THREAT ANALYSIS REPORT

THE HUNT FOR IOT

THE GROWTH AND EVOLUTION OF THINGBOTS ENSURES CHAOS

by Sara Boddy and Justin Shattuck

VOLUME 4
March 2018

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

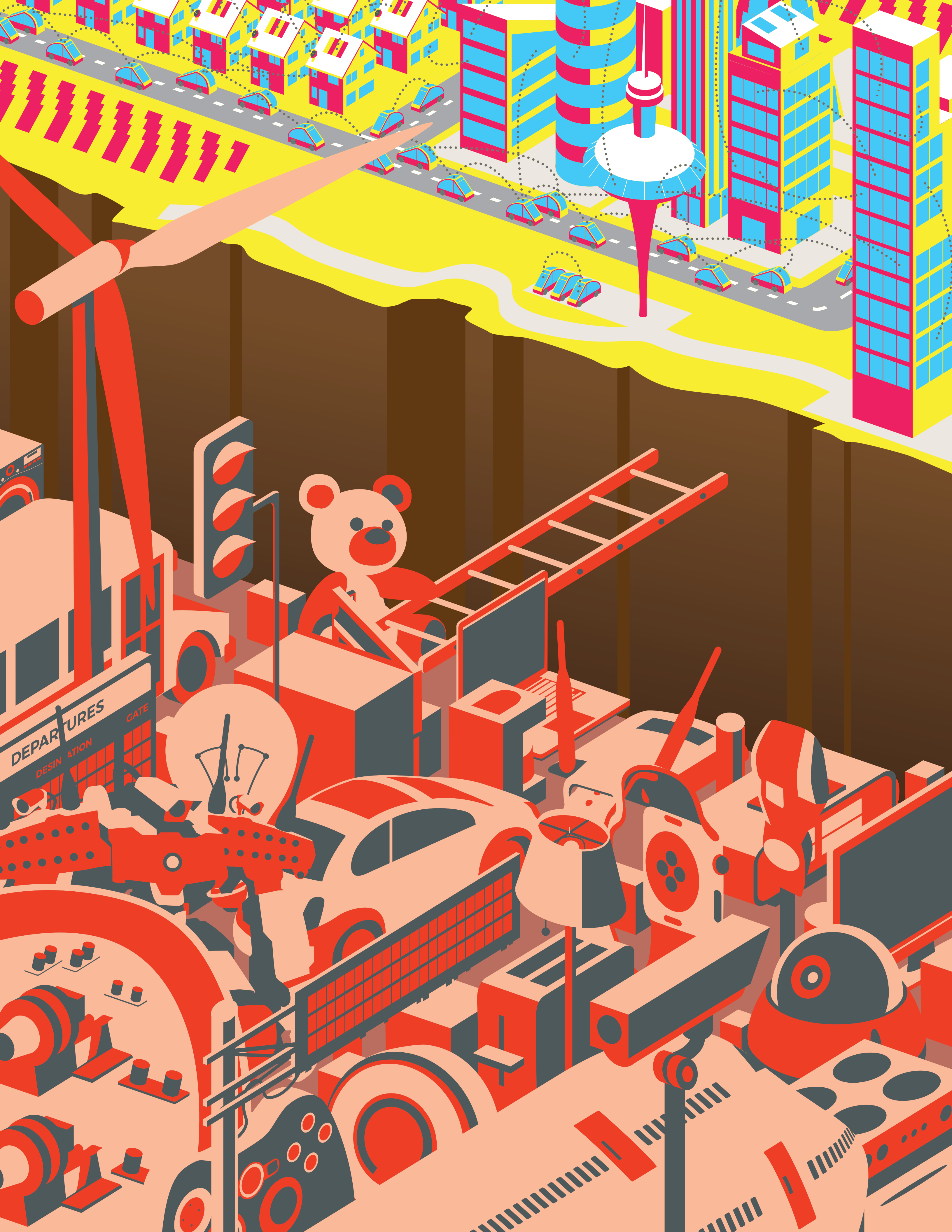
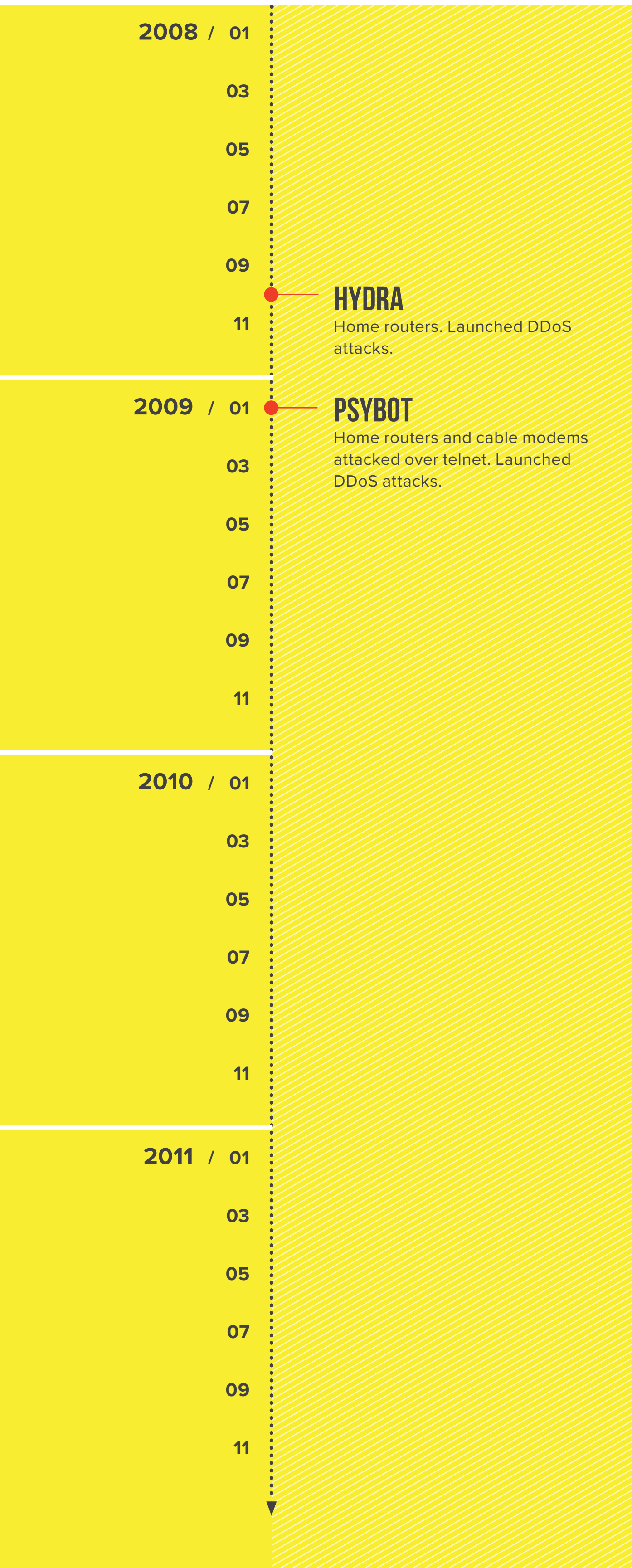

