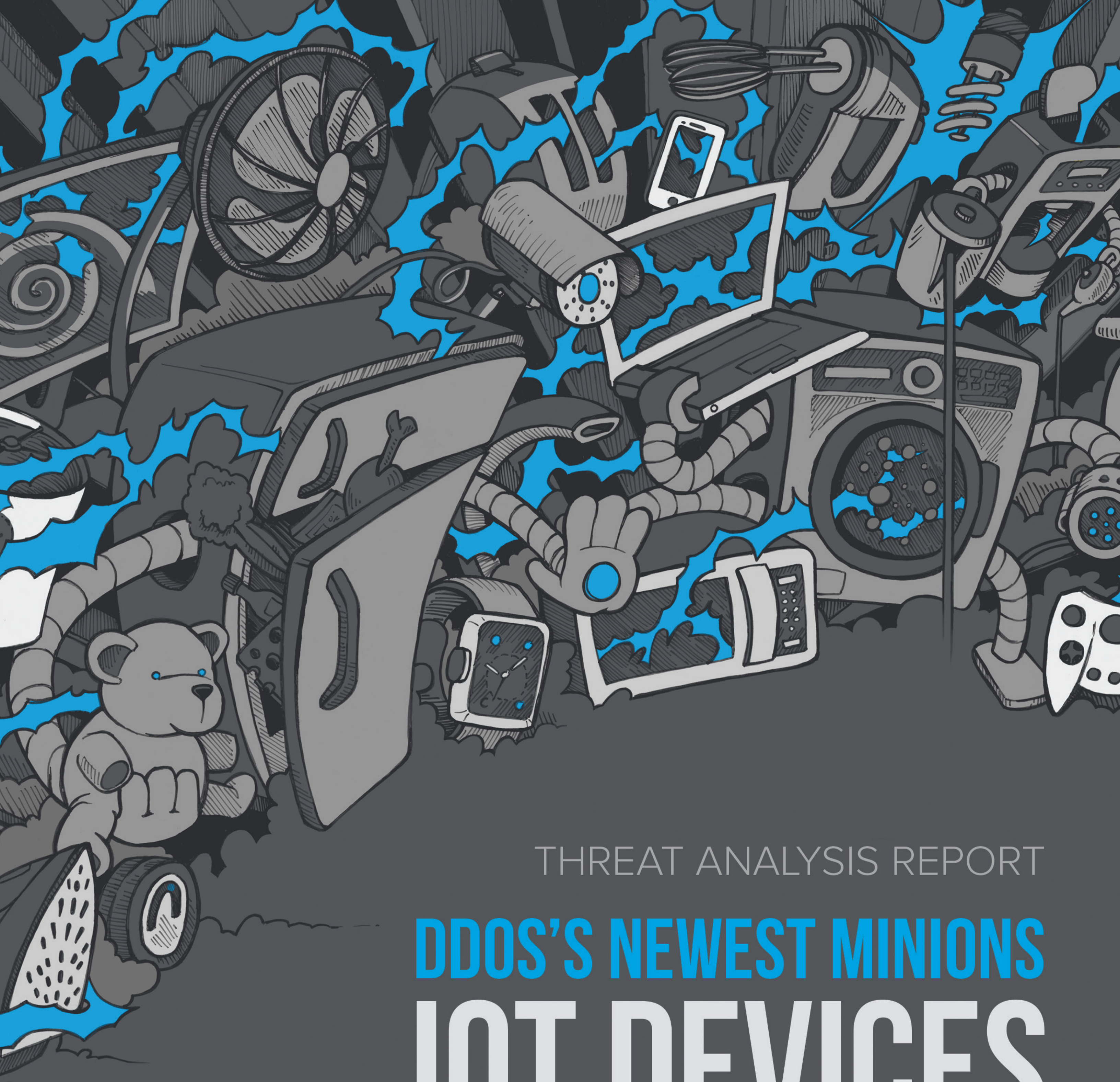


THREAT ANALYSIS REPORT

DDOS'S NEWEST MINIONS
IOT DEVICES

by Justin Shattuck and Sara Boddy

VOLUME 1
JULY 2016

TABLE OF CONTENTS

WRITTEN BY F5 LABS IN CONJUNCTION WITH OUR PARTNER LORYKA

TABLE OF FIGURES

INTRODUCTION

Ten years ago, if someone had told you that a toaster would someday play a role in disrupting service or entirely disabling your company's website, you probably would've laughed them out of the room. The idea was completely absurd. It's not anymore.

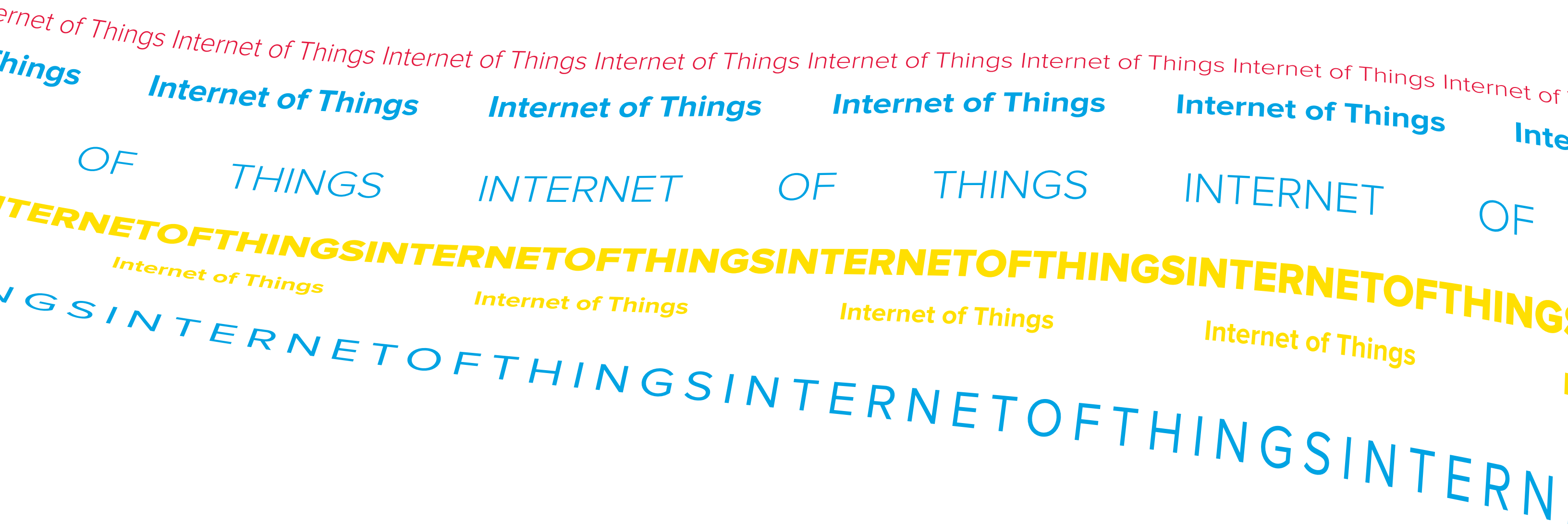
Distributed denial-of-service (DDoS) attacks, which take down websites by flooding them with unwanted traffic, aren't anything new, but they have evolved over the years. Attack volumes today regularly exceed 100 Gbps, and many attacks have been reported in the 400-500 Gbps range.

Most attackers don't possess the resources to generate such enormous attacks, so where are they getting them? From you, the unwitting pawns in their game. They create botnets—networks of computers infected with malicious software—that they control without your knowledge to carry out such attacks.

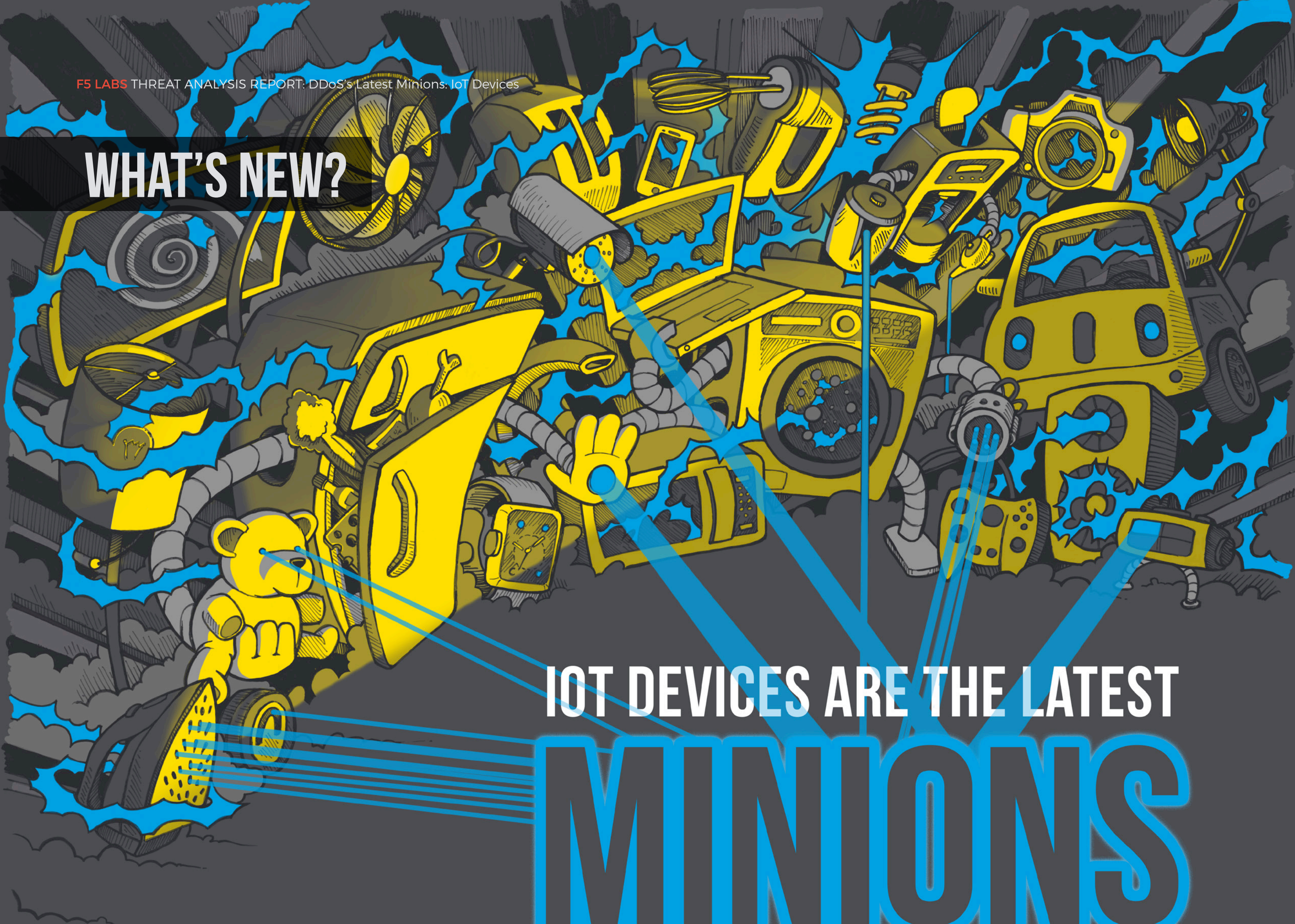
In this report, we look at the growth of IoT devices as attack tools, who is on the hunt for these devices, how they're using them, and what attack trends are emerging.

