[Volume 4 / Number 3]

[state of the internet] / security

Q3 2017 Report

Akamai

AT A GLANCE

Web application attacks, Q3 2017 vs. Q3 2016
69% increase in total web application attacks
217% increase in attacks sourcing from the U.S.
62% increase in SQLi attacks

Web application attacks, Q3 2017 vs. Q2 2017
30% increase in total web application attacks
48% increase in attacks sourcing from the U.S. (Q2 2017 Top Source Country)
19% increase in SQLi attacks

DDoS attacks, Q3 2017 vs. Q3 2016
3% decrease in total DDoS attacks
2% decrease in infrastructure layer (layers 3 & 4) attacks
2% decrease in reflection-based attacks

DDoS attacks, Q3 2017 vs. Q2 2017
8% increase in total DDoS attacks
8% increase in infrastructure layer (layers 3 & 4) attacks
4% increase in reflection-based attacks

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

What you need to know

- We welcome Chris Wysopal, Veracode Co-Founder and CTO, as our guest author this quarter. Mr. Wysopal highlights his view of the dangers presented by vulnerable code on the Internet.
- Akamai mitigated 4,376 Distributed Denial of Service (DDoS) attacks through Akamai's routed platform, an 8% increase over the previous quarter. These attacks were overwhelmingly volumetric attacks (99%).
- Germany was the origin of the greatest number of unique IP addresses (58,746) used in volumetric DDoS attacks — 22% of the global total.
- Gaming customers were targeted by 86% of all volumetric DDoS attacks. One customer suffered 612 attacks.
- Akamai researchers collaborated with multiple organizations in order to research the WireX malware, which led to the takedown of the Android-based malware and the removal of affected applications.
- The use of Fast Flux DNS by botnets is examined, highlighting why the use of rapidly changing DNS information helps attackers, by making it harder to track and disrupt botnets and malware.

LETTER FROM THE EDITOR / The *Q3 2017 State of the Internet / Security Report* represents analysis and research based on data from Akamai's global infrastructure and routed DDoS solution.

The third quarter of 2017 had its share of cyber security disasters. The Yahoo breach, which had previously been reported to have affected 1 billion accounts, now appears to have affected all 3 billion accounts on the platform. A major credit reporting company, Equifax, announced it was compromised, exposing the sensitive data of 146 million U.S. citizens. At Akamai, security data collected in Q3 revealed that DDoS extortion appears to be on the rise once more, and we saw the rise (and fall) of WireX, which leveraged compromised Android applications to fuel DDoS attacks with mobile phones and tablets. Additionally, both pharmaceutical giant Merck and shipping company FedEx have announced losses in excess of $300 million each, stemming from the impact of the NotPetya malware campaign.

The WireX malware research was interesting on multiple levels. First, this was one of the biggest Android-based botnets we've seen to date. Second, it gave Akamai's researchers an opportunity to work together with a number of organizations, including several direct competitors, to achieve a speedy takedown of both the botnet itself and the applications that had been compromised to generate the botnet.

Research and cooperation, like that which lead to the WireX botnet being dismantled, is becoming increasingly important, not only to the businesses doing the research, but to the overall health of the Internet. Even an organization like Akamai, which delivers on average more than 30 terabits per second of traffic, only sees a fraction of the total traffic of the Internet. No single organization has all the resources necessary to combat the ever-growing breadth of vulnerabilities — past, present, and future.

Collaboration and communication across organizations, researchers, and peers need to be consciously and actively supported in order for the Internet to be the robust growth engine it has been for the last two decades. If your industry has an Information Sharing and Analysis Center (ISAC) or if there is a local chapter of the Information Systems Security Association, get involved. At the business level, interact with your customer and supplier security teams whenever possible. It may be one of these relationships that save your organization from the next malware outbreak or major protocol vulnerability.

Finally, I write this from one of Akamai's main offices in Ft. Lauderdale, Florida. While we were hit by Hurricane Irma, and ***the office was shut down for several days***, most of our staff escaped the worst of the storm's fury. We were much luckier than the residents of Puerto Rico, Texas, Virgin Islands, and Mexico during this hurricane season. Our thoughts go out to the residents of all affected regions and hope for the best recovery possible for them.

— 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***.

In May 1998, the members of the Lopht Heavy Industries hacker collective sat before a U.S. Senate panel to warn the nation, and the world, about the inherent insecurity of software. A lot has changed since then. Software is far more pervasive — controlling the devices and applications that are the lifeblood of modern commerce and the digital economy. Cyber attacks are more far-reaching and consequential than we could have imagined 20 years ago — or even 10 years ago, when myself and fellow Lopht member Christien Rioux founded Veracode to secure the world's software.

Yet despite the promising and necessary growth in application security testing over that time, applications are generally no more secure today than they were a decade ago. Our scans over the past year of thousands of applications and trillions of lines of code have found a widespread weakness in applications — a top target of cyber attackers. Three in every four applications have at least one vulnerability, and nearly 12% of applications have a high or very high severity vulnerability. Less than a third of applications pass the Open Web Application Security Project (OWASP) Top 10 policy on the initial scan. As the security skills gap (the difference between experienced, skilled workers and those new to the field) grows, we're seeing the same coding errors cropping up, year after year. Most open source components remain unpatched once they're built into software. According to Veracode research, 88% of Java applications containing components had at least one flaw in a component.

If that weren't concerning enough, the stakes continue to rise. The unprecedented cyber attacks on elections in the U.S. and other democracies over the past year demonstrate that our most critical systems underpinning our modern, Internet-based society are being targeted. Global cyber attacks on a massive scale, such as the WannaCry and Petya ransomware attacks, have brought past warnings to reality.

GUEST AUTHOR

Chris Wysopal
Co-Founder & CTO
Veracode

The earlier predictions of cyber attacks knocking out electric utilities have proved to be not just possible, but increasingly likely. The threat of a cyber war between nation-state actors, with potential damage to infrastructure like hospitals, gets closer with every provocation. This should create a sense of urgency to finally tackle the problem of insecure software. Yet, conventional wisdom in security circles has drifted away from prevention in recent years toward detection and response. A reactive approach utterly failed to stop the destruction of the WannaCry and Petya attacks. The impact of potential future attacks, aimed specifically to be destructive, could create much greater damage.

Safe coding everyone.

Chris Wysopal
Veracode Co-Founder & CTO

6 [SECTION][1] = EMERGING TRENDS

8 [SECTION][2] = DDoS ACTIVITY

8 2.1 / DDoS Attack Vectors

11 2.2 / Attack Spotlight: The Lingering Effects of Mirai

13 2.3 / Reflection Attacks

15 [SECTION][3] = WEB APPLICATION ATTACK ACTIVITY

15 3.1 / Web Application Attack Vectors

16 3.2 / Top 10 Source Countries

19 [SECTION][4] = AKAMAI RESEARCH

19 4.1 / Digging Deeper—In-Depth Analysis of Fast Flux Networks

21 4.2 / The Wirex Botnet: An Example of Cross-Organizational Cooperation

22 [SECTION][5] = LOOKING FORWARD

[SECTION][1] EMERGING TRENDS

The DDoS trends in the third quarter of 2017 reflect an interesting mix of changes to the statistics we measure. While the overall number of attacks were up 8% compared with previous quarter, they were still down 3% from the same time the previous year. Similarly, after trending downward for the past couple quarters, the median attack size trended upward in Q3, returning to the record levels of 2016. This is also reflected in Figure 2-10: Attack Density and Trends.