DEPARTURES
GATE

FIGURE 1 **TIMELINE OF THINGBOT DISCOVERY**



EXECUTIVE SUMMARY

F5 Labs, in conjunction with our data partner Loryka, has been tracking "The Hunt for IoT" for two years. We have focused our hunt primarily around port 23 telnet brute force attacks—the "low-hanging fruit" method—as they are the simplest, most common way to compromise an IoT device. (Telnet was also the most prominent attack type when we started this research series.)

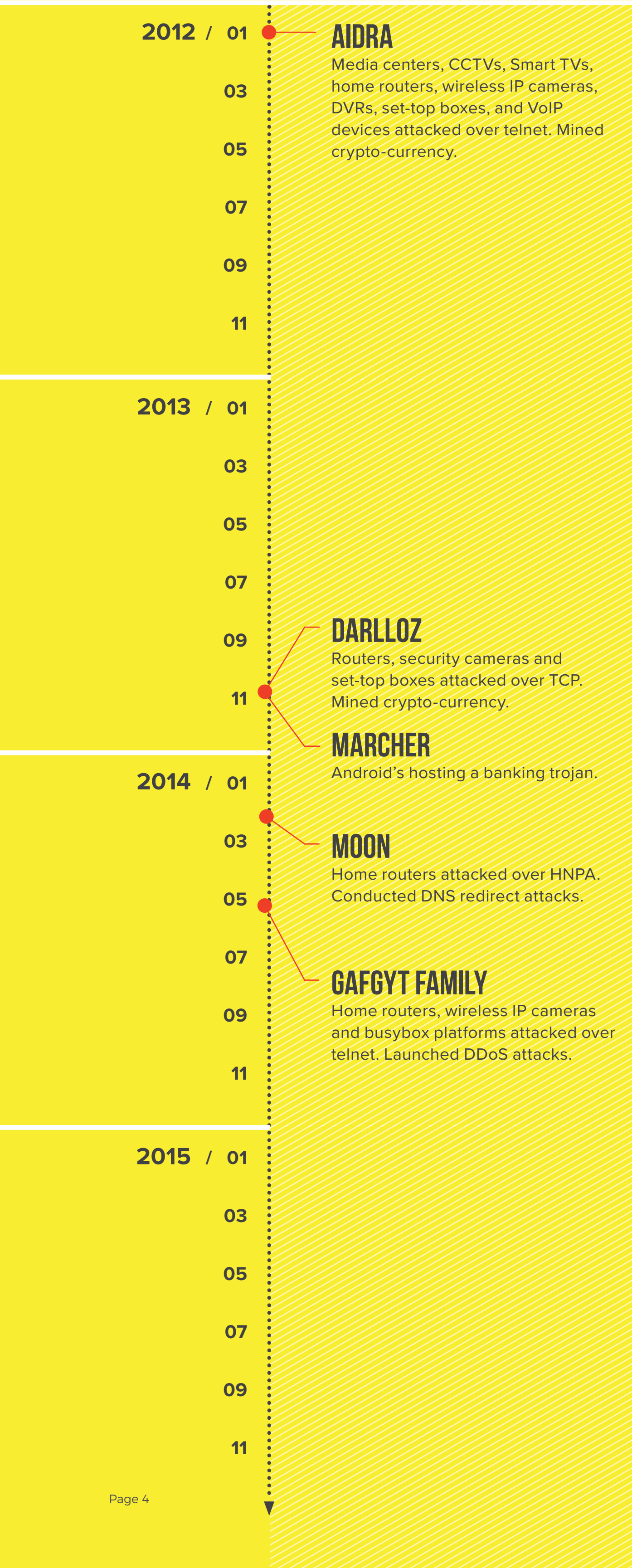
We think the low-hanging IoT fruit are in their last season of picking as we have been seeing attackers use other methods to compromise IoT devices for at least a year now. These other methods are equally easy from a technical standpoint. They just require a few more steps in the attack plan, and also affect fewer devices as they target non-standard ports and protocols, specific manufacturers, device types, or models.