Before we dive into the details, here are some high-level observations from our threat researchers derived from both the research conducted for this report between mid-February 2016 and the end of July 2016, and common industry knowledge:

- China, a major player in cyber-attacks, is unlikely to stop censoring the Internet in its own country or dial back its cyber opposition forces and nation-state espionage activities.
- Global leaders like the US, Canada, and members of the EU will continue to be top monetary targets because they are strong financial sectors. As a result, a lot of today's malware is targeted at the financial industry specifically, especially since the release of Zeus in 2011.
- China, Russia, Ukraine, Brazil, and India will likely remain the top five countries from which DDoS attacks are launched.
- China, followed by Russia, Romania, Brazil, and Vietnam, are the most likely countries where Command and Control (C&C) servers will be located.


Internet of Things Internet of Things Internet of Things Internet of Things Internet of Things Internet of Things Internet of Things Internet of Things
Internet of Things Internet of Things Internet of Things Internet of Things
OF THINGS INTERNET OF THINGS INTERNET OF
INTERNETOFTHINGSINTERNETOFTHINGSINTERNETOFTHINGSINTERNETOFTHINGS
Internet of Things Internet of Things Internet of Things Internet of Things
GSINTERNETOFTHINGSINTERNETOFTHINGSINTERN

WHAT'S NEW?



IOT DEVICES ARE THE LATEST MINIONS IN CYBER WEAPONRY TOOLKITS

Cyber weaponry has evolved. In the past, botnets were mostly made up of vulnerable home computers whose owners understood little about viruses and malware. "Odd" behavior (such as extremely slow response time or annoying pop-up windows) was often interpreted as a sign that something was "broken" when really the computer was infected with malware and had become part of a botnet.

Home computers still account for a significant portion of today's botnet armies used to perpetrate DDoS attacks, but the latest easy targets for conscription are everyday network-connected devices that make up the "Internet of Things" (IoT).

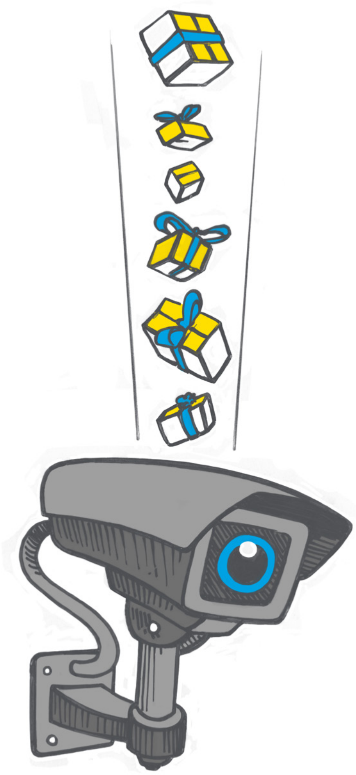
Most of us have yet to grasp the IoT and its impact on our daily lives. Virtually everything we come in contact with throughout the day is becoming connected online. The obvious ones are the smartphones we use to manage our day-to-day activities, do our jobs, access bank accounts, catch up on the latest world news, find a restaurant, get driving directions, watch TV, and play video games. Less obvious are the things in our homes—refrigerators that cycle through family portraits, residential security cameras designed to increase our personal sense of security, baby monitors that give us peace of mind. Even the cars we drive, the doors we walk through and the airplanes we fly in are all connected online.

We know residential modems for cable and DSL are plagued with vulnerabilities that the manufacturers haven't fixed yet. And we know that residential routers from consumer-friendly all-in-one devices, from popular manufacturers to the pro-consumer products from less known companies are seemingly all vulnerable. We know this because they have reported CVEs detailing how the uPnP protocol (as an example) can be exploited and used as a traffic source for SSDP-based DDoS attacks. The list of "smart" devices coming online grows by the week. Meanwhile, consumers are unaware of the possibility they could be compromised, and the security industry doesn't yet understand the full scope of vulnerable IoT devices.

Even lesser known, but more threatening from a cyber risk standpoint, are public infrastructure Supervisory Control and Data Acquisition (SCADA) systems that are used to monitor and control things like traffic lights at intersections, air traffic control systems, water systems and power grids, the 911 system, and a range of systems used by hospitals (everything from breathing systems to physical doors).

In this report, we prove what the security community has been speculating for quite some time—that IoT devices are already compromised and actively being used to launch attacks. Before we get into the attack details, we explore the hunt for IoT devices. The interest is shockingly high. While there are the "expected" top threat actors (it's no surprise that China is leading the charge), the interest globally is vast and rapidly expanding, with participants in every part of the world. This is an area where there is as much sprawl as there is concentration. We also proved that although individually, IoT devices can be small in terms of bandwidth used to launch attacks, collectively they can cause great damage. The idea that IoT devices are "too small to worry about" just isn't true, and the industry needs to start paying careful attention.

Welcome to cyberspace and the IoT.



THE INTEREST IN IOT DEVICES IS HIGH

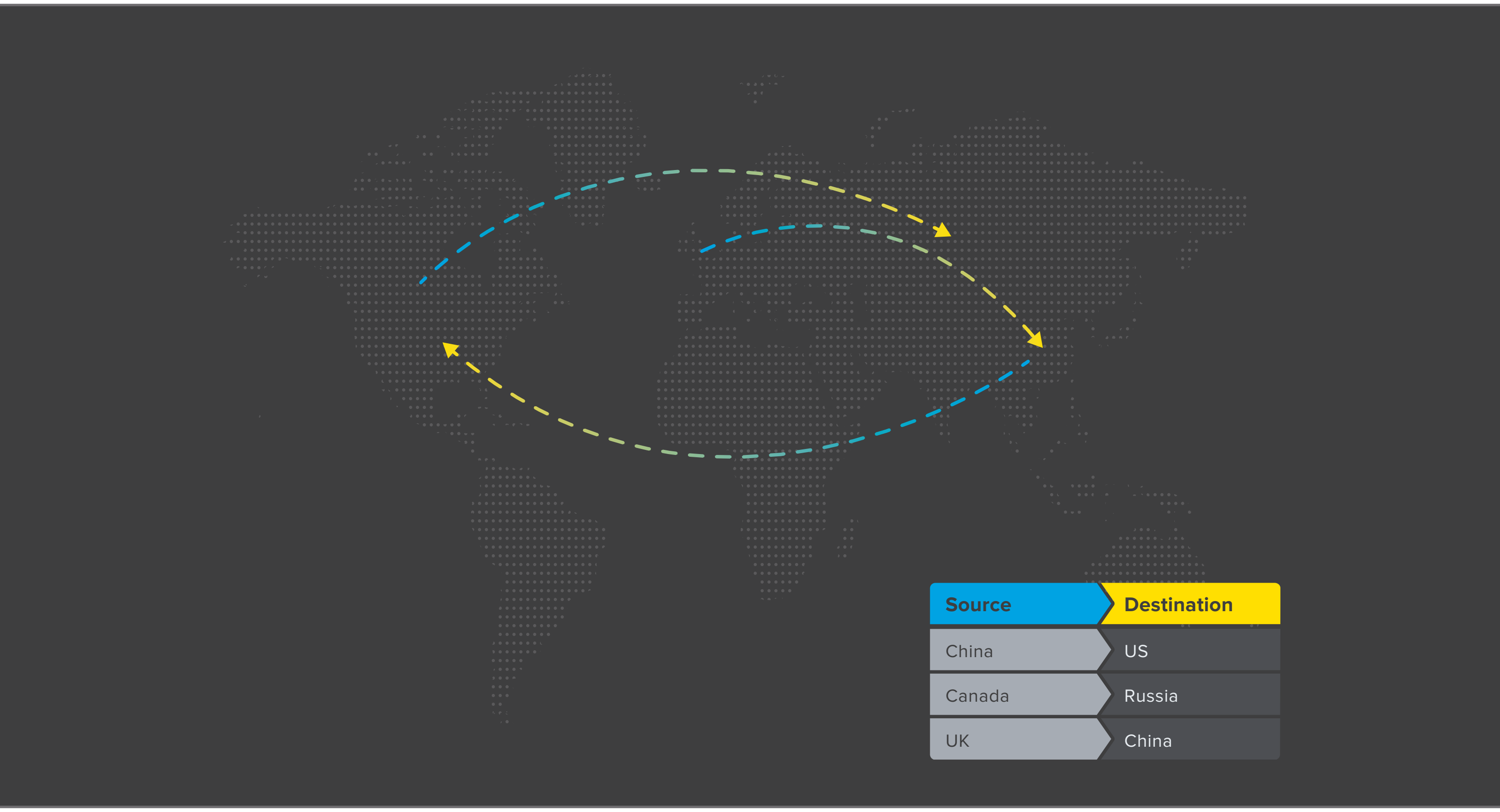
Any device that's connected online is subject to vulnerabilities and therefore exploit. What's concerning is that many IoT devices were *never designed with security in mind.* These devices—and the applications that run them—typically don't go through vulnerability testing, nor have they been designed to enable secure remote management. And because many ship with default passwords that users either don't change or can't change, these IoT devices have become the latest pawns in hackers' cyber weaponry. The fact that these devices are so easy to exploit, and that DDoS attack tools are readily available to bad guys[2], makes for a far more vulnerable world in the future.

Just how interested are hackers in these devices? Very.

GARTNER ESTIMATES A 43% INCREASE IN IOT DEVICES COMING ONLINE IN 2016.[1]

HUNTING FOR IOT DEVICES WITH DEFAULT PASSWORDS

We are observing a steady increase of SSH and Telnet brute force attacks hunting for IoT devices. These activities are targeting vendor default passwords in a likely effort to expand threat actors' IoT toolsets. Trending in July 2016 was China looking for IoT devices in the US, Canada looking for IoT devices in Russia, and the UK looking for IoT devices in China.



Source	Destination
China	US
Canada	Russia
UK	China

Figure 1: Trends in default password scanning

When reviewing a longer period from mid-February to end of July 2016, China remained the overwhelming leader in brute force scans looking for vulnerable IoT devices. All other countries were distant followers that varied drastically when we compared the sum of activities from February–July to the most recent 30 days of activity in July.

WHY BRUTE FORCE TELNET AND SSH?

SSH, or Secure Socket Shell, is a network protocol that gives administrators a secure way to access a remote computer. Telnet is another protocol that enables remote access to a device. A large number of IoT devices leverage SSH and Telnet for remote administration. These devices are often "protected" with vendor default credentials (which is really no protection at all), and are susceptible to brute force attacks (guessing username and password combinations until the right one is found), because there are no account lock restrictions in place after a number of failed login attempts. When vendor default credentials are used, they are typically the same across all of that vendor's devices so when hackers crack one, they crack them all.