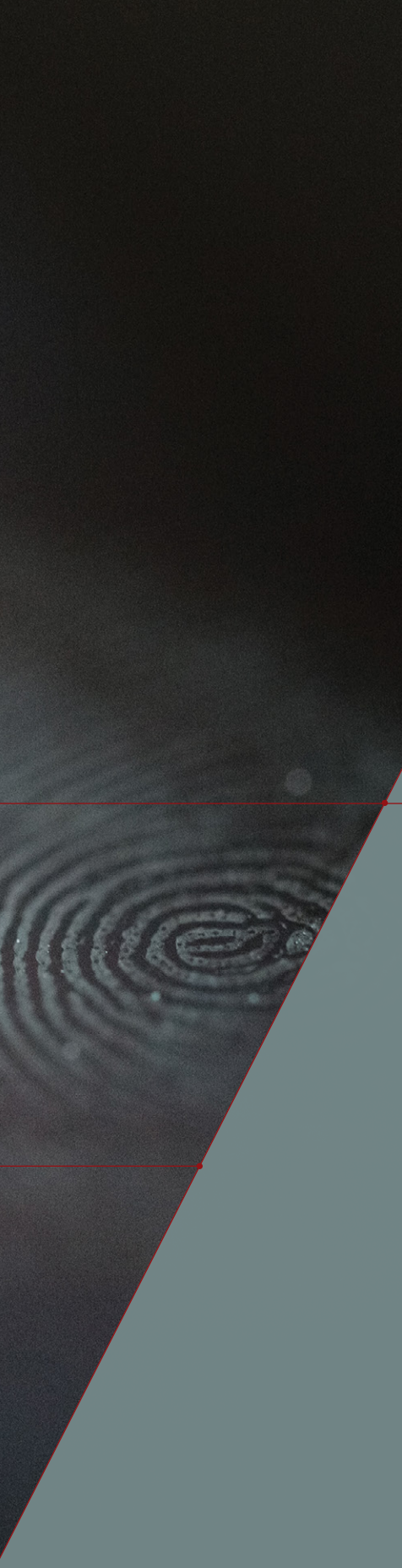
While the number of unique IP addresses involved in DDoS attacks increased last year, driven primarily by the Mirai botnet and its use of Internet of Things (IoT) devices, we saw a precipitous drop in the count in Q2. In Q3, the number of involved IP addresses rose modestly compared with the previous quarter, led by Germany, with Akamai seeing nearly 59,000 German IP addresses originating attack traffic in the third quarter.

Although we have not seen attacks of the same magnitude as those it generated late last year, the Mirai botnet is neither gone nor forgotten. This quarter saw two attacks that exceeded 100 Gbps, with one reaching 104 Gbps and a second measuring 109 Gbps. It is this second attack, and its use of a Mirai botnet, that is the focus of this quarter's Attack Spotlight. The lure of easy access to poorly secured end nodes and easily available source code make it likely that Mirai-based attacks won't be fading in the near future.

The Gaming industry continues to suffer from the most significant number of DDoS attacks seen by Akamai, with one client experiencing 612 attacks in the third quarter. This industry provides a rich target space that draws attackers who are expressing frustration or who hope to gain an advantage by slowing or interrupting the play of other gamers. Note that Akamai reclassified a group of customers into the Gaming vertical in the second quarter of 2017.

This quarter's report also highlights two recent Akamai research efforts. The first, an in-depth white paper titled ***Digging Deeper — In-Depth Analysis of Fast Flux Networks***, studies a growing trend in malware: the use of rapidly changing DNS information in order to obfuscate communications with botnet command and control structures, making it harder to identify and combat these threats.

The second research highlight focuses on WireX, showcasing a highly effective cross-company endeavor to take down the Android-based botnet, which had quickly reached more than 100,000 nodes. Researchers from more than half a dozen different companies, many of them competitors, collaborated to quickly and effectively defang the malware and remove it from the Android app store.



[SECTION]²
DDoS ACTIVITY

Building on the momentum from last quarter, Q3 witnessed a significant increase in the total number of DDoS attacks. In fact, there was a jump of 69% in the number of web alerts recorded year over year. In particular, there was a jump in attack traffic in September. The average number of attacks per target rose to a new high for 2017 of 36 per target.

2.1 / DDoS Attack Vectors / The spike in September's attack traffic can potentially be explained as correlating with the return of students to school. While this is speculative, it is possible the rise in attack traffic could be linked to students sharing information and trying new techniques that they might have learned during the summer break in North America, the United Kingdom, and Europe, among other places.

UDP fragment, DNS, and NTP topped the list for Q3 as the top three DDoS attack vectors, as shown in Figure 2-1. Infrastructure-related attacks such as these accounted for more than 99% of DDoS traffic, as has been typical in recent quarters. Infrastructure attacks dominate as the stock in trade of the attackers. The barrier to entry for someone to launch a DDoS attack, particularly at the infrastructure layer, is incredibly low right now. Anyone with interest and access to a search engine can find the resources needed to launch volumetric DDoS attacks with very little cost or effort.

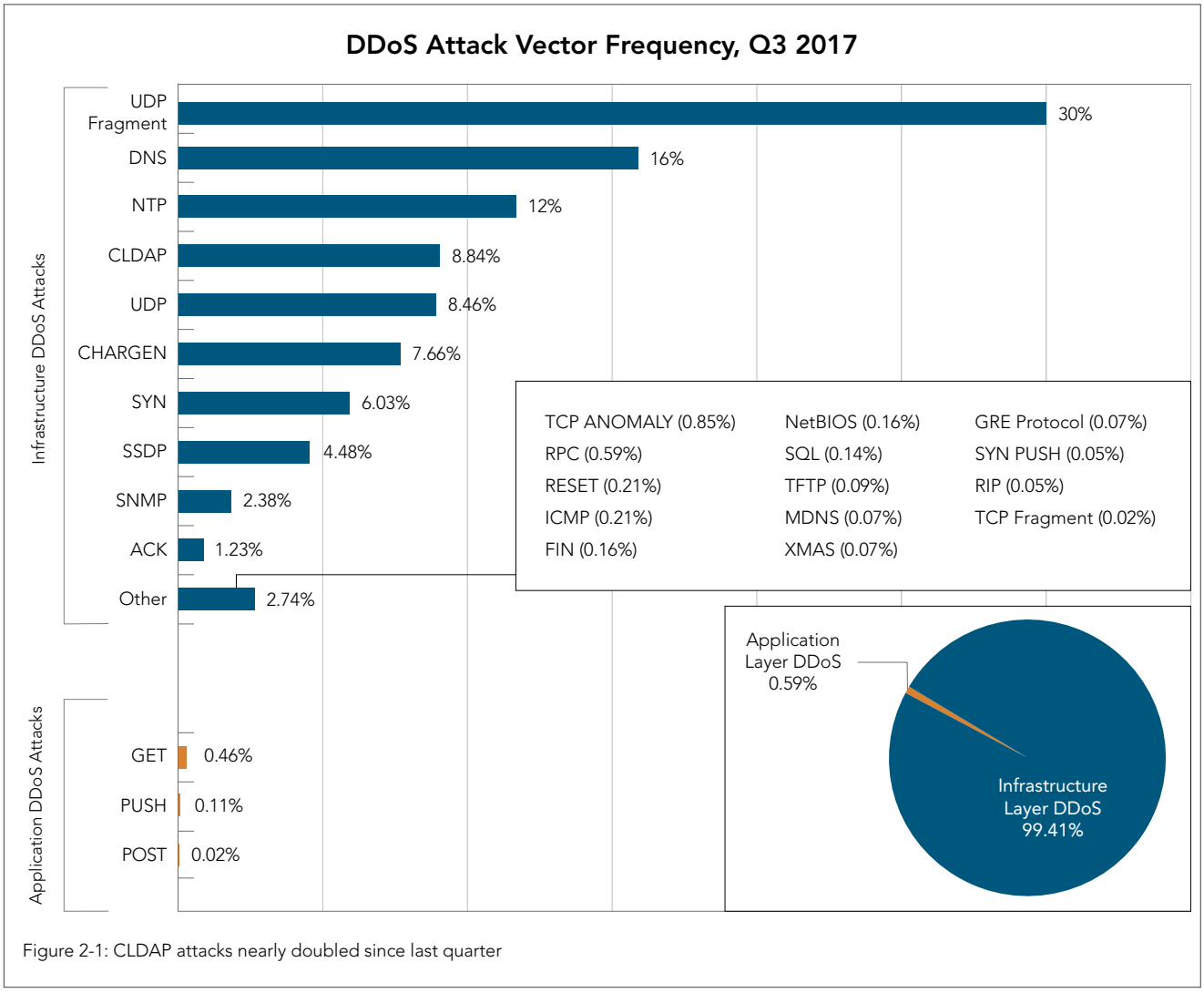


Figure 2-1: CLDAP attacks nearly doubled since last quarter

In the third quarter, application layer DDoS attacks, such as GET, PUSH, and POST floods, again accounted for less than 1% of overall DDoS attacks seen by Akamai. Most application layer attacks aren't meant to cause a denial of service but rather are used in an attempt to gain access to a system or its data via a weakness in the application.

