. Depending on the attack type, some events can be directly attributed to a particular attack tool.

2.1 / DDoS Attack Vectors / As we peel back the layers of data from the end of the year, we see few changes in Q4 2017. UDP fragment floods remained the most frequent attack vector, followed by DNS, just as in the third quarter. CLDAP attack traffic moved up to the third spot overall this quarter, while NTP dropped to fourth place in Q4, though there was less than a single percentage point difference between the two. As seen in Figure 2-1, the rest of the top 10 attack vectors stayed the same from the third quarter to the fourth.

Infrastructure-related attacks accounted for more than 99% of recorded DDoS traffic in Q4, much like the previous quarters. Infrastructure-layer attacks continued to dominate, as noted in prior reports, because the barrier to entry is incredibly low. It is a simple exercise for anyone with access to a search engine to find the methods and tools for launching volumetric DDoS attacks in minimal time, with minimal cost.

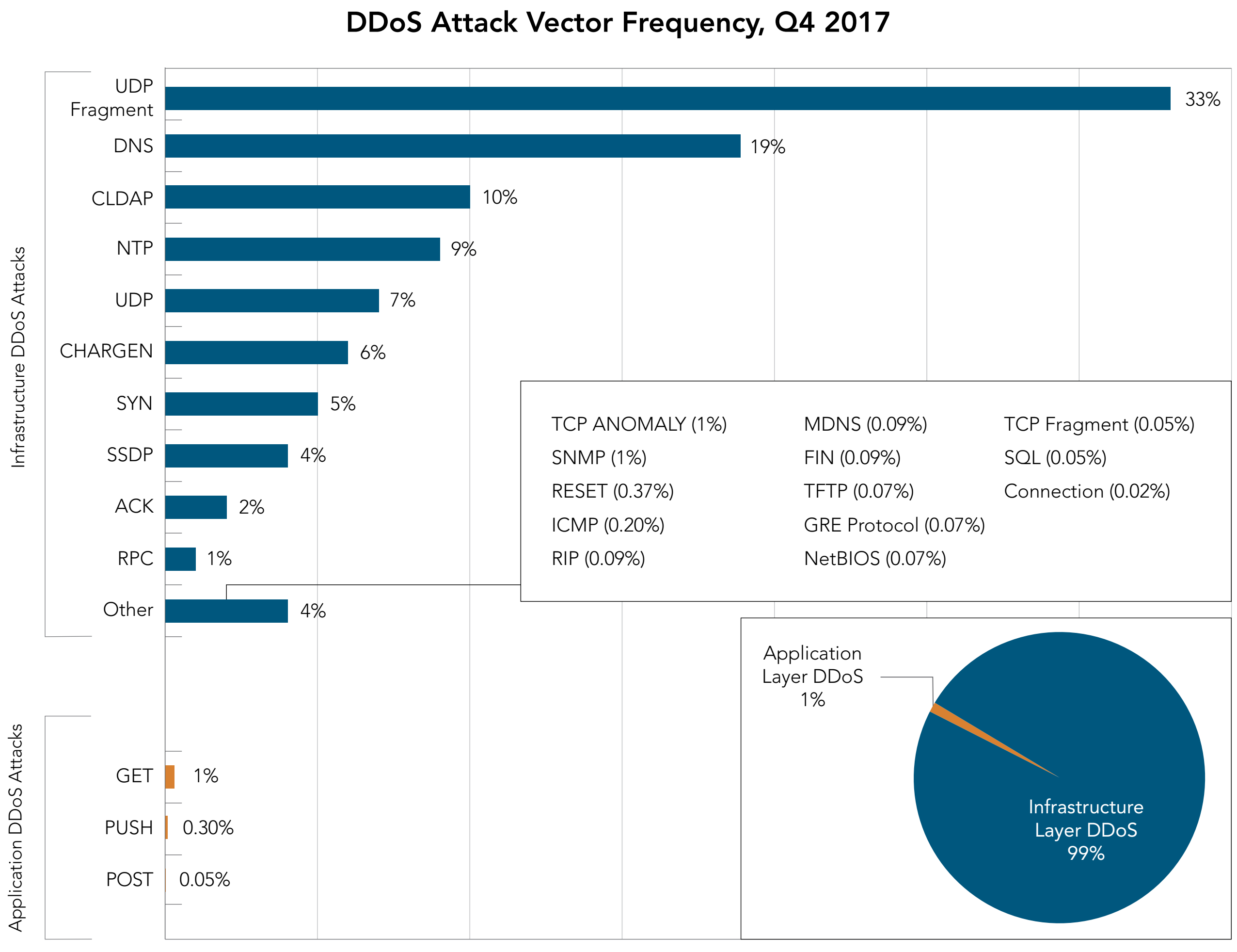


Figure 2.1: UDP fragment floods topped the DDoS attack vectors chart, while DNS flood came in second

This quarter, we saw application-layer attacks such as GET, PUSH, and POST floods increase in volume. These types of attacks typically attempt to compromise or corrupt applications and application data. While they accounted for only roughly 1% of the overall DDoS attacks seen by Akamai in the fourth quarter, the data showed a 115% increase over the previous quarter.

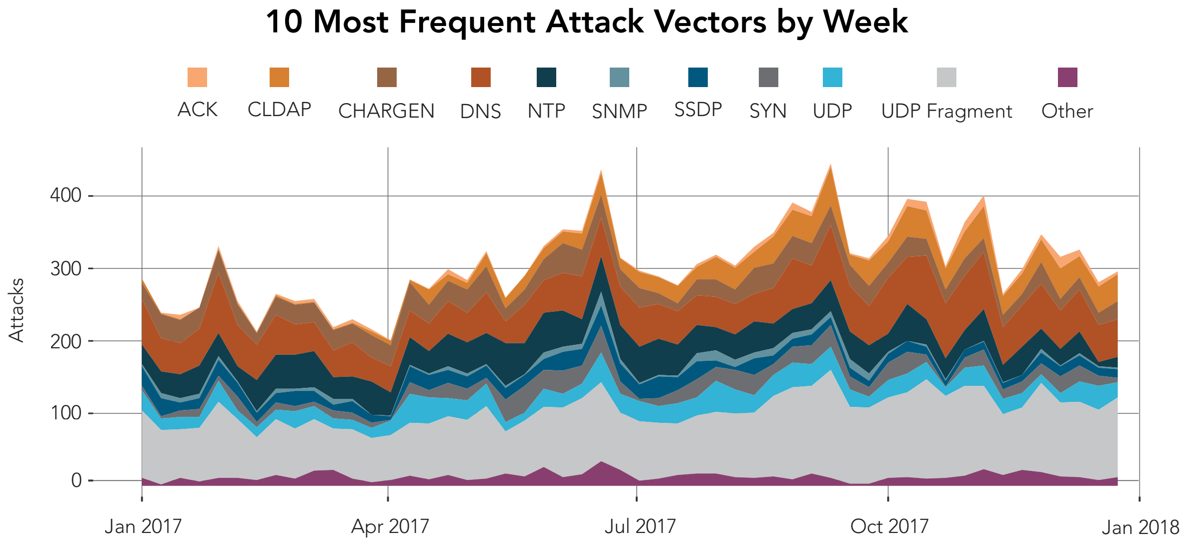


Figure 2-2: December was uncharacteristically quiet on the DDoS front

UDP fragments continued to be the most common attack vectors seen in attacks, primarily because traffic fragmentation is a side effect of many other attack types. DNS flooding, driven by reflection traffic, was still the most popular attack type, with CLDAP reflection following closely. Overall, the number of attacks rose early in the quarter before declining at the end of the year.

Top 5 Source Countries for DDoS Attacks, Q1 2017–Q4 2017

Q4 2017		Q3 2017		Q2 2017		Q1 2017	
Country	Percentage	Country	Percentage	Country	Percentage	Country	Percentage
	Source IPs		Source IPs		Source IPs		Source IPs
Germany	30%	Germany	22%	Egypt	32%	U.S.	44%
	128,350		58,746		44,198		594,986
China	28%	U.S.	14%	U.S.	8%	U.K.	13%
	118,716		38,628		11,113		177,579
U.S.	8%	India	7%	Turkey	5%	Germany	7%
	36,441		19,722		7,049		87,780
Ecuador	3%	China	6%	China	4%	Canada	5%
	14,685		15,323		5,711		60,581
Austria	3%	Mexico	5%	India	4%	Brazil	3%
	13,503		13,501		5,224		43,863

Figure 2-3: In a quarter when the number of IP addresses involved in attacks rose drastically, Germany retained the lead

Across industry verticals, gaming once again shouldered the brunt of overall attack traffic in Q4, though it saw a minor reprieve with a 7% drop in attack traffic compared with Q3. Nearly 80% of the DDoS attack traffic against gaming companies was directed at their Internet-facing assets.

The overall number of attacks per target dropped this quarter to 29, as shown in Figure 2-5. This is down from an average of 36 per target in Q3, a drop of nearly 20%. In contrast, the quarter-over-quarter drop in total DDoS traffic was less than 1%.

DDoS Attack Frequency By Industry Q4 2017–Q3 2017

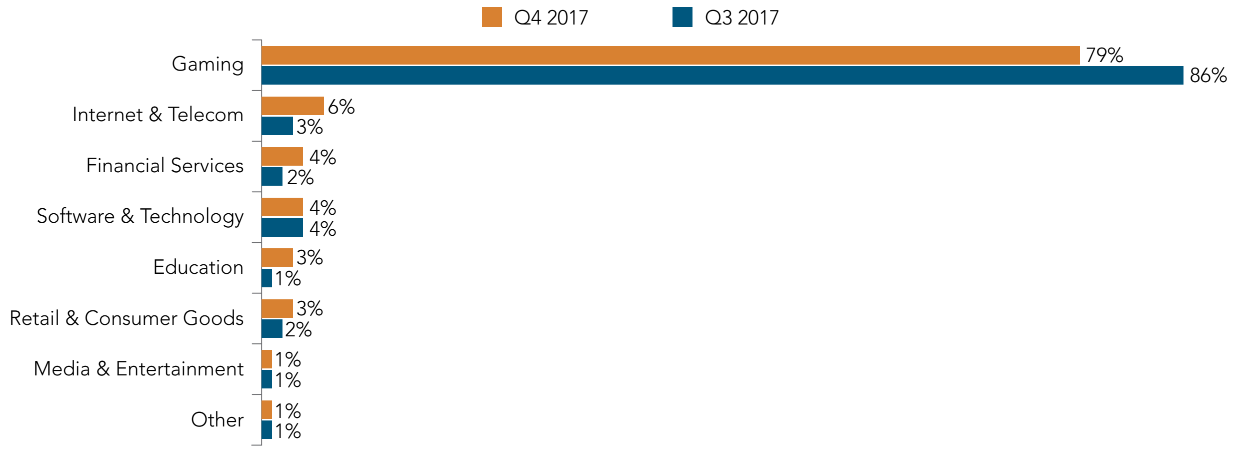


Figure 2-4: The gaming industry saw the most attacks, but attacks against financial services grew significantly