SSH BRUTE FORCE ATTACKS AND TRENDS

Between mid-February and end of July 2016, we collected data on 6,293,889 SSH brute force attacks. These attacks were sourced from 3,385 autonomous system numbers (ASNs) and 28,616 IP addresses. Daily SSH brute force attack volumes during this period remained consistent with infrequent spikes

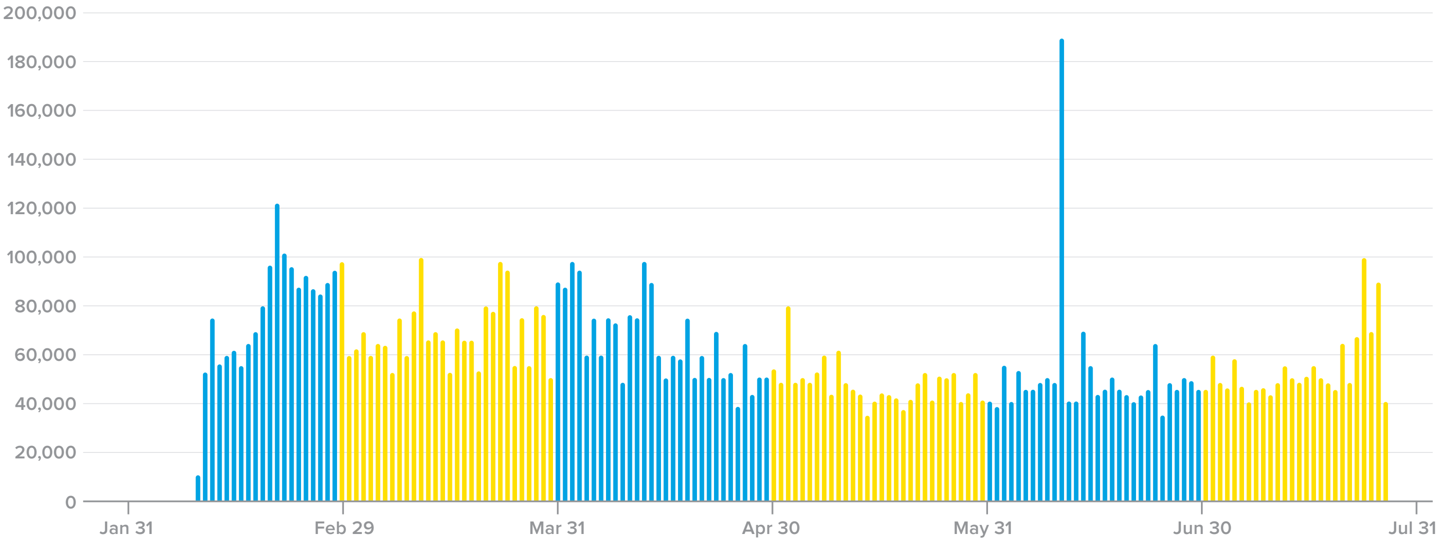


Figure 2: SSH brute force attacks observed by day

When viewing the SSH brute force attacks by day of week to see if there was a pattern that might give insight into the threat actors' "work" days, it was relatively consistent. This was expected because these scans are all automated and require very little human interaction.

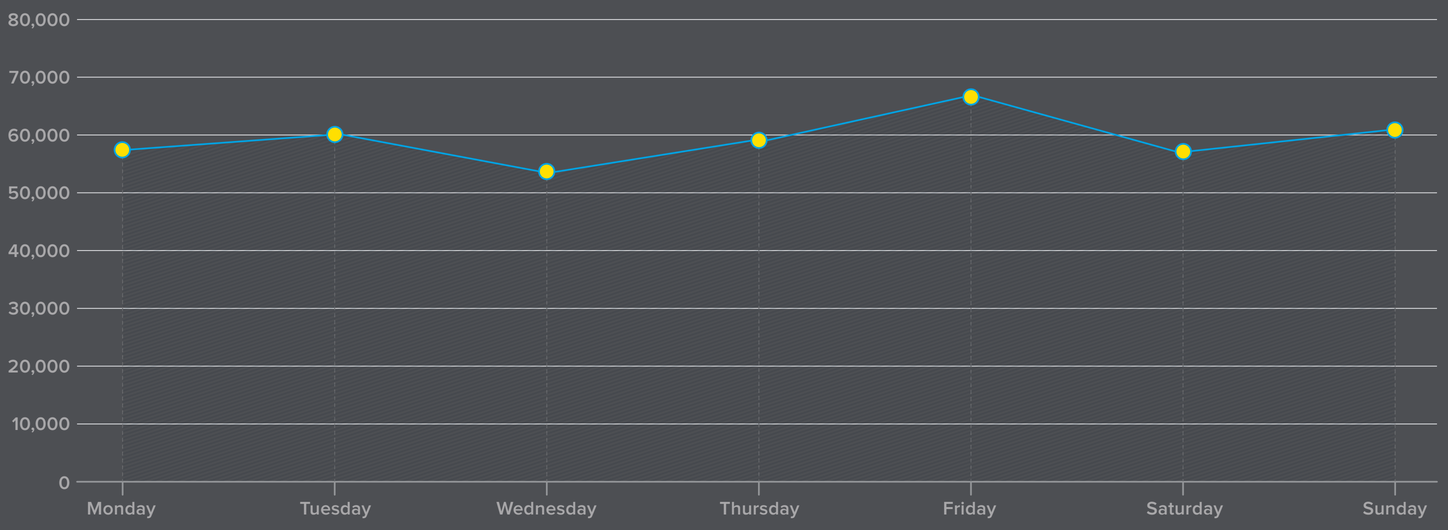
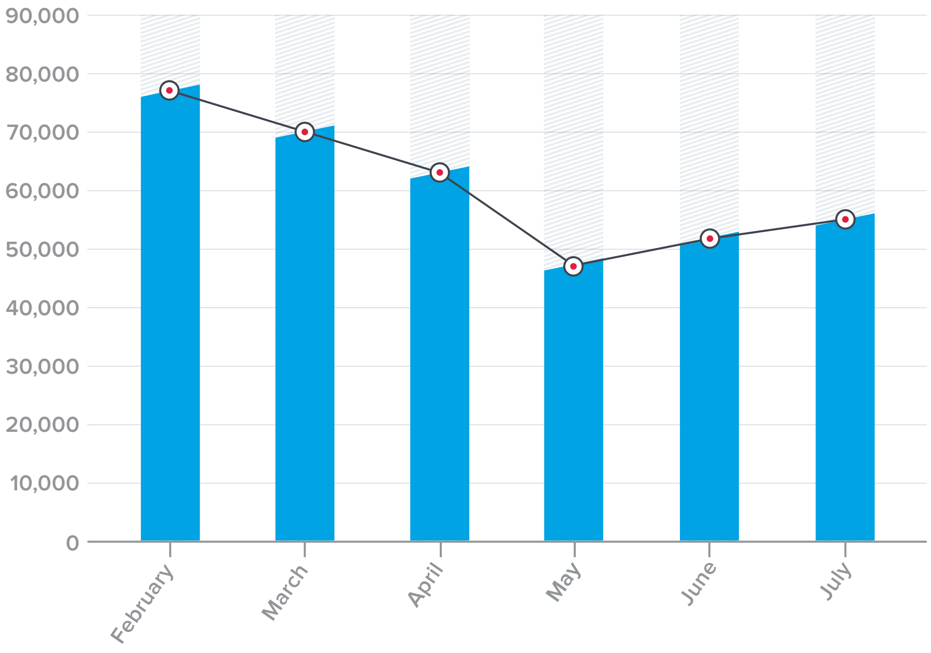


Figure 3: SSH brute force attacks day-of-week average



Looking at the average daily volume of SSH brute force attacks by month, it declined almost 30% from February through May, and then began climbing again in June and July.

Figure 4: SSH Brute force attacks by month (daily average)

TELNET BRUTE FORCE ATTACKS AND TRENDS

Between mid-February and end of July 2016, we collected 2,174,216 Telnet brute force attacks—about one-third the number of the SSH attacks detected in the same timeframe. The Telnet attacks, however, were sourced from a much broader scope of ASNs (8,516) and included 543,819 IP addresses.

TELNET SCANS HAVE INCREASED 140% YEAR OVER YEAR FROM JULY 2015

Looking purely at volume, Telnet scans were a rising attack vector and spiked significantly in late June through mid-July.

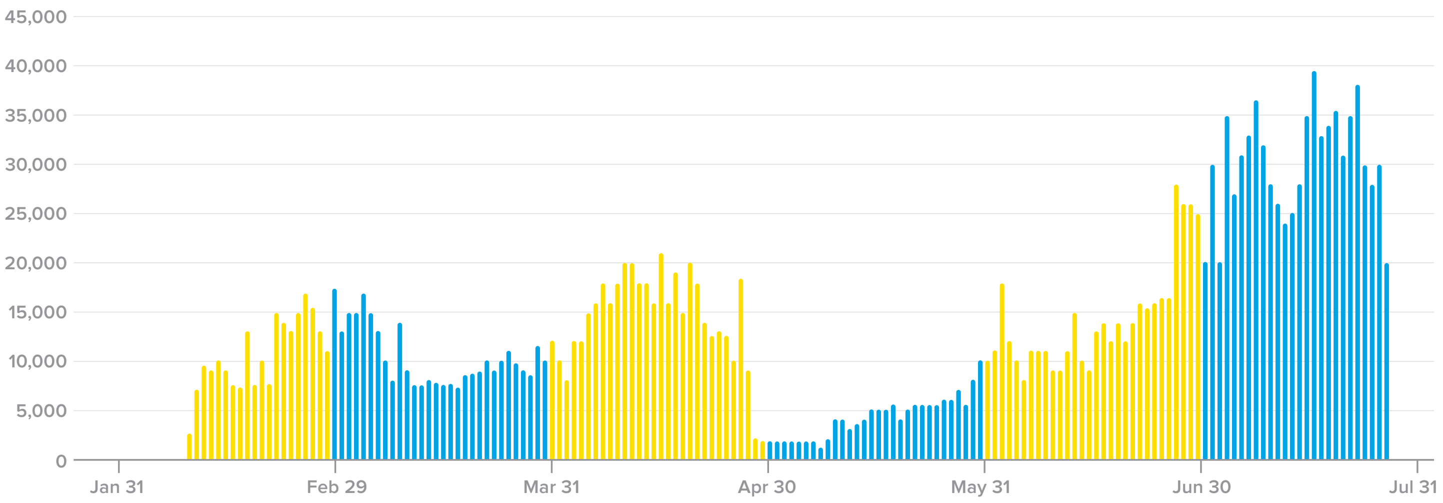


Figure 5: Telnet attacks increased slowly and then suddenly spiked.

When reviewing the Telnet scans by day of week, there was a lot less consistency in behavior from day to day.

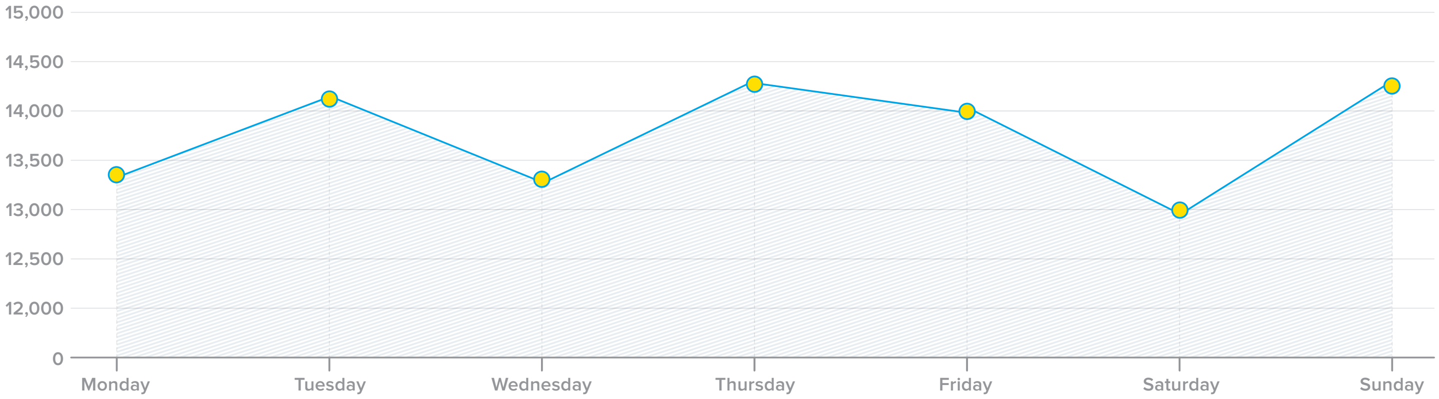


Figure 6: Telnet brute force attacks day of week average

Based on a trend line of the average daily Telnet attacks from mid-February through July, we expect to see attack continue to rise.