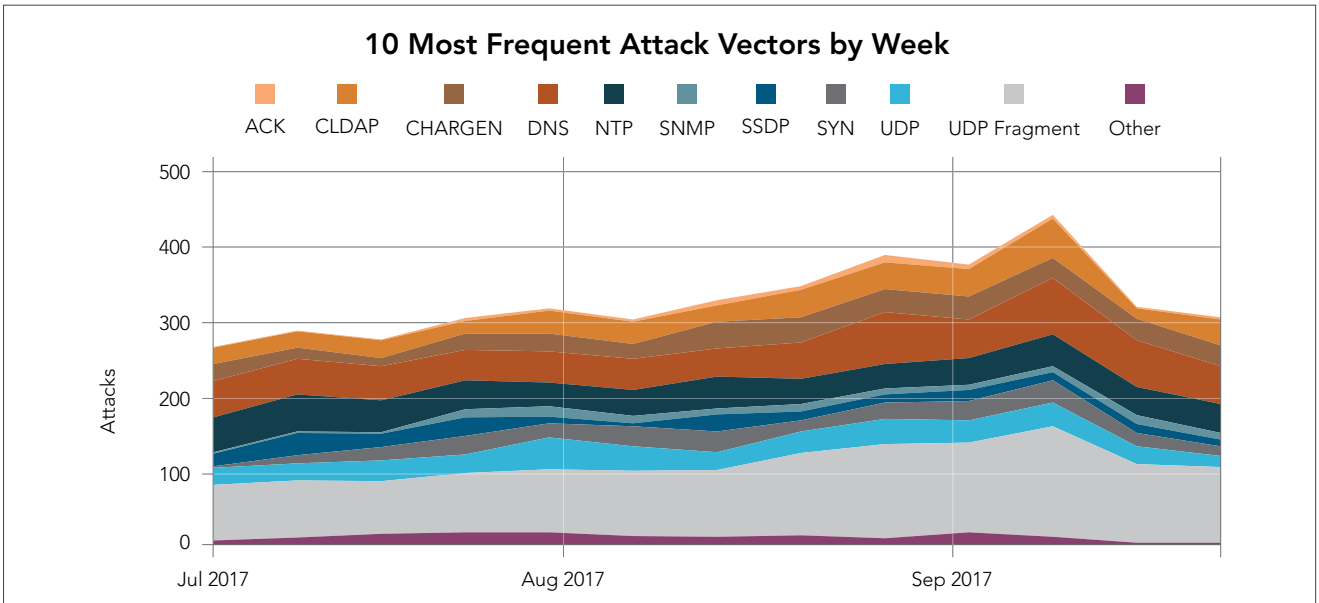


Figure 2-2: Attacks steadily climbed until the middle of September this quarter

In Q3, the 10 most frequent attack vectors showed a shift from the previous quarter, with ACK, CHARGEN, and CLDAP taking over the top three positions. UDP Fragment traffic technically had the highest frequency counts, because it includes fragments from protocols like DNS and NTP, which often require fragmentation of large packets and thus tracking of the fragments is less precise.

Despite not being among the top five source countries for DDoS attack traffic in the previous quarter, Germany had the largest number of attack traffic source IPs in Q3. Last quarter's leader, Egypt, fell out of the top five in the current quarter, while the U.S. maintained its second-place status.

Top 5 Source Countries for DDoS Attacks, Q4 2016–Q3 2017

Q3 2017		Q2 2017		Q1 2017		Q4 2016	
Country	Percentage Source IPs	Country	Percentage Source IPs	Country	Percentage Source IPs	Country	Percentage Source IPs
Germany	22%	Egypt	32%	U.S.	44%	U.S.	24%
	58,746		44,198		594,986		180,652
U.S.	14%	U.S.	8%	U.K.	13%	U.K.	10%
	38,628		11,113		177,579		72,949
India	7%	Turkey	5%	Germany	7%	Germany	7%
	19,722		7,049		87,780		49,408
China	6%	China	4%	Canada	5%	China	6%
	15,323		5,711		60,581		46,783
Mexico	5%	India	4%	Brazil	3%	Russia	4%
	13,501		5,224		43,863		33,211

Figure 2-3: Despite the continued effects of the Mirai botnet, the count of IP addresses involved in DDoS attacks normalized after spiking in Q1

DDoS Attack Frequency By Industry Q3 2017–Q2 2017

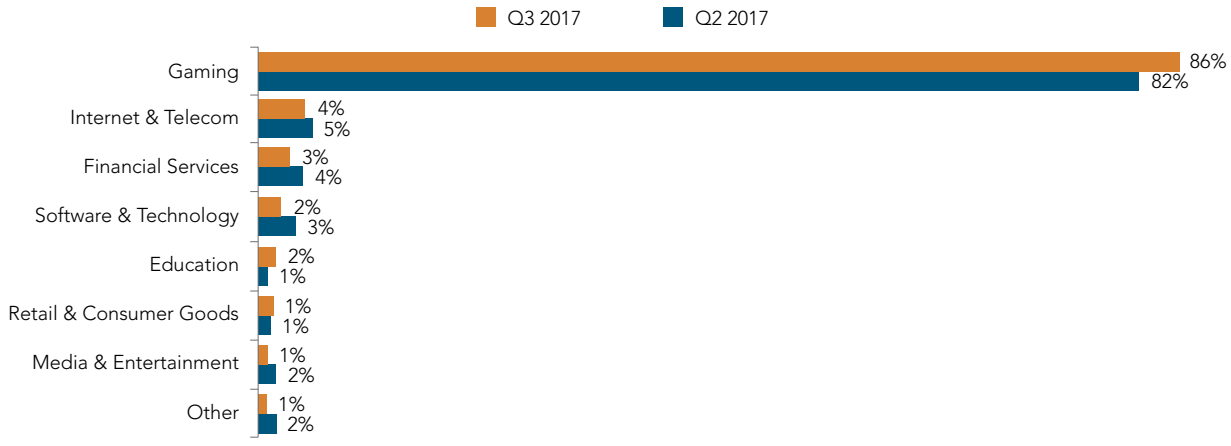


Figure 2-4: Gaming continues to be the most attractive target to attackers

Looking at DDoS attack frequency across industry verticals, in the third quarter, the Gaming industry again suffered the lion's share, with 86% of DDoS attack traffic being directed at their assets, up from 82% in the previous quarter. One gaming company experienced 612 such attacks during the third quarter of 2017 alone.

The overall number of attacks per target rose this quarter to a new high of 36, as shown in Figure 2-5. This average is up from 32 in the second quarter, due in part to the one gaming company targeted 612 times.

2.2 / Attack Spotlight: The Lingering Effects of Mirai / Summary / In Q3 2016, Akamai mitigated the initial wave of attacks from Mirai — a type of malware that infects and commandeers Internet of Things (IoT) devices. One of those attacks still stands as the highest peak bandwidth for a DDoS event ever recorded by Akamai, at 623 Gbps. Since the release of the Mirai source code, as well as the investigations and arrests that followed, attacks based on Mirai botnets have been less consistent; however, they are still occurring. One such attack this quarter peaked at 109 Gbps. While not at the record-breaking levels of last year, these targeted attacks can still greatly impact an organization.

Attack characteristics / Mirai has several well-known attack vectors built in. In the aforementioned attack, the ACK Flood vector was used. Peaking at 109 Gbps and almost 15 Mpps, this was the highest Gbps peak DDoS attack mitigated this quarter.

The signature of this attack indicates that many known defaults were used for the ACK Flood attack. One exception was that the data size was 900 bytes instead of the 512-byte default.

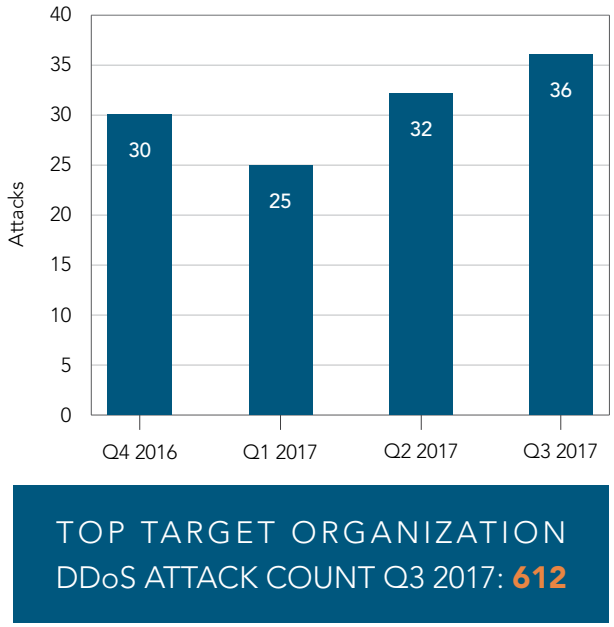


Figure 2-5: This quarter, the top target customer was hit an average of nearly 7 times every day