For example, at least 46 million home routers are vulnerable to a remote command injection attack against the custom remote management protocols TR-069 and TR-064. These protocols were created for ISPs to manage their routers deployed at customer homes and were exploited by the Annie thingbot, causing widespread outages for customers of the German ISP Deutsche Telekom and Ireland's Eircom.[i] Annie is one of five (Annie, Persirai, Satori, Masuta, and Pure Masuta) spin-off thingbots created with various parts of Mirai, only two of which (Persirai and Satori) attack telnet to initially exploit devices.

We have already witnessed attackers evolving their methods and markets for making money with compromised IoT devices, just like legitimate businesses and financial markets do, and IoT is a rich, trillion-dollar market based on IDC's estimations for 2020,[ii] ripe with vulnerable devices waiting to be exploited. Every expectation should be set that attackers will continue targeting IoT devices.

FIGURE 1

TIMELINE OF THINGBOT DISCOVERY



Moving forward in the hunt for IoT, it will be a competition among attackers to find IoT vulnerabilities, compromise those devices, and build the strongest thingbot—much like we see today with traditional IT infrastructure.

Regardless of when the easy pickings end, the volume of telnet brute force attacks launched between July 1 and December 31, 2017, maintained levels equivalent to what we saw before and after Mirai. In context, the telnet attacks we have been reporting on have built Remaiten, Mirai, Hajime, and Brickerbot (vigilante thingbots created to take out devices that could have been infected by Mirai), IRCTelnet, Satori, Persirai, Reaper and Hide 'N Seek.[iii] The telnet attacks we publish do not cover the whole IoT attack spectrum, yet they are enough to create nine sizable thingbots capable of massive destruction or surveillance, with room to create more thingbots we don't know about yet.

OUR RESEARCH SHOWS THAT THERE ARE NEW THREAT ACTORS CONTINUALLY JOINING THE IOT HUNT, AND THERE ARE CONSISTENT TOP THREAT ACTORS OVER TIME.

The thingbot discovery timeline shows the evolution of the hunt for IoT through the discovery of thingbots over the past decade, their protocol exploit methods, the devices they target, and the attacks they launch.

Our research shows that there are new threat actor networks and IP addresses continually joining the IoT hunt, and there are consistent top threat actors over time—perhaps using favored networks. Networks that allow attackers to do whatever they want with little to no involvement (bulletproof hosting providers) or have limited ability to detect and respond to abuse (residential IoT devices in telecom networks). What's more interesting is the pattern created by the

FIGURE 1

TIMELINE OF THINGBOT DISCOVERY

2016 / 01 03 05 07 09 11

2017 / 01 03 05 07 09 11

2018 / 01 03 05 07 09 11

REMAITEN
Home routers and WAPs attacked over telnet. Launched DDoS attacks.

CRASH OVERRIDE
ICSs attacked over IEC 101, 104, 61850, OPC. Launched PDoS attacks.

MIRAI
Home routers, wireless IP cameras and DVRs attacked over telnet. Launched DDoS attacks.

HAJIME
Home routers, wireless IP cameras and DVRs attacked over telnet. Launched PDoS attacks.

IRCTELNET
Home routers, wireless IP cameras and DVRs attacked over telnet. Launched DDoS attacks.

ANNIE
Home routers attacked over TR-064 and TR-069. Launched DDoS attacks.

BRICKERBOT
Home routers, busybox platforms and wireless chipsets attacked over telnet and UPnP. Launches PDoS attacks.

SATORI FAMILY
Home routers and wireless chipsets attacked over telnet, UPnP and SOAP. Launches DDoS attacks.

PERSIRAI
Wireless IP cameras attacked over telnet, UPnP and TCP.

REAPER
Home routers and NRV surveillance attacked over telnet, TCP and others. Recon / spy bot.

MATSUTA & PURE MATSUTA
Home routers attacked over telnet and HNAP. Launches DDoS attacks.

HIDE 'N SEEK
Wireless IP cameras attacked over telnet.

JEN X
Home routers and wireless chipsets attacked over UPnP and SOAP. Launches 300 Gbps DDoS attacks for $20.

OMG
Home routers, wireless IP cameras and DVRs attacked over telnet. Creates proxy servers.

count of attacks by IP address and the count of IP addresses used inside networks. The pattern is too clean to be random. It appears calculated and automated. In the same way the networks being used are intentionally picked, the number of systems and IP addresses used within those networks (and the number of attacks they launch) are calculated to avoid detection, and it's all automated with the same code. We haven't pinpointed the threat actors, but we see their strategy in action.