AVERAGE DAILY TELNET ATTACKS PER MONTH

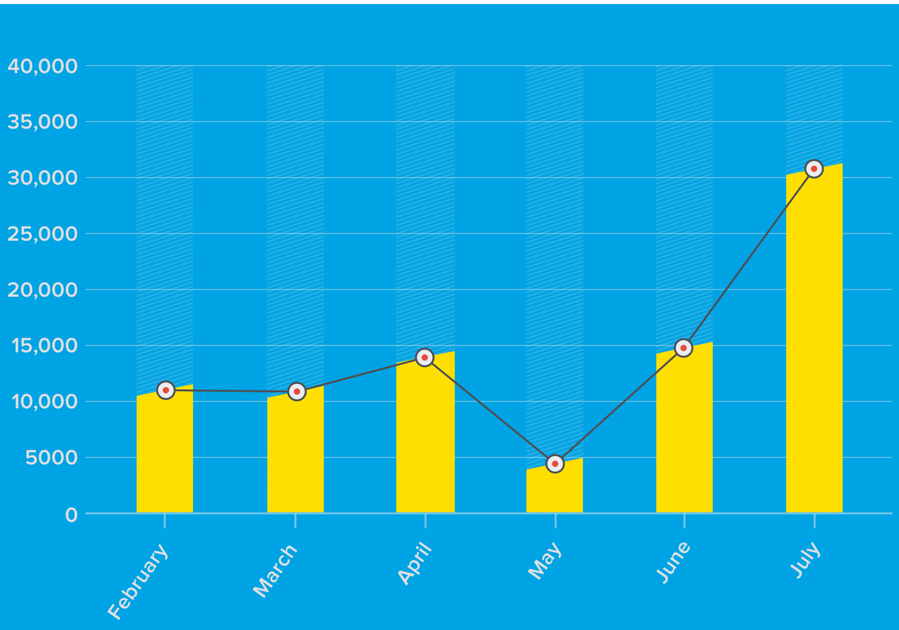


Figure 7: Telnet attacks daily average by month

July Remaiten Spike

The rise in Telnet attacks in late June and early July was due to Remaiten, an IoT botnet composed largely of home routers, gateways, and wireless access points running Linux.

The anatomy of a Remaiten toolkit attack is as follows:

1. Initial bootstrapped servers (C&C servers) established and set as download servers.
2. Attacker begins scanning for new victim hosts that have Telnet running.
3. Brute force against Telnet with varying dictionaries; starts and is distributed across infected hosts.
4. Upon successful authentication, Remaiten attempts to identify the host's architecture and requests the appropriate download (pack) from C&C server(s).
5. Attempts to identify and subsequently kill additional rootkits and malware present on the host.
6. Connects to C&C server(s) via commonly used IRC.
7. Awaits commands to start performing additional Telnet scanning and brute forcing hosts or begin an attack using various L4-L7 attack vectors.

TELNET BRUTE FORCE ATTACK ORIGIN COUNTRIES

The most persistent country hunting for vulnerable IoT devices was China. When looking at the period from mid-February to end of July, the US was number two in overall scanning traffic observed. However, when looking at the last 30 days of the period, the US didn't show up in the top 20 list. There was a significant flux in the top 20 list of scanning countries from the beginning of the year to July. Given the spike in Telnet attacks over June and July, it's possible the scanning activities in US didn't slow down, rather other countries started and/or increased their scanning efforts.

TOP 10 COUNTRIES SCANNING FOR IOT DEVICES

Figures 8 and 9 show the flux in Telnet brute force attacks by country origin between mid-February to late July 2016, and the last 30 days of the sampled period.

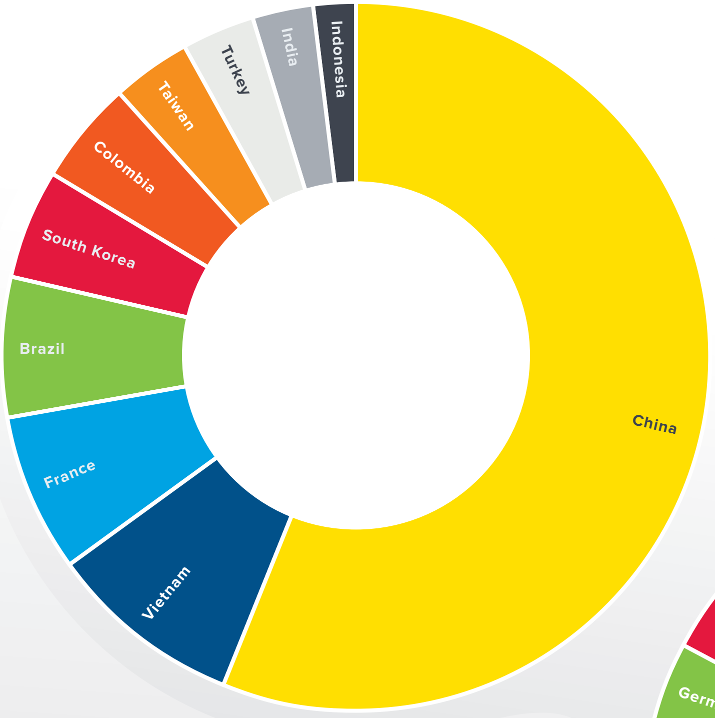


Figure 8: Telnet brute force attacks by country of origin, last 30 days of sampled period

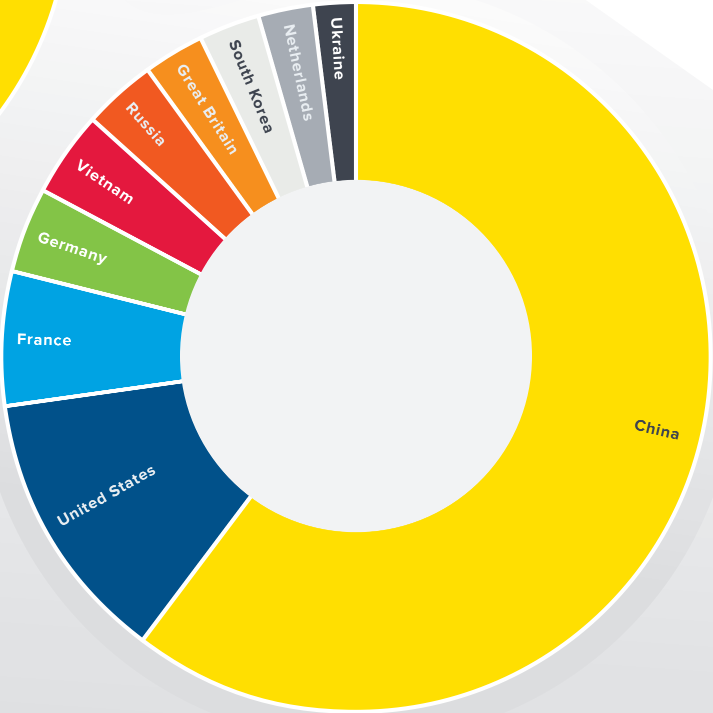


Figure 9: Telnet brute force attacks by country, mid-February through end ofJuly 2016

TOP 20 COUNTRIES CONDUCTING TELNET BRUTE FORCE ATTACKS

POSITION	LAST 30 DAYS	POSITION	LAST 6 MONTHS
1	China	1	China
2	Vietnam	2	United States
3	France	3	France
4	Brazil	4	Germany
5	South Korea	5	Vietnam
6	Colombia	6	Great Britain
7	Taiwan	7	Russia
8	Turkey	8	Netherlands
9	India	9	South Korea
10	Indonesia	10	Ukraine
11	Phillipines	11	India
12	Mexico	12	Poland
13	Thailand	13	Indonesia
14	Argentina	14	Brazil
15	Malaysia	15	Turkey
16	Pakistan	16	Chile
17	Kazakhstan	17	Canada
18	American Samoa	18	Hong Kong
19	South Africa	19	Japan

Sixty percent of the countries on the top 20 scanning list between mid-February through end of July 2016 were not on the top 20 actors list for the last 30 days of that sampled period. The chart below highlights the country of origin changes in the top 20 country threat actors.

The hunt for vulnerable IoT devices is global, but China is leading the race by a very wide margin. More Telnet brute force scans come out of China than all of the other top 19 countries combined. Out of the total volume of Telnet brute force attacks in the last 30 days of the sample period by the top 20 countries (not total attacks in that period), China conducted 52% of the attacks compared to a combined total of 48% by all the countries. On average, the other countries contributed 2.5% each to the total attack volume.

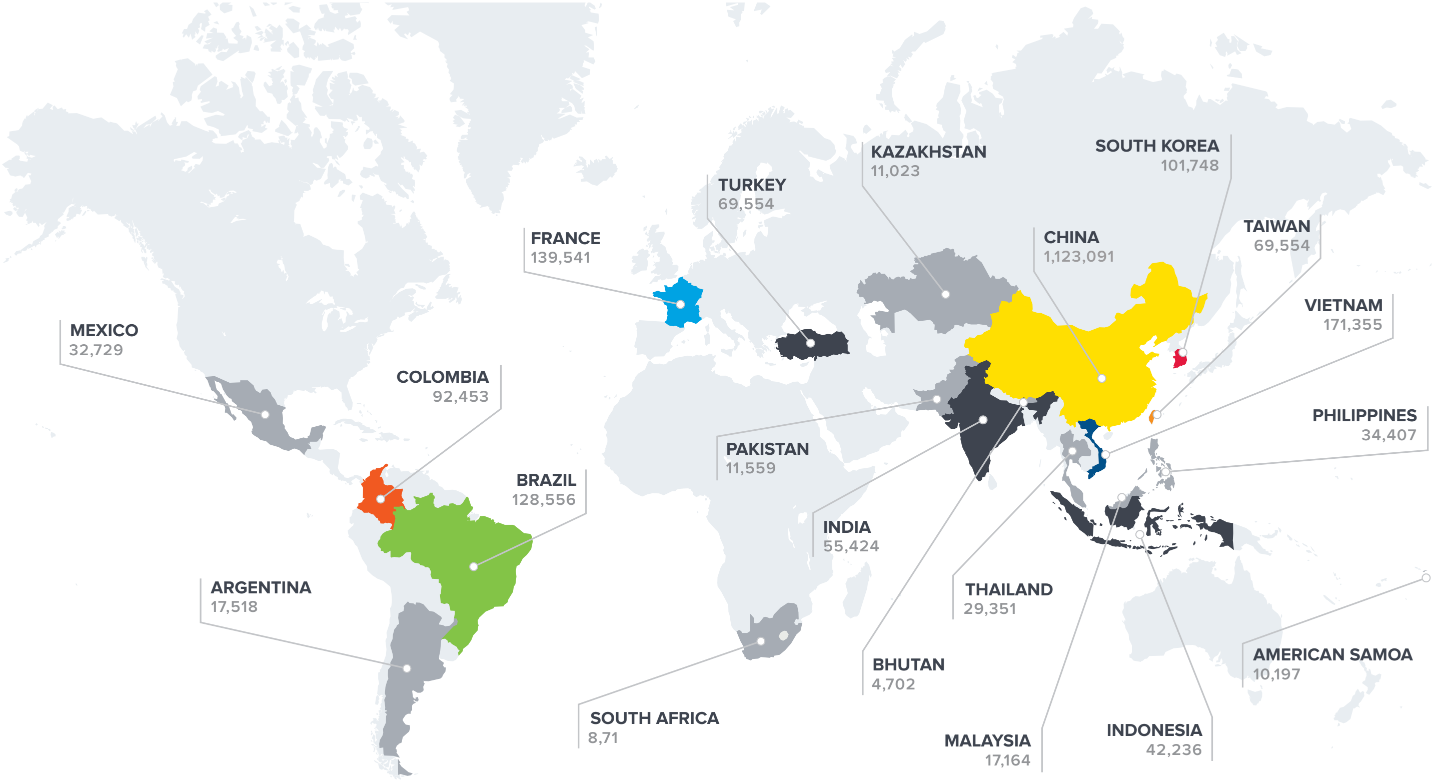


Figure 10: Top 20 countries hunting for IoT devices with Telnet brute force scans (last 30 days of sampled period)

TELNET AND SSH ATTACKS BY ASN

ASNs participating in Telnet and SSH brute force attacks vary day by day but have been steadily increasing throughout 2016.