Mirai ACK Flood (900 Bytes of data padding)

```
23:11:10.702178 IP x.x.x.x.5761 > x.x.x.x.443: Flags [.], seq 238012458:238013358, ack 0, win
4527, length 900
23:11:10.702180 IP x.x.x.x.20140 > x.x.x.x.443: Flags [.], seq 1226016205:1226017105, ack 0,
win 12942, length 900
23:11:10.702188 IP x.x.x.x.16071 > x.x.x.x.443: Flags [.], seq 3394386813:3394387713, ack
1218155831, win 48297, length 900
23:11:10.702192 IP x.x.x.x.24894 > x.x.x.x.443: Flags [.], seq 1412836081:1412836981, ack
136022005, win 7248, length 900
E...-}..4...x.j..Q.da>..T6*.....P..P.....@'E[-..`.:...JI<..6P.'.v&x..s....o']....\".F...e,.L..
.U..o..      G.....W.Bz.....Y(....o..F.O...j/0..:........y1D.2b.X&}.M;...e.....m[.$1.S..1.D..
jE^....._~..|{Y..-.t...c|c..Z...U...O....-!.5.Yr      .....j][..?.....G.
|.f...m..s.M.$@..u ==...eN.5.8.(4...
.`..u..9..>.......38.....^.K/y...?..+.I9jFv..U.c.d....F.dk!`.7}.=J.....(;.....oq6G.Af3r..`....
.t.|.~q.d.3..A....&.`...b.....0.....}s..N...
...2..%.........R|...qi.....&.0.*..,#5[....83.{....#.....G.n.1...3V..Y1.-U.d...Z..%|......?l.
g..R...V.TL.....N*....2...v......E...t.GD.*N.M...L....k.<.....L..hzV25
....DC...9u.T:y...JH.y1.......)!.|....6%~........h....<".._/.@.|U....(R...........P....
..x.p4..........^..b..N..%.Yw....Hlb.....b....J....FI...]_i.I..r!....$....*..{.H...;.
.........e]..^..P..........^       ."vI/...o....|.....7..-6.~.....Af.;u ..........`...
DDR...g.../...z.s.S........{.[..[j8p.<C.Xk.H...7}W..=._'...N....rz.?...!.j..F.\l.#Z.`.I.Tg=...
```

Figure 2-6: Mirai ACK Flood signature for 109 Gbps attack

Furthermore, the signature was a close match to those observed during initial lab testing of the Mirai malware.

```
September 2016 - Akamai SIRT Lab Mirai ACK Flood(Single Source IP)
14:49:29.824663 IP x.x.x.x.21284 > x.x.x.x.80: Flags [.], seq 2845540187:2845540699, ack
2139545487, win 17777, length 512: HTTP
14:49:29.824664 IP x.x.x.x.17994 > x.x.x.x.80: Flags [.], seq 4073811652:4073812164, ack
3725369436, win 17777, length 512: HTTP
14:49:29.824665 IP x.x.x.x.64897 > x.x.x.x.80: Flags [.], seq 2572430443:2572430955, ack
3944923942, win 17777, length 512: HTTP
E..(Z...@..........l...P.T,k.".&P.Eq.......8/...*....um..d..........l:...:O'...d..`....6!.
.h......Xn.m...O........N...z.Q.p..-..Sg.Iw.....D..W...Y.....g....U....E.3....x.K~...'......
Vjc.4H..^[..G.......t.J..U. ..F.w.^.G..#...pd.|...$....N..&@..”lP.......h..T5x'...F....%)
U..m.g.@.n.E..e_...q6....T..[.s.yD....?D\.h...3.. ....]f.4.......1.Zk._;.]&t.Y#;....”l.jx-
.iR...3FP.
..x<._..@0R@.x.e6.....\...C.}Y.7f...#.hg......E. .-....:Q....rO`6>..pw.....T...{!./......~ko..
X.H.....$....^...#.X.........6....D...{P3w..aI.....ukd.:$.....R.....s.h.0r.N.2.`...$...
```

Figure 2-7: Mirai malware Lab testing shortly after last years attacks

The only obvious differences were in basic parameter changes, such as port destination (80 versus 443) and data size (900 bytes versus 512). The rest of the signature matches closely, indicating that the code used for this portion of the attack likely had little if any revision after the source was released.

Mirai Interaction and distribution / Akamai SIRT has been monitoring Mirai activity since the initial attacks late last year. The distribution method for this malware has not changed much: It scans the Internet for vulnerable IoT devices and tries logging into them using common default passwords. To reiterate the importance of taking extreme care in what devices we expose on the Internet, consider the time it takes for a well-known scanner to discover an open port. ZMap, when well connected, has the capability to scan the entire Internet in five minutes. Consequently, Mirai, even at its currently diminished capacity, is capable of infecting a device in seconds.

A recent test conducted by Akamai SIRT using MTPot, a Python-based honeypot developed by Cymmetria Research, found that an IP can be discovered in about 30 seconds.

```
MTPot log - time to infection
2017-10-12 16:07:59,549 [HoneyTelnet] INFO MTPot.py:218 Listening on 0.0.0.0:23 with timeout=60
2017-10-12 16:38:02,576 [HoneyTelnet] INFO MTPot.py:111 [x.x.x.x:54112] logon credentials
used: user:root pass:root
2017-10-12 16:38:02,576 [HoneyTelnet] DEBUG MTPot.py:123 [x.x.x.x:54112] session started
2017-10-12 16:38:03,974 [HoneyTelnet] DEBUG MTPot.py:77 [x.x.x.x:54112] executed: MIRAI
2017-10-12 16:38:03,975 [HoneyTelnet] DEBUG MTPot.py:51 [x.x.x.x:54112] Responding:
2017-10-12 16:38:36,501 [HoneyTelnet] INFO MTPot.py:111 [x.x.x.x:54190] logon credentials
used: user:666666 pass:666666
2017-10-12 16:38:36,501 [HoneyTelnet] DEBUG MTPot.py:123 [x.x.x.x:54190] session started
2017-10-12 16:38:38,971 [HoneyTelnet] DEBUG MTPot.py:77 [x.x.x.x:54190] executed: MIRAI
2017-10-12 16:38:38,972 [HoneyTelnet] DEBUG MTPot.py:51 [x.x.x.x:54190] Responding:
2017-10-12 16:38:56,611 [HoneyTelnet] INFO MTPot.py:111 [x.x.x.x:48264] logon credentials
used: user:root pass:12345
2017-10-12 16:38:56,612 [HoneyTelnet] DEBUG MTPot.py:123 [x.x.x.x:48264] session started
2017-10-12 16:38:58,812 [HoneyTelnet] DEBUG MTPot.py:77 [x.x.x.x:48264] executed: MIRAI
2017-10-12 16:38:58,814 [HoneyTelnet] DEBUG MTPot.py:51 [x.x.x.x:48264] Responding:
```

Figure 2-8: A Mirai scanner bot is discovered in this script

The easy potential for rapid discovery and infection of IoT devices sheds some light on why Mirai is still so prevalent today. In addition, new Mirai command and control servers continue to be formed, making it a very difficult type of malware to completely eradicate.

Summary / The Mirai botnet continues to be a threat. Given scanner activity, we must all be aware of the implications of connecting devices to the Internet. While the primary target port for Mirai still appears to be telnet, other malware may be searching for different ports. In addition, when new vulnerabilities are revealed, they may be followed by proofs of concept. In the case of remotely exploitable vulnerabilities, this code would also highlight a particular target port for exploit that should be secured and monitored if it exists in within a given network. These vulnerabilities can often be rapidly deployed, as was the case with Mirai, WannaCry, and Struts, to name a few.

The security of the Internet would be well served if devices were securely locked with restricted access and had the latest firmware installed prior to being enabled with remote Internet access. In many cases, convenience is seen to outweigh the security concerns of system configuration. Because of this, the impact of insecure devices extends beyond the device being compromised, spreading to include other networks or devices the compromised device may threaten.

2.3 / Reflection Attacks / For the Q3 report, we see that reflection attacks continued to hound defenders. In prior quarters, we saw that DNS, NTP, and CHARGEN were the top three reflection attack vectors. This quarter, however, CLDAP reflection jumped to third place, pushing CHARGEN to fourth. The continued use of these reflection attacks demonstrates a collective need to address these accessible services by patching and properly configuring them. 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.