Below is a summary of our key findings based on data collected from July through December 2017:

- Telnet brute force attacks against IoT devices rose 249% year over year (2016–2017).
- 44% of the attack traffic originated from China, and from IP addresses in Chinese networks that were top threat actor networks in prior reports. Behind China in total attack volume was the U.S., followed by Russia.
- We have consistently seen the same attacking IP addresses and networks over the span of our two-year research, proving that this abusive traffic is either not being detected, or it's being allowed. Because of this, we have published the top 50 attacking IP addresses.
- The destinations of attack traffic span the globe, presumably without bias. Wherever vulnerable IoT infrastructure is deployed, attackers are finding it. The most attacked countries were the U.S., Singapore, Spain, and Hungary.
- Attackers have already begun to use other methods of finding and compromising IoT devices, which we will profile in future reports.
- Despite broad awareness of Mirai, it's growing in size. From June to December 2017, it grew significantly in Latin America and moderately in Europe and Asia.
- Persirai has slightly declined in size over the last six months, most notably in India and Central Asia.

INTRODUCTION

The security community commonly refers to IoT as the "Internet of Threats," and for good reason. According to Gartner, there are now 8.4 billion IoT devices implemented, and that number is expected to grow to 20.4 billion by 2020.[iv]

Gartner is the most conservative analyst firm when it comes to the IoT market growth. IHS estimates 30 billion by 2020,[v] and the semiconductor maker SoftBank estimates a trillion by 2035. In perspective, we haven't begun to hit mass consumer adoption of IoT devices yet. If we don't change our development standards now, we'll be bringing insecure IoT devices into our future two to three times faster than we have previously, yet those devices will be compromised at the same rate. That's a formula that ensures a future of chaos between the physical and virtual world.

Because of the threat that insecure IoT devices pose to our modern world, the ethics of hacking back with good intentions has become a hot topic again. As security researchers, we are usually 7 to 16 months behind the attackers. So much of what we know in the security world is based on post-discovery, often post-attack, when we have something to analyze. Researchers can't break into the attacker's infrastructure to watch what they are doing—that would be illegal. But attackers don't abide by laws, so it's never a level playing field. "Janit0r," the author of the vigilante thingbot Brickerbot, discussed this very conundrum in his retirement letter that both acknowledged our research and faulted us for not putting two and two together (crediting his vigilante efforts to the spike in attack traffic), even though we referenced "vigilante efforts" contributing to the attack volume in *The Hunt for IoT: Rise of Thingbots.*

MANY ORGANIZATIONS HAVE LIKELY BEEN ATTACKED BY A THINGBOT AND DIDN'T KNOW IT.

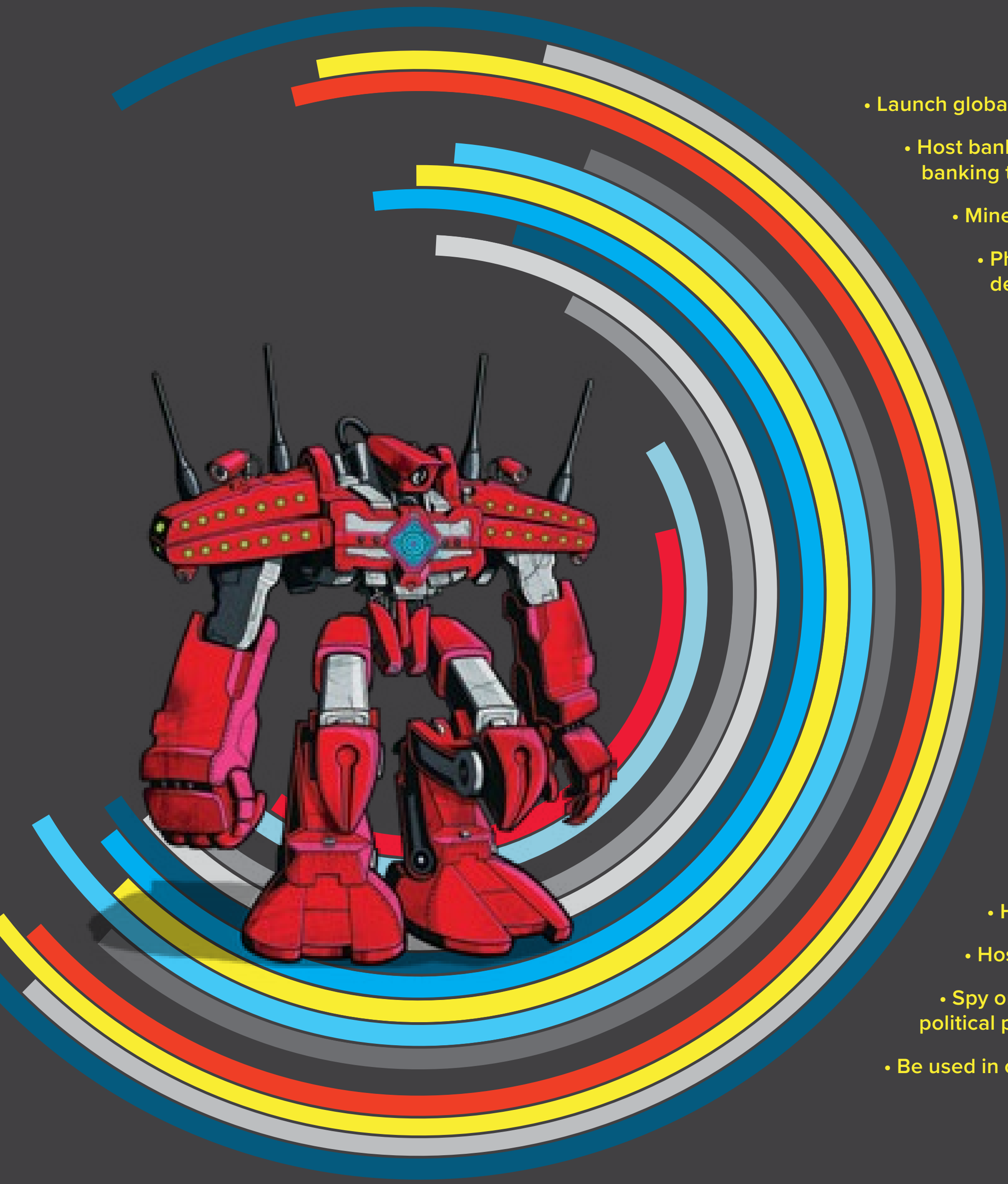
There were no major attack headlines from thingbots in 2017, but that doesn't mean thingbots weren't being built, or that they weren't attacking. Companies get attacked around the clock, but attributing those attacks to a threat actor is difficult. How many companies got hit with a DDoS attack by a 60,000-device botnet and just mitigated the attack without capturing packets or researching the data? Likely thousands. How many companies have gotten hit with a thingbot DDoS attack that they couldn't classify? How do you mitigate an attack that consists of thousands of events coming from tiny IoT devices that issue small samples of data at high rates of speed? Packets generated from a cell phone, for example, are different than packets sent from a server (from a standard DDoS standpoint). Those are difficult attacks to identify and mitigate, simply because our current defenses were not designed around this type of traffic. Many organizations have likely been attacked by a thingbot and didn't know it.