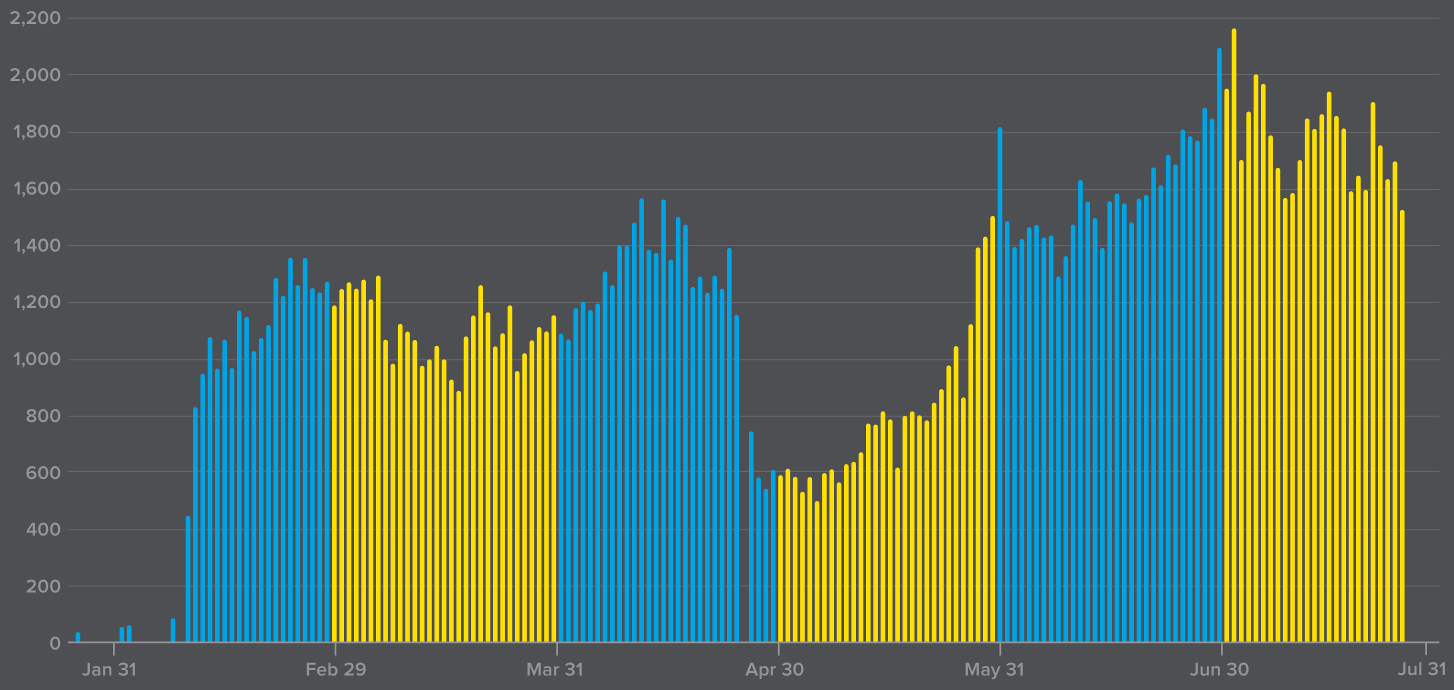


Figure 11: Total ASNs launching Telnet and SSH brute force attacks

Separating out ASNs participating in Telnet versus SSH attacks, we saw a consistent use of ASNs in the SSH attacks, indicating the threat actors are consistent.

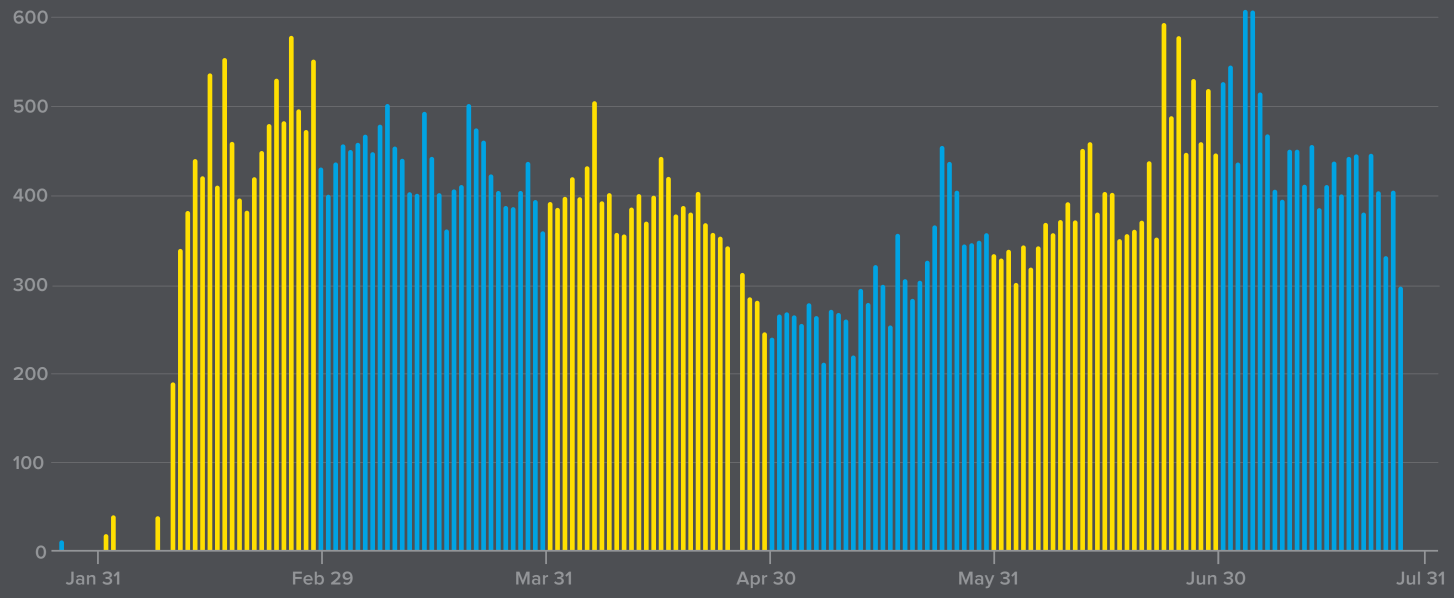


Figure 12: Total ASNs participating in SSH attacks

The brute force Telnet attacks fluctuated and increased significantly in the last two months of the sample period indicating two things: Telnet attacks are largely responsible for the total attack volume spike in June through July, and its likely that new threat actors are coming on board.

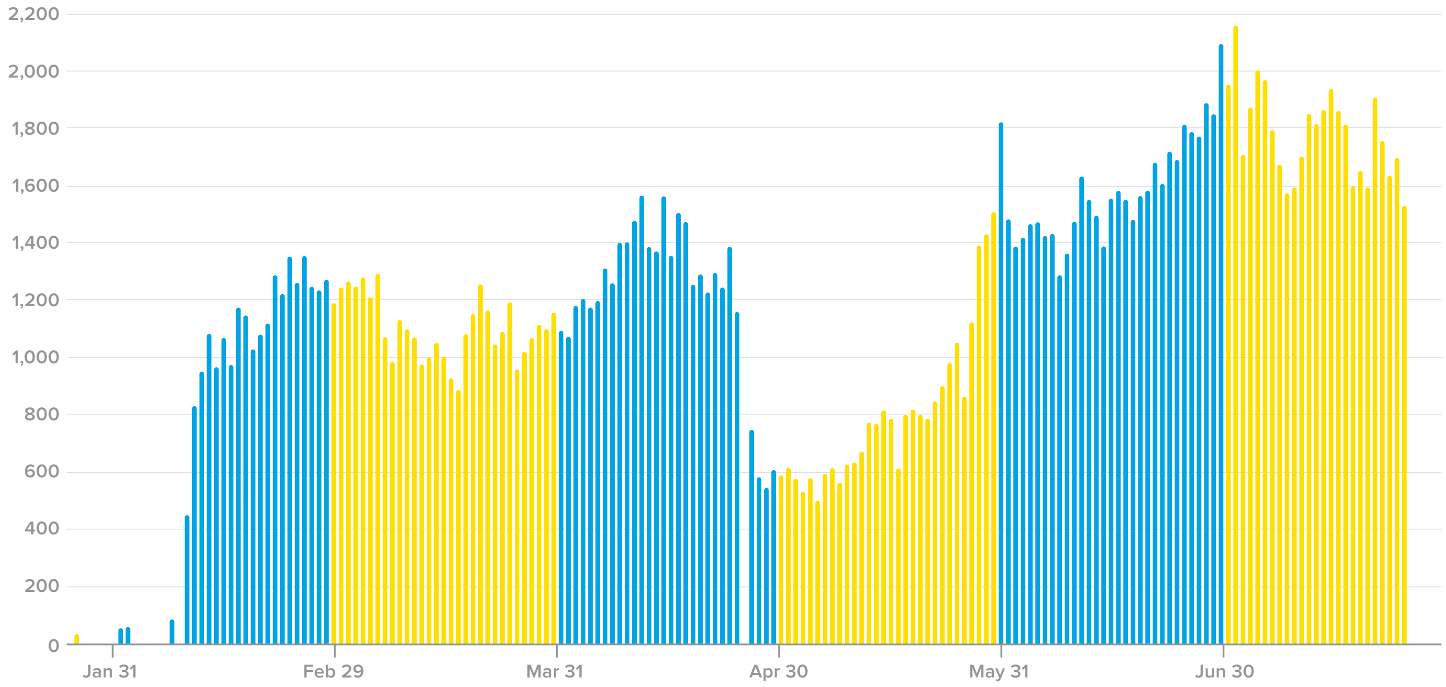


Figure 13: Total ASNs participating in Telnet attacks

Ninety-two ASNs participated the more than 2.1 million Telnet brute force scans conducted by the top 20 scanning countries during the last 30 days of the sampled period. The top four contributing ASNs, all of them in China, make up 57% of the total scans. The ASNs are owned by Chinese telecom, backbone, and peering providers.

TOP 1,000 ASNS LAUNCHING SSH BRUTE FORCE ATTACKS

The balance of threat actor ASNs and their contribution to the total attacks gives us a good indication of how many threat actors are out there. Is it a concentrated few or many everywhere? In looking at the top 1,000 contributing ASNs in SSH brute force attacks, half of the attacks were launched from six ASNs—less than 1% of the 1,000. Even within the top six ASNs, the distribution of attack percentages varies greatly and is top-heavy, from 22% at the highest down to 3% at the lowest.