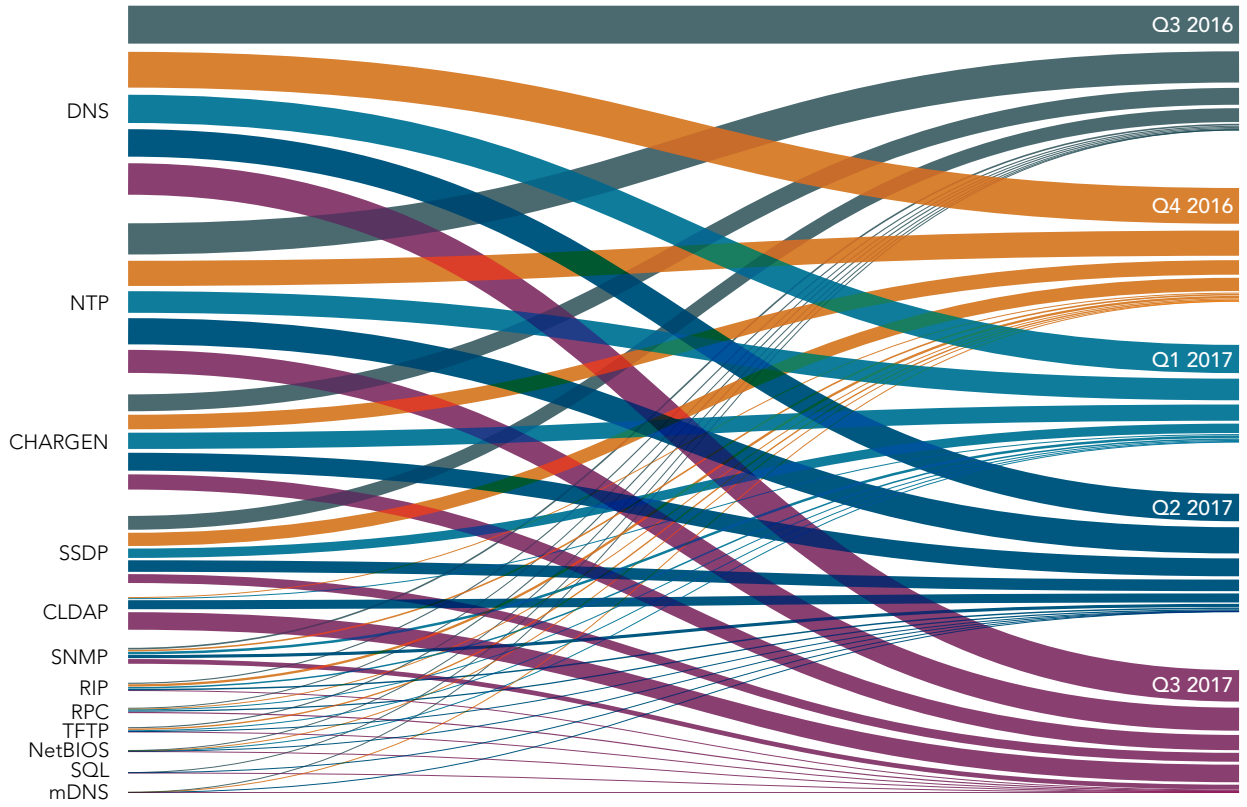


Figure 2-9: Attacks from reflector sources are a popular source of attack traffic, because they mimic legitimate traffic

Attack density and trends / Figure 2-10 shows changes in DDoS attack traffic since the beginning of June 2015, illustrating the density of attacks by volume, with trend lines representing the 5th, 25th, 50th, 75th, and 95th percentile of attacks. Specifically, the dotted red line at the top of the plot shows the traffic level that 95% of all attacks fall under, similar to what a high school student might see on her SAT report.

The color of the dots indicates how many attacks of a certain size occurred each week, with brighter colors representing a higher concentration of attacks. Yellow dots represent the highest density of attacks, shading to dark purple, which indicates the lowest density of attacks. The plot uses a logarithmic scale, so the difference in bandwidth increases tenfold between each major horizontal line. As a result, attacks on the lower end of the scale appear to be more spread out, but they are actually more tightly clustered than attacks on the high end of the scale.

The black curve represents the 50th percentile or median attack size for each time period, meaning that half the attacks were smaller and half were larger. In June of 2015, the median attack size was roughly 1.5 Gbps. The median had dropped as low as 520 Mbps by the beginning

of this year, but has since started to trend upward to 675 Mbps by the end of Q3. This highlights one of the themes we often discuss in the *SOTI/S Report*: DDoS attacks are cyclical and generally rise and fall again over time.

The solid blue and solid red curves represent the 25th and 75th percentile of attack sizes, respectively. As of September 2017, half of all volumetric attacks seen by Akamai were between 240 Mbps and 1.8 Gbps. The dotted blue and red lines show the 5th and 95th percentiles and indicate that at the end of the third quarter, 90% of all attacks were between 50 Mbps and 8.8 Gbps. In the first quarter, these numbers were closer together and trending downward, but now they are trending upward, and the spread between the upper and lower limits is increasing.

This data can help organizations better understand what size of DDoS attack to prepare for and how that is changing. When we first looked at this type of data in the Q1 2017 report, provisioning defenses for a 1.3 Gbps attack would have been sufficient to protect against 75% of all DDoS attacks, but that number has now gone up to 1.8 Gbps. Will the same defenses protect against attacks that are nearly 40% larger? Organizations need to understand how their existing protections might or might not hold up to the changing threat landscape, and re-evaluate their defenses based on their appetite for risk. Currently, 95% of all DDoS attacks peak at less than 8.8 Gbps, but with the proliferation of insecure IoT devices, that size will likely grow in the foreseeable future.

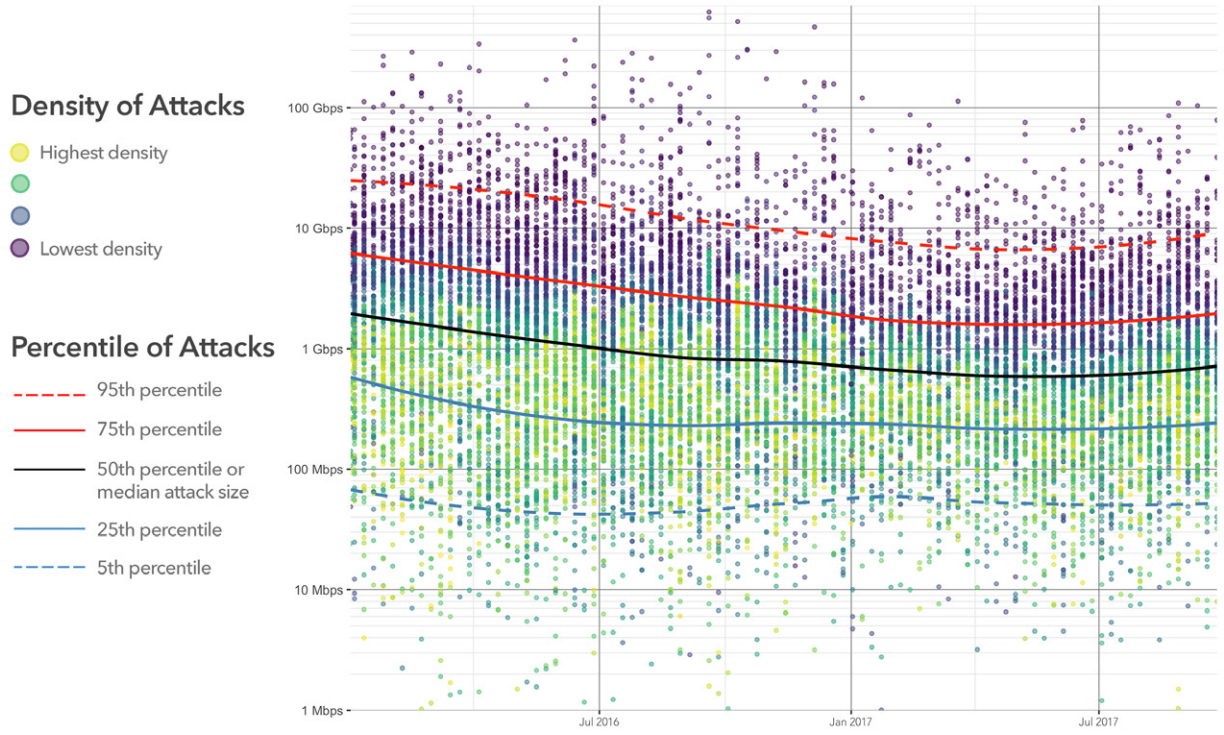


Figure 2-10: Numerous mid-sized attacks have a stronger influence on the median attack size than the rare outliers

[SECTION]3 WEB APPLICATION ATTACK ACTIVITY

In the third quarter of 2017, we saw a significant jump in web attacks overall. The number of attacks rose by 30% in Q3 while the number of attacks in the U.S. jumped 48% over what was documented in the Q2 report. The overall number of web attacks jumped 69% year over year.