The attribution effort becomes a lot harder with various cyber attack types used to compromise organizations, especially when the compromised organization doesn't have security controls in place to identify attacks, collect the proper logs, or conduct forensics and determine root cause, much less attribute the attack to a threat actor or bot. It's very likely that thingbots have launched attacks we will never know about, and their creators are reaping the rewards. Cryptocurrency mining is a good example of an IoT attack that would likely go undetected if the mining didn't cause a noticeable (slow device performance) impact to the consumer. And these kinds of attacks have been occurring since at least 2012 with the discovery of Aidra.[vi]

With IoT devices as hot as 3-D printers in the hacker community right now, we should be uncomfortable knowing that thingbots have been hiding in the shadows for at least a decade. Attackers are building highly capable cyberweapons under the radar and launching attacks from them, which are also under the radar. These thingbots can be used to:

FIGURE 2

THINGBOT ATTACKS



- Launch globally impacting DDoS attacks
- Host banking Trojans (that are now evolving beyond banking targets)
- Mine cryptocurrency
- Physically destroy devices with permanent denial-of-service (PDoS) attacks
- Collect data from man-in-the-middle (MiTM) traffic
- Serve as massive reconnaissance systems to spy on populations
- Leverage stolen credentials to stuff into applications
- Deploy proxy servers on infected IoT devices to be used to hide malicious activity
- Redirect DNS and force traffic to malicious sites
- Deploy ransomware
- Build new darknets or deep webs
- Launch new Tor networks
- Distribute spam
- Host web content for phishing
- Host click-fraud farms
- Host ad-fraud farms
- Spy on people and spread fake news for political purposes
- Be used in cyberwarfare

Cyberattacks are not just about data loss, identity theft, and costly system downtime anymore. They are increasingly more frequent in the physical world, and this threat is accelerating through IoT. As we've highlighted in prior reports, we rely on healthy IoT devices to manage our day-to-day lives as the devices assist in the flow of traffic, emergency warning systems, emergency services operations, airport functions, and critical infrastructure communication and operations. If we don't start tackling this problem soon, we will be measuring the impact of cyberattacks in human lives, not just dollars.

