THREAT ANALYSIS REPORT

THE HUNT FOR IOT

THE NETWORKS BUILDING DEATH STAR-SIZED BOTNETS FROM IOT MINIONS

by Sara Boddy and Justin Shattuck

F5 LABS

VOLUME 2
February 2017

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

For over a year now, F5 Labs and our data partner, Loryka, have been monitoring the ongoing hunt by attackers to find vulnerable IoT devices they can compromise. In our first report, DDoS's Newest Minions: IoT Devices,[i] our research proved what many security experts had long suspected: IoT devices were highly vulnerable to exploit, the level of interest in exploiting them was high, and distributed denial-of-service (DDoS) attacks using these devices were already occurring. Our findings and conclusions in Volume 1[1] rang true, and the new numbers show even steeper growth than we had imagined.

In 2016, "the hunt" trendline mimics a hockey stick, with an annual growth rate of 1,473%, rising steadily and then spiking in Q4. This spike isn't surprising, given the timing and events of the Mirai botnet. Although Mirai is self replicating, it's a stretch to attribute all Q4 traffic (1.5 times greater than Q1 through Q3 combined), to Mirai because of the continual cleanup of infected devices and ISPs blocking Mirai traffic. What's interesting is a comparison of the growth in attack voume to the growth in participating networks (autonomous system numbers, or ASNs). From calendar Q3 to Q4, IoT attacks grew 110% while participating networks stayed relatively flat at 10%. Yet, the number of unique IP addresses participating within those ASNs grew at a rate of 74%. **This indicates that threat actors within the same networks are increasing their activity.** Furthermore, we can infer that threat actors are becoming more efficient because the rate of unique user name and password combinations attempted is decreasing.

1,473%
2016 IOT HUNT GROWTH RATE

[1] Volume 1 of this series of reports covered roughly five and a half months of data collected between mid-February and July 27, 2016. Volume 2 (this report) covers six months of data collected from July 1, 2016 through December 31, 2016.

Key findings:

- Networks in China (primarily state-owned telecom companies and ISPs) headlined the threat actor list, accounting for 44% of all attacks in Q3 and 21% in Q4 (that drop likely due to global interest in Mirai).
- Behind China, the top threat actors in Q3 were Vietnam and the US, and Russia and the UK in Q4. Surprisingly, the UK jumped from number 15 in Q3 to number 3 in Q4, with most activity coming from an online gaming network.
- In Q3 and Q4, the top 4 targeted countries were Russia, followed by Spain, then the US, then Turkey. Russia was a top target of all top 50 source countries, at 31% in Q3 and 40% in Q4. These efforts coincided with the high-profile US election and allegations of Russian hacking.
- Most attacks were launched from Linux systems within hosting provider and telecom companies.

Defense strategies for IoT attacks:

1. Have a DDoS strategy that can support attack sizes beyond your network capacity.
2. Ensure that all your critical services have redundancy, even those you outsource.
3. Put pressure on IoT manufacturers to secure their products by doing your own security testing before you buy large quantities of IoT devices that will be deployed to your customers. And don't buy products (personally or professionally) that are known to be insecure or compromised.
4. Share your knowledge—including information about vulnerable devices, attacks and threat actors, mitigation efforts that are working, and potential solutions—with other security professionals.

INTRODUCTION

Since we published Volume 1 of this report, the world has felt the stinging blow of the Mirai attacks[ii] on Krebs On Security and OVH (in September 2016), and Dyn, Inc. (in October 2016). When we began writing this report, we were still trying to wrap our heads around the startling allegation that Dyn's DNS service was attacked by tens of millions of unique IP addresses[iii] that belonged to seemingly innocuous IoT devices (IP cameras). Even more startling was that the Mirai attacks measured in the terabits-per-second (Tbps).

A year ago, 60 Gbps was considered a large attack. In June 2016, we published an article[iv] predicting that 100 Gbps DDoS attacks would be the "new normal," with peaks in the 400–500 Gbps range. Yet, like rapid fire, attack sizes rose astonishingly to Tbps with Mirai. And, because Mirai's creator decided to release the source code, the capability to launch IoT DDoS attacks is now in the hands of anyone with the skills to use it.

THE CAPABILITY TO LAUNCH IoT DDoS ATTACKS IS NOW IN THE HANDS OF ANYONE WITH THE SKILLS TO USE IT.

IN THIS REPORT

The value of threat intelligence is in its ability to drive change to be prepared for an attack. In the wake of these high-profile attacks, the attackers' "reconnaissance phase" in which they probe, scan, and search for vulnerable IoT devices to compromise and control in their botnets, is very telling. What level of activity built an IoT botnet capable of launching Tbps DDoS attacks? Which networks participated in these activities? Who were they targeting? In this report, we show you the hunt for IoT devices before, during, and after Mirai, because the volume of the hunt is an indicator of what's to come. We expose the networks behind the hunt for IoT devices, the companies that own those networks, and which countries are being targeted.

Why this focus? A big reason many companies are caught by surprise is that, until now, most of our security controls have focused solely on the attack and post-attack phases—both of which occur months, if not years, after the attackers' recon phase. The recon phase is always followed by a build phase when attackers use the data they've collected to plan an attack. Afterward, they strike quickly and decisively, and then get out. By focusing on what's happening in the early and intensive recon and build phases, we can provide valuable threat intelligence that organizations can use to anticipate and prepare for attacks before[v] they happen. When it comes to IoT, the high-volume hunt, plus the vast attacking capabilities beyond just DDoS[vi] ("IoT Bots of X"), are the threats all businesses globally must pay attention to.

WHAT WE KNOW POST-MIRAI

A point worth noting from our Volume 1 report is the 140% year-over-year increase in Telnet brute force attacks, which are used to compromise IoT devices. The industry has been calling this attack method "brute force," but that's not terribly accurate anymore when all it takes is one attempt if an attacker already knows the user name and password. (Consumers often don't bother to (or aren't able to) change the vendor default passwords on IoT devices, so when attackers crack one, they crack them all. In an instant, the attacker has access to potentially thousands, if not millions, of devices to add to a botnet.) This is why we believe that IoT attacks will soon be referred to as "credential stuffing" attacks.

Attackers used exactly this technique—scanning for Telnet ports and vendor default passwords on IoT devices—to create the Mirai botnet. It might seem like these attacks happened overnight but, in reality, a bot herder had been slowly searching for, finding, and compromising vulnerable IoT devices for at least a year prior.

> ***"Perimeter-less" and "identity-less," IoT devices are the perfect target for attackers with world-routable IP addresses, lack of security controls, and ridiculously simple default admin passwords that leave them virtually unprotected.***

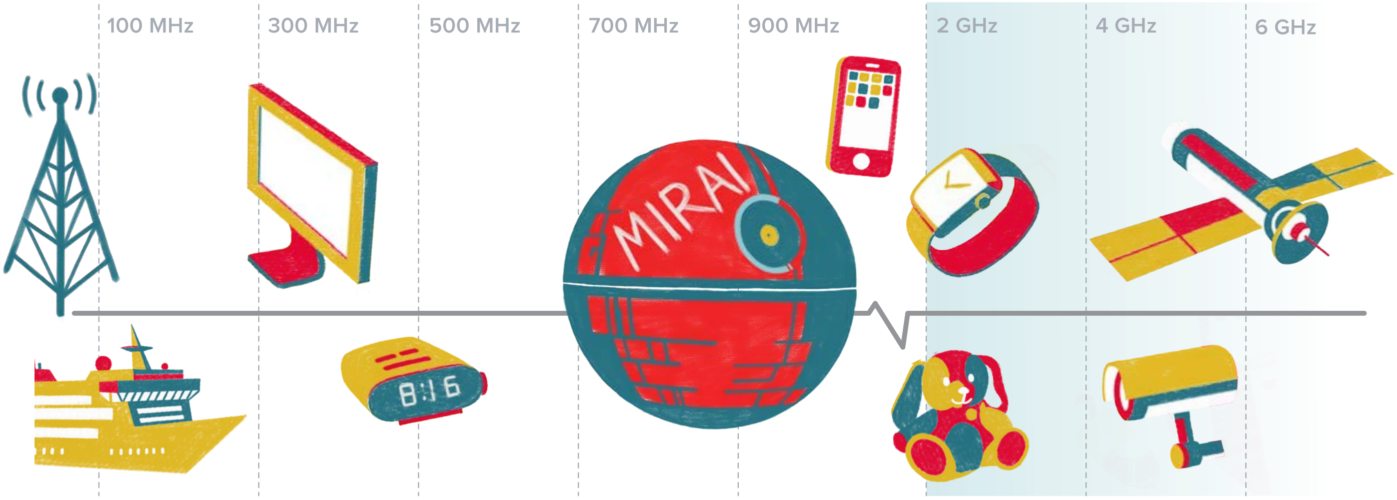
Here's what we know today about IoT threats in the shadow of Mirai:

1. **IoT devices are critically vulnerable, and the scope is global.** IoT devices have little capacity for securing themselves. An end user can reboot a compromised IoT device to clear its memory of malware, but unless the access issue is fixed (that is, default passwords are changed; security controls are added), the device will just get compromised again. There are many Mirai botnets now, and they're constantly scanning for new devices.

2. **IoT attacks can impact large targets, previously thought to be untouchable.** The collective firepower of an IoT botnet can be greater than terabits per second, and we don't yet know just how big they can get.

3. **Bot operators aren't afraid to turn their cyber weapons against some of the largest providers in the world.**

We know that there are billions of IoT devices in use around the world today[vii], but we don't yet know what percentage are vulnerable or already compromised. A billion IoT devices is at best a huge number of small things, but a lot of them require more bandwidth to function then a teddy bear, toaster, or door knob, and some have outbound capabilities upwards of 200 megabytes (like DVRs and digital signage systems). If the spectrum of IoT devices by strength goes from a light bulb at the low end to a DVR at the high end, Mirai was supposedly built with security cameras, which probably fall somewhere in the middle of the spectrum. We are just beginning to see the tip of the iceberg of what's possible with IoT devices and their attacks. The full threat hasn't been realized yet.



THE 2016 HUNT VOLUME

This report focuses on the Telnet attack activity that occurred in calendar Q3 and Q4 of 2016. Because we are focusing on the hunt for IoT only in this report, we included SSH brute force attack data (with one exception in table 2 below). The full-year trend is also significant, so we provide multiple views of the dataset—quarterly and monthly—to illustrate growth trends and activities both pre- and post-Mirai.