3.1 / Web Application Attack Vectors / In Q3 2017, SQL injection (SQLi) attacks remained the preeminent web attack vector as shown in Figure 3-1, despite a 4% drop in the percentage of SQLi attacks as compared with Q2 (when SQLi comprised 51% of web application attacks). The percentage of SQLi attacks this quarter did show an increase from the first quarter of 2017, when SQLi attacks made up 44% of all web application layer attacks recorded across the Akamai network. The fact that SQLi remains in the top position shows that organizations have not taken the steps needed to sanitize data input and protect their applications. Attackers will continue to utilize these vectors to gain access to systems as long as there few or no protections

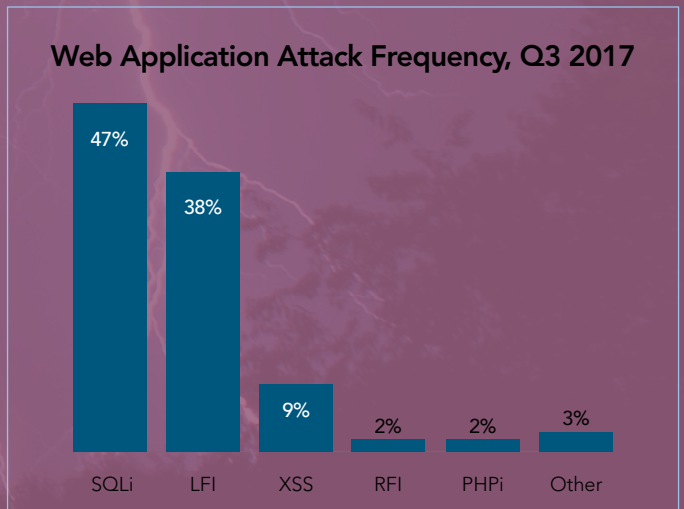


Figure 3-1: SQLi and LFI attacks accounted for 85% of web application attacks in Q3

in place and applications are not sanitizing data input and output. These attacks are easily automated and scalable, and they will typically look for any vulnerable system to attack, rather than targeting specific organizations.

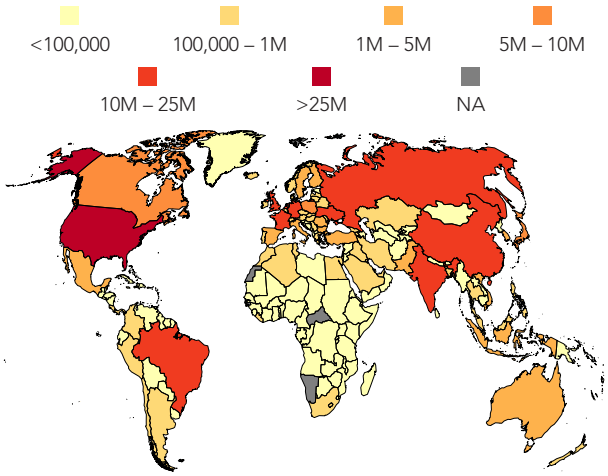
After SQLi attacks, Local File Inclusion (LFI) was the second most frequently used attack vector in the third quarter, comprising 38% of all application layer attacks. Cross-site scripting (XSS) came in third, used in 9% of the attacks recorded in Q3.

3.2 / Top 10 Source Countries / Q3 saw some changes in the overall landscape for web application attack source countries, although the U.S. remained the top source country, with 39% of all recorded attack traffic in Q3 having IP addresses originating in the U.S. Russia jumped to second place among source countries, up from eighth in the previous quarter, serving as the source of 7% of Q3 attacks. The Netherlands, also sourcing 7% of Q3 attacks, dropped from second place in Q2 to third place in Q3. Canada had been in 11th place for the last two quarters, and this quarter it dropped to the 12th position. The top three origins of attack traffic were the U.S. (39%), Russia (7%), and the Netherlands (7%).

Akamai tracks attacks against the Kona Web Application Firewall (WAF) based on the number of alerts and the region the attacks were detected in. Several countries, such as the Netherlands and Brazil, show a much higher amount of attack traffic than might be expected based on population. One explanation for these alerts is that significant attack traffic is originating from the country of record, while another is the use of VPNs with end nodes in the listed country.

In the EMEA region, Russia moved into the top position among web application attack sources in the third quarter, with more than 32 million attacks recorded, just surpassing the Netherlands' 31 million attacks. Ukraine rounded out the top three, with more than 29 million attacks recorded this quarter.

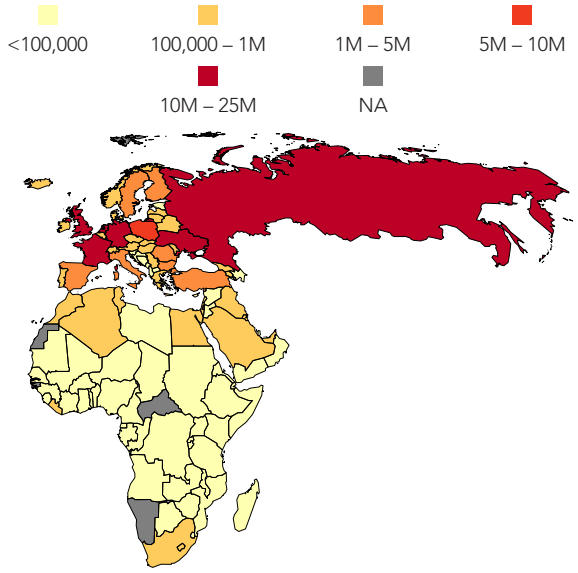
Source Countries for Web Application Attacks—Worldwide, Q3 2017



Country	Attacks Sourced	Percentage
U.S.	180,627,565	38.70%
Russia	32,164,336	6.90%
Netherlands	31,359,207	6.70%
Ukraine	29,678,769	6.40%
Brazil	28,626639	6.10%
China	22,046,824	4.70%
India	20,174,984	4.30%
Germany	16,285,895	3.50%
France	12,339,984	2.60%
Great Britain	11,363,904	2.40%

Figure 3-2: The majority of the web application attack traffic was detected as coming from the U.S., Russia, and the Netherlands this quarter

Web Application Attack Source Countries—EMEA, Q3 2017

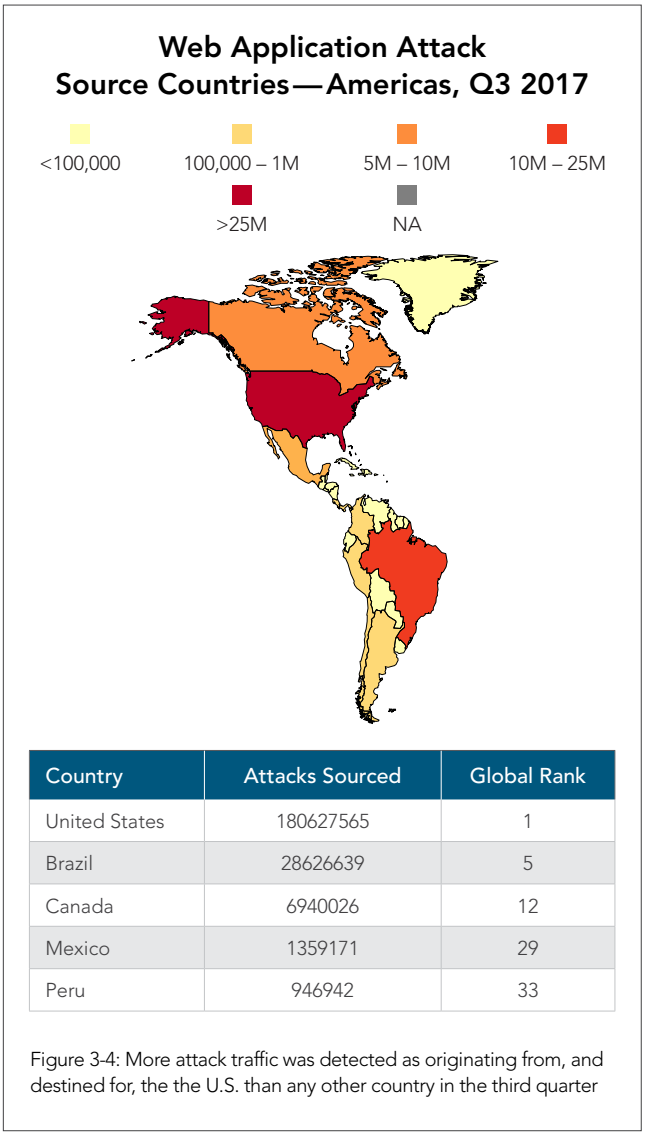


Country	Attacks Sourced	Global Rank
Russia	32164336	2
Netherlands	31359207	3
Ukraine	29678769	4
Germany	16285895	8
France	12339984	9

Figure 3-3: Russia, The Netherlands, and Ukraine were significant sources of web application attack traffic this quarter