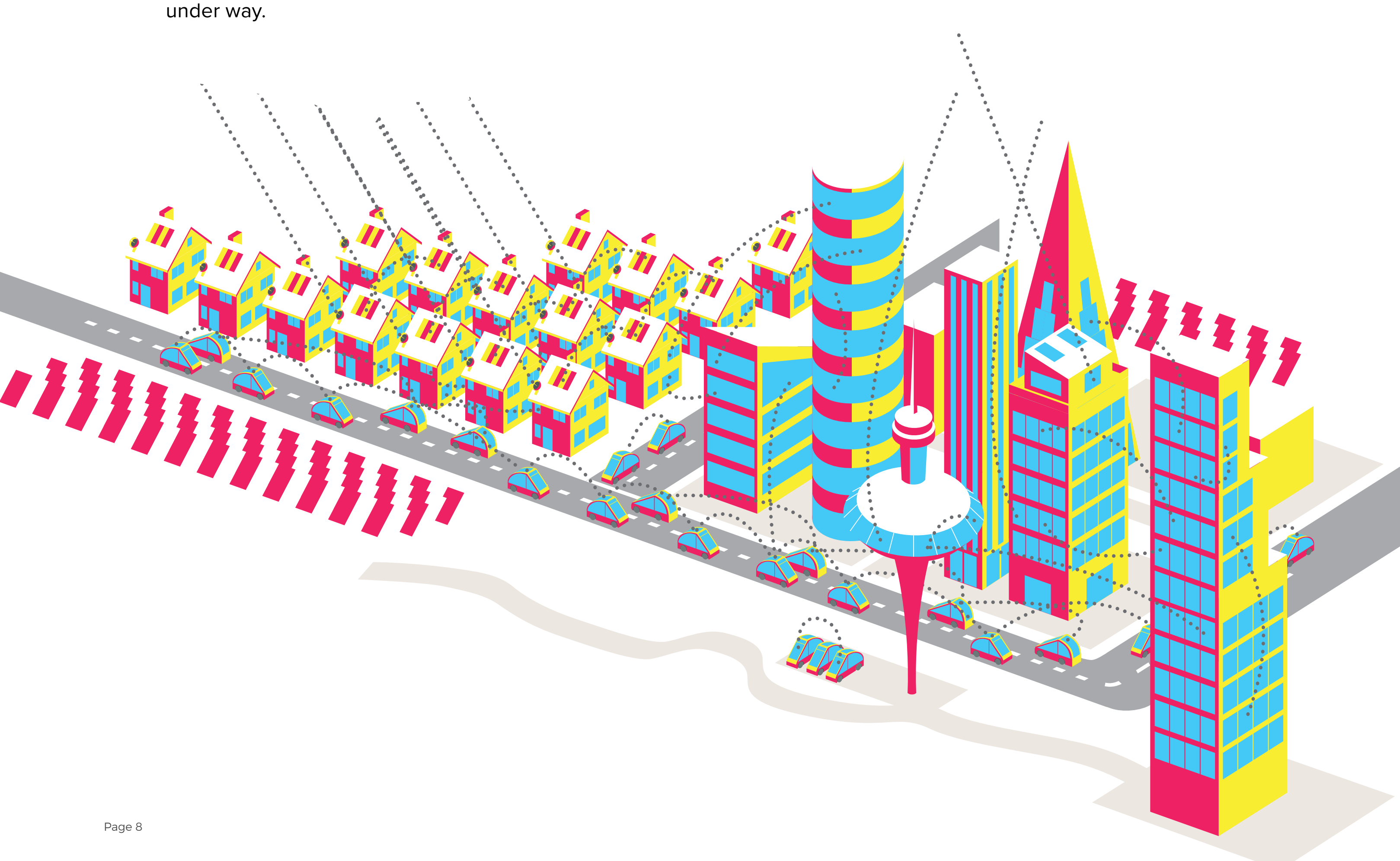
IoT legislation in the U.S. has been proposed, but even if it's implemented, it will only have an impact on IoT devices purchased and deployed by the U.S. government on a go-forward basis. It will not address the currently deployed threat, nor the global issue of IoT devices being deployed everywhere, and their attacks having no borders. This is worth repeating and re-emphasizing to stress the importance of immediate action. We will keep highlighting the impact that insecure IoT devices can have on life in each IoT hunt report until tangible action is under way.

Raymond Pompon
Principal Threat Research Evangelist at F5 Networks

There are worse things than privacy leakage. I went shopping for a new oven and turns out that some models of ovens have built-in WiFi. Yeah, that's what I want–a remotely controllable device in my house that produces fire. What could possible go wrong?

Gary Adams
Principal/Consultant at Adams-IT Consulting

I have a friend whose "smart oven" set fire to the house. Took almost two years for the insurance settlement and to get the house repaired. Insurance company sued the manufacturer who didn't want to take responsibility. Buy simple or remove the connectivity.