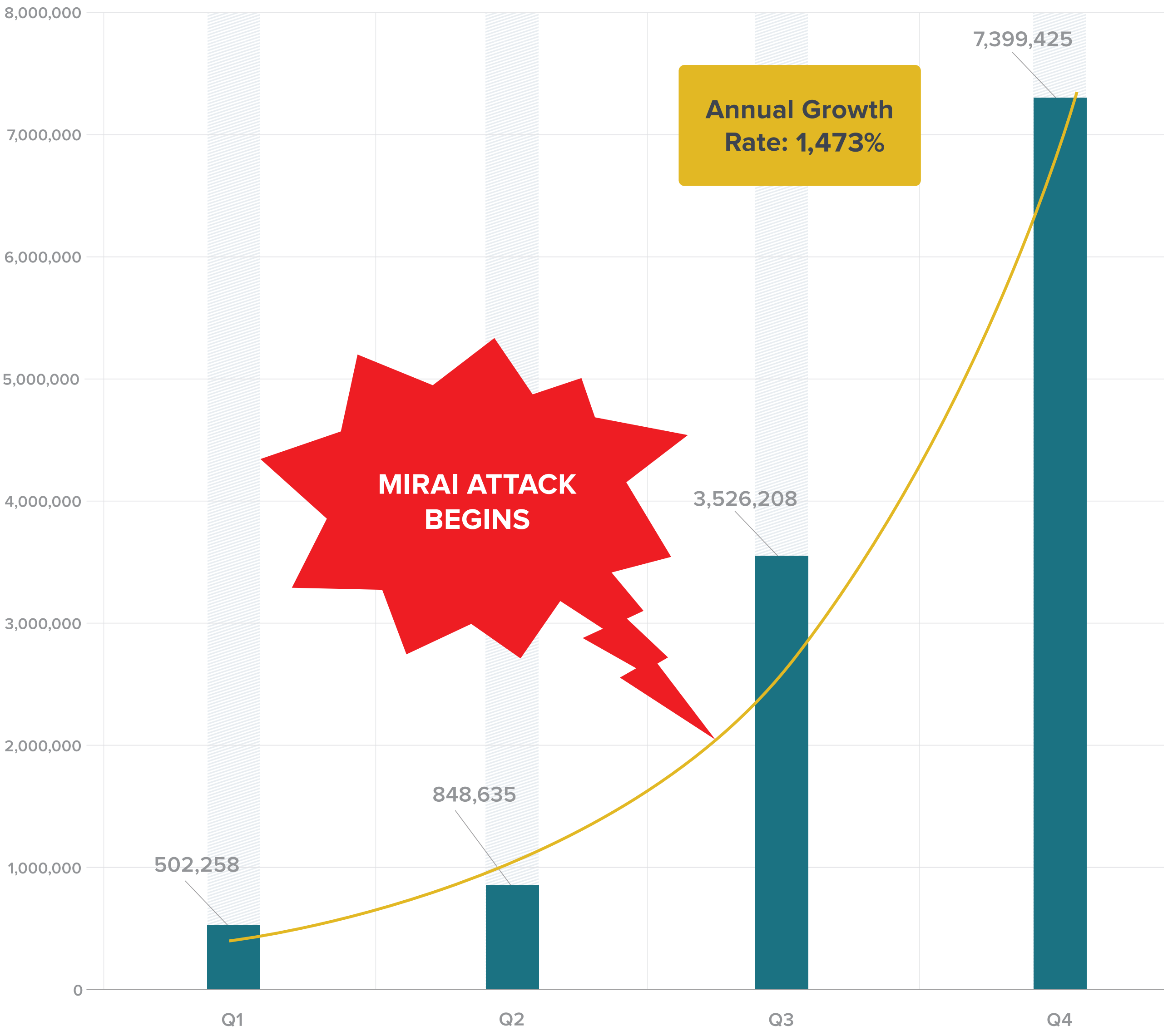


Figure 1. 2016 IoT Telnet attacks by quarter

The IoT attack volume in Q4 spiked in October, most likely driven by interest in Mirai. While the number of attacks fell off in November and December, the Q4 total was still significantly higher than in Q3, and the total volume in Q4 was 1.5 times greater than the combined attacks across Q1, Q2, and Q3.

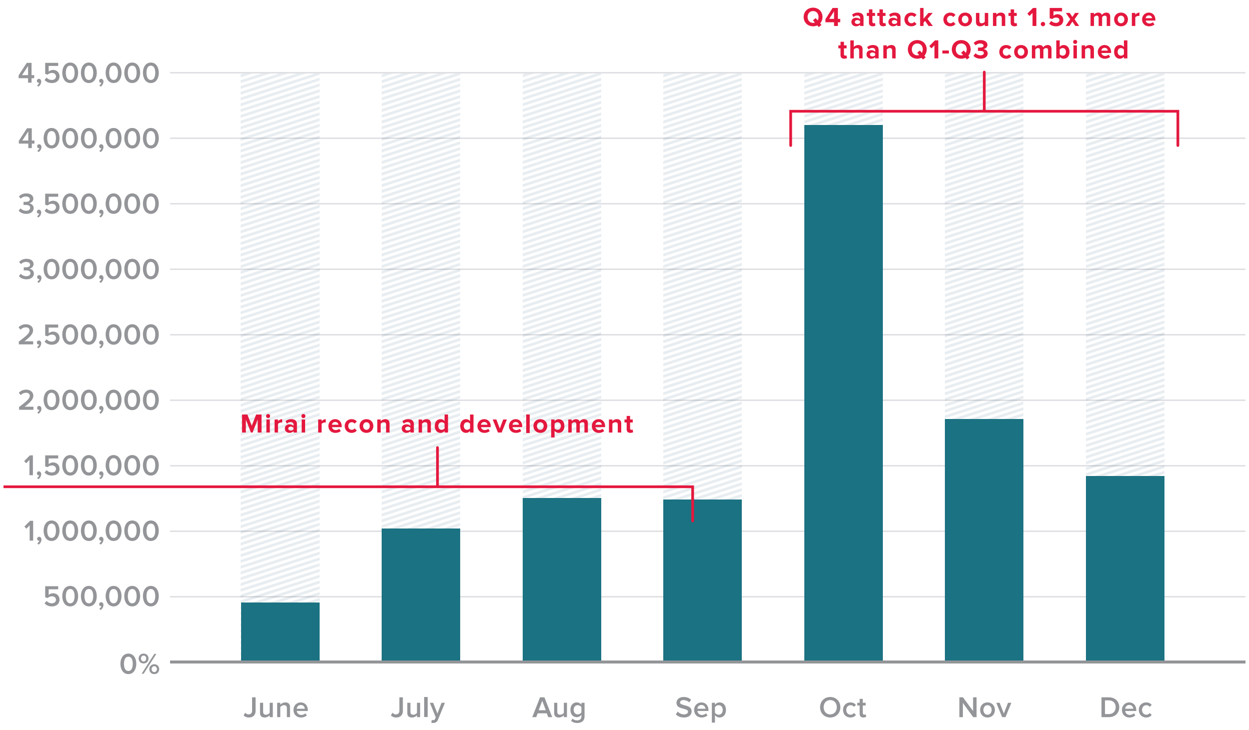


Figure 2. Q3 and Q4 IoT Telnet attacks by month

While the number of recorded events (IoT-based attacks) increased globally by 110% from Q3 and Q4, the networks (autonomous system numbers, or ASNs) participating in these attacks stayed relatively flat at 10%. Meanwhile, the unique IP addresses participating within those ASNs grew at a rate of 74%, indicating that threat actors are launching attacks from within the same networks. This is the primary reason we decided to publish threat actor networks in this report. Note, however, that we will not publish the source IP addresses of the recorded attack events (except to the ASNs to which the subnets are delegated.)

TELNET EVENT DETAILS	Q3	Q4	Q/Q GROWTH
Telnet Attacks	3,526,208	7,399,425	110%
Telnet Unique IPv4 Addresses	993,167	1,727,348	74%
Telnet ASNs	8,976	9,869	10%

Table 1. Q3 and Q4 IoT attack summary: attack count, unique IPv4 addresses and ASNs

Outside the scope of Telnet attacks, looking at SSH events can give us relevant insight into the capabilities of threat actors. For instance, we see that the number of username and passwords attempted in SSH events decreased from Q3 to Q4, indicating that threat actors are likely becoming "smarter"—that is, they already have the correct credentials.

TELNET EVENT DETAILS	Q3	Q4	Q/Q GROWTH
Total Unique Passwords	89,237	82,152	-8%
Total Unique Usernames	23,444	19,843	-15%

Table 2. Q3 and Q4 attack authentication summary: unique passwords, unique user names

In the months leading up to Mirai's Tbps attacks, brute force Telnet scanning grew at a steady pace (as one might expect), and that activity was enough to create the Mirai botnet. The spike in early October after Mirai was released is consistent with the increase in the number of ASNs participating in Telnet scans over the same period (see figure 9). This is likely due to the botnet source becoming public and resulting in increased activity. While this spike was short-lived, the daily volume didn't drop off to pre-Mirai levels, driving the large quarter-over-quarter growth.

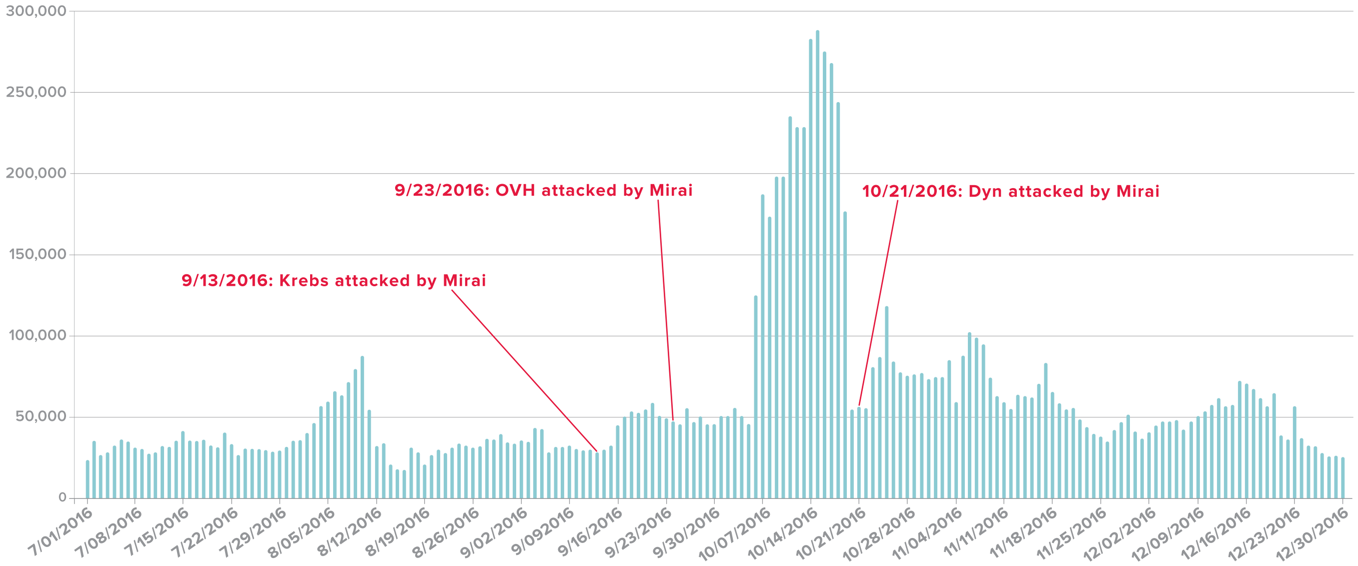


Figure 3: Q3 and Q4 IoT Telnet attacks by day

Note: We are not showing attacks by day of week or daily average by month in this report because it doesn't provide any deeper understanding of threat actor behavior.

HUNTING COUNTRIES AND DESTINATIONS

Th roughout Q3 and Q4, China continued to be the largest source (threat actor) from which attack traffic originated (see Figures 7 and 8 and Table 4). The Chinese networks that launched attacks belong to state-owned telecom companies and Internet Service Providers (ISPs), so it's not a stretch to call this "nation-state" activity. In Q3, Canada and the UK were bumped off the Q1/Q2 top attackers list by Vietnam and the US. In Q4, China again held its lead as the top attacker, followed by Russia and the UK, which replaced Vietnam and the US respectively from Q3.

The most targeted destination (see Table 3) was Russia (the 2016 US election might have had something to do with that), followed by Spain, then the US. Note that while China is consistently a primary source, China (excluding Hong Kong) hasn't been in the top 10 destination bucket since we started collecting data in early 2016.

In Q3, Spain became a top target of all three primary attackers, with China leading that charge. Behind Spain, China also targeted the US and Turkey, in that order. The US was also a primary target in both Q3 and Q4 (and interestingly, attacks itself more than any other country). Turkey is new on the top target list for both Q3 and Q4.