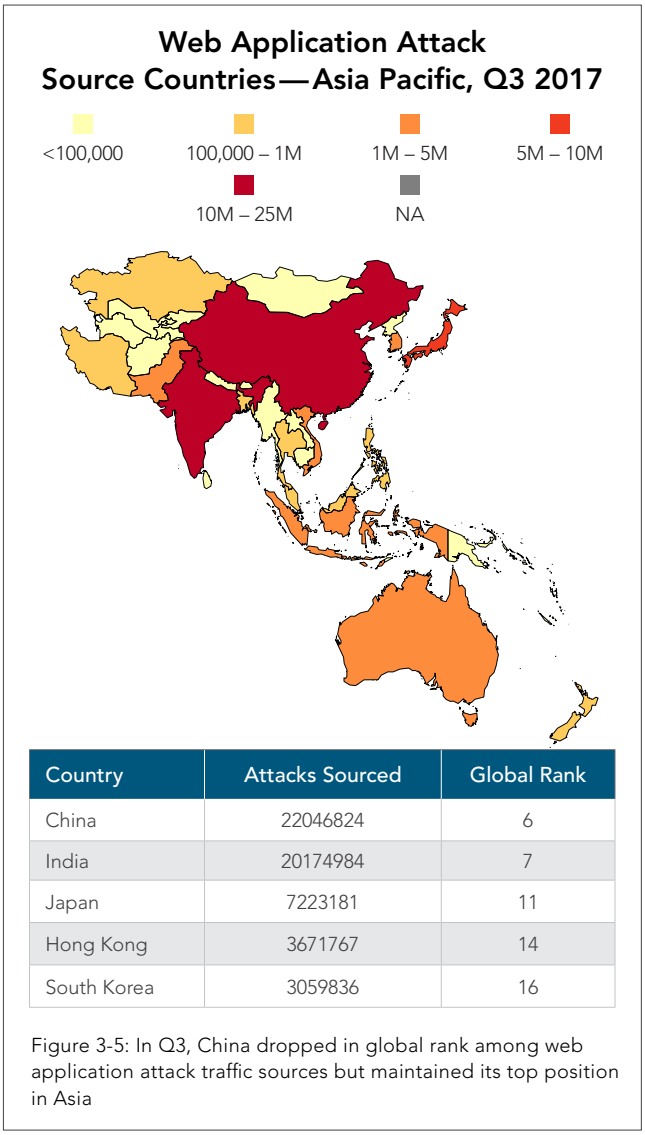
In the Americas this quarter, the top three attack traffic source countries — the U.S., Brazil, and Canada — all retained their positions relative to the second quarter, with millions of detected attacks per country. Mexico and Peru were in 4th and 5th position, with attack counts that were an order of magnitude smaller than the top three countries.

As illustrated by Figure 3-5, China ranked first in the Asia-Pacific region and sixth globally in the third quarter. China remained the overall top source country for web application attacks in the Asia-Pacific region, followed by India and Japan, just as in the previous quarter.



Country	Attacks Sourced	Global Rank
United States	180627565	1
Brazil	28626639	5
Canada	6940026	12
Mexico	1359171	29
Peru	946942	33

Figure 3-4: More attack traffic was detected as originating from, and destined for, the the U.S. than any other country in the third quarter

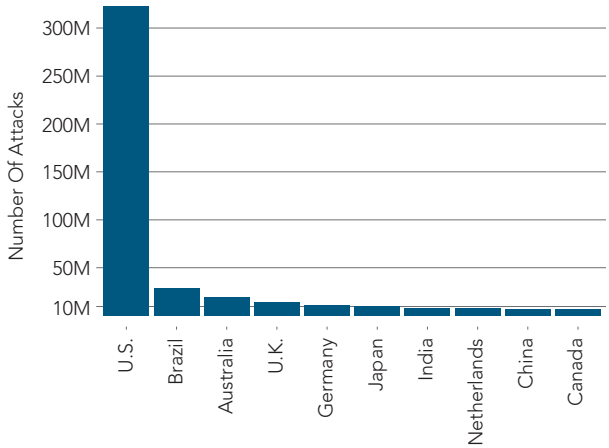


Country	Attacks Sourced	Global Rank
China	22046824	6
India	20174984	7
Japan	7223181	11
Hong Kong	3671767	14
South Korea	3059836	16

Figure 3-5: In Q3, China dropped in global rank among web application attack traffic sources but maintained its top position in Asia

The U.S. continued to shoulder the brunt of web application attacks, seeing more than 300 million attacks in the third quarter. This was a significant increase from the number of attacks (221 million) that targeted the U.S. in Q2, and was 10 times the number of attacks targeting Brazil, the country with the second-highest number of attacks in Q3. Brazil saw a 15% increase in attacks compared with the previous quarter. Australia was the country that suffered the third-most number of attacks in Q3, despite not even registering among the top 10 target countries in Q2.

Top 10 Target Countries for Web Application Attacks, Q3 2017



Target Country	Count
USA	323,185,079
Brazil	28,600,515
Australia	19,115,151
United Kingdom	14,637,260
Germany	10,656,679
Japan	10,098,902
India	8,369,704
Netherlands	8,230,129
China	7,041,135
Canada	6,389,153

Figure 3-6: The U.S. continues to be the prime target for attackers

[SECTION]4 AKAMAI RESEARCH

Akamai, like most security companies, is continually conducting research in order to better understand the types of attacks that affect our customers and our networks. Curiosity drives our engineers to look into the problems facing us on a daily basis, and often this leads to external publications to help other organizations better learn from our discoveries. This section of the *State of the Internet / Security Report* highlights recent research, providing brief excerpts of larger papers. Most research can be read in full on the Akamai blog, ***https://blogs.akamai.com***.

4.1 / Digging Deeper—In-Depth Analysis Of Fast Flux Networks / The following is an excerpt from a white paper authored by Or Katz, Senior Researcher at Akamai. The full white paper is available at ***https://www.akamai.com/uk/en/multimedia/documents/white-paper/digging-deeper-in-depth-analysis-of-fast-flux-network.pdf.***

Introduction / Recently, we have seen ***large-scale botnets*** used to execute attacks rarely seen in the past. These botnets incorporate new features and have bigger capabilities. How do these botnets remain resilient to detection?

Fast Flux is a DNS technique used by botnets to hide various types of malicious activities, such as phishing, web proxying, malware delivery, and malware communication, behind an ever-changing network of compromised hosts acting as proxies. The Fast Flux network concept was first introduced in 2006, with the emergence of ***Storm Worm***

malware variants. The Fast Flux network is typically used to make the communication between malware and its command and control server (C&C) more resistant to discovery. Akamai's Enterprise Threat Protector (ETP) Research Team has analyzed sophisticated botnet infrastructure that leverages Fast Flux techniques including domains, nameservers, and IP address changes. Figure 4-1 shows an overview of such a network, which can also be referred to as a form of ***bulletproof hosting***, that hosts various malicious services. These networks empower bad actors to execute attack campaigns by utilizing network capabilities to host malware binaries, proxy communication to C&C servers, phishing websites, or proxy attacks on websites across the Internet.

Akamai's high visibility to both web and enterprise traffic gave us the ability to get new and unique insights on the behavior of such Fast Flux networks.

According to our research, we were able to track a botnet that is using Fast Flux techniques with more than 14,000 IP addresses associated with it, with most of the IP addresses originating from eastern Europe. Some of the associated IP addresses are in address space that is assigned to Fortune 100 companies. These addresses are most likely used by the Fast Flux network owner as spoofed entities and are not genuine members of the Fast Flux network. This allows the botnet to inherit the reputation of the Fortune 100 companies.