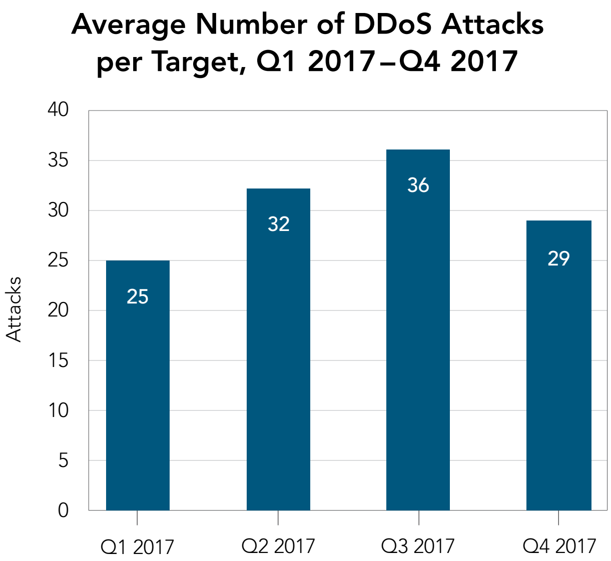
2.2 / Attack Spotlight: Financial Industry DDoS /

Summary / This quarter's attack spotlight focuses on attacks on the Financial industry vertical. DDoS attacks on the industry in Q4 were not as intense as those earlier this year but were much more frequent, with the bulk of the attacks being concentrated in the last week of October and beginning of November. Observations gathered from the attacks this quarter, along with attack data from the rest of the year, are outlined below.

Financial Industry Attacks — Year in Review / The year didn't start off well for the Financial vertical. In early January, attacks from the Mirai botnet peaked as high as 120 Gbps and were the subject of our Q1 2017 attack spotlight. Attackers were able to use Mirai with precision as they targeted customer-facing infrastructure. In Q2, the Financial vertical faced attacks that leveraged PBot, a much older attack tool. The Pbot attacks peaked at 75 Gbps and were covered in more depth in our Q2 2017 spotlight. Despite the limited number of attack sources, the PBot attacks were somehow able to generate a significant amount of attack power, and did not appear to come from the same actors launching Mirai attacks in Q1. This offers a grim reminder of the sheer number of effective tools attackers have at their disposal.

The attacks continued through Q3, at a lower intensity and frequency than the first two quarters.

Q4 2017 saw the highest single-week attack count against the Financial industry for the year. The second highest, outside of Q4, was a 23-attack week in Q2 2017.



TOP TARGET ORGANIZATION
DDoS ATTACK COUNT Q4 2017: **512**

Figure 2-5: Attacks against gaming customers were down this quarter, reducing the average number of attacks overall

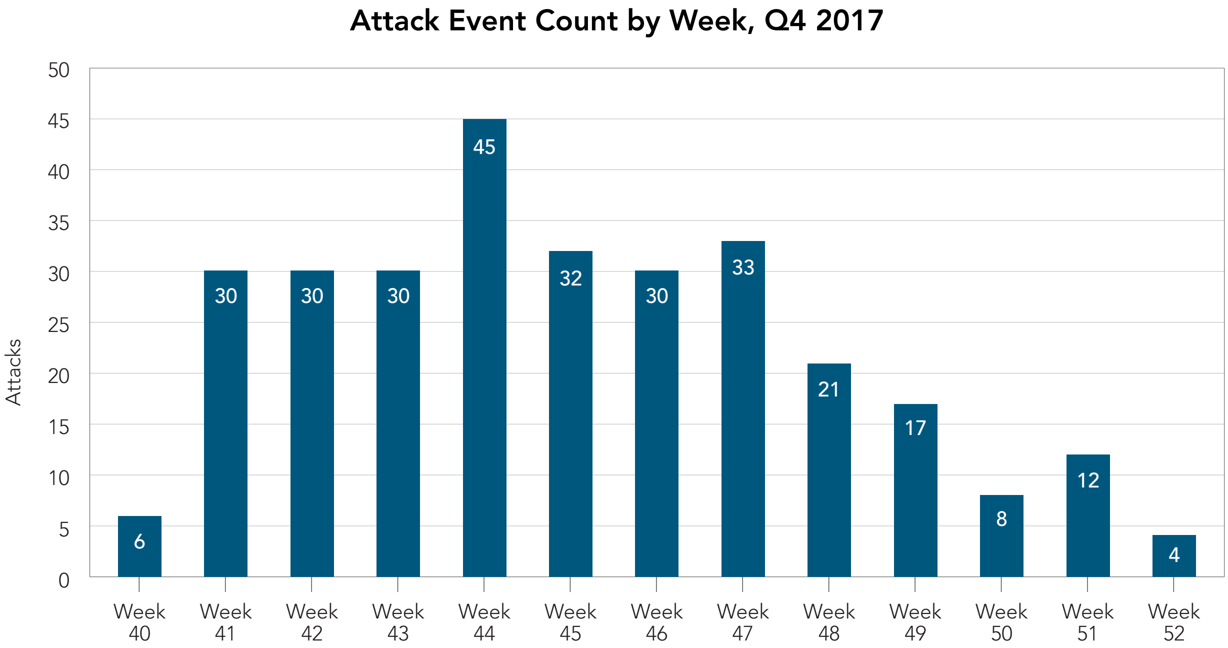


Figure 2-6: Q4 saw the largest number of attacks against the financial industry, with a high of 45 in a single week

Attack Timeline and Vectors — Q4 2017 / The DDoS attacks seen in Q4 were notable for their frequency rather than for their size. In total, the Financial industry saw 298 DDoS attacks against them in the fourth quarter, targeting 37 distinct organizations. Peak traffic levels for reflection, non-reflection, and combined reflection/non-reflection attacks hit 48 Gbps, 24 Gpbs, and 56 Gbps, respectively, on November 4, October 30, and October 16.

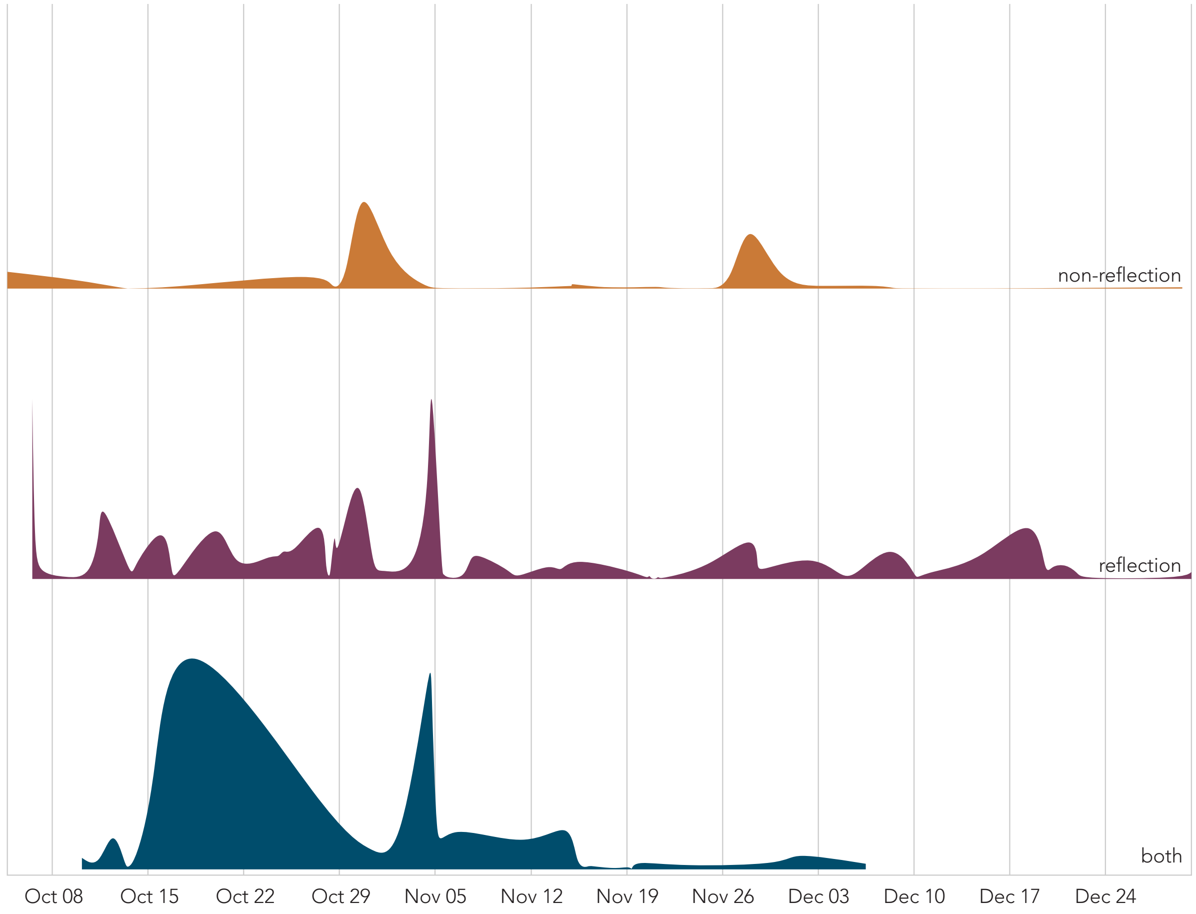
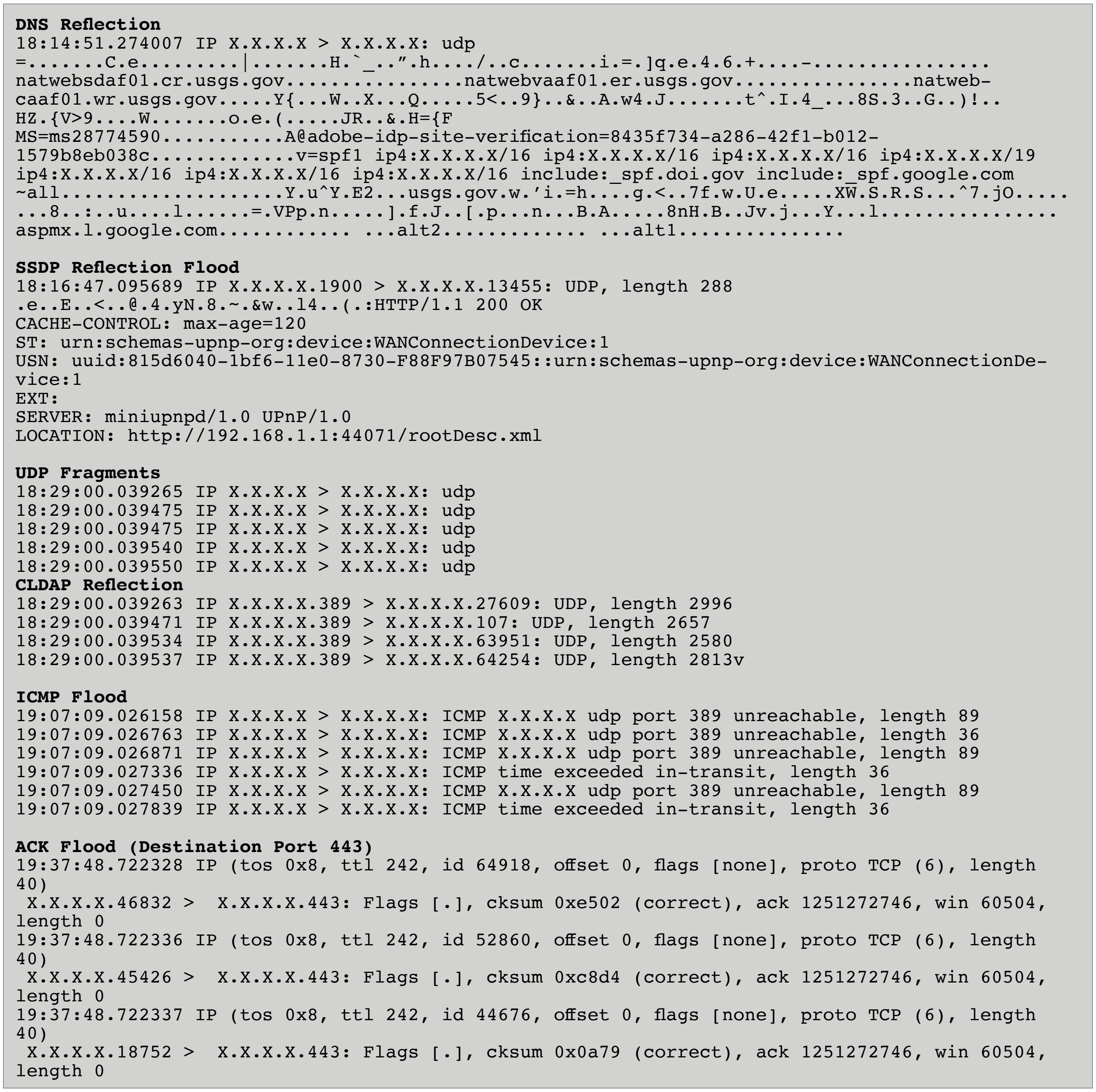