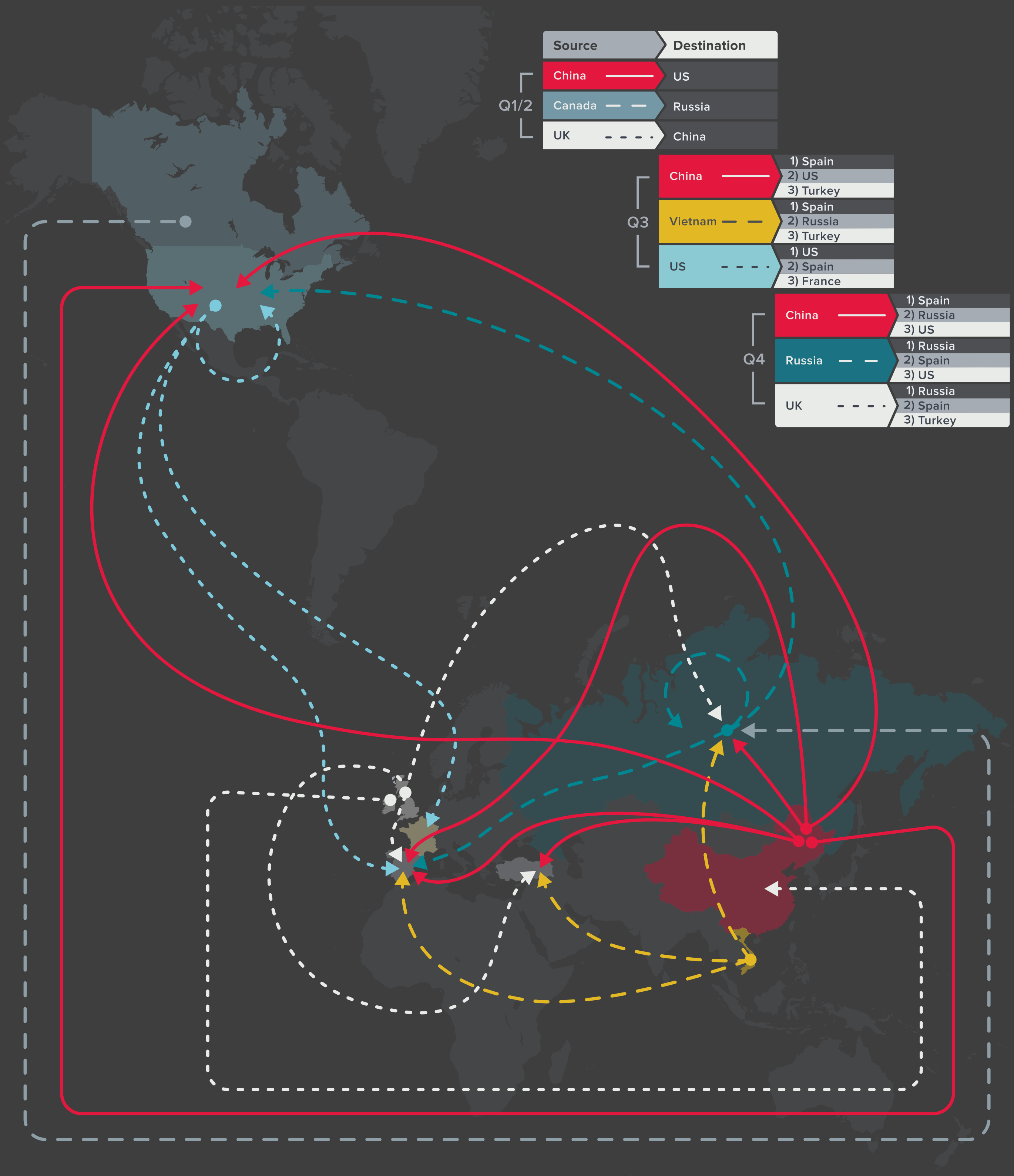


Figure 4. Top 3 attacking countries and their targets: Q1 - Q4 2016

Q3 TOP 20 THREAT ACTOR SOURCE COUNTRIES

China was responsible for almost half (44%) of all attacks launched in Q3, the majority of which came from Chinanet (see Table 4), a state-sponsored ISP. Vietnam and the US were number 2 and number 3, dramatically far behind China with only 6% and 7% respectively. All other countries fell below 5% contribution to the total attack volume. The top 10 countries account for 78% of the total attack volume for Q3; the top 20 are shown only to represent the vast interest in a dominated market.

Note: A large source of France's Q3 traffic is from OVH's ASN, which was a victim of Mirai in early October 2016.

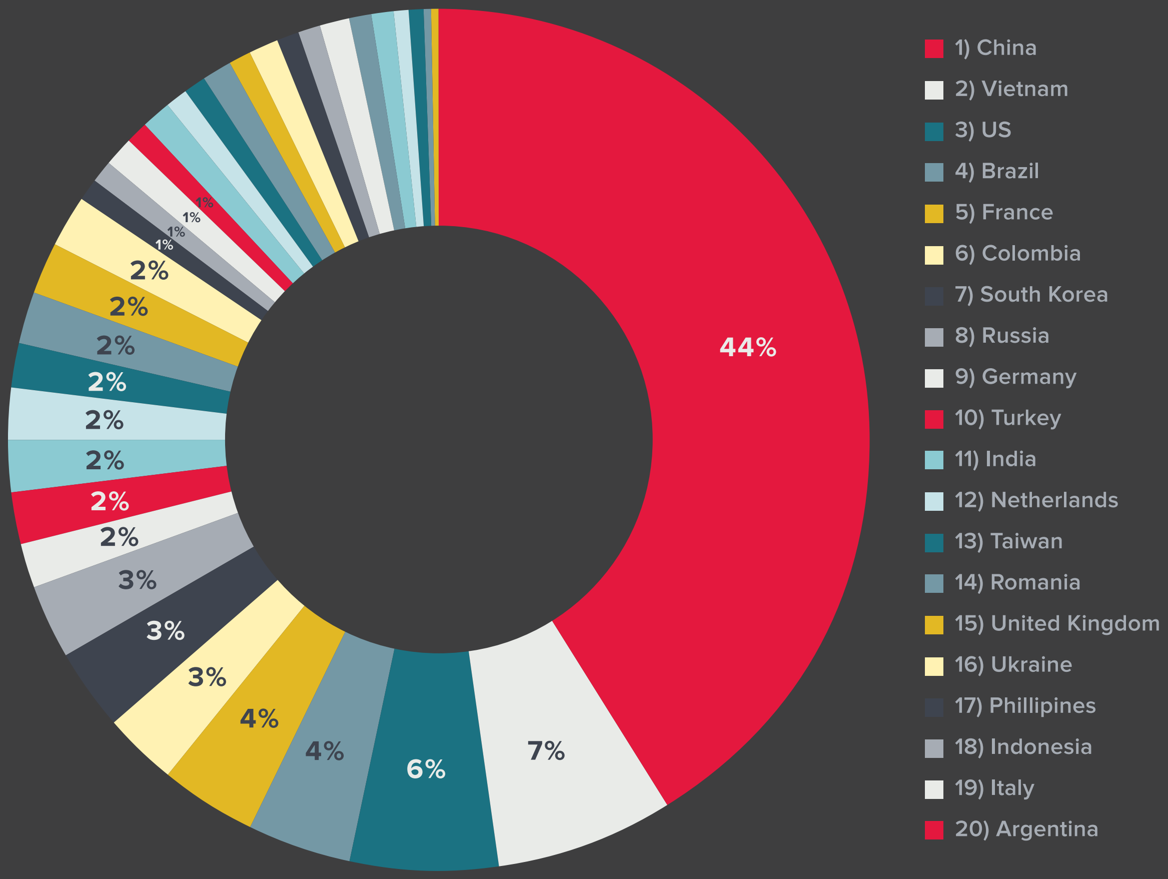


Figure 5. Top 20 attack source countries in Q3

Q4 TOP 20 THREAT ACTOR SOURCE COUNTRIES

Since the Mirai attacks, Telnet attack activity has intensified all over the globe in Q4. As a result, China's share in the overall total narrowed from a significant 44% in Q3 to 21% in Q4, as other countries began participating more heavily. For example, the UK jumped from number 15 in Q3 to number 3 in Q4, with activity coming largely from an online gaming network. Russia at number 2 and the UK at number 3 each took much larger pieces of the pie in Q4 than in Q3. Russia's share of attacks grew nearly five-fold from 3% in Q3 to 14% in Q4; likewise, UK attacks rose more than 10 times, from 1% in Q3 to 11% in Q4. This caused a significant redistribution in the percentage of attacks, at least at the highest levels.

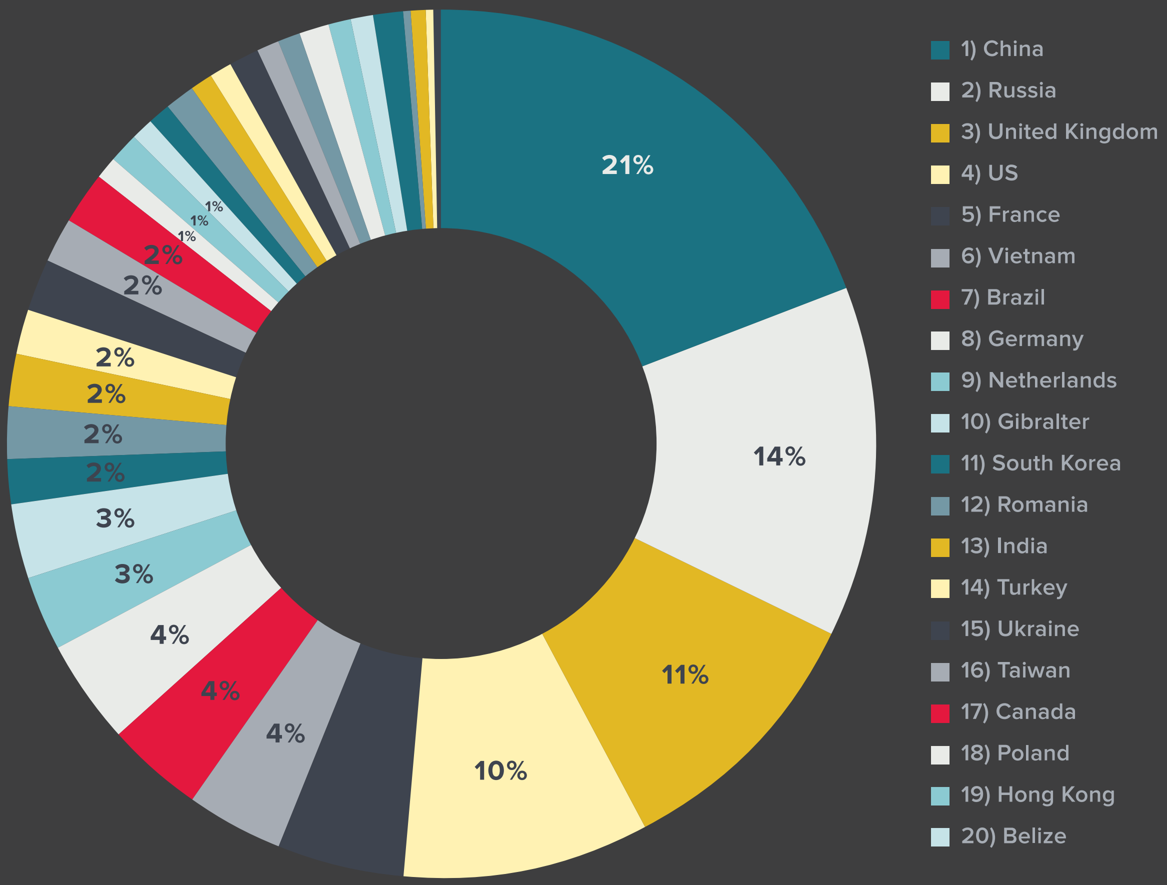
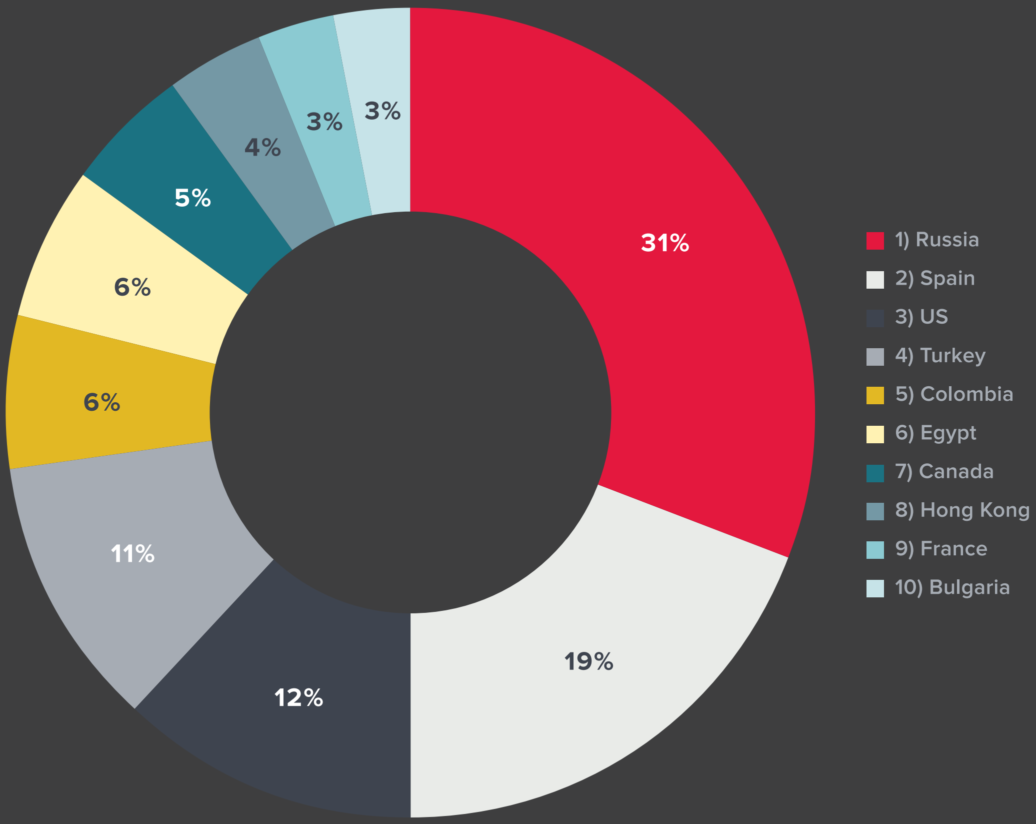


Figure 6. Top 20 attack source countries in Q4

While Russia has moved up the numbered list of threat actor (source) countries (from number 8 in Q3 to number 2 in Q4), it has consistently been the top target of attacks (destination country). In fact, throughout Q3 and Q4, the top 4 targeted countries remained consistent, with the number of attacks sometimes almost doubling from fourth position to third, third to second, and second to first.