This research includes an in-depth analysis of the discovered Fast Flux network, and presents:

- How network fluxing is using domains, IP addresses, and even nameservers to become resistant to discovery
- How a Fast Flux network is being segregated to different sub-networks based on the offered malicious service
- How the analyzed Fast Flux Network offers services such as malware communication (proxying) and hosting malware binaries, websites that sell various stolen credentials, and phishing websites
- How web attacks such as web scraping and credential abuse go through the Fast Flux network
- How to detect and defend against such networks

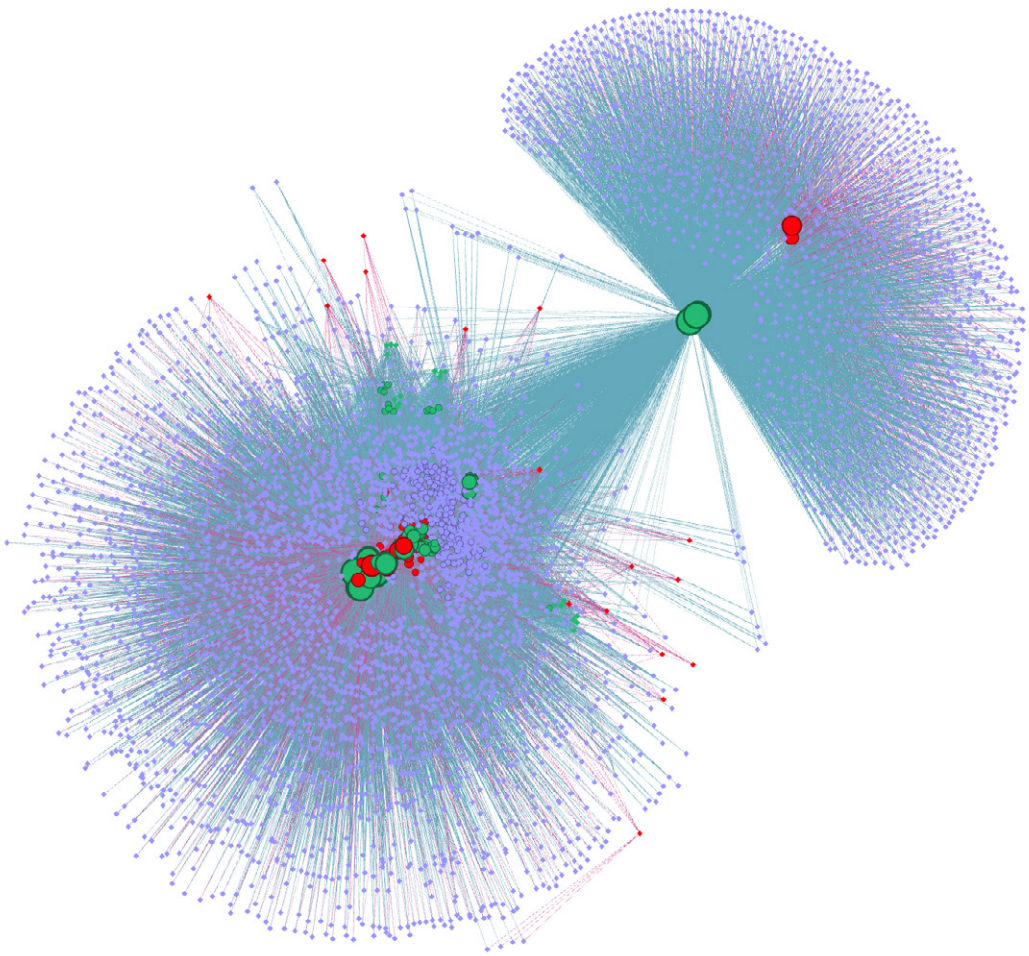


Figure 4-1: Graph network of Fast Flux domains, associated IP addresses, and associated nameservers

4.2 / The Wirex Botnet: An Example of Cross-Organizational Cooperation / The following is an excerpt from a blog post written by researchers at Akamai and other organizations in cooperation. Included is the text of the introduction and conclusions of the research. For the full post, please visit ***https://blogs.akamai.com/2017/08/the-wirex-botnet-an-example-of-cross-organizational-cooperation.html***.

Introduction / On August 17, 2017, multiple Content Delivery Networks (CDNs) and content providers were subject to significant attacks from a botnet dubbed WireX. The botnet is named for an anagram for one of the delimiter strings in its command and control protocol. The WireX botnet comprises primarily Android devices running malicious applications and is designed to create DDoS traffic. The botnet is sometimes associated with ransom notes to targets.

A few days ago, Google was alerted that this malware was available on its Play Store. Shortly following the notification, Google removed hundreds of affected applications and started the process to remove the applications from all devices.

Researchers from Akamai, ***Cloudflare***, ***Flashpoint***, Google, Oracle Dyn, ***RiskIQ***, Team Cymru, and other organizations cooperated to combat this botnet. Evidence indicates that the botnet may have been active as early as August 2, but it was the attacks on August 17 that drew the attention of these organizations. This post represents the combined knowledge and efforts of the researchers working to share information about a botnet in the best interest of the Internet community as a whole. This blog post was written together by researchers from numerous organizations and released concurrently by Akamai, Cloudflare, Flashpoint, and RiskIQ.

Conclusion / These discoveries were only possible due to open collaboration between DDoS targets, DDoS mitigation companies, and intelligence firms. Every player had a different piece of the puzzle; without contributions from everyone, this botnet would have remained a mystery.

The best thing that organizations can do when under a DDoS attack is to share detailed metrics related to the attack. With this information, those of us who are empowered to dismantle these schemes can learn much more about them than would otherwise be possible.

These metrics include packet captures, lists of attacking IP addresses, ransom notes, request headers, and any patterns of interest. Such data should not contain any legitimate client traffic, to reduce privacy concerns and also because legitimate traffic can pollute and slow down analysis. And most importantly, give permission to share this data — not only to your vendors, but to their trusted contacts in the broader security community who may have expertise or visibility not available in your own circle of vendors.

There is no shame in asking for help. Not only is there no shame, but in most cases it is impossible to hide the fact that you are under a DDoS attack. A number of research efforts have the ability to detect the existence of DDoS attacks happening globally against third parties no matter how much those parties want to keep the issue quiet. There are few benefits to being secretive and numerous benefits to being forthcoming.

Sharing detailed attack metrics also allows for both formal and informal information sharing groups to communicate about and understand the attacks that are happening at a global scale, rather than simply what they see on their own platforms. This report is an example of how informal sharing can have a dramatically positive impact for the victims and the Internet as a whole. Cross-organizational cooperation is essential to combat threats to the Internet and, without it, criminal schemes can operate without examination.

We would like to acknowledge and thank the researchers at Akamai, Cloudflare, Flashpoint, Google, RiskIQ, Team Cymru, and other organizations not publicly listed. We would also like to thank the FBI for their assistance in this matter.

[SECTION]5
LOOKING FORWARD

Natural disasters have continued to provide some of the best bait for phishing attacks, as criminals prey on people who are frightened and desperate, expecting to be contacted by governmental agencies or aid organizations offering help in their time of need.

However, natural disasters do not seem to correlate with other types of attacks on the Internet. The data collected by Akamai this quarter showed no definitive indication of changes in attack patterns driven by this quarter's devastating hurricanes, fires, or earthquakes, for example.

In many ways, this makes sense. The majority of DDoS attacks seem to be motivated either by money or anger. In other words, attackers are either hoping to extort money from the owners of the site, or they are attempting to take a site offline for political, ideological, or other personal reasons. Application attacks are even more commonly financially motivated, though politics are playing an increasing role in this threat landscape as well.

With the holiday shopping season upon us, Akamai expects that both the monetary and emotional aspects of attack dynamics will strongly influence behavior in the fourth quarter. Criminals will leverage the fact that the final quarter of the year is critical for merchants, making the merchants much more likely to pay an extortion letter threatening an attack on Black Friday or Cyber Monday than at many other times of year.

In past years, we have also seen a trend of attacks on gaming companies during the holiday season, reaching volumes that are much higher than those seen during the rest of the year. While some of these attacks come from criminals for their own ends, others appear to be coming from gamers themselves, either as an expression of frustration at losing a game, or possibly to achieve a competitive advantage over a gaming opponent.

While warnings of holiday season attacks are hardly novel, this season could see new attacks such as those based on IoT devices or mobile platforms. As noted in the Attack Spotlight, the code base from Mirai is still being used and is evolving. In addition, criminals are getting better at hiding their command and control structures, using techniques like Fast Flux DNS. And despite defenders' best efforts, malicious software authors are learning how to better penetrate stores where we buy the applications for our smart phones and tablets.

On the other hand, defenders are getting better at working together and sharing important information to help detect and combat attacks. Through the *SOTI/S Report*, as well as more in-depth research reports, Akamai brings you cutting-edge insight into the ever-changing landscape of attacks and attack tools — delivering the insight to help you and your team protect your organization.

***State of the Internet / Security* Team**
Jose Arteaga, Akamai SIRT, Data Wrangler — Attack Spotlight
Dave Lewis, Global Security Advocate — DDoS Activity, Web Application Attack Activity
Chad Seaman, Akamai SIRT — Attack Spotlight, WireX
Wilber Mejia, Akamai SIRT — Attack Spotlight
Alexandre Laplume, Akamai SIRT — Attack Spotlight
Elad Shuster, Security Data Analyst, Threat Research Unit
Ory Segal, Senior Director, Threat Research Unit
Or Katz, Principal Lead & Security Researcher — Fast Flux Networks
Jon Thompson, Custom Analytics

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

Creative
Shawn Doughty, Creative Direction
Brendan O'Hara, Art Direction & Graphic Design
Georgina Morales-Hampe & Billy Kamenides, Project Management

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 11/17