Figure 2-7: Attacks combining both reflection and non-reflection traffic peaked on October 16 at 56 Gbps

The 56 Gbps attack on October 16 targeted four distinct destination IPs within a three-hour window. This event saw a heavy reliance on reflection-based vectors, like many of the attacks on the Financial industry this quarter. Reflection attacks may not be as damaging as the largest volumetric attacks stemming from traditional bot-based DDoS, but attribution of the attacks becomes more difficult. This makes reflection attacks attractive when anonymity is preferred.

From the list of vectors used in this attack, only one — the ACK flood — is either not reflection-based or a reflection attack byproduct. DNS and CLDAP reflection attacks both exceed the maximum packet length allowed (1,500 bytes). These result in fragmented UDP packets. As the attacks go on, the reflectors themselves may become overwhelmed or just be unavailable, resulting in the ICMP unreachable messages.

The attack vectors seen in this quarter's attacks, including six reflection-based vectors, were a familiar blend found in the DDoS-for-hire market — online sites that allow a would-be perpetrator to easily launch attacks at a target organization for a small fee. The accessibility of these attacks and their high percentage of use in DDoS attacks adds to the difficult attribution. Not all the attacks against the Financial industry this quarter originated from this attack framework, but the more common vectors did. These included the mix of reflection vectors and some additional TCP- and UDP-based attacks that generate spoofed source IPs.



```
DNS Reflection
18:14:51.274007 IP X.X.X.X > X.X.X.X: udp
=......C.e.........|.......H.`_..”.h..../..c.......i.=.]q.e.4.6.+....-...............
natwebsdaf01.cr.usgs.gov................natwebvaaf01.er.usgs.gov................natweb-
caaf01.wr.usgs.gov.....Y{...W..X...Q.....5<..9}..&..A.w4.J.......t^.I.4_...8S.3..G..)!..
HZ.{V>9....W.......o.e.(.....JR..&.H={F
MS=ms28774590...........A@adobe-idp-site-verification=8435f734-a286-42f1-b012-
1579b8eb038c.............v=spf1 ip4:X.X.X.X/16 ip4:X.X.X.X/16 ip4:X.X.X.X/16 ip4:X.X.X.X/19
ip4:X.X.X.X/16 ip4:X.X.X.X/16 ip4:X.X.X.X/16 include:_spf.doi.gov include:_spf.google.com
~all....................Y.u^Y.E2...usgs.gov.w.’i.=h....g.<..7f.w.U.e.....XW.S.R.S...^7.jO.....
...8..:..u....l......=.VPp.n.....].f.J..[.p...n...B.A.....8nH.B..Jv.j...Y...l................
aspmx.l.google.com............ ...alt2............. ...alt1...............

SSDP Reflection Flood
18:16:47.095689 IP X.X.X.X.1900 > X.X.X.X.13455: UDP, length 288
.e..E..<..@.4.yN.8.~.&w..l4..(.:HTTP/1.1 200 OK
CACHE-CONTROL: max-age=120
ST: urn:schemas-upnp-org:device:WANConnectionDevice:1
USN: uuid:815d6040-1bf6-11e0-8730-F88F97B07545::urn:schemas-upnp-org:device:WANConnectionDe-
vice:1
EXT:
SERVER: miniupnpd/1.0 UPnP/1.0
LOCATION: http://192.168.1.1:44071/rootDesc.xml

UDP Fragments
18:29:00.039265 IP X.X.X.X > X.X.X.X: udp
18:29:00.039475 IP X.X.X.X > X.X.X.X: udp
18:29:00.039475 IP X.X.X.X > X.X.X.X: udp
18:29:00.039540 IP X.X.X.X > X.X.X.X: udp
18:29:00.039550 IP X.X.X.X > X.X.X.X: udp
CLDAP Reflection
18:29:00.039263 IP X.X.X.X.389 > X.X.X.X.27609: UDP, length 2996
18:29:00.039471 IP X.X.X.X.389 > X.X.X.X.107: UDP, length 2657
18:29:00.039534 IP X.X.X.X.389 > X.X.X.X.63951: UDP, length 2580
18:29:00.039537 IP X.X.X.X.389 > X.X.X.X.64254: UDP, length 2813v

ICMP Flood
19:07:09.026158 IP X.X.X.X > X.X.X.X: ICMP X.X.X.X udp port 389 unreachable, length 89
19:07:09.026763 IP X.X.X.X > X.X.X.X: ICMP X.X.X.X udp port 389 unreachable, length 36
19:07:09.026871 IP X.X.X.X > X.X.X.X: ICMP X.X.X.X udp port 389 unreachable, length 89
19:07:09.027336 IP X.X.X.X > X.X.X.X: ICMP time exceeded in-transit, length 36
19:07:09.027450 IP X.X.X.X > X.X.X.X: ICMP X.X.X.X udp port 389 unreachable, length 89
19:07:09.027839 IP X.X.X.X > X.X.X.X: ICMP time exceeded in-transit, length 36

ACK Flood (Destination Port 443)
19:37:48.722328 IP (tos 0x8, ttl 242, id 64918, offset 0, flags [none], proto TCP (6), length
40)
 X.X.X.X.46832 >  X.X.X.X.443: Flags [.], cksum 0xe502 (correct), ack 1251272746, win 60504,
length 0
19:37:48.722336 IP (tos 0x8, ttl 242, id 52860, offset 0, flags [none], proto TCP (6), length
40)
 X.X.X.X.45426 >  X.X.X.X.443: Flags [.], cksum 0xc8d4 (correct), ack 1251272746, win 60504,
length 0
19:37:48.722337 IP (tos 0x8, ttl 242, id 44676, offset 0, flags [none], proto TCP (6), length
40)
 X.X.X.X.18752 >  X.X.X.X.443: Flags [.], cksum 0x0a79 (correct), ack 1251272746, win 60504,
length 0
```

Figure 2-8: The largest attack this quarter combined three reflection vectors

Summary / The reasons for attacks on Financials can vary, but a few threats have been persistent. The Anonymous collective has had an ongoing campaign, OpIcarus, against the industry since early 2016. While they are known to use a specific set of attack tools, the use of reflection-based attacks offers the advantage of anonymity, as such attacks are very difficult to trace. DDoS-for-hire sites, offering stress-testing services that use many of the same reflection- and other TCP-based vectors, further muddy attribution. For all organizations — including but not limited to those listed as potential targets of attack — preparation, along with an implemented mitigation strategy, is key. This is true even for known empty threats like DDoS extortion emails; alerts should be in place for even low-risk threats. A DDoS mitigation provider can assist with the nuisance of reflection and other volumetric attacks, but simultaneous monitoring and mitigation of web application attacks are important as well, as attacks combining DDoS and application breaches can quickly catch organizations off guard.

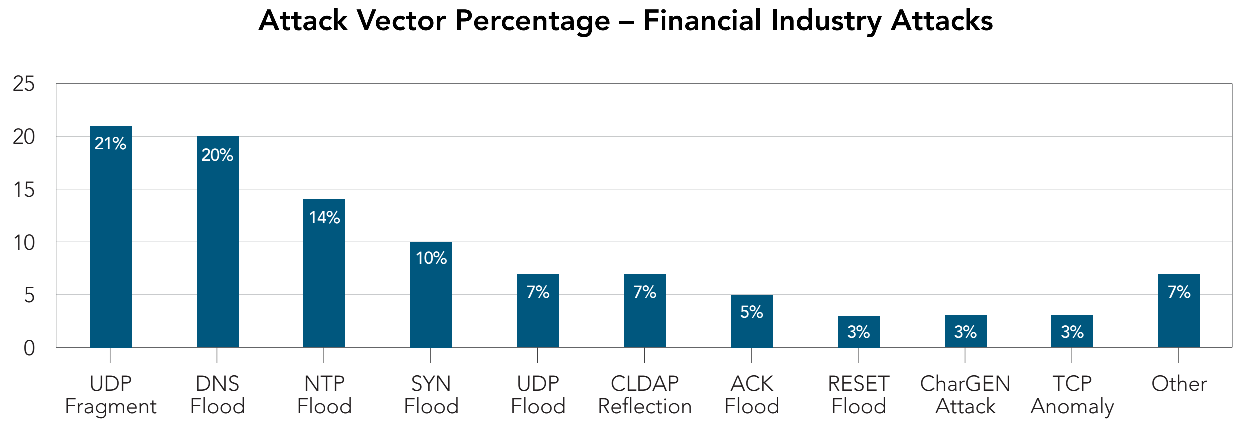


Figure 2-9: Attacks against the financial services industry included 6 different reflection vectors

2.3 / Reflection Attacks / In this report, the data reveals that reflection attacks continue to be utilized for distributed denial of service. As in prior quarters, we saw that DNS, NTP, and CHARGEN were the top three reflection attack vectors. This activity continued in Q4. The continued use of these reflection attacks demonstrates a collective need to address these accessible services by patching and properly configuring them. As an example, it is advisable to ensure that NTP is patched to current revision or N-1 in order to remove this as a vector for DDoS reflection attacks. System administrators need to be continually applying security patches and ensuring that systems are properly configured. All externally exposed configurations should be reviewed on a regular basis or assigned to a vendor partner that does so.