DESTINATION COUNTRY	Q3 COUNT	DESTINATION COUNTRY	Q4 COUNT
1 Russia	2,177,284	1 Russia	3,726,740
2 Spain	1,293,975	2 Spain	1,856,719
3 US	821,629	3 US	1,218,234
4 Turkey	776,900	4 Turkey	780,028
5 Colombia	403,212	5 Hong Kong	629,433
6 Egypt	385,676	6 UK	260,579
7 Canada	365,603	7 Netherlands	253,387
8 Hong Kong	274,428	8 Egypt	238,939
9 France	219,141	9 France	224,875
10 Bulgaria	178,663	10 Finland	176,232

Table 3. Count of attacks by top 10 source countries Q3 and Q4



Q3 TOP 10 ATTACK DESTINATION COUNTRIES

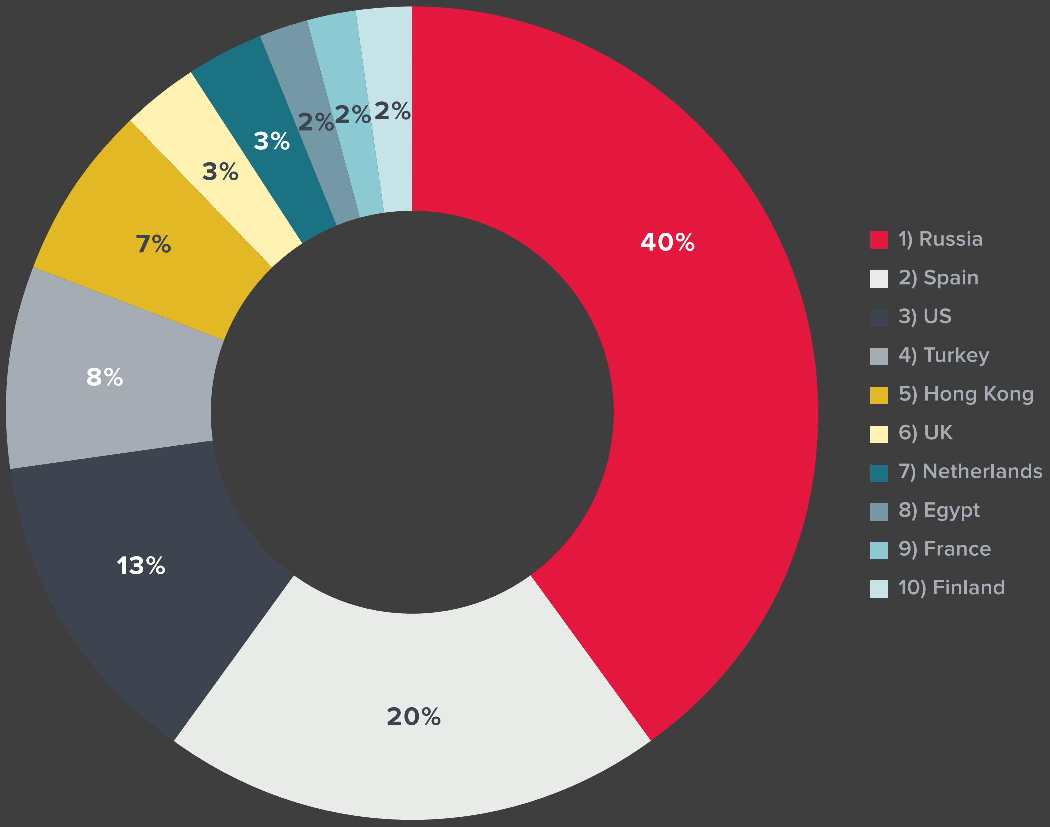
Russia is a top target from virtually all countries on the top 50 list. Russia outpaced attacks received by Spain (in the number 2 position) by almost 2:1, and by 12:1 when compared to Bulgaria in the tenth position.

Figure 7. (Left) Top 10 target countries in Q3

Q4 TOP 10 ATTACK DESTINATION COUNTRIES

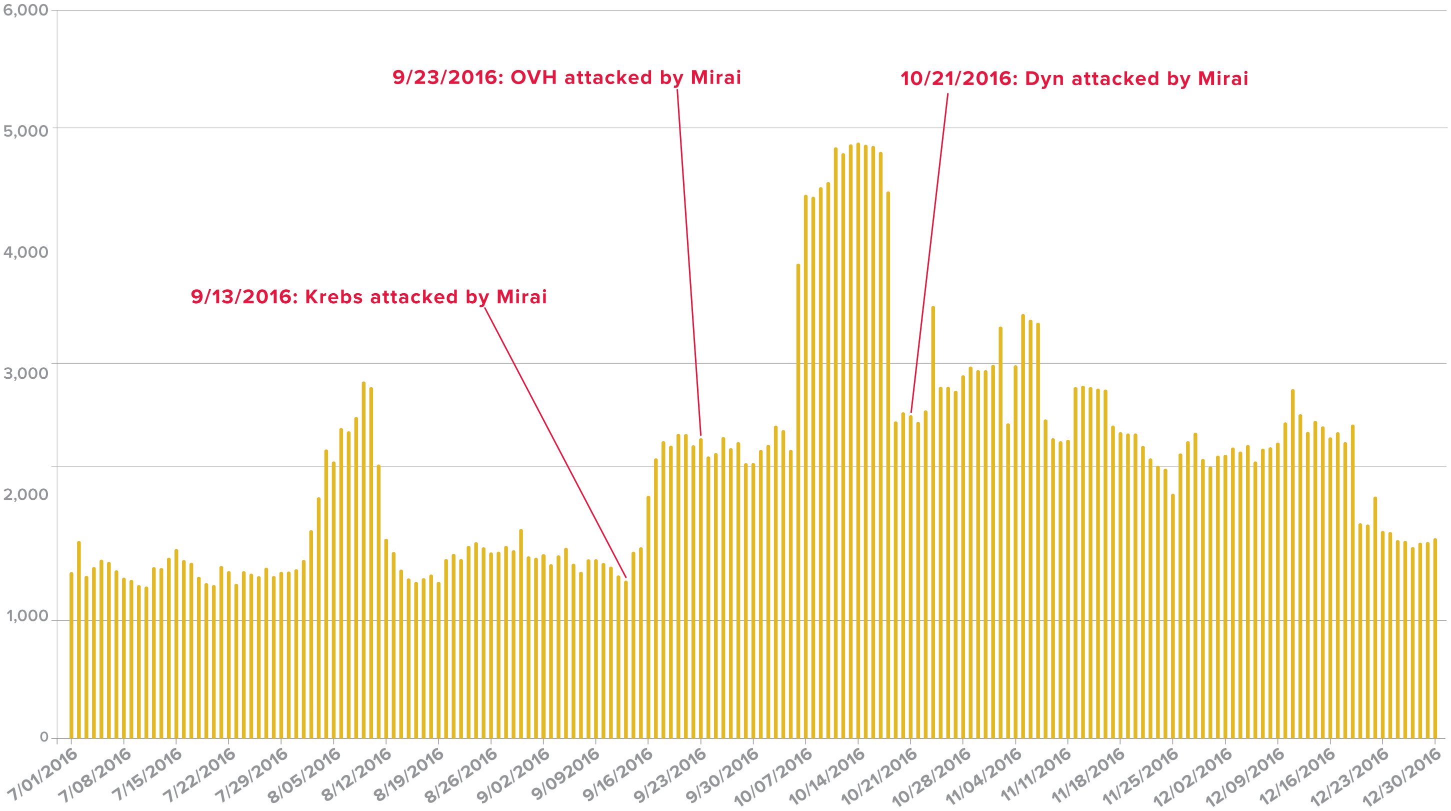
Interest in Russia increased in Q4, jumping from 31% of total attacks to 40%. Colombia, Canada, and Bulgaria were bumped off the top 10 targets list in Q4, replaced by the UK, Netherlands, and Finland.

Figure 8. (Right) Top 10 target countries in Q4



HUNTING NETWORKS (ASNs)

The pattern of threat actor networks (also identified by their ASNs) attacking IoT devices was consistent with the total Telnet attack volume, indicating that the same networks, if not the same threat actors, were consistently participating in the hunt. This rings true when comparing the participating ASNs from Q3 and Q4.



9/23/2016: OVH attacked by Mirai

10/21/2016: Dyn attacked by Mirai

9/13/2016: Krebs attacked by Mirai

Figure 9. Q3 and Q4 count of ASNs participating in attacks by day

Q3 TOP 50 THREAT ACTOR NETWORKS (ASNs)

Table 4 lists the top 50 ASNs conducting attacks in Q3 and includes the number of unique IP addresses in relation to attacks. Because these ASNs are mostly ISPs and hosting companies, it gives us an idea of whether the activity is vast across a lot of customers, or if there were standout threat actors. The rows highlighted in yellow are consistent networks from Q3 to Q4. Seventy percent of the top 20 participating networks in Q3 landed on the top 50 list in Q4, proving that consistent networks were participating in these attacks. China Telecom contributed almost 20% to the total attack volume from 219 IP addresses at an average of 9,000 attacks each. Europe has relatively few top actors, with French hosting companies Online SAS, OVH (which happened to be targeted by Mirai), and German company Hetzner Online.