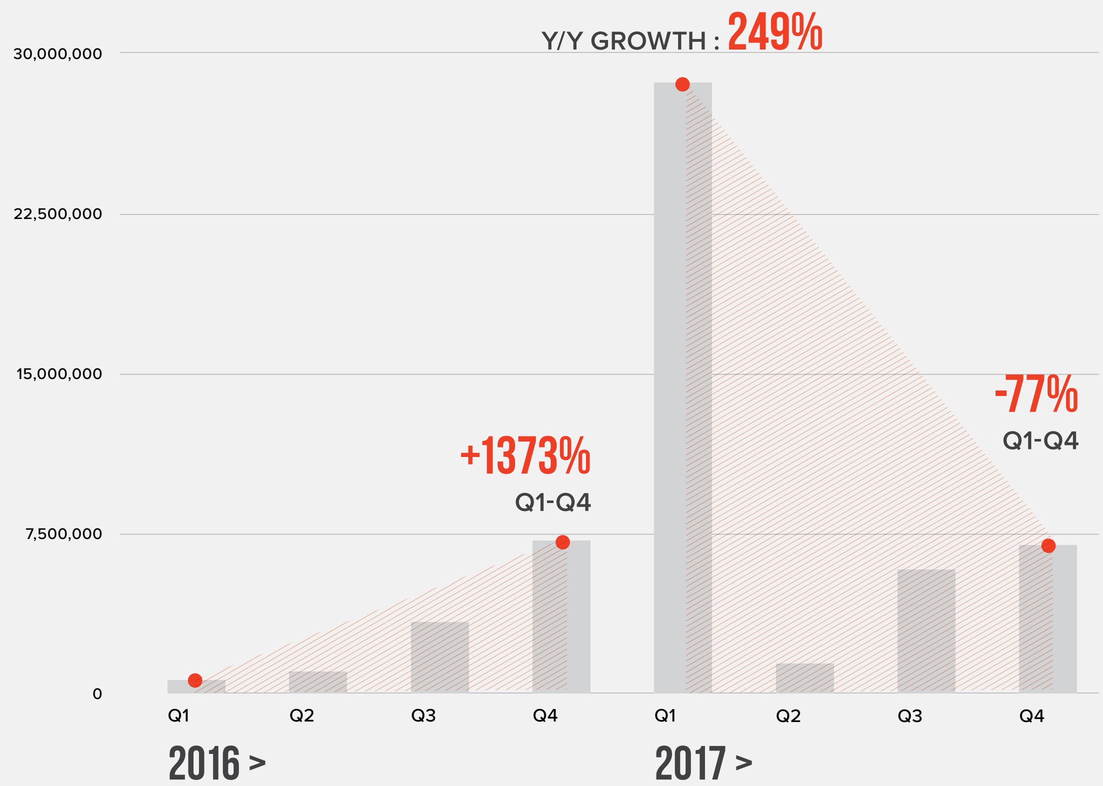
TELNET BRUTE FORCE ATTACK VOLUME

This report focuses on the telnet brute force attack data collected from July 1 through December 31, 2017. Because no one really knows how much attack traffic it takes to build thingbots capable of mass destruction, we look for trends by comparing current attack volume to prior periods that pre-date the discovery of sizable thingbots.

FIGURE 3

TELNET ATTACK VOLUME BY QUARTER

2016-17



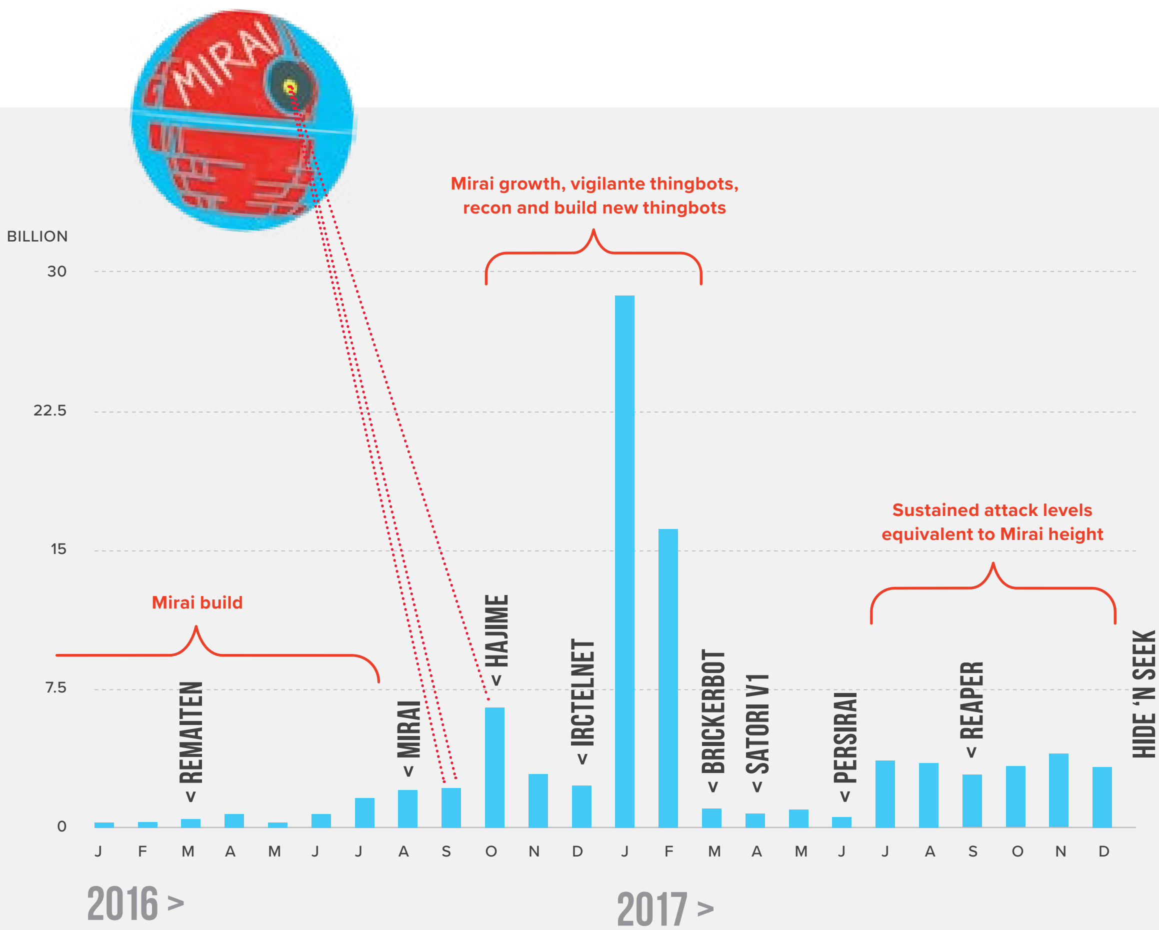
ALL SIGNS POINT TOWARD IOT DEVICES BECOMING THE ATTACK INFRASTRUCTURE OF THE FUTURE.