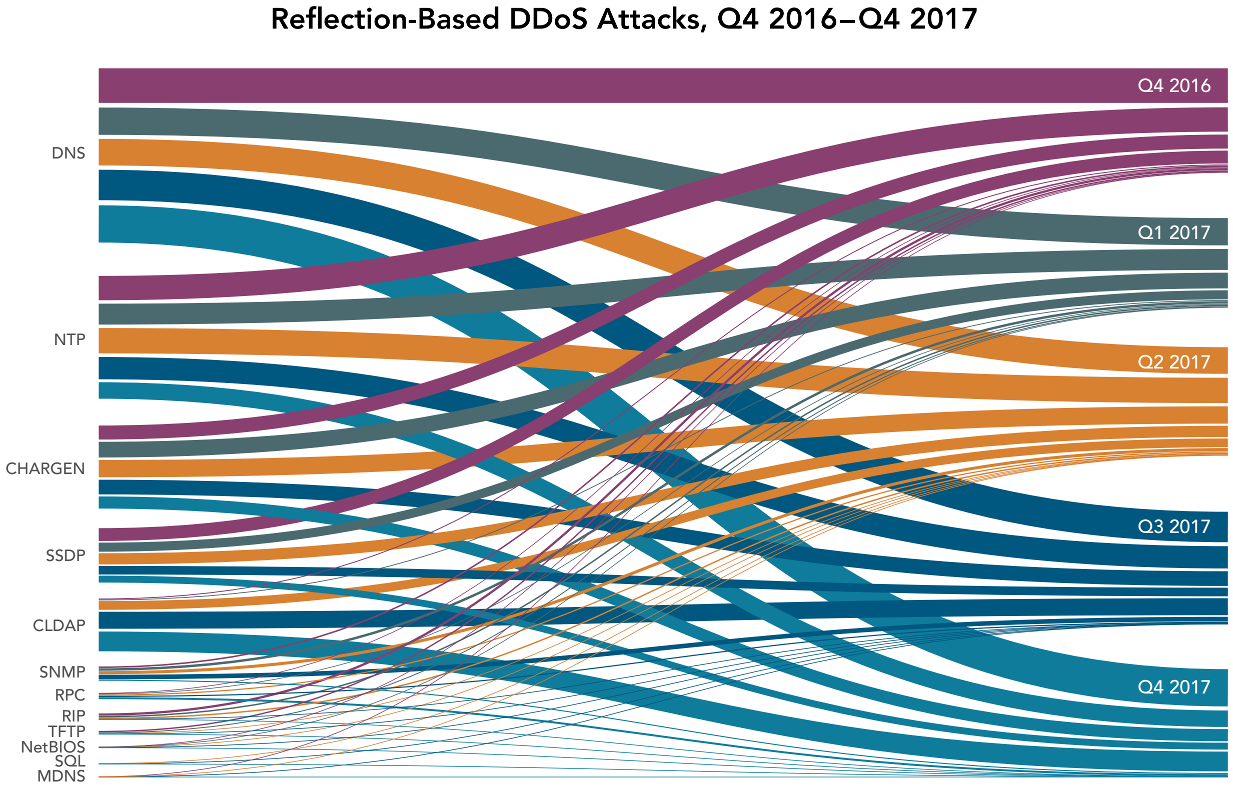


Figure 2-10: Attacks from reflector sources are popular because they amplify the volume of attack traffic

2.4 / A Year Of Mirai / The Mirai botnet has been with us for more than a year, after exploding onto the scene in September 2016. A tool that was originally created to help a small group of college students who wanted an unfair advantage as a Minecraft hosting provider has now become one of the most well-known DDoS tools on the Internet. While the botnet is now much smaller than it was at its peak, the Mirai code base is still being updated to give it new capabilities.

We first covered Mirai in the Q3 2016 *State of the Internet / Security report*, when the botnet was the tool of choice for attacking the blog of security writer Brian Krebs. This series of attacks culminated in a 623 Gbps mega-attack, the biggest Akamai has seen to date. Our indicators showed more than 2.5 million unique IPs associated with the botnet, although evidence suggests some inflation due to devices changing DHCP leases and other types of IP address changes. Additional research in the Q4 2016 *State of the Internet / Security* report suggests that Mirai had actually been in development for several months, scanning and probing the Internet before its debut.

In October 2016, Mirai was also responsible for attacks that took down a large number of major sites around the world when it caused an outage at Dyn, a provider of DNS services. This was a wake-up call for many people. Several weeks prior, Mirai's source code had been publicly released by its author, Anna-sempai. This move ensured Mirai's longevity by making it possible for hackers around the globe to evolve and modify it for their own use.

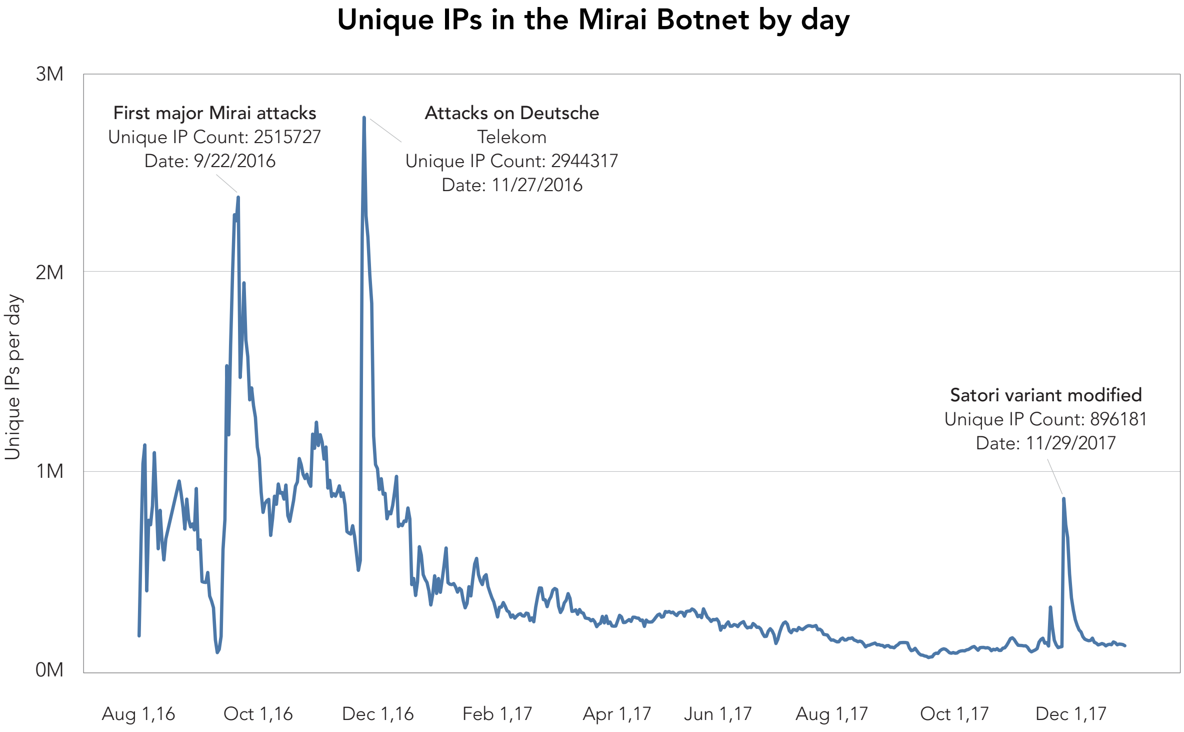


Figure 2-11: The release and modification of the Mirai code have kept the botnet active

The best example of the code base being modified for an individual's use occurred on November 27, 2017, when a British hacker used his variant of Mirai to attack more than 900,000 Deutsche Telekom (DT) routers. On that day, Akamai saw more than 2.9 million unique IP addresses that were scanning the Internet and identifiable as part of a Mirai botnet. An interesting point on this attack is that while the Deutsche Telekom devices were compromised, they did not take part in the scanning Akamai saw at the time. The expectation is that the compromised systems would scan the Internet as a whole, but they did not follow typical Mirai behaviors. Rather than scanning for additional nodes, the DT routers were taken offline by the malware.

The number of IP addresses and IoT devices associated with Mirai fell steadily for several months afterward, although there were still a number of large attacks associated with the botnet. This changed significantly in late November 2017, when a Mirai variant dubbed Satori was modified to use a new list of usernames and passwords, as well as take advantage of a new vulnerability (CVE-2017-17215) against Huawei home routers. On November 29, the number of IP addresses involved in scanning and attacking surged dramatically to nearly 900,000.

One of the interesting things that the change in Mirai code highlights is the geographic distribution of certain devices. Both the initial and secondary attack spikes were driven primarily by devices in Brazil, apparently because a large pool of vulnerable devices had been discovered in that region. According to Akamai's initial research, a significant part of this pool consisted of Internet-enabled security cameras. On the other hand, the Satori variant that surfaced in November has been primarily driven by devices located in Egypt. We don't know the specific device that was added, but it is most likely a router or other network device heavily used by a service provider unique to Egypt.