Q3 TOP 50 ATTACKING ASNS

Pos	Source ASN	Owner	Country	Attack Count	% Of Attack Total
1	AS58543	CHINA TELECOM Guangdong	China	1,993,269	19.0%
2	AS4134	Chinanet backbone	China	957,190	9.1%
3	AS4837	China Unicom-Jiangsu Province Network	China	686,142	6.5%
4	AS23650	Chinanet (jiangsu province backbone)	China	471,124	4.5%
5	AS12876	Online SAS	France	348,028	3.3%
6	AS3816	Colombia Telecomunicaciones	Colombia	263,427	2.5%
7	AS45899	VNPT Corp	Vietnam	217,311	2.1%
8	AS24940	Hetzner Online GmbH	Germany	167,478	1.6%
9	AS4766	Korea Telecom	South Korea	151,105	1.4%
10	AS7552	Viettel Corp	Vietnam	150,231	1.4%
11	AS3462	HiNet Data Communications Business Group	Taiwan	133,727	1.3%
12	AS16276	OVH	France	123,493	1.2%
13	AS18403	The Corporation for Financing & Promoting Technology	Vietnam	118,440	1.1%
14	AS47331	TTNet A.S.	Turkey	115,361	1.1%
15	AS28573	Claro S.A.	Brazil	113,196	1.1%
16	AS18881	Telefnica Brasil S.A.	Brazil	98,364	0.9%
17	AS9299	Philippine Long Distance Telephone Company	Philippines	93,634	0.9%
18	AS50673	Serverius	Netherlands	92,595	0.9%
19	AS37963	Hangzhou Alibaba Advertising Co., Ltd.	China	73,928	0.7%
20	AS8560	1&1 Internet Inc.	Germany	73,660	0.7%
21	AS9050	Telekom Romania Communications SA	Romania	68,507	0.7%
22	AS24086	Viettel Corp	Vietnam	67,144	0.6%
23	AS9829	BSNL (Bharat Sanchar Nigam LTD)	India	62,773	0.6%
24	AS36351	SoftLayer	US	59,715	0.6%
25	AS13886	Cloud South	US	56,571	0.5%
26	AS27699	Telefnica Brasil S.A.	Brazil	54,217	0.5%
27	AS17974	PT Telekomunikasi Indonesia	Indonesia	53,375	0.5%
28	AS8075	Microsoft	US	49,963	0.5%
29	AS7738	Telemar Norte Leste S.A.	Brazil	45,826	0.4%
30	AS45595	Pakistan Telecom Company Ltd	Pakistan	44,005	0.4%
31	AS3786	LG DACOM Corporation	–	40,499	0.4%
32	AS8151	Uninet S.A. de C.V.	Mexico	37,306	0.4%
33	AS23724	CHINANET-IDC	China	36,000	0.3%
34	AS14061	Digital Ocean	US	35,188	0.3%
35	AS24560	Bharti Airtel Ltd.	Indonesia	33,897	0.3%
36	AS4812	China Telecom Group	China	32,145	0.3%
37	AS7922	Comcast Cable Communications	US	31,579	0.3%
38	AS29182	ISP System Autonomous System	Luxembourg	30,251	0.3%
39	AS29073	Quasi Networks LTD.	Netherlands	30,232	0.3%
40	AS9121	TTNet	Turkey	30,221	0.3%

Q3 TOP 50 ATTACKING ASNS					
Pos	Source ASN	Owner	Country	Attack Count	% Of Attack Total
41	AS39383	TELESYSTEM	Romania	29,902	0.3%
42	AS8708	RCS & RDS SA	Romania	29,768	0.3%
43	AS24088	Hanoi Telecom Joint Stock Company	Vietnam	28,867	0.3%
44	AS3215	Orange S.A.	France	28,411	0.3%
45	AS131293	TOT Public Company Limited	Thailand	28,080	0.3%
46	AS4808	China Unicom Beijing Province Network	China	27,799	0.3%
47	AS8167	BrasilTelecomS/A-FilialDistrito	Brazil	26,584	0.3%
48	AS25092	OPATELECOM	Ukraine	26,025	0.2%
49	AS12252	America Movil Peru	Peru	26,018	0.2%
50	AS9318	Hanaro Telecom Inc.	South Korea	25,080	0.2%

Table 4. Q3 Top 50 attacking ASNs

Q4 TOP 50 THREAT ACTOR NETWORKS (ASNs)

Table 5 lists the top 50 ASNs launching attacks in Q4 in the same format as the Q3 data shown in Table 4 (blue highlighted rows are consistent networks from quarter to quarter).

Two affiliated networks that didn't exist in Q3 jumped into top 10 positions; William Hill Organization, and WHG International. These correspond to the top attacking IP addresses shown in Table 8.

Q4 TOP 50 ATTACKING ASNS					
Pos	Source ASN	Owner	Country	Attack Count	% Of Attack Total
1	AS57002	William Hill Organization Ltd	UK	2,992,404	16.47%
2	AS4134	Chinanet backbone	China	2,382,222	13.11%
3	AS58543	CHINA TELECOM Guangdong	China	1,924,037	10.59%
4	AS12876	ONLINE S.A.S.	France	1,290,742	7.10%
5	AS49061	WHG (International) Limited	Gibraltar	844,825	4.65%
6	AS23650	Chinanet (jiangsu province backbone)	China	737,716	4.06%
7	AS16276	OVH SAS	France	641,771	3.53%
8	AS45899	VNPT Corp	Vietnam	513,094	2.82%
9	AS4837	China Unicom-Jiangsu Province Network	China	488,829	2.69%
10	AS3462	HiNet Data Communications Business Group	Taiwan	451,842	2.49%
11	AS20738	123 Reg Limited	UK	430,173	2.37%
12	AS47331	TTNet A.S.	Turkey	364,959	2.01%
13	AS4766	Korea Telecom	South Korea	353,778	1.95%
14	AS20473	Choopa, LLC	US	304,269	1.67%
15	AS262254	Dancom LTD	Belize	304,234	1.67%

Q4 TOP 50 ATTACKING ASNS

Pos	Source ASN	Owner	Country	Attack Count	% Of Attack Total
16	AS14061	Digital Ocean	US	298,878	1.64%
17	AS7552	Viettel Corporation	Vietnam	297,558	1.64%
18	AS18881	Global Village Telecom	Brazil	279,435	1.54%
19	AS24961	myLoc managed IT	Germany	263,237	1.45%
20	AS29066	velia.net Internetdienste GmbH	Germany	241,088	1.33%
21	AS24940	Hetzner Online	Germany	232,331	1.28%
22	AS34259	TOV Highload Systems	Ukraine	229,869	1.27%
23	AS13335	CloudFlare	US	218,682	1.20%
24	AS8560	1&1 Internet AG	Germany	208,368	1.15%
25	AS18403	The Corporation for Financing & Promoting Technology	Vietnam	198,258	1.09%
26	AS28573	CLARO S.A.	Brazil	191,865	1.06%
27	AS9829	National Internet Backbone	India	184,236	1.01%
28	AS29073	Quasi Networks LTD.	Netherlands	179,876	0.99%
29	AS15895	Kyivstar PJSC	Ukraine	167,318	0.92%
30	AS3303	Swisscom (Switzerland) Ltd	Switzerland	167,082	0.92%
31	AS37963	Hangzhou Alibaba Advertising	China	161,262	0.89%
32	AS16125	BALTIC SERVERS	Lithuania	156,909	0.86%
33	AS19531	Nodes Direct	US	154,248	0.85%
34	AS13301	United Gameserver GmbH	Germany	154,106	0.85%
35	AS50113	SUPER SERVERS DATACENTER	Russia	151,631	0.83%
36	AS24086	Viettel Corporation	Vietnam	139,741	0.77%
37	AS36351	Soft Layer Technologies Inc.	US	134,615	0.74%
38	AS27699	TELEFÔNICA BRASIL S.A.	Brazil	134,123	0.74%
39	AS49544	INTERACTIVE 3D	Netherlands	132,622	0.73%
40	AS10429	Telefonica Data S.A.	Brazil	123,774	0.68%
41	AS16509	Amazon.com	US	113,016	0.62%
42	AS7738	Telemar Norte Leste S.A.	Brazil	112,485	0.62%
43	AS17974	PT Telekomunikasi Indonesia	Indonesia	110,958	0.61%
44	AS50673	Serverius Holding B.V.	Netherlands	108,495	0.60%
45	AS7643	Vietnam Posts and Telecommunications (VNPT)	Vietnam	107,369	0.59%
46	AS8708	RCS & RDS SA	Romania	106,977	0.59%
47	AS7922	Comcast Cable Communications	US	103,215	0.57%
48	AS8151	Uninet S.A. de C.V.	Mexico	99,475	0.55%
49	AS49981	WorldStream	Netherlands	98,684	0.54%
50	AS9318	Hanaro Telecom Inc.	South Korea	98,054	0.54%

Table 5. Q4 Top 50 attacking ASNs

HUNTING IP ADDRESSES

As stated previously, we're not disclosing the actual IP addresses publicly. We are, however, publishing the percentage that the top 50 attacking IP addresses contributed to the total attack volume because it indicates whether attacks were initiated by a large threat actor (or actors) in a network or a lot of smaller actors. It also provides clues as to whether those IP addresses belonged to the same networks quarter over quarter, and whether they were the same IP addresses or attackers quarter over quarter.

In Q3, the top 50 attacking IP addresses accounted for 26% of all attacks, the majority of which were from Chinanet. Q4 saw that number increase to 35%. That number likely would have been higher if it weren't for the early October spike of Mirai interest that caused a lot of new threat actor IP addresses to jump on the Top 50 list.

	Q3	Q4
Top 50 IP's Count of Attacks	2,783,447	6,331,709
Total Count of Attacks	10,516,577	18,169,269
Top 50 IP's % Contribution to Total	26%	35%

Table 6. Top 50 IP addresses and their contribution to total attacks

Q3 TOP 50 ATTACKING IP ADDRESS ASNS

In Q3, 11 ASNs owned the top 50 IP addresses. This was dominated by Chinese state-owned telecom companies, including China Telecom, Chinanet, and China Unicom. Note the other 7 ASNs had 1 IP address each on the top 50 attacking IP list, which are standout threat actors that they could likely track down.