50% OF SSH ATTACKS WERE GENERATED FROM TOP 6 ASN THREAT ACTORS

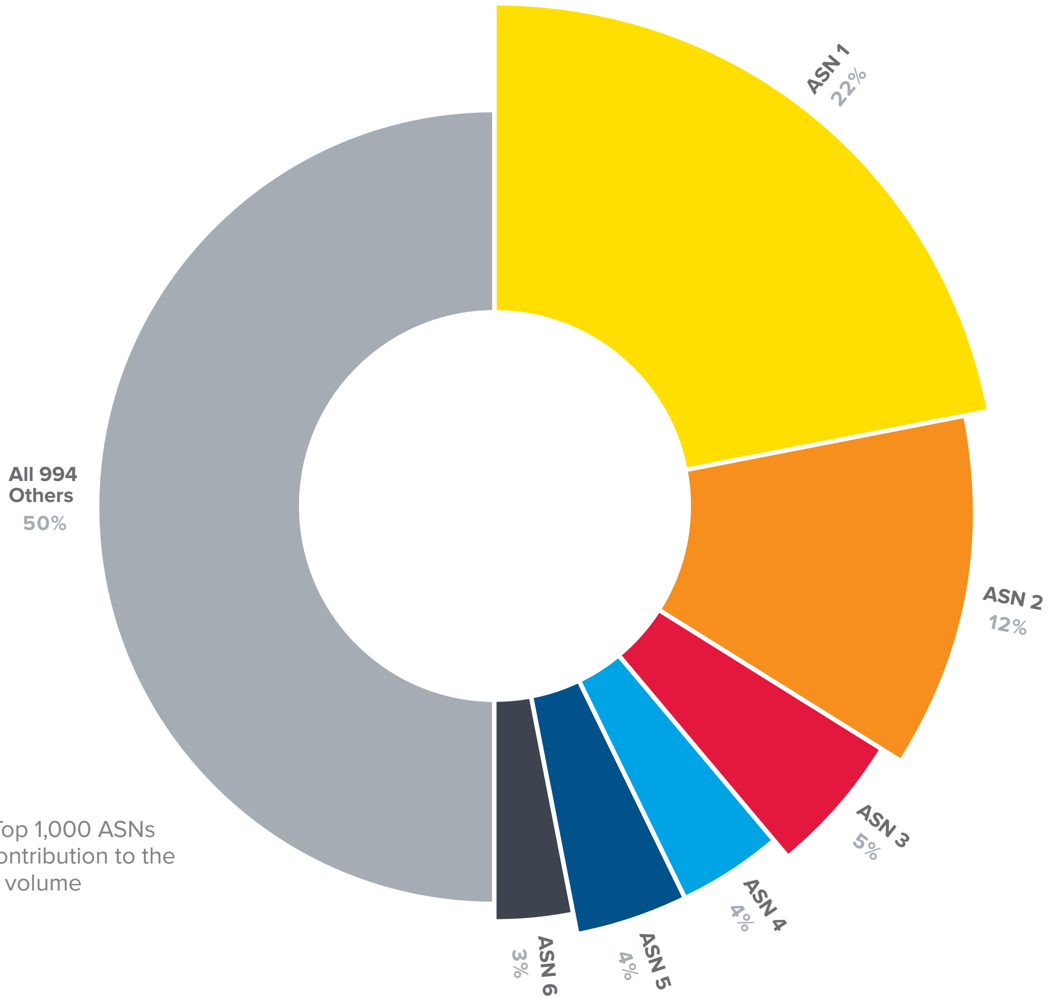


Figure 14: Top 1,000 ASNs and their contribution to the SSH attack volume

To see how top heavy the threat actors really are, we looked at ASNs contributing over 1% to the total attack volume, which is a very low bar for the percentage of attack contribution. Sixteen ASNs contributed more than 1% for a combined total of 63% of the top 1,000 attack volume. The bottom 984 attacking ASNs launched on average 4,195 attacks each. This indicates that although we have some standout leaders, we have a lot of threat actors around the world engaging in this activity.

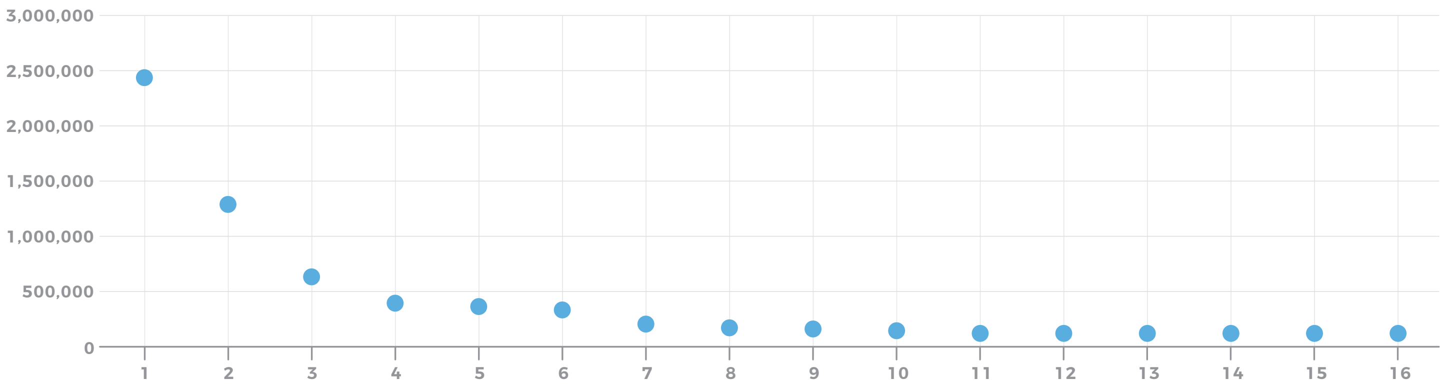


Figure 15: 16 ASNs contributing more than 1% to the total SSH attack volume

TOP 1,000 ASNS LAUNCHING TELNET ATTACKS

An analysis of the top 1,000 ASNs participating in Telnet attacks netted interesting results because this attack vector is less concentrated than SSH, although still very top heavy. Contribution to the total attack number is more evenly spaced throughout the top 1,000 ASNs with 968 of them producing less than one half of 1% each to the total. The average contribution per ASN is .10%, and the top threat actor only contributed to 8% of the total attacks in comparison to the top threat actor of SSH attacks contributing 22%.

50% OF TELNET ATTACKS WERE GENERATED FROM TOP 13 ASN THREAT ACTORS

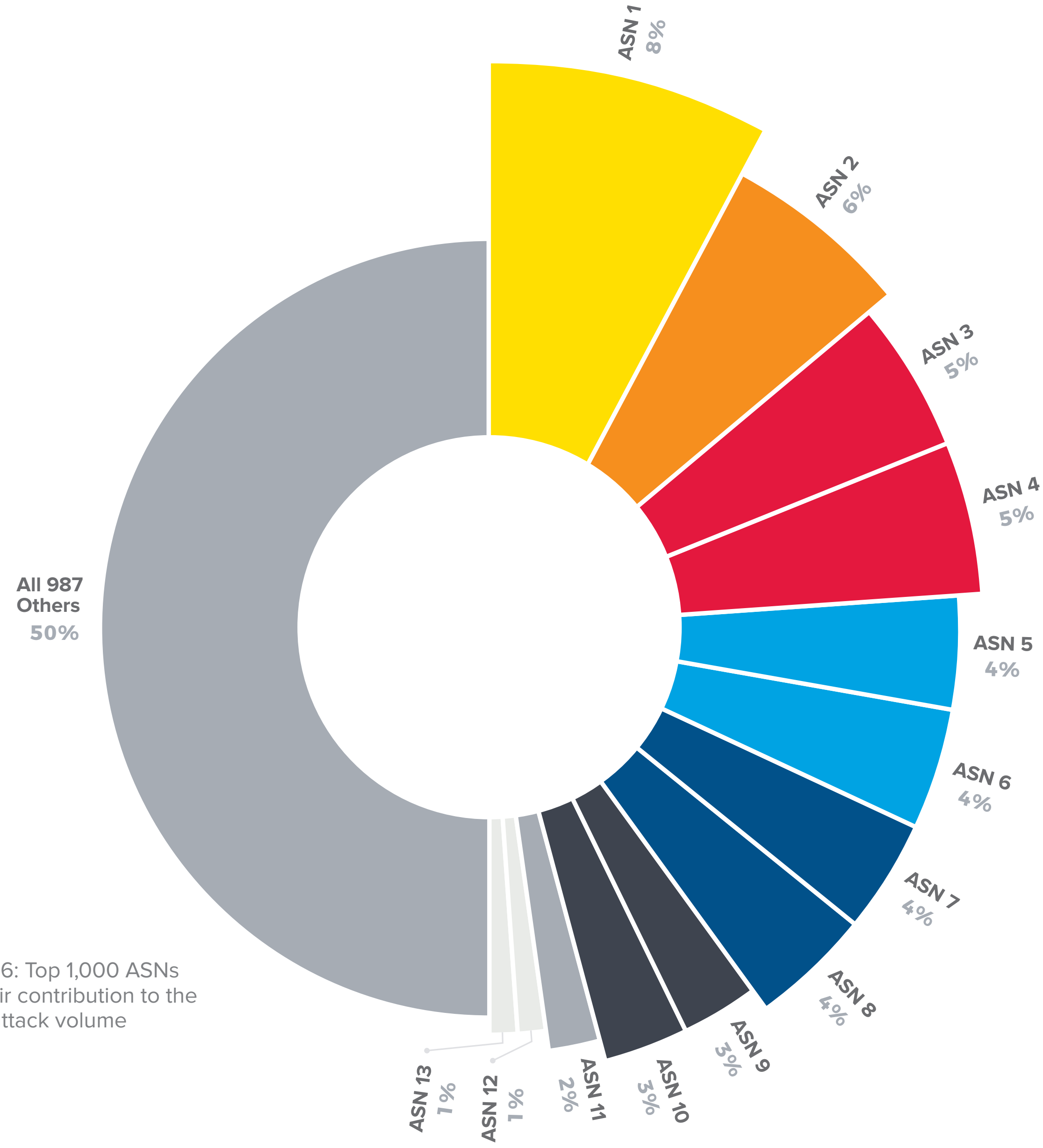


Figure 16: Top 1,000 ASNs and their contribution to the Telnet attack volume

When looking at the ASNs that contributed more than 1% to the total Telnet attack volume, the numbers are slightly more diverse than the SSH attacks and include 19 ASNs that account for 57% of the attack total.

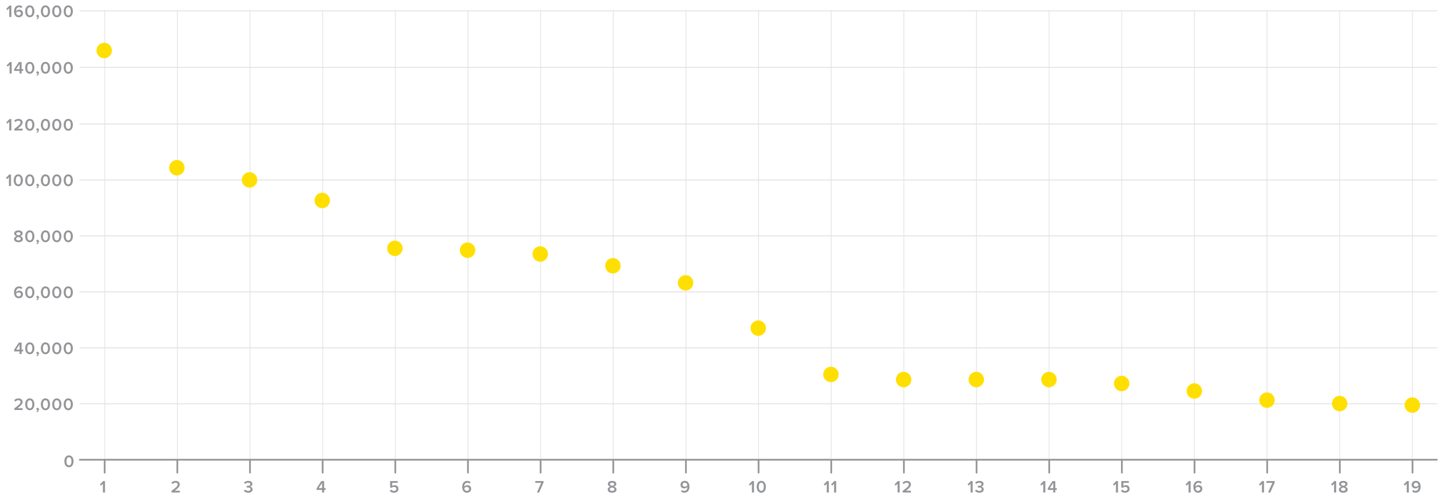


Figure 17: Top 19 ASNs contributing more than 1% to the total Telnet attack volume

The scatter chart shown in Figure 18 is a great representation of the current Telnet scanning going on, which is the precursor to botnet creation.