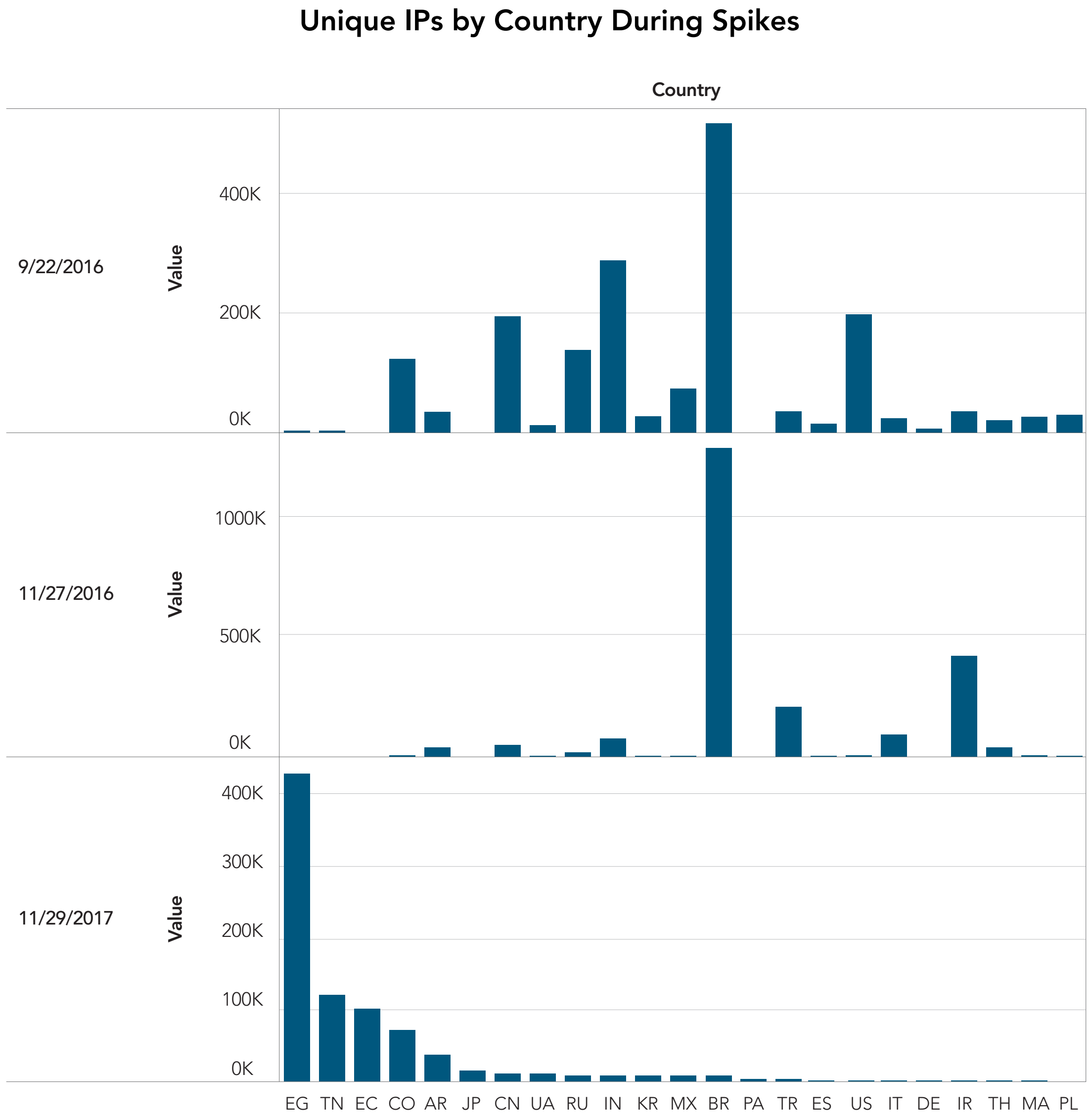


Figure 2-12: The changing geographic distribution of active Mirai IPs reflects the location of newly discovered vulnerable devices

Few pieces of malicious code have had the impact of Mirai in recent years. The release of Mirai's source code was supposedly an attempt to muddy the trail for investigators looking for the author, but it has additionally enabled the botnet to have a powerful and lingering impact. The release of the source code has allowed hackers to create their own modified versions of the botnet, extending it with capabilities beyond what the original author intended.

But the biggest impact of Mirai may have been to open the eyes of the botnet world to the fact that the Internet of Things is a huge pool of resources waiting to be tapped for mayhem.

[SECTION]^3 WEB APPLICATION ATTACK ACTIVITY

3.0 / Methodology / Akamai's Kona Site Defender protects customers from millions of web application attacks every day. This data is saved to Akamai's Cloud Security Intelligence data repository, which collects nearly 9 petabytes of data every 30 days. Akamai researchers use the data to develop insight into the nature of such attacks on the Internet.

3.1 / Web Application Attack Vectors / ISQL injection (SQLi) attacks remained the dominant web attack vector in Q4 2017, as seen in Figure 3-1. They made up 50% of all web application attacks in Q4, up from Q3 2017. SQLi is a well-known and well-understood attack that has remained in the top position over time simply because organizations have not taken the time to protect their sites. Attackers will continue to utilize these vectors to gain access to systems if applications do not take the simple but necessary step of sanitizing data input and output. These types of attacks are easily automated and scalable, looking for any vulnerable system, rather than targeting specific organizations.

Local File Inclusion (LFI) came in second after SQLi attacks on the list of most used attack vectors, with a 36% share of the Q4 attacks, down from 38% in Q3. Cross-site Scripting (XSS) came in third with 8% of the attacks, down from 9% in the third quarter.

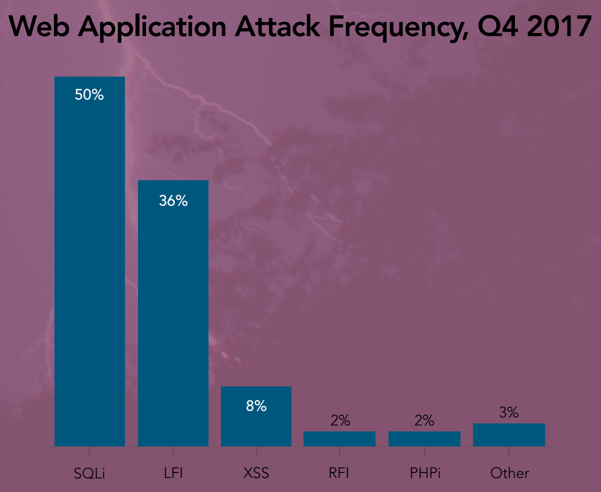


Figure 3-1: The ease and effectiveness of SQLi attacks ensures their popularity will continue

3.2 / Top 10 Source Countries / In Q4, the top 10 countries for web application attack sources saw some changes, although the United States again remained firmly in first place, sourcing 32% of attacks. The Netherlands moved up to second place with 12% of attacks, while China moved up to third place with 7%. Russia, which held the second spot in Q3, dropped to 5th place this quarter, while Canada returned to the top 10 after being in 11th for the previous two quarters.

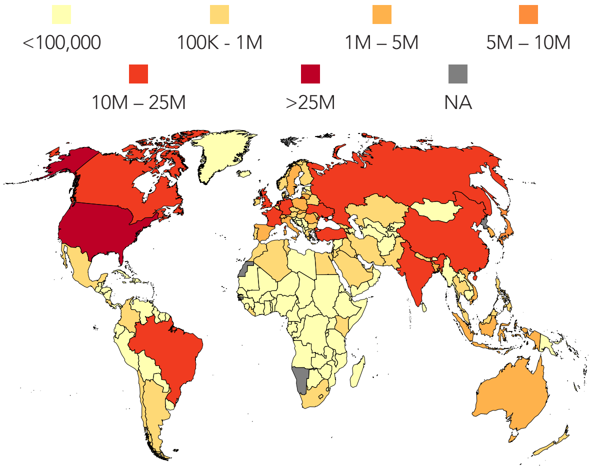
The Netherlands took the top spot for attack sourcing among among EMEA countries in Q4, with more than 47 million attacks recorded (up from 31 million in Q3). The Russian Federation dropped to second place, though it was still responsible for more than 18 million attack alerts. Ukraine held on to its third place position in Q4, with more than 17 million attacks recorded.

The United States once again claimed the top spot for web application attack sources in the Americas, with 128 million alerts recorded in Q4 (down from more than 180 million in Q3). Brazil and Canada also remained in second and third places respectively, although the number of alerts generated from Brazil dropped by more than 5 million in comparison with Q3, while the number of alerts from Canada rose by more than 5 million. Mexico and Argentina held the 4th and 5th positions in the Americas, with attack counts in the hundreds of thousands, as opposed to the millions seen in the top three.

China, India, and Japan maintained their rankings this quarter as the top three attack source countries in the Asia Pacific region. In first place regionally and third place globally, China had more than 28 million alerts recorded in Q4, up from 22 million in Q3. Meanwhile, Australia moved into the top five, supplanting South Korea with 2.5 million attacks recorded.

The United States remained firmly in first place as the top target country for web application attacks, with more than 238 million attack triggers recorded in Q4, down from 323 million in Q3. Although the United States continued to be the largest target country by far, its 29% quarter-over-quarter drop in recorded attacks outpaced the global 9% drop in attacks. Meanwhile, Brazil remained in second place as

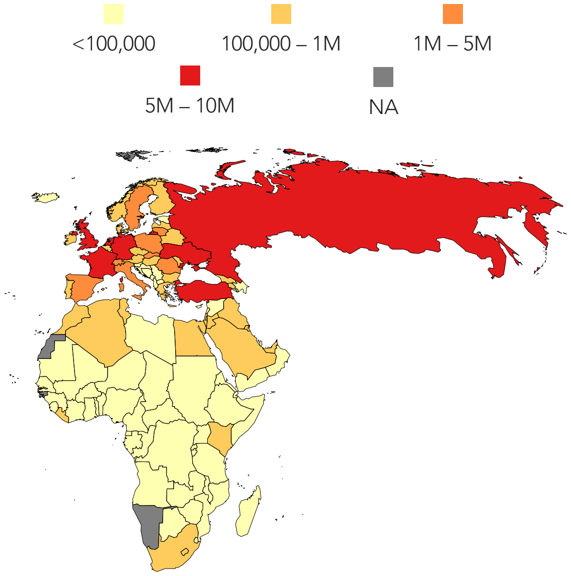
Source Countries for Web Application Attacks—Worldwide, Q4 2017



Country	Attacks Sourced	Percentage
United States	128,013,378	32.0%
Netherlands	47,433,432	11.9%
China	28,171,775	7.1%
Brazil	22,945,844	5.7%
Russia	18,370,802	4.6%
Ukraine	17,182,960	4.3%
India	16,489,773	4.1%
Germany	13,046,096	3.3%
United Kingdom	12,790,735	3.2%
Canada	12,634,269	3.2%

Figure 3-2: The United States tops the list for source countries for web application attacks in Q4 2017

Web Application Attack Source Countries—EMEA, Q4 2017

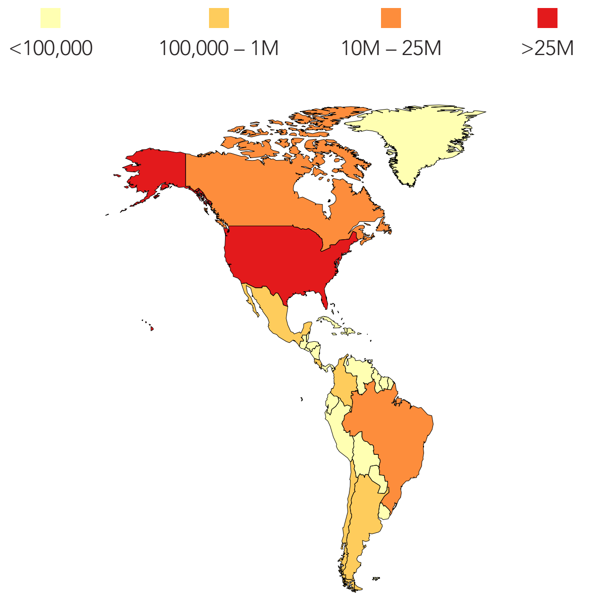


Country	Attacks Sourced	Global Rank
Netherlands	47,433,432	2
Russia	18,370,802	5
Ukraine	17,192,960	6
Germany	13,046,096	8
United Kingdom	12,790,735	9

Figure 3-3: The Netherlands claimed the top spot for source countries in EMEA

the target of 2.2 million attacks, while Australia, which had been in third position as a target in Q3, dropped to 9th overall among target countries in Q4.