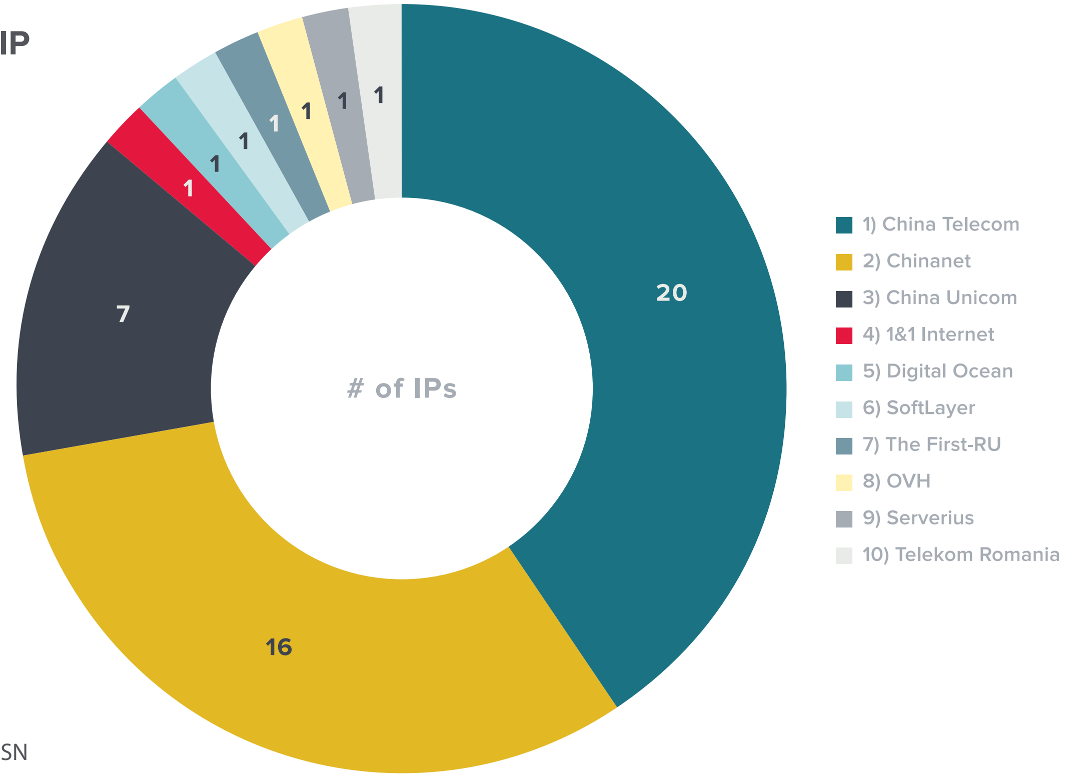


Figure 10. Q3 top 50 attacking IPs by ASN

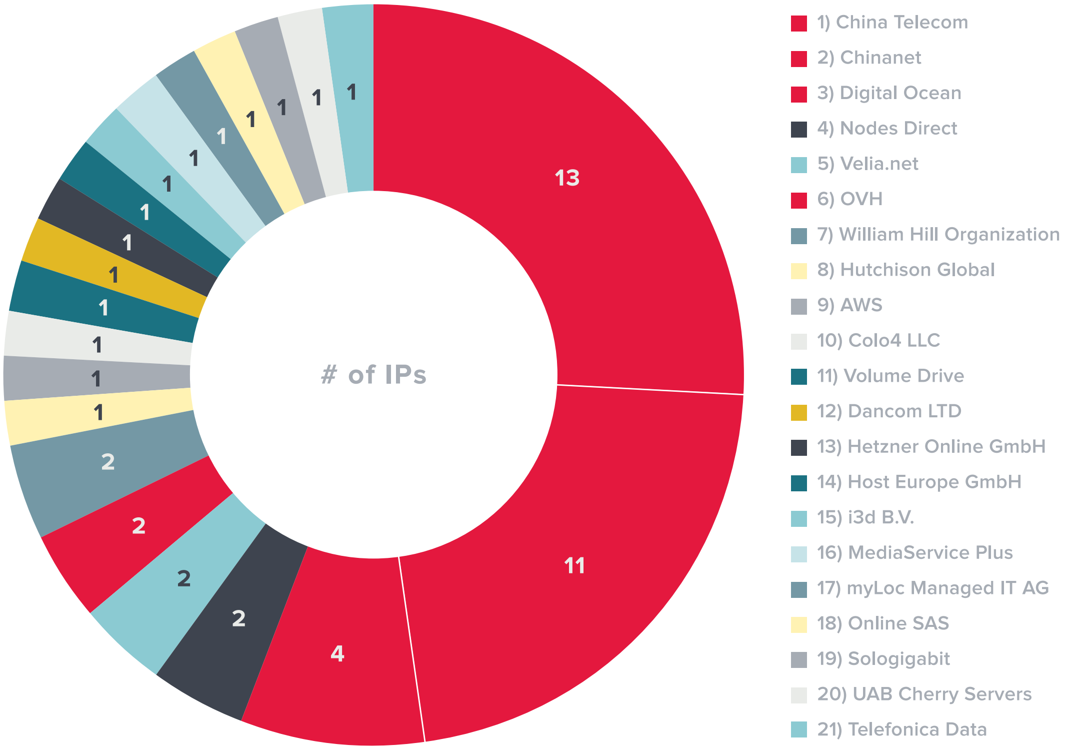
Table 7 shows the ASN numbers and countries associated with the data shown in Figure 12.

ASN #/s	ASN Owner	IP Addresses on Top 50 list	Country	Industry
AS58543	China Telecom	20	China	Telecom (State-Owned)
AS4134 AS23650	Chinanet	16	China	Telecom (State-Owned)
AS4837	China Unicom	7	China	Telecom (State-Owned)
AS8560	1&1 Internet	1	Germany	Hosting
AS14061	Digital Ocean	1	US	Hosting
AS36351	SoftLayer	1	US	Hosting
AS29182	The First-RU	1	Russia	Unknown
AS16276	OVH	1	France	Hosting
AS50673	Serverius	1	Netherlands	Hosting
AS9050	Telekom Romania	1	Romania	Telecom

Table 7. AS numbers and owners of top 50 attacking IP addresses in Q3

Q4 TOP 50 ATTACKING IP ADDRESS ASNs

Q4 saw a wider distribution of ASNs owning the top 50 attacking IP addresses, which is not surprising given Mirai, and new threat actors entering the picture. Four threat actor networks (ASNs) from Q3's top 50 IP list—China Telecom, Chinanet, Digital Ocean, and OVH—were also on the Q4 top 50 IP list as shown in red in Tables 7 and 8.



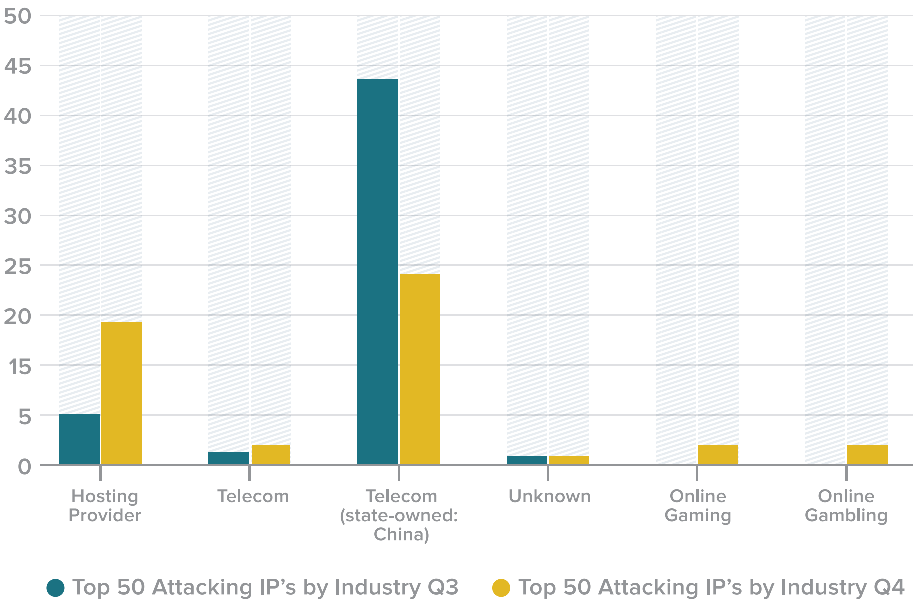
The only IP addresses that are consistent from Q3 to Q4 are from China Telecom and Chinanet, of which there are 11, or 22% of the top 50. Digital Ocean and OVH IP addresses used from Q3 to Q4 are different.

Figure 11. Q4 top 50 attacking IPs by ASN

Table 8 lists the ASN numbers associated to the pie chart shown in Figure 12.

ASN #/s	ASN Owner	IP Addresses on Top 50 list	Country	Industry
AS58543	China Telecom	13	China	Telecom (State-Owned)
AS4134 AS23650 AS133774	Chinanet	11	China	Telecom (State-Owned)
AS14061	Digital Ocean	4	US	Hosting
AS19531	Nodes Direct	2	US	Hosting
AS29066	Velia.net	2	Germany	Online Gaming
AS16276	OVH	2	France	Hosting
AS49061 AS57002	William Hill Organization	2	UK / Gibraltar	Online Gambling
AS9304	Hutchison Global	1	China	Telecom
AS16509	AWS	1	US	Hosting
AS36024	Colo4 LLC	1	US	Hosting
AS46664	Volume Drive	1	US	Hosting
AS262254	Dancom LTD	1	Belize	Hosting
AS24940	Hetzner Online GmbH	1	Germany	Hosting
AS20738	Host Europe GmbH	1	UK	Hosting
AS49544	i3d B.V.	1	Netherlands	Hosting
AS50113	MediaService Plus	1	Russia	Unknown
AS24961	myLoc Managed IT AG	1	Germany	Hosting
AS12876	Online SAS	1	France	Hosting
AS56934	Sologigabit		Spain	Hosting
AS16125	UAB Cherry Servers	1	Lithuania	Hosting
AS10429	Telefonica Data	1	Brazil	Telecom

Table 8. AS numbers and owners of top 50 attacking IP addresses in Q3



THE HUNT BY INDUSTRY

As we've seen from the numerous charts and tables already presented, the top industries conducting attacks are telecom companies, mainly Chinese state-owned, followed by hosting providers. The "unknown" are ASNs in Russia.

Figure 12. Q3 and Q4 top 50 attacking IP addresses by industry

THE HUNT BY OPERATING SYSTEMS

The overwhelming majority of attacking systems are Linux-based (Linux, Unix, Darwin, BSD, etc.). It's interesting to see the percentages from an anecdotal perspective, but it's not surprising, given that the vast majority of botkits currently available don't affect Windows.

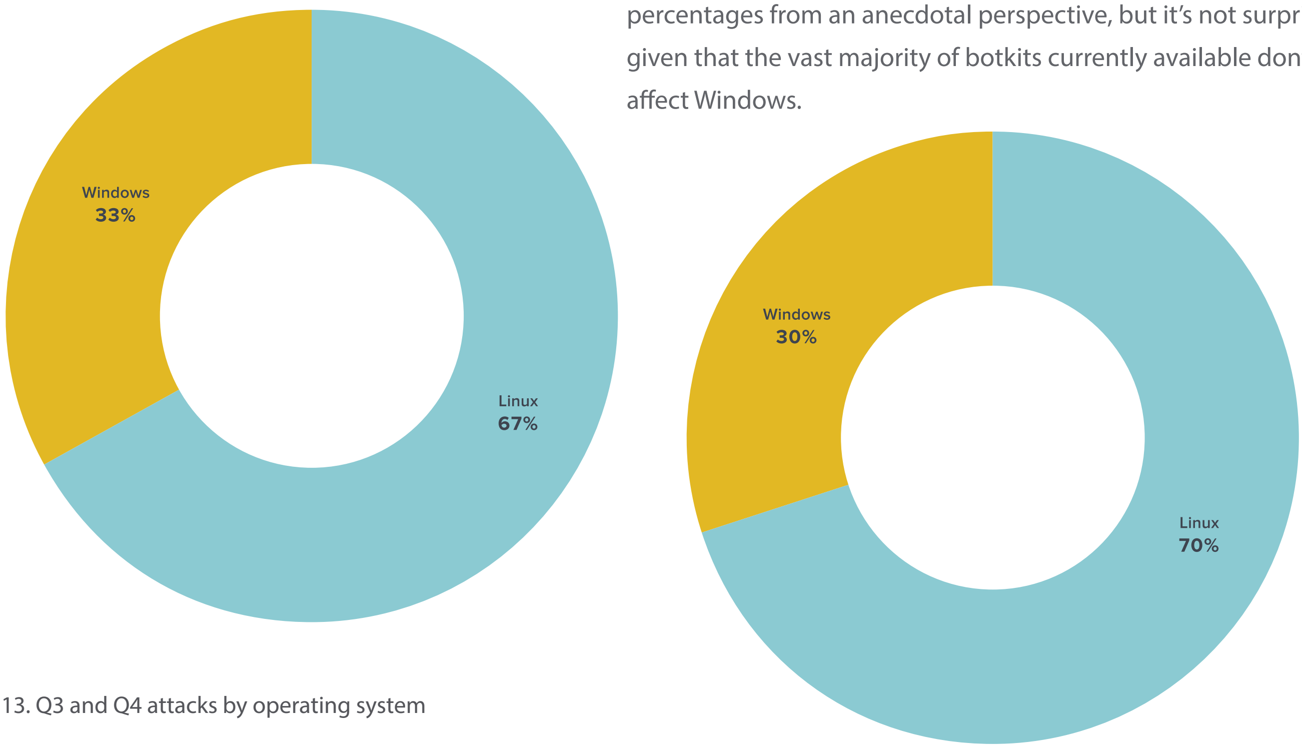


Figure 13. Q3 and Q4 attacks by operating system

CONCLUSION

It's fair to say that when it comes to IoT, we still haven't fully grasped the impact of these enormous IoT DDoS attacks, nor do we know what the global response effort will be. Needless to say, we no longer need to convince anyone of the vast threat that IoT devices pose.

The vulnerability posture of IoT devices in general, combined with the expected growth and adoption rate of IoT devices, make for an ever-expanding exploit surface. These factors, in conjunction with the highly active and growing hunt—almost 1,400% increase in 2016!—and subsequent "Bots of X" construction, make the threat of IoT attacks very real for all businesses.

Over the course of 2017, we will continue to monitor and publish the IoT hunt and resulting botnets, as well as any new IoT threat research, including but not limited to vulnerable chipsets and manufacturers, validating IoT device type attack capabilities, the impact of Message Queue Telemetry Transport (MQTT), and the implications that the use of IPv6 addresses could have on the overall IoT threat.

No doubt there will be hiccups over the next few years while DDoS attacks grow in size, scrubbing services grow in bandwidth to accommodate multiple Tbps DDoS attacks, new IoT attack vectors are realized (while the industry scrambles to mitigate them), and IoT device manufacturers and telecom companies, ISPs, and hosting providers come under increasing pressure to deal with this problem. Right now, organizations and consumers have no choice but to get used to this evolving threat—like all other major threats before this one.