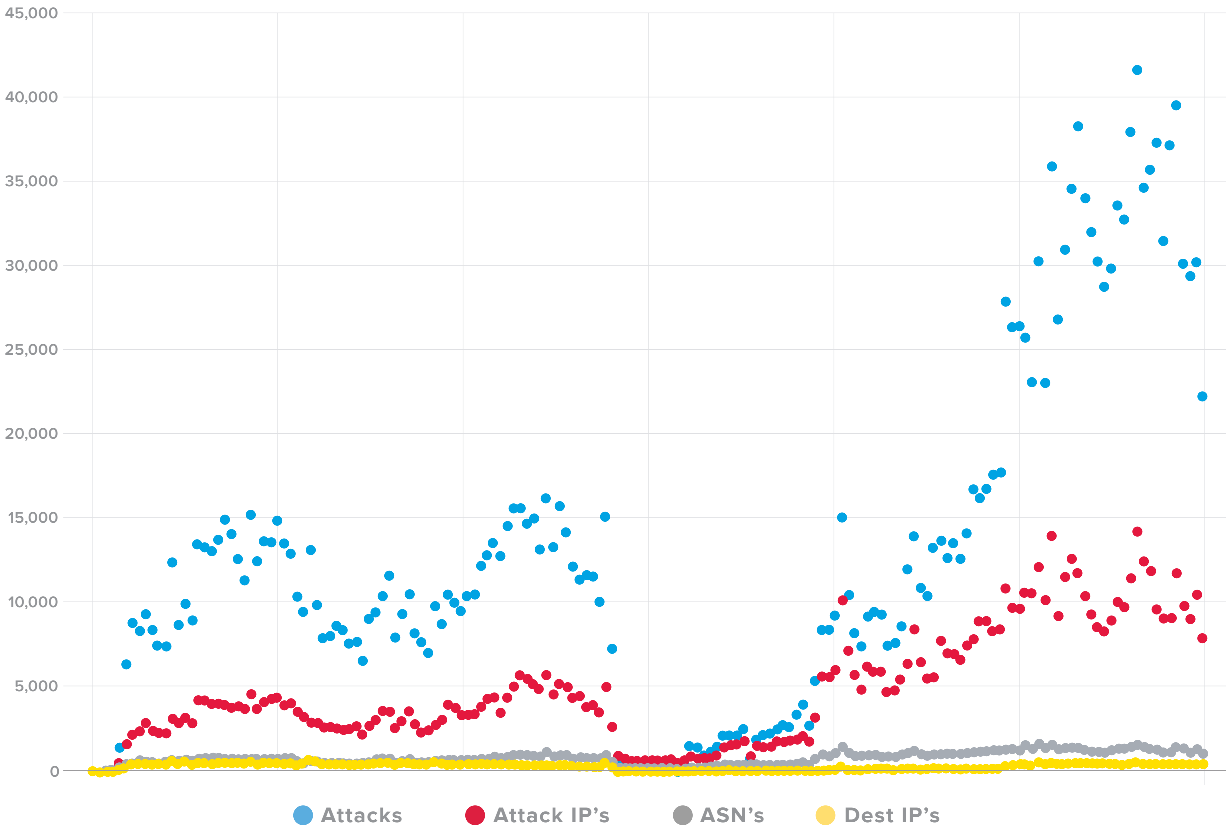


Figure 18: Telnet attacks in relation to the attacking IP addresses, ASNs, and destination IP

IOT BOTNETS GENERATING DDOS ATTACKS

Several outlets have reported DDoS attacks using the “lizard stresser” tool, which leverages home routers. Recent data confirms active botnets are generating DDoS attacks from a new variant and mash-up of older tools that are refactored for infecting additional architectures such as x86_64, MIPS, and ARM.

IOT BOTNET ATTACKED MULTIPLE US STATE AGENCIES

We are tracking an IoT botnet leveraging 52,000 unique IP addresses that targeted a US State entity in July 2016 on port 80. The attack lasted roughly 30 minutes between shortly after 10:30 PM on July 18 to shortly after midnight on July 19.

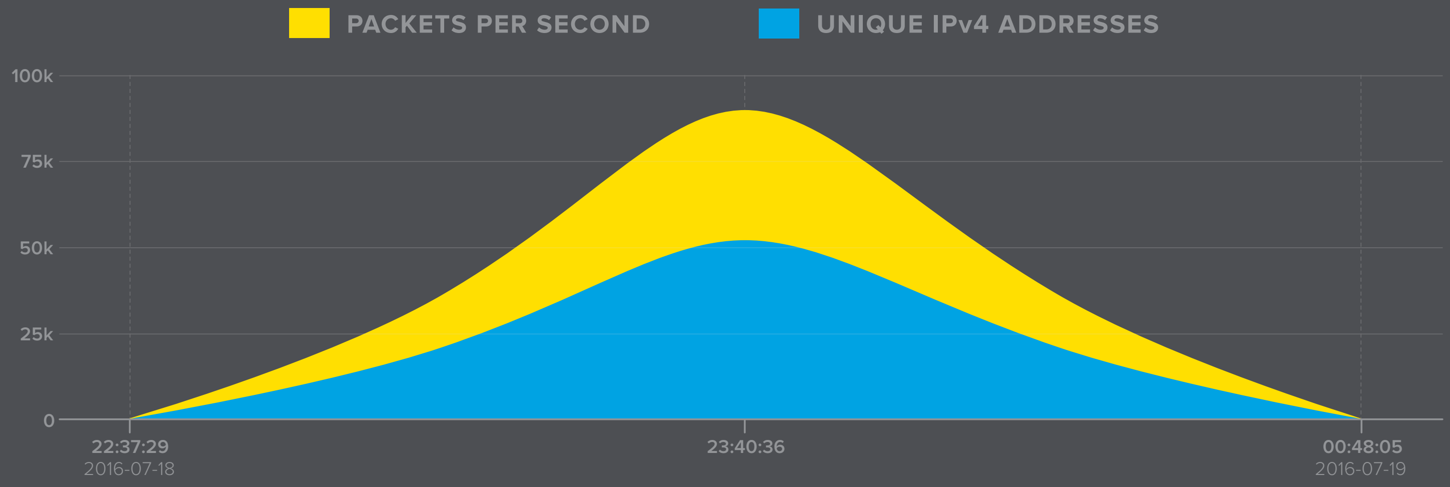
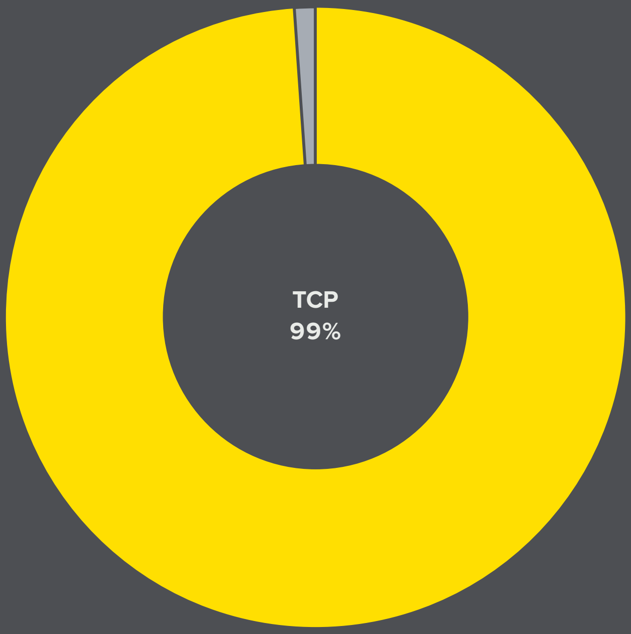


Figure 19: US State agency sampled attack traffic



The destination port of the attack was 99% on port 80 using protocol TCP.

Figure 20: US State agency attack was 99% TCP-based

Attacking sources used random unprivileged ports, primarily between 20000-60000, in addition to modest use of port 53 and protocol UDP.