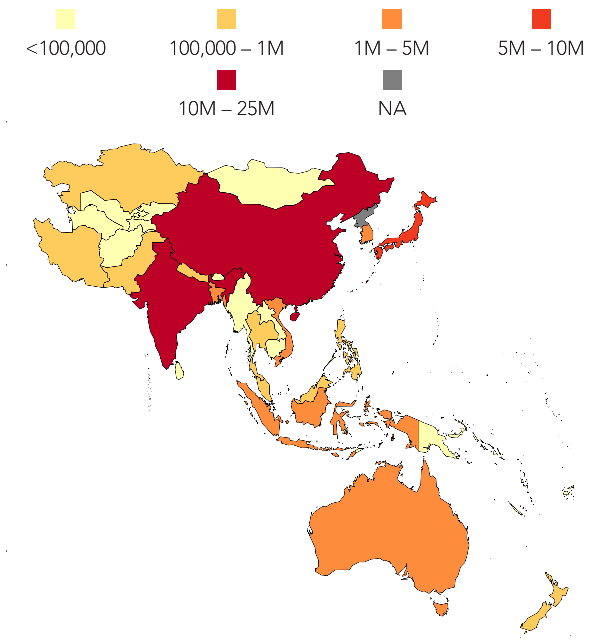
Web Application Attack Source Countries—Americas, Q4 2017



Country	Attacks Sourced	Global Rank
United States	128,013,378	1
Brazil	22,945,844	4
Canada	12,634,269	10
Mexico	783,642	33
Argentina	407,376	48

Figure 3-4: The United States held onto the first spot for source countries for web application attacks in the Americas, with more than 100 million attacks separating it from the second spot - Brazil

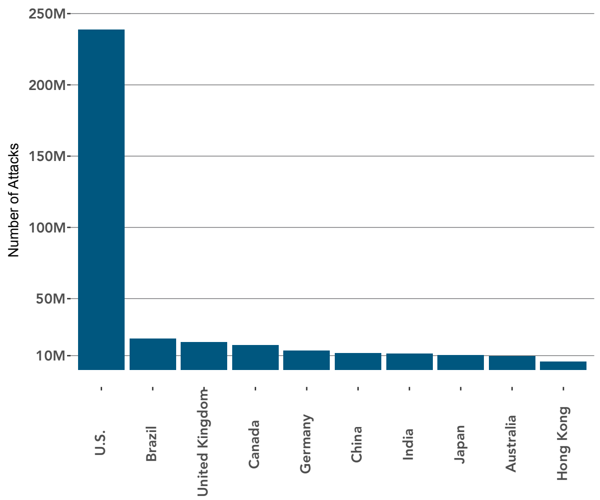
Web Application Attack Source Countries—Asia Pacific, Q4 2017



Country	Attacks Sourced	Global Rank
China	28,171,775	3
India	16,489,773	7
Japan	6,576,046	13
Hong Kong	3,214,895	16
Australia	2,519,512	18

Figure 3-5: China tops the list of source countries in Asia Pacific, with India coming in second place and Japan in third

Top 10 Target Countries for Web Application Attacks, Q4 2017



Target Country	Count
United States	238,643,360
Brazil	21,900,411
United Kingdom	19,385,710
Canada	17,459,934
Germany	13,432,389
China	11,906,342
India	11,546,530
Japan	10,510,981
Australia	9,758,428
Hong Kong	5,733,649

Figure 3-6: Many organizations maintain their web presence in the United States, even if they are international

[SECTION]4 AKAMAI RESEARCH

The Akamai network serves a significant portion of the Internet's total web traffic. On January 1, 2018, our average traffic was 34.7 terabits per second (Tbps) and peaked at 44.2 Tbps, both of which were exceeded by our peak of 61.3 Tbps on September 12, 2017. In comparison, the Library of Congress' web archives are approximately 750 terabytes, which is what is transmitted across Akamai's network every three minutes. In other words, Akamai is responsible for monitoring and moving Internet traffic on a scale that few other companies can begin to imagine, and is in a unique position to capture comprehensive data about the continually changing health of the global Internet. In this section of the *State of the Internet / Security* report, we give examples of how digging deeper into that data and combining it with relevant external data sets can help us better understand the Internet as a whole and how we can improve it.

The three examples in this quarter's report draw from very different data sets. The first looks at a trio of issues from the Common Vulnerabilities and Exposures (CVE) database to help us prepare for what we might see in 2018. The second uses Akamai's network-measuring tools to look at measuring the connectivity between networks in graphical terms. The third introduces research about Internet botnet and credential abuse traffic. Each is a small highlight of the bigger research efforts going on within Akamai.

4.1 / Web Vulnerabilities to Watch / Last year, IoT threats, high-profile data breaches, and the skyrocketing price of Bitcoin dominated the headlines. After Mirai's author published its source code, several Mirai-based IoT botnet variants appeared. Botnets focused largely on harvesting default credentials for widely deployed IoT devices, including DVRs, IP-enabled cameras, and routers. While enterprise systems mainly feared attacks from IoT botnets, we are now seeing a startling trend emerging whereby adversaries are hijacking corporate systems and bringing them into the botnet fold, using remote code execution vulnerabilities in enterprise-level software.

These types of vulnerabilities are being aggressively scanned for and exploited — not just to create a toehold in a network, but to monetize its CPU cycles and other resources for profit. The vulnerabilities we chose to highlight below are of the most severe type. They allow execution on the vulnerable system without require authentication.

CVE-2017-17562 / 2017 saw a change in paradigm for IoT botnets when the Satori variant began to appear in our honeypots. Instead of using a list of known login credentials, the authors of Satori chose to exploit a zero-day vulnerability in Huawei routers. This will become the new standard as IoT manufacturers patch known weaknesses in their software configurations. Late in 2017, a vulnerability (CVE-2017-17562) was found in the GoAhead embedded HTTP server. It allows remote command execution without authentication. The Shodan search engine shows more than 700,000 devices running GoAhead — all potential targets. The exploit is simple and reliable across multiple platforms due to the way GoAhead is configured by default.

We started seeing exploitation attempts for the GoAhead web server LD_PRELOAD Vulnerability on December 20, 2017, only two days after the vulnerability was publicly released by security researcher Daniel Hodson. GoAhead released a patch in July of 2017; however, updating software on embedded devices varies by manufacturer. We worry this inconsistency might lead to hundreds of thousands of vulnerable devices still lingering on the Internet ripe for abuse. Embedded-device consumers should be aware of pending updates to their devices and apply them when and if available

CVE-2017-10271 / In October 2017, Oracle released an update for a remote code execution vulnerability in the Oracle WebLogic Server. This vulnerability allowed an adversary to execute code on the target server without any authentication. A working exploit was published December 28 on GitHub. Akamai's Kona WAF saw scanning and attack indications by the very next day. The origin of this traffic appeared to come from servers hosted by InterServer (***https://www.interserver.net/***), a web and virtual server hosting company located in New Jersey.

The scanning appeared to be a shotgun blast across multiple industry verticals, including Online Retail, Security Vendors, Online Banking, and Government Sites.

On January 3, 2018, researchers from Google's Project Zero published details on two vulnerabilities affecting chip manufacturers. The vulnerabilities, titled Spectre and Meltdown, allow an unprivileged user to read arbitrary data from the vulnerable host. This might allow sensitive information like private keys and passwords to be exfiltrated from memory by routine applications such as a web browser.

The publication of Spectre and Meltdown, along with the remote code execution vulnerabilities in Oracle's WebLogic and the GoAhead embedded HTTP server, could lead to a new round of highly damaging, targeted attacks. In addition, with the popularity of cryptocurrencies, there is also a risk that adversaries will leave systems intact only to install crypto mining software on vulnerable systems. We suspect CVE-2017-10271 will be the primary target of this type of attack as the servers hosting the vulnerable software would most likely be high-end, multi-processor systems. Instead of attempting to exfiltrate data or install back doors, attackers could attempt to hijack the high-end resources by quietly installing crypto mining malware. If cryptocurrencies continue to gain value, this type of attack could become a new trend.

4.2 / Visualizing a Planetary Scale Network / Akamai's network is built on a planetary scale. It encompasses hundreds of thousands of servers distributed across more than 130 countries worldwide, making the task of visualizing the network incredibly complicated. How does one create a useful visual representation of something so large, complex, and interconnected? One approach we have successfully used is a heat map of the latency gradient, a powerful tool for developing an intuitive understanding of the network topology. Whereas a traditional map of Internet connectivity quickly becomes too complex and convoluted to be useful, the heat map makes it easier to identify weaknesses in network connectivity.

Figure 4-1 is a heatmap — a visual representation of a nearly symmetric matrix. Each row and column of the matrix represents a physical location (region) where Akamai has a cluster of servers. Each element of the matrix shows the latency, measured in milliseconds, between its row and column regions, with darker colors implying lower connection delays. Figure 4-1 shows latency information for roughly 800 regions and contains 640,000 elements. To better organize the heat map, a clustering algorithm was used to order the rows (and columns) so that regions with similar connectivity characteristics are ordered close to one another. In other words, suppose that region X and region Y are both in Frankfurt and both connect to the Internet through the same network partner; these two regions would be placed close to one another in the ordering. However, if region A is in Los Angeles and region Q is in Doha, these would be very separate in the ordering, as their Internet connectivity characteristics are very different from one another.