Beyond just "getting used to it," here are some steps security professionals can take, both personally and professionally:

1. **Have a DDoS strategy.** If you don't already have a DDoS strategy in place, now is the time for one, and there are three good options:
    a. **On-premises equipment** is great for customers who are routinely targeted with DDoS attacks (below their network capacity) and have trained resources to effectively mitigate them on their own.
    b. **Hybrid on-premises and cloud scrubbing** for customers that receive frequent DDoS attacks they mitigate with their on-premises equipment and resources (because it's not cost effective to outsource), but who are also at risk of large attacks that exceed their capabilities and therefore need backup DDoS scrubbing services.
    c. **Cloud scrubbing** for companies that don't deal with DDoS on a regular basis and do not have in-house expertise or equipment. This includes any company at risk of large scale attacks that exceed their network capabilities (that's essentially every business on the Internet outside of service providers and DDoS scrubbing services!).
2. **Ensure critical services have redundancy.** Consider that you are not always going to be the target, but the services you use could be, in which case you are a potential downstream casualty. Have a business continuity plan that includes disaster recovery for your critical services so you don't find yourself in the same boat as Twitter, Github, and Spotify when Dyn DNS suffered a DDoS attack offline—or any other

company that solely leveraged OVH for hosting and was down when their network was attacked. Have a dual strategy in place (or even a multi strategy, in the case of DNS) to protect yourself. Remember that DNS can be your friend, too; Anycast your global data centers for replicated content to diffuse DDoS attacks when they happen.

3. **Don't buy IoT products known to be insecure or compromised.** Money talks! Choosing not to spend money on the products built by irresponsible manufacturers is a quick way to drive change, at both a grassroots level personally with consumer products that become weapons against your business, and professionally if you are an IoT implementer.

    a. If you are a company that deploys but does not manufacture IoT devices, test and verify the safety of a vendor's products before you buy them.

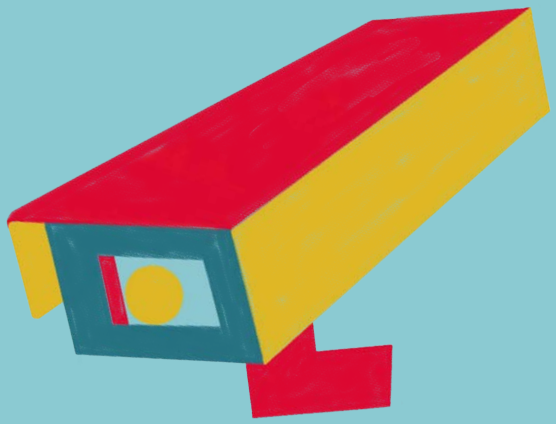
    b. If you are a security professional, the general public needs help knowing which devices are vulnerable or compromised, so share your knowledge with your family and friends and encourage them to share, as well. Social media is a powerful tool; so is security awareness training for your employees.

4. **Share your knowledge.** Security professionals around the world can chip away at this global problem by communicating more with each other and sharing knowledge. Attackers are known for sharing information with each other; they even shared the most powerful botnet to date! Security professionals—even among competitors—need to take a page from attackers' playbooks by sharing more key information about vulnerable devices, attacks and threat actors, mitigation efforts that are working, and potential solutions, no matter how wild the ideas might seem.

ABOUT F5 LABS

F5 Labs combines the threat intelligence data we collect with the expertise of our security researchers to provide actionable, global intelligence on current cyber threats—and to identify future trends. We look at everything from threat actors, to the nature and source of attacks, to post-attack analysis of significant incidents to create a comprehensive view of the threat landscape. From the newest malware variants to zero-day exploits and attack trends, F5 Labs is where you'll find the latest insights from F5's threat intelligence team.

For more information, visit: www.f5.com/labs



ABOUT LORYKA

Loryka is a team of dedicated researchers that monitor and investigate emerging attacks, advanced persistent threats, and the organizations and individuals responsible. The team also develops research tools to identify, investigate, and track ongoing attacks and emerging threats.

For more information, visit: www.loryka.com

[i] https://f5.com/labs/articles/threat-intelligence/ddos/ddoss-newest-minions-iot-devices-v1-22426

[ii] https://f5.com/labs/articles/threat-intelligence/ddos/mirai-the-iot-bot-that-took-down-krebs-and-launched-a-tbps-attack-on-ovh-22422

[iii] http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/

[iv] https://f5.com/labs/articles/threat-intelligence/ddos/are-you-ready-to-handle-100-gbps-ddos-attacksthe-new-normal-22627

[v] https://f5.com/labs/articles/threat-intelligence/cyber-security/using-f5-labs-threat-intelligence-24665

[vi] https://f5.com/labs/articles/threat-intelligence/cyber-security/iot-threats-a-first-step-into-a-much-larger-world-of-mayhem-24664

[vii] http://www.gartner.com/newsroom/id/3165317

US Headquarters: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447
Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com

APPENDIX A: ATTACK COUNTS PER IP LAUNCHING GREATER THAN 10K ATTACKS

The following tables list the quantity of attacks launched from a single IP, limited to IP's launching more than 10k attacks, and their associated ASN and country. Each line item is a different IP within the associated network. The owning ASN can request the IP details from F5 Labs.

Q3 Attack Count of IP Addresses Launching >10K Attacks, by ASN, by Country

Source ASN	Attack Count	ASN Owner	Country
as23657	21,441	Blue Sky	American Samoa
as58543	184,304	CHINA TELECOM Guangdong	China
as58543	173,873	CHINA TELECOM Guangdong	China
as58543	159,324	CHINA TELECOM Guangdong	China
as58543	141,398	CHINA TELECOM Guangdong	China
as58543	132,591	CHINA TELECOM Guangdong	China
as58543	115,941	CHINA TELECOM Guangdong	China
as58543	91,646	CHINA TELECOM Guangdong	China
as58543	77,843	CHINA TELECOM Guangdong	China
as58543	74,562	CHINA TELECOM Guangdong	China
as58543	70,897	CHINA TELECOM Guangdong	China
as58543	67,755	CHINA TELECOM Guangdong	China
as58543	62,888	CHINA TELECOM Guangdong	China
as58543	62,146	CHINA TELECOM Guangdong	China
as58543	51,231	CHINA TELECOM Guangdong	China
as58543	42,854	CHINA TELECOM Guangdong	China
as58543	32,794	CHINA TELECOM Guangdong	China
as58543	32,186	CHINA TELECOM Guangdong	China
as58543	28,940	CHINA TELECOM Guangdong	China
as58543	27,319	CHINA TELECOM Guangdong	China
as58543	24,466	CHINA TELECOM Guangdong	China
as58543	22,224	CHINA TELECOM Guangdong	China
as58543	22,104	CHINA TELECOM Guangdong	China
as58543	21,729	CHINA TELECOM Guangdong	China
as58543	21,611	CHINA TELECOM Guangdong	China
as58543	20,555	CHINA TELECOM Guangdong	China
as58543	19,832	CHINA TELECOM Guangdong	China
as58543	18,543	CHINA TELECOM Guangdong	China
as58543	16,541	CHINA TELECOM Guangdong	China
as58543	16,523	CHINA TELECOM Guangdong	China
as58543	15,937	CHINA TELECOM Guangdong	China
as58543	15,070	CHINA TELECOM Guangdong	China
as58543	14,645	CHINA TELECOM Guangdong	China
as58543	11,508	CHINA TELECOM Guangdong	China
as58543	11,017	CHINA TELECOM Guangdong	China
as4837	23,547	China Unicom Backbone	China

Q3 Attack Count of IP Addresses Launching >10K Attacks, by ASN, by Country

Source ASN	Attack Count	ASN Owner	Country
as4837	22,338	China Unicom Backbone	China
as4837	106,234	China Unicom-Jiangsu Province Network	China
as4837	56,320	China Unicom-Jiangsu Province Network	China
as4837	25,369	China Unicom-Jiangsu Province Network	China
as4837	24,874	China Unicom-Jiangsu Province Network	China
as4837	24,764	China Unicom-Jiangsu Province Network	China
as4837	24,376	China Unicom-Jiangsu Province Network	China
as4837	24,302	China Unicom-Jiangsu Province Network	China
as4837	21,437	China Unicom-Jiangsu Province Network	China
as4837	21,050	China Unicom-Jiangsu Province Network	China
as4837	20,483	China Unicom-Jiangsu Province Network	China
as4837	20,324	China Unicom-Jiangsu Province Network	China
as4837	20,240	China Unicom-Jiangsu Province Network	China
as4837	17,363	China Unicom-Jiangsu Province Network	China
as4837	16,892	China Unicom-Jiangsu Province Network	China
as4134	128,470	Chinanet backbone	China
as4134	61,228	Chinanet backbone	China
as4134	49,878	Chinanet backbone	China
as4134	36,666	Chinanet backbone	China
as4134	31,534	Chinanet backbone	China
as4134	29,742	Chinanet backbone	China
as4134	29,668	Chinanet backbone	China
as4134	28,805	Chinanet backbone	China
as4134	26,962	Chinanet backbone	China
as4134	26,352	Chinanet backbone	China
as4134	24,114	Chinanet backbone	China
as4134	23,799	Chinanet backbone	China
as4134	16,190	Chinanet backbone	China
as4134	15,870	Chinanet backbone	China
as4134	14,267	Chinanet backbone	China
as4134	12,666	Chinanet backbone	China
as4134	12,394	Chinanet backbone	China
as4134	11,534	Chinanet backbone	China
as4134	10,186	Chinanet backbone	China
as23650	33,560	Chinanet-Jiangsu Province Network	China
as23650	29,250	Chinanet-Jiangsu Province Network	China
as23650	27,330	Chinanet-Jiangsu Province Network	China
as23650	25,355	Chinanet-Jiangsu Province Network	China
as23650	21,249	Chinanet-Jiangsu Province Network	China
as23650	19,549	Chinanet-Jiangsu Province Network	China
as23650	19,452	Chinanet-Jiangsu Province Network	China
as23650	15,687	Chinanet-Jiangsu Province Network	China

Q3 Attack Count of IP Addresses Launching >10K Attacks, by ASN, by Country

Source ASN	Attack Count	ASN Owner	Country
as23650	13,619	Chinanet-Jiangsu Province Network	China
as23650	12,952	Chinanet-Jiangsu Province Network	China
as23650	12,674	Chinanet-Jiangsu Province Network	China
as23650	12,006	Chinanet-Jiangsu Province Network	China
as23650	10,447	Chinanet-Jiangsu Province Network	China
as23650	10,318	Chinanet-Jiangsu Province Network	China
as23724	11,035	IDC	China
as9394	12,301	TieTong Telecommunications Corporation	China
as12876	13,730	Online SAS	France
as12876	12,112	Online SAS	France
as12876	11,533	Online SAS	France
as16276	28,951	OVH	France
as16276	19,457	OVH	France
as8560	31,862	1&1 Internet	Germany
as8560	17,902	1&1 Internet	Germany
as7540	10,628	Hong Kong Commercial Exchange	Hong Kong
as17995	19,066	iForte Global Internet	Indonesia
as17974	13,834	PT Telekomunikasi Indonesia	Indonesia
as1267	11,030	Wind Telecomunicazioni SpA	Italy
as48716	10,112	PS Internet	Kazakhstan
as50673	28,474	Serverius	Netherlands
as50673	19,352	Serverius	Netherlands
as50673	11,598	Serverius	Netherlands
as12252	16,900	America Movil Peru S.A.C.	Peru
as8399	15,978	America Movil Peru S.A.C.	Peru
as49349	18,366	Dotsi	Portugal
as39383	13,538	Annarsy SRL	Romania
as39383	10,941	Annarsy SRL	Romania
as9050	52,108	Telekom Romania	Romania
as3216	13,053	PJSC Vimpelcom	Russia
as29182	28,080	The First	Russia
as3786	13,666	LG Dacom/LG Uplus Corp	South Korea
as131293	14,155	TOT Public Company Limited	Thailand
as9121	17,625	Turk Telekomunikasyon Anonim Sirketi	Turkey
as40965	17,919	Rise-v	Ukraine
as15395	13,976	Rackspace	United Kingdom
as14061	32,549	Digital Ocean	US
as36351	27,513	SoftLayer	US
as36351	22,156	SoftLayer	US
as24088	11,409	Hanoi Telecom Joint Stock Company	Vietnam

Table 9. Q3 ASNs launching 10K attacks or greater from 1 IP address—listed by country