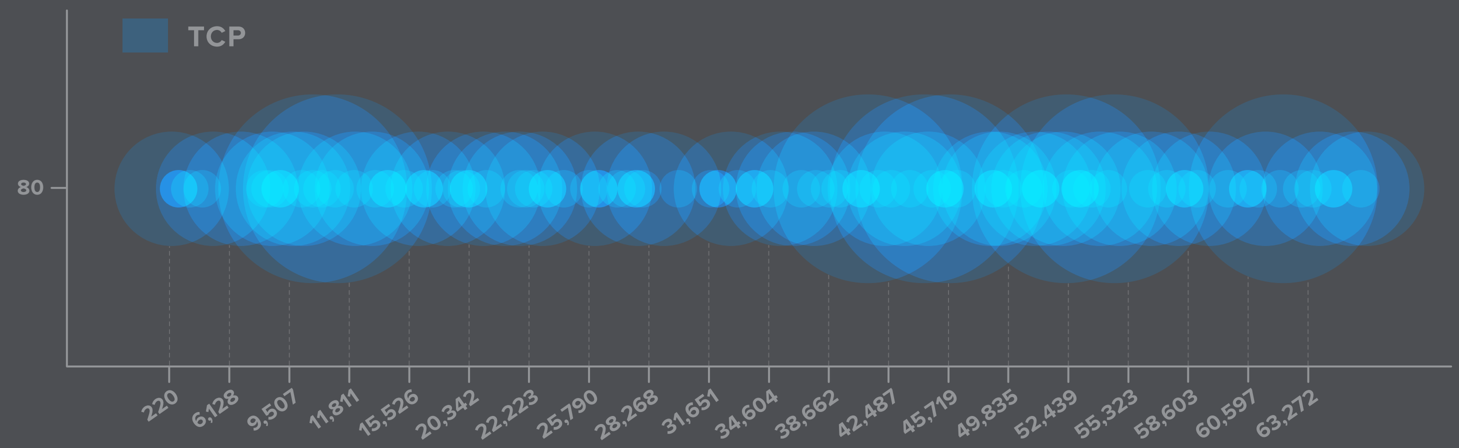


Figure 21: Source ports of the attack

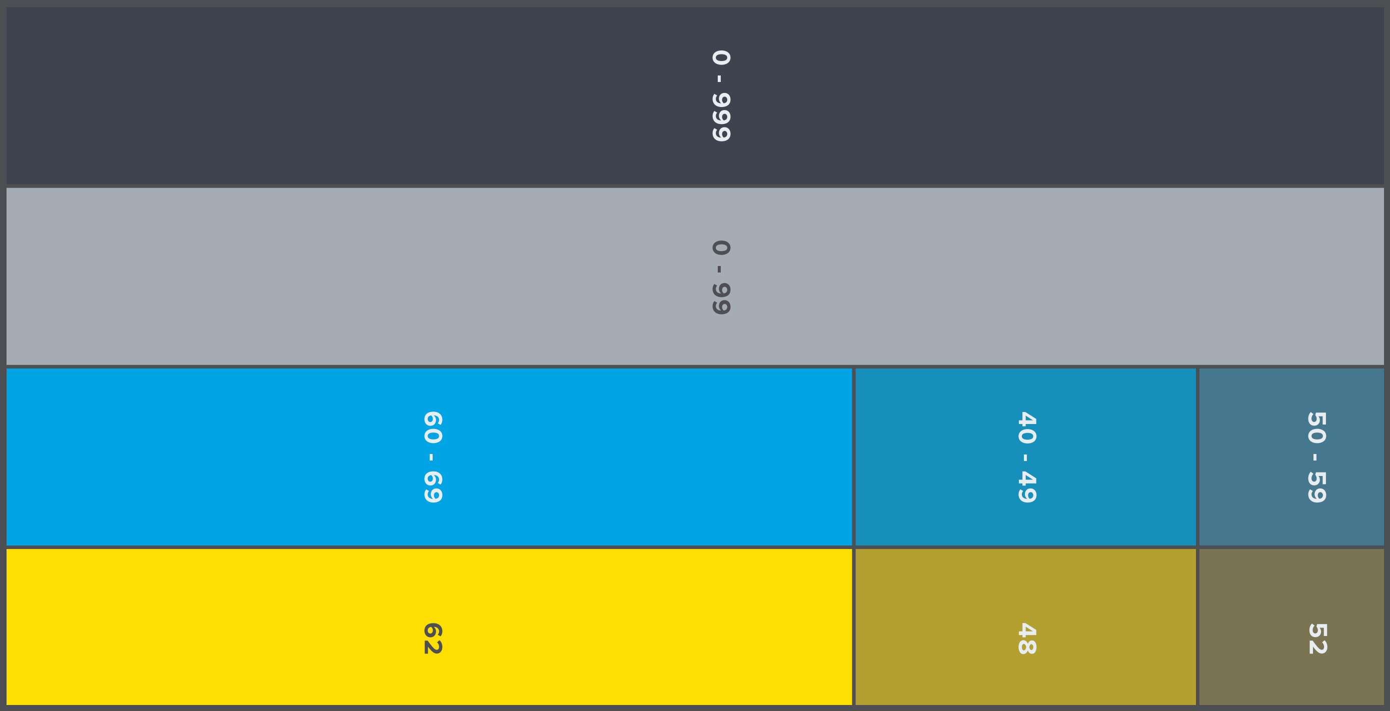


Figure 22: Attack byte distribution breakdown

We witnessed a similar SYN flood attack targeting port 80 on another US government target that was 2.3 Gbps logged, but we cannot provide more details on this attack.

How much can one IoT device do?

Figure 23 indicates that each infected IoT device contributed 0.1% to the total attack. What's interesting, and frankly scary, about IoT devices is the virtually unlimited number that are available for compromise and the damage they can do collectively once they've joined a botnet. When hundreds of thousands of small devices participate in a botnet, none of them individually need to have a large capacity.

SOURCE	PROTOCOL	PERCENT
58979	TCP	0.1%
54644	TCP	0.1%
44727	TCP	0.1%
5255	TCP	0.1%
53	TCP	0.1%

Figure 23: Primary source ports used in IoT DDoS attacks

DEST PORT	PROTOCOL	PERCENT
80	TCP	99.9%
1785	UDP	0%
19603	UDP	0%
33337	UDP	0%

Figure 24: Primary destination ports used in IoT DDoS attacks

ANDROID BOTNET DDOS ATTACK

Another attack witnessed against the US State Agency IP space came from an Android phone botnet. In this attack, each infected device does not contribute more than .01% to the total attack.

SOURCE	PROTOCOL	PERCENT
39989	TCP	0.0%
37880	TCP	0.0%
28111	TCP	0.0%
31115	TCP	0.0%
46034	TCP	0.0%

Figure 25: Primary source ports used in Android botnet DDoS attack

DEST PORT	PROTOCOL	PERCENT
80	TCP	99.9%
1785	UDP	0%
19603	UDP	0%
33337	UDP	0%

Figure 26: Primary destination ports used in Android botnet DDoS attack

There was no contest when it came to the choice of protocols for this Android attack; it was entirely TCP-based.

Figure 27: Andriod botnet was 100% TCP traffic

IOT DDOS ATTACKS INCREASING

The DDoS attacks we are monitoring from IoT botnets have been steadily increasing, with spikes occurring on July 6 and July 12 of 2016.

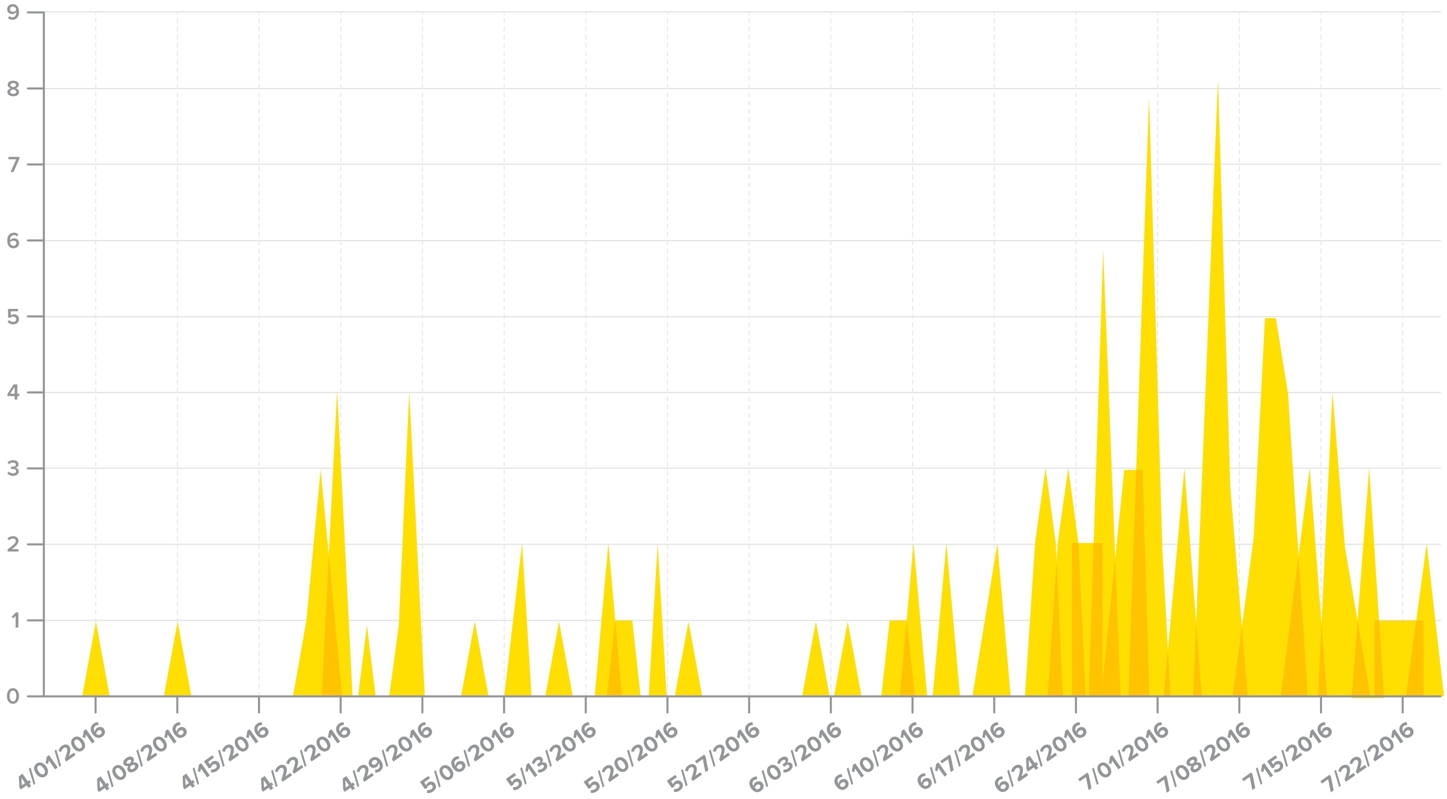


Figure 28: DDoS attacks per day by IoT botnets

IOT BOT C&C SERVERS IN CHINA AND U.S.

We are not authorized to share the C&C details, but we can disclose their country locations and their ASN's industry.

- 70% of the C&Cs are in China
- 30% are in the U.S.
- The C&C server ASNs correlate with the ASNs conducting brute force attacks looking for vulnerable devices

TCP ATTACK ABUSE WARNINGS!

What's most interesting in the attacks we observed is that 70% of the packets did not originate from a spoofed source address because many of the originating networks (the networks the IoT devices resided on), were following BCP-38 (network ingress filtering) and, due to the attack vectors, relied on TCP instead of UDP. As a result, our partner Loryka sent an average of 30,000 Messaging Abuse Reporting Format (MARF) messages daily!

Loryka sends an average of 30,000 Messaging Abuse Reporting Format (MARF) messages daily!

CONCLUSION

The blessing and curse of IoT devices is that they are stateless devices that reboot under stress, so they have limited capacity for launching attacks. But once recycled, they can become re-infected and leveraged all over again. We've seen that a lot of bandwidth per device is not necessary when thousands of devices can be leveraged at once. It is, however, becoming abundantly clear that these devices have seemingly endless attack potential, given their vast quantity and their state of vulnerability. As such, they should be seen as a very serious threat to the global Internet.

It's also clear that threat actors are targeting IoT devices around the world with increasing frequency and evolving their toolsets as new devices are released. We are already seeing the results of their continual efforts to compromise IoT devices and perpetuate the trend that nearly everything connected to the Internet can be exploited.

So, what's next? These devices will continue to be exploited and used as weapons to attack individuals and businesses until they are properly protected by their manufacturers.

The idea that individuals must protect themselves and that every network is responsible for mitigating its own attacks won't scale in an IoT world. The bad guys will win if manufacturers don't implement a plan, quickly, to remediate basic access control vulnerabilities within their IoT devices.

How many more IoT devices online have management ports publically accessible that are vulnerable simply because they are "protected" by vendor default password?

- Delivery driver scanners
- Transportation cards
- Barcode scanners
- Elevators
- Our Raspberry Pi developer kit
- Home security systems that lock your door from your cell phone
- Microprocessor development boards and other DIY project kits
- Automatic thermostats
- LED bulbs that change color based on time of day or via an application on your smartphone
- Digital signage that's used virtually everywhere—from freeways to shopping malls
- Traffic cameras used by cities to monitor traffic and issue traffic tickets or track toll charges

Think of everything around us that's online...how many are already compromised? Are they armed with malware ready for attack? Have they attacked already?

Until manufacturers become good "netizens," we must update our detection mechanisms for IoT DDoS attacks since their behavior patterns are different (lots of smaller, not typically monitored packet sizes). On the flip side, counter measures are just like those for any other DDoS attack, so at least organizations can mitigate the attacks once identified—assuming they have appropriate DDoS mitigation devices in place or a service provider to help.

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: F5Labs.com

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: loryka.com

[1] http://www.gartner.com/newsroom/id/3236718

[2] https://F5Labs.com/articles/vulnerabilities/thanks-to-anonymous-latest-toolset-anyone-can-play-the-ddos-game-22423

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