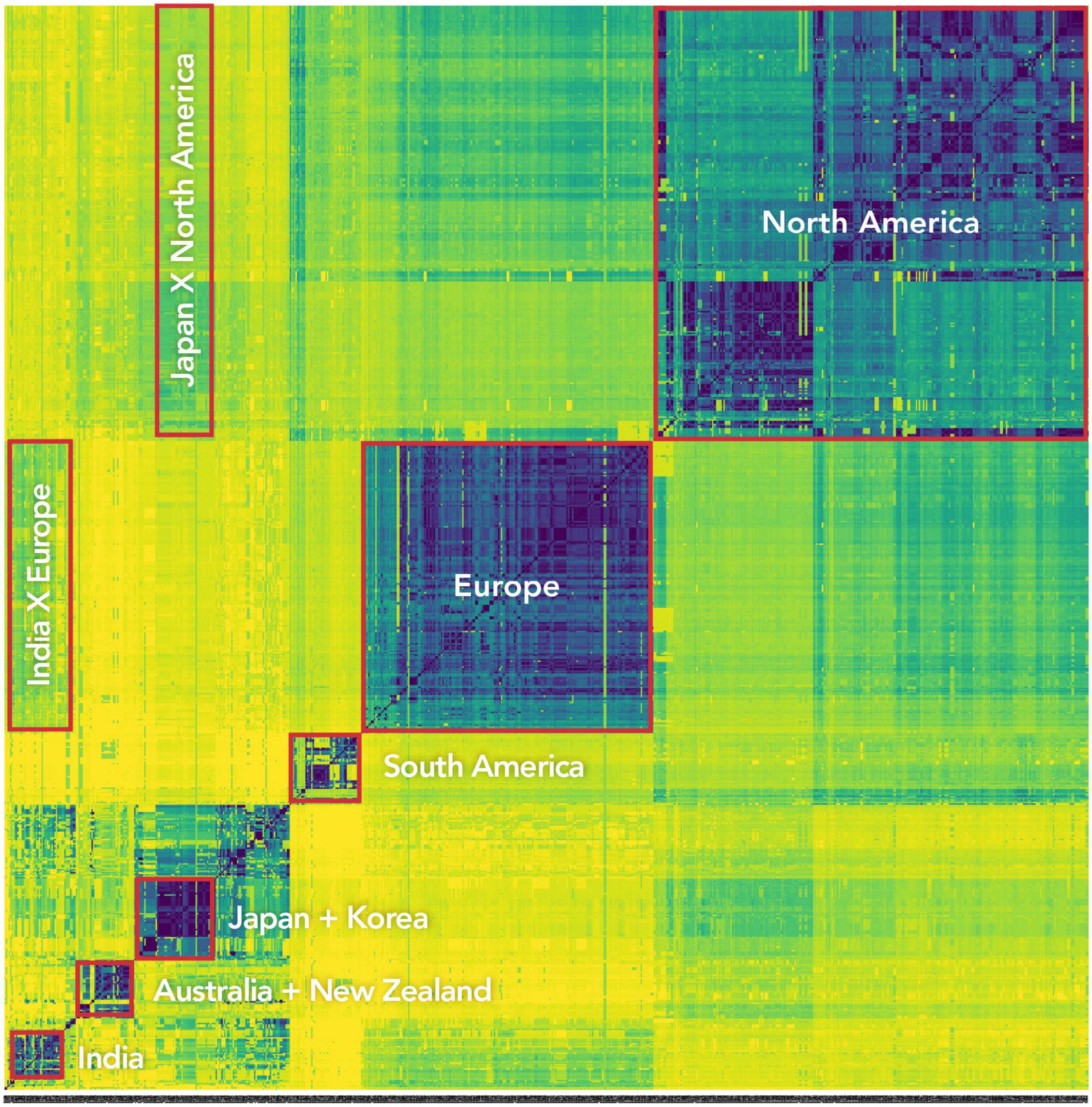


Figure 4-1: Dark colors like purples and blues show short latencies between regions, while light colors (greens and yellows) represent long latencies

The clustering algorithm creates visible attributes when we plot the heatmap. The most noticeable is a purple line running from the bottom left corner to the top right corner. This is simply because the latency between a point and itself is zero (represented by the dark purple color), giving us a dark purple line along the matrix's line of symmetry where the row and column region are the same.

The next set of visual attributes is a series of bluish squares arrayed along the diagonal. Each square represents a cluster of regions that are well connected to each other and have similar connectivity characteristics. The darker the color, the more closely connected the regions are, and therefore the more similar the regions' connectivity characteristics are. Using North America, in the upper right corner, as an example, we can quickly identify the regions that comprise it. North America subdivides quite neatly into the East Coast (upper right) and the West Coast (lower left). The East Coast square can be further subdivided into smaller blocks representing New York City, Reston, and Miami — all regions where Akamai deploys a large number of systems. Similarly, when examining the large square that represents Europe, we see a significant number of tightly connected regions.

What these dark squares represent are large pools of interconnection capacity. Imagine that someone got careless with a backhoe and killed the network link to one or more regions in New York City. This would cause little disruption to the Akamai network because of other regions with almost identical connectivity characteristics. Traffic would spill over to the next nearest region and customers would continue to be served.

Imagine two more serious outages. In the first, a hurricane disrupts all the regions in the greater Miami area. Customer traffic would be served from slightly further away, but there still would not be a meaningful increase in end-user latency outside the affected area. In contrast, an undersea quake that breaks all the links between Australia and New Zealand would have a much more significant effect, which this heat map allows us to see and anticipate.

A final point of interest is the pieces of the heat map that are further from the diagonal. This part of the graph shows information about the latency between regions that are located "far away" from one another in a network-topological sense. For example, in the upper left-hand corner is a box labeled "Japan X North America." This shows the latency between regions in Japan and connected regions in North America. Suppose that something crazy went on and we had to start using capacity located in North America to serve customers who are physically located in Japan. The heatmap colors tell us that this scenario would cause a noticeable increase in end-user latency; however, this increase would be significantly less if serving traffic from the West Coast of the United States rather than the East Coast.

The heat map provides a visual representation of the physical topology of the Internet. The network distance between regions is based on many external constraints, such as where carriers run their fiber, peering points locations, and even the speed of light. The heat map turns this complex data into a relatively simple visual representation that we can use to guide discussion around capacity deployment, understand the impacts of region failure on end-user experience, and help improve quality of service. Connectivity has become more important than the physical layers of the Internet, and a heat map helps identify the weak points in the fabric of networks.

4.3 / Capturing Bot And Credential Abuse Data / This quarter, we have our first opportunity to look at two data sets that have not been part of the State of the Internet / Security report before: analysis of bot traffic and analysis of credential abuse attempts. The former is based on logs from our Bot Manager product, which relies on multiple heuristics to identify potential bots in real time. These heuristics range from bot self-identification to complex behavioral analysis of bot traffic. Meanwhile, the analysis of credential abuse and logins in this report occurred during post-processing.

November marked the first time we captured this data for purposes of the State of the Internet / Security report, and the analysis below leverages data from November and December 2017, covering the full time period for the bot data and 50 days for the credential abuse data. Even this initial look at a relatively brief data set has revealed interesting insights, and we hope to continue monitoring both data sets over the longer term in order to provide deeper research and analysis in future reports.

Bot Analysis / Our bot data spans the full months of November and December 2017. It is always interesting to look at the holiday season because these months represent so much online activity, especially for retailers around the globe. It is important to point out that we are not categorizing bot traffic as "good" or "bad," since this is a subjective characteristic. A well-behaved bot that is crawling a site on behalf of a search engine is often viewed as beneficial, but the same bot might not be seen as favorably by a smaller website with fewer resources available. Similarly, there are a number of site-scraping bots that fall within grey areas; they might be considered good by one site, but bad by another.

Akamai saw 146 Petabytes of traffic in November and 145 Petabytes in December in bot traffic alone. This translates to approximately 550 Mbps, or roughly 1.6% of all traffic flowing across the Akamai networks. Analysis conducted in 2016 showed that bots are responsible for in excess of 30% of our traffic when we examine only web traffic and don't include streaming video or other types of traffic we handle. Over this period, Akamai handled in excess of 7.3 trillion bot requests a month, or an average of 2,750 requests per second.

Unsurprisingly, spidering activity by search engines is responsible for a large majority of the bot traffic seen in our data, including nearly 40 billion requests in November alone. The second-largest source of bot traffic came from site-monitoring applications, which received 9.3 billion requests in November. The statistics were nearly identical in December, but only long-term tracking of this data can tell us how stable these numbers will remain.

Retail organizations saw the largest amount of bot traffic, with 2.4 trillion requests in November alone. This isn't surprising, as both spiders and scrapers have good reason to come back to Retail sites often as prices and products are updated. Figure 4-2 highlights the top 10 verticals seen in Akamai's bot data. The High Tech vertical, which came in second for bot traffic, saw just over half the request traffic that Retail did, with 1.28 trillion requests.

Bot traffic is a small but growing component of web traffic, and its impact is something organizations need to be aware of and tracking. One factor we expect to become increasingly important is bot activity targeting APIs. In many cases the safeguards organizations have in place to protect their site from attackers are not tuned to protect APIs, making them tempting targets. This is one of many potential stories hidden in the data for future analysis.