Q4 Attack Count of IP Addresses Launching >10K Attacks, by ASN, by Country

Source ASN	Attack Count	ASN Owner	Country
as262254	156,893	Dancom LTD	Belize
as262254	25,674	Dancom LTD	Belize
as262254	17,589	Dancom LTD	Belize
as262254	17,168	Dancom LTD	Belize
as262254	12,188	Dancom LTD	Belize
as10429	120,015	Telefonica Data S.A.	Brazil
as49699	18,014	Internet Corporated Networks LTD	Bulgaria
as33554	13,665	Neutral Data Centers Corp	Canada
as23650	56,773	Chinanet-Jiangsu Province Network	China
as23650	44,930	Chinanet-Jiangsu Province Network	China
as23650	34,825	Chinanet-Jiangsu Province Network	China
as23650	34,607	Chinanet-Jiangsu Province Network	China
as23650	34,411	Chinanet-Jiangsu Province Network	China
as23650	31,507	Chinanet-Jiangsu Province Network	China
as23650	25,366	Chinanet-Jiangsu Province Network	China
as23650	23,514	Chinanet-Jiangsu Province Network	China
as23650	19,574	Chinanet-Jiangsu Province Network	China
as23650	16,643	Chinanet-Jiangsu Province Network	China
as23650	15,824	Chinanet-Jiangsu Province Network	China
as23650	14,027	Chinanet-Jiangsu Province Network	China
as23650	13,961	Chinanet-Jiangsu Province Network	China
as23650	13,638	Chinanet-Jiangsu Province Network	China
as23650	13,386	Chinanet-Jiangsu Province Network	China
as23650	10,695	Chinanet-Jiangsu Province Network	China
as37963	17,587	Hangzhou Alibaba Advertising Co	China
as37963	11,888	Hangzhou Alibaba Advertising Co	China
as37963	10,209	Hangzhou Alibaba Advertising Co	China
as4134	194,661	Chinanet backbone	China
as4134	148,163	Chinanet backbone	China
as4134	122,199	Chinanet backbone	China
as4134	74,560	Chinanet backbone	China
as4134	71,591	Chinanet backbone	China
as4134	70,782	Chinanet backbone	China
as4134	64,844	Chinanet backbone	China
as4134	58,706	Chinanet backbone	China
as4134	58,413	Chinanet backbone	China
as4134	39,334	Chinanet backbone	China
as4134	22,590	Chinanet backbone	China
as4134	21,988	Chinanet backbone	China
as4134	20,057	Chinanet backbone	China
as4134	19,662	Chinanet backbone	China
as4134	16,781	Chinanet backbone	China

Q4 Attack Count of IP Addresses Launching >10K Attacks, by ASN, by Country

Source ASN	Attack Count	ASN Owner	Country
as4134	15,703	Chinanet backbone	China
as4134	14,663	Chinanet backbone	China
as4134	14,586	Chinanet backbone	China
as4134	14,465	Chinanet backbone	China
as4134	12,602	Chinanet backbone	China
as4134	12,254	Chinanet backbone	China
as45090	11,045	Tencent	China
as45090	10,214	Tencent	China
as4816	37,695	Chinanet-Guangdong Province Network	China
as4837	11,361	China Unicom	China
as4837	11,284	China Unicom	China
as4837	11,190	China Unicom	China
as4837	11,100	China Unicom	China
as4837	10,991	China Unicom	China
as4837	10,966	China Unicom	China
as4837	10,897	China Unicom	China
as4837	10,787	China Unicom	China
as4837	10,787	China Unicom	China
as4837	10,701	China Unicom	China
as58466	10,157	CHINA TELECOM Guangdong	China
as58543	178,465	CHINA TELECOM Guangdong	China
as58543	178,103	CHINA TELECOM Guangdong	China
as58543	171,747	CHINA TELECOM Guangdong	China
as58543	158,209	CHINA TELECOM Guangdong	China
as58543	128,164	CHINA TELECOM Guangdong	China
as58543	104,287	CHINA TELECOM Guangdong	China
as58543	100,573	CHINA TELECOM Guangdong	China
as58543	83,742	CHINA TELECOM Guangdong	China
as58543	74,885	CHINA TELECOM Guangdong	China
as58543	72,395	CHINA TELECOM Guangdong	China
as58543	51,849	CHINA TELECOM Guangdong	China
as58543	50,476	CHINA TELECOM Guangdong	China
as58543	50,010	CHINA TELECOM Guangdong	China
as58543	43,308	CHINA TELECOM Guangdong	China
as58543	35,697	CHINA TELECOM Guangdong	China
as58543	34,856	CHINA TELECOM Guangdong	China
as58543	34,820	CHINA TELECOM Guangdong	China
as58543	30,478	CHINA TELECOM Guangdong	China
as58543	30,210	CHINA TELECOM Guangdong	China
as58543	26,205	CHINA TELECOM Guangdong	China
as58543	24,445	CHINA TELECOM Guangdong	China
as58543	19,850	CHINA TELECOM Guangdong	China

Q4 Attack Count of IP Addresses Launching >10K Attacks, by ASN, by Country

Source ASN	Attack Count	ASN Owner	Country
as58543	19,778	CHINA TELECOM Guangdong	China
as58543	19,144	CHINA TELECOM Guangdong	China
as58543	18,135	CHINA TELECOM Guangdong	China
as58543	17,291	CHINA TELECOM Guangdong	China
as58543	16,510	CHINA TELECOM Guangdong	China
as58543	15,119	CHINA TELECOM Guangdong	China
as58543	13,936	CHINA TELECOM Guangdong	China
as58543	12,940	CHINA TELECOM Guangdong	China
as58543	10,989	CHINA TELECOM Guangdong	China
as9304	72,980	Hutchison Global Communications	China
as3292	13,231	TDC A/S	Denmark
as14420	18,165	CORPORACION NACIONAL DE TELECOMUNICACIONES - CNT EP	Ecuador
as12876	840,386	Online SAS	France
as12876	21,315	Online SAS	France
as12876	18,932	Online SAS	France
as12876	18,418	Online SAS	France
as12876	14,362	Online SAS	France
as12876	13,864	Online SAS	France
as12876	13,120	Online SAS	France
as12876	13,082	Online SAS	France
as16276	83,306	OVH	France
as16276	80,753	OVH	France
as16276	18,244	OVH	France
as16276	15,734	OVH	France
as16276	15,276	OVH	France
as16276	14,727	OVH	France
as16276	14,426	OVH	France
as16276	13,144	OVH	France
as16276	12,910	OVH	France
as16276	12,728	OVH	France
as16276	12,584	OVH	France
as16276	12,426	OVH	France
as16276	11,401	OVH	France
as16276	10,862	OVH	France
as13301	18,126	United GameServer GmbH	Germany
as13301	14,269	United GameServer GmbH	Germany
as13301	11,272	United GameServer GmbH	Germany
as13301	10,132	United GameServer GmbH	Germany
as24940	107,539	Hetzner Online GmbH	Germany
as24940	39,725	Hetzner Online GmbH	Germany
as24940	17,811	Hetzner Online GmbH	Germany

Q4 Attack Count of IP Addresses Launching >10K Attacks, by ASN, by Country

Source ASN	Attack Count	ASN Owner	Country
as24940	16,054	Hetzner Online GmbH	Germany
as24940	11,425	Hetzner Online GmbH	Germany
as24961	180,370	myLoc Managed IT AG	Germany
as24961	14,683	myLoc Managed IT AG	Germany
as29066	134,197	Velia.net	Germany
as29066	100,092	Velia.net	Germany
as51167	13,571	Contabo GmbH	Germany
as51167	12,633	Contabo GmbH	Germany
as5464	10,143	NAG Datacenter AG	Germany
as8560	28,624	1&1 Internet SE	Germany
as8560	15,745	1&1 Internet SE	Germany
as8560	14,838	1&1 Internet SE	Germany
as8560	14,579	1&1 Internet SE	Germany
as8560	14,190	1&1 Internet SE	Germany
as8560	10,923	1&1 Internet SE	Germany
as8560	10,614	1&1 Internet SE	Germany
as8972	25,964	Host Europe GmbH	Germany
as8972	12,404	Host Europe GmbH	Germany
as49061	338,609	William Hill Organization LTD	Gibraltar
as134121	18,147	Rainbow network limited	Hong Kong
as58779	32,770	i4HK Limited	Hong Kong
as9829	18,663	BSNL (Bharat Sanchar Nigam Ltd)	India
as8551	10,186	Bezeq International	Israel
as16125	144,590	UAB Cherry Servers	Lithuania
as16125	12,255	UAB Cherry Servers	Lithuania
as29073	20,486	Quasi Networks	Netherlands
as29073	12,282	Quasi Networks	Netherlands
as49544	118,623	i3d B.V	Netherlands
as49981	38,459	WorldStream B.V.	Netherlands
as49981	18,165	WorldStream B.V.	Netherlands
as49981	10,570	WorldStream B.V.	Netherlands
as50673	17,970	Serverius Holding B.V.	Netherlands
as50673	13,969	Serverius Holding B.V.	Netherlands
as198414	42,977	H88	Poland
as57807	17,887	Oxylion S.A.	Poland
as12790	12,326	LTD "TB"	Russia
as48172	10,534	Oversun LTD	Russia
as49335	11,538	Mir Telematiki LTD	Russia
as50098	12,179	DDoS Protection LTD	Russia
as50113	104,740	MediaService Plus LLC	Russia
as50113	16,928	MediaService Plus LLC	Russia
as50113	10,491	MediaService Plus LLC	Russia

Q4 Attack Count of IP Addresses Launching >10K Attacks, by ASN, by Country

Source ASN	Attack Count	ASN Owner	Country
as9318	22,380	SK Broadband Co Ltd	South Korea
as9318	13,527	SK Broadband Co Ltd	South Korea
as56934	50,213	Sologigabit	Spain
as37027	20,410	Simbanet Limited	Tanzania
as39609	14,936	Habari Node Ltd	Tanzania
as24299	23,674	Internet Solution & Service Provider Co	Thailand
as57844	15,251	SPDNet Telekomunikasyon Hizmetleri Bilgi Teknolojileri Taahhut Sanayi Ve Ticaret A.S.	Turkey
as40965	10,814	Rise-v Ltd	Ukraine
as43110	27,186	Joint Ukrainian-American enterprise Ewropol	Ukraine
as43110	26,600	Joint Ukrainian-American enterprise Ewropol	Ukraine
as20738	428,068	Host Europe GmbH	United Kingdom
as35017	14,493	Swiftway SP Z O O	United Kingdom
as57002	311,969	William Hill Organization LTD	United Kingdom
as57002	25,171	William Hill Organization LTD	United Kingdom
as14061	68,075	Digital Ocean	US
as14061	66,256	Digital Ocean	US
as14061	59,953	Digital Ocean	US
as14061	55,436	Digital Ocean	US
as15083	23,053	Infolink Global Corporation	US
as16509	53,354	AWS	US
as16509	11,746	AWS	US
as174	13,461	Cogent	US
as19318	21,850	NEW JERSEY INTERNATIONAL INTERNET EXCHANGE LLC	US
as19437	15,000	Secured Servers	US
as19437	10,507	Secured Servers	US
as19531	80,131	Nodes Direct	US
as19531	63,388	Nodes Direct	US
as19905	11,607	Neustar	US
as20454	13,634	Secured Servers	US
as20473	15,979	Choopa	US
as20473	13,756	Choopa	US
as20473	13,358	Choopa	US
as20473	11,737	Choopa	US
as20473	10,907	Choopa	US
as20473	10,856	Choopa	US
as20473	24,401	Choopa	US
as25761	23,214	Staminus Communications	US
as25761	21,850	Staminus Communications	US
as26484	12,226	Hostspace	US
as30083	32,679	HEG US Inc	US
as30083	13,051	HEG US Inc	US

Q4 Attack Count of IP Addresses Launching >10K Attacks, by ASN, by Country			
Source ASN	**Attack Count**	**ASN Owner**	**Country**
as36024	79,630	Colo4 LLC	US
as36678	12,622	CHINA TELECOM (AMERICAS) CORPORATION	US
as46664	49,931	Volume Drive	US
as701	16,396	Verizon Business	US
as7018	39,388	AT&T	US
as7922	12,572	Comcast	US
as45899	24,384	VNPT	Vietnam

Table 10. Q4 ASNs launching 10K or greater attacks from one IP address—listed by country