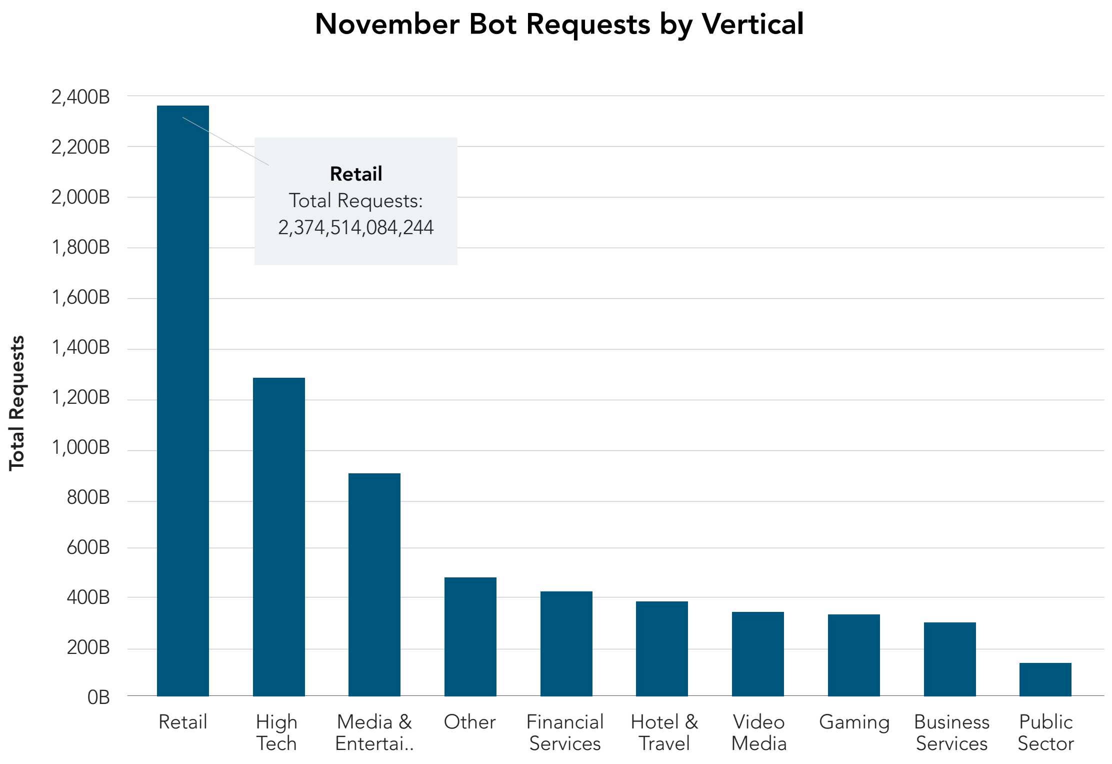


Figure 4-2: Retail organizations see more bot traffic than the high tech and media verticals combined

Credential Abuse / Credential abuse, the attempt to log into a site with stolen or captured credentials, is where the data gets really interesting. Akamai classifies this type of data by identifying IP addresses that make multiple attempts to log into accounts using leaked credentials with no other activity to the target site. This methodology helps us identify both bursty, high-speed login attempts as well as the "low and slow" attempts to avoid apprehension by spreading login tries across longer time periods. Akamai's ability to label traffic as credential abuse is based on analysis of a variety of factors, including initial request logic, site responses, and the activity of the requesting IP addresses against other properties protected by Akamai. This data set covers 50 days from November and December 2017, and focuses primarily on November. Our data is principally collected from sites that use an email address as the login name, and may under-represent industries such as Financial Services that require clients to have a username not based their email address.

Akamai saw 8.3 billion login attempts across the Akamai platform in November and 8.75 billion logins during December, despite a slightly shorter data collection window. Of the logins in November, a whopping 3.6 billion were determined by us to be malicious login attempts. In other words, 43% of all logins seen by Akamai were attempts to log in to an account using password guessing or account details gathered from elsewhere on the Internet.

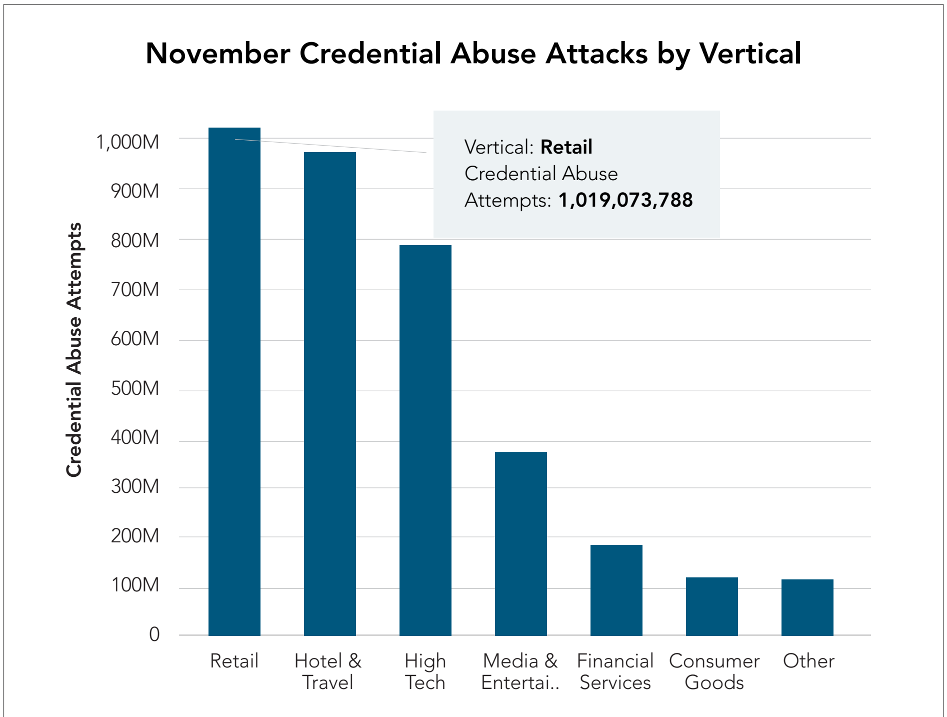


Figure 4-3: The retail vertical tops the chart with over a billion credential abuse attempts

As shown in Figure 4-3, Retail organizations saw the largest number of malicious login attempts in November (1 billion), followed closely by Hotel & Travel (968 million) and High Tech (781 million), but these numbers tell only half the story. When we compare the number of total login attempts to the malicious attempts, a different picture is painted. Retail organizations saw a total of 2.8 billion login attempts, of which 36% were considered to be malicious. Compared to the cross-industry average of 43%, Retail received relatively few attacks. High Tech companies saw 1.4 billion total login attempts, of which 57% were deemed malicious. But the far and away winner (or loser) in this category was the Hospitality industry!

Anecdotally, it has long been known that hotel and airline sites are tempting targets for attackers, who are aware that these sites have large pools of credit card numbers for them to drain. Ask anyone on the security team at a hotel chain and they will tell you how hard they have to work to protect their user accounts. But it's hard to understand exactly how big of a target these sites are until you look at the actual numbers. The Hotel & Travel industry saw 1.2 billion login attempts in November, and 968 million were attempts that Akamai has judged to be malicious. This means 82% of login attempts at these sites, or more than four out of every five, were malicious!

Breaking this down further, there are three main types of organizations most affected by credential abuse: airlines, hotels and resorts, and online travel agencies. Cruise lines also face a significant amount of login attempts, but in comparison their numbers are relatively small.

Credential abuse, whether by brute-force guessing or through the use of illegitimately acquired username and password lists, isn't a problem that will go away soon. People constantly reuse passwords, and far too many organizations aren't sufficiently monitoring logins. If your organization is in one of the high-threat industries, it may be time to re-examine how seriously you take the threat.

[SECTION]^{5} LOOKING FORWARD

Ah, the glory of cryptocurrency! By the time you're reading this, bitcoins might be worth $25,000 each. Or $250,000. Or maybe $250. But on January 1, 2017, the price of bitcoins hit $1,000 for the first time and was more than $13,500 at the beginning of 2018. Hype and speculation fuel a market in cryptocurrency that is likely to continue throughout 2018. Until the bubble bursts.

Why is the price of cryptocurrency important to the security industry? Because one group that adopted its use early was the hackers and criminals who used cryptocurrencies as a way for their targets to pay off extortion bribes. When groups like Lizard Squad and DDoS4Bitcoin (DD4BC) sent their threatening letters, they asked for just a few bitcoins. When the price of a bitcoin was under a thousand dollars, some businesses paid the price to avoid hassle. But their targets are wising up, as many organizations are aware that the threat is often a ruse, with the sender unable to follow through on their threats. Many extortionists rely on for-rent botnets and can't sustain long-term attacks or never had intent to attack at all.

In response, criminals are going to do the same thing that any good businessman does when their market dries up: switch to an adjacent market that has greater potential. We've already seen cryptocurrency exchanges be on the receiving end of DDoS attacks. Rather than being part of an extortion campaign though, it's more likely that these attacks are aimed at frustrating users to get them to move to the attacker's exchange.

Another attack we've already seen is compromise of exchanges, with criminals making off with millions of dollars' worth of cryptocurrencies. The problem with this type of attack, for the attackers, is that it kills the targeted exchange and makes users less likely to trust any exchange in the future. While it makes sense in the short term, long-term killing of Bitcoin exchanges is going to be killing a cash cow. It never makes sense to kill your supply of cash, which is why criminals will evolve further.

Instead, criminals may evolve tactics to try to infiltrate cryptocurrency exchanges and skim bits and bytes off the top of a large number of transactions. It's better to have a long-term, relatively stable income than take one big bite and run. This means attackers will compromise accounts and the APIs that make the exchanges accessible. The accounts are monitored by their account owners, but in large part the APIs that communicate and control most sites are underprotected.

This leads us to the final prediction of this report for 2018: APIs are going to be an increasingly popular attack surface for hackers. Akamai has seen growth in this area throughout 2017, and the lack of controls and safeguards most organizations have around their APIs make them tempting targets for people who want to compromise systems without being detected.

Are you confident your defenses cover your APIs sufficiently? Or at all?

State of the Internet / Security Team

Jose Arteaga, Akamai SIRT Lead, Data Wrangler — Attack Spotlight
Dave Lewis, Global Security Advocate — DDoS Activity, Web Application Attack Activity
Chad Seaman, Akamai SIRT — Attack Spotlight
Wilber Mejia, Akamai SIRT — Attack Spotlight
Larry Cashdollar, Akamai SIRT, Sr. Engineer — Web Vulnerabilities to Watch
Richard Willey, Sr. Data Scientist — How to Make Sense of a Planetary Scale Network
Elad Shuster, Security Data Analyst, Threat Research Unit
Jon Thompson, Custom Analytics

Editorial Staff

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

Note on the Library of Congress

The Library of Congress web archive was approximately 525 terabytes as of March 2014, and had a growth rate of 5 terabytes per month at the time, giving a conservative estimate of 750 terabytes of data as of January 2018. There are 8 bits to a byte, therefore this is equal to 6,000 terabits, since bits are used to measure traffic flows, not bytes. At a rate of 35 terabits per second the Library of Congress would require slightly more than 170 seconds to transmit, or 3 minutes to transmit. https://web.archive.org/web/20140731152821/http://www.loc.gov/webarchiving/faq.html#faqs_05

About Akamai

As the world's largest and most trusted cloud delivery platform, Akamai makes it easier for its customers to provide the best and most secure digital experiences on any device, anytime, anywhere. Akamai's massively distributed platform is unparalleled in scale with over 200,000 servers across 130 countries, giving customers superior performance and threat protection. Akamai's portfolio of web and mobile performance, cloud security, enterprise access, and video delivery solutions are supported by exceptional customer service and 24/7 monitoring. To learn why the top financial institutions, e-commerce leaders, media & entertainment providers, and government organizations trust Akamai please visit *www.akamai.com*, *blogs.akamai.com*, or *@Akamai* on Twitter. You can find our global contact information at *www.akamai.com/locations*. Published 02/18