The last half of 2017 saw a decrease in attack volume from the first half of the year (77% decline Q1–Q4), but the attack levels were still greater than the volume during Mirai development, Mirai attacks, and the resulting fervor. Based on the level of traffic we saw from July through December 2017, it's possible that numerous, very sizable, thingbots are being created.

We know that Mirai never attacked with its full potential. Many thingbots capable of global, “lights-out” attacks have been built during the past two years. Figure 4 is a timeline of the telnet attacks collected by month in relation to the telnet-attacking thingbots we have discovered over the same time period.

FIGURE 4

TELNET ATTACK VOLUME BY MONTH AND DATE OF TELNET THINGBOT DISCOVERY



The summary of attack volume by source IP address (Table 1) the number of attacks launched by the unique network identifier “ASN” (Autonomous System Number), and the average number of IP addresses used per ASN is too tight a pattern to be random. This summary of the attack data has all the signs of automation, where sophisticated attackers are selecting networks from which to start their attacks and automating the rest with the same attack plan. They’re breaking attacks out between multiple systems, IP addresses, and networks at volumes that will go undetected.

TABLE 1

SUMMARY OF ATTACKS

Month	Average Attacks per Source IP Address	Average Attacks per ASN	Average Count of IP Addresses Used per ASN
July 2017	16	374	23
August 2017	15	377	25
September 2017	14	281	20
October 2017	15	319	21
November 2017	11	375	33
December 2017	10	373	38

TOP ATTACK SOURCE AND DESTINATION COUNTRIES

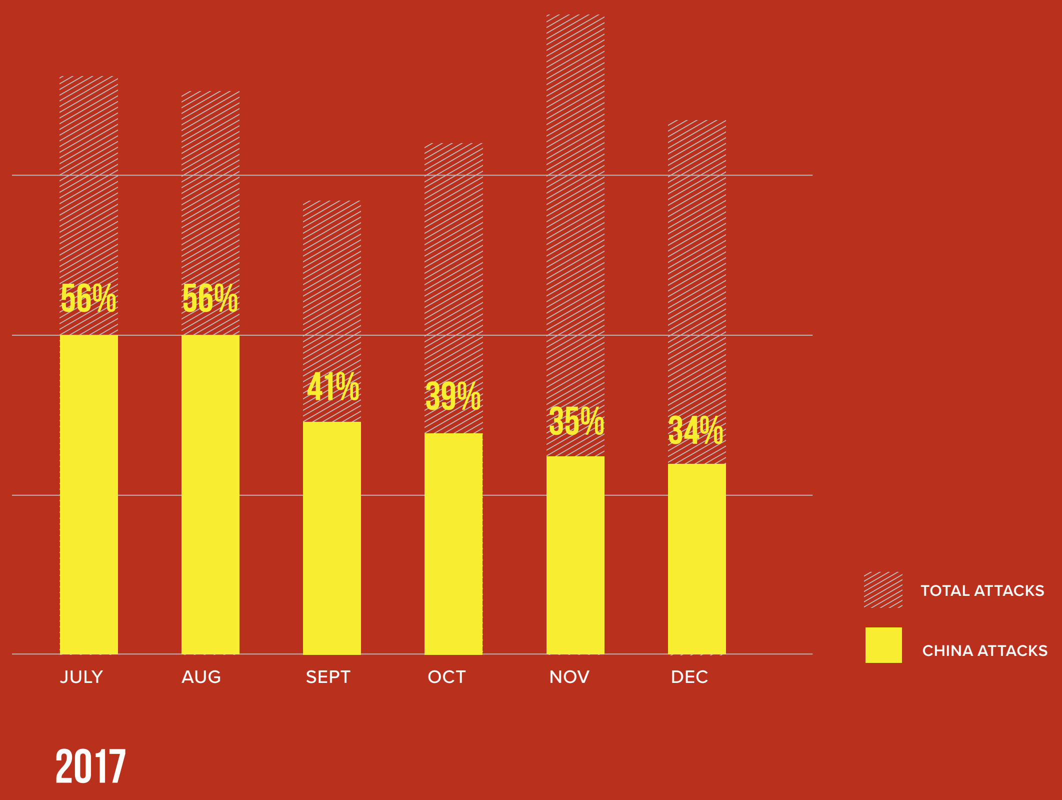
China is the most prominent attacking country. When looking at the destinations of these attacks, they are broadly dispersed globally and don't clearly favor one country over another.

TOP SOURCE TRAFFIC COUNTRIES

China was the number one attacker by a wide margin; 44% of the total telnet brute force attacks against IoT devices from July through December were launched from China.

FIGURE 5

ATTACKS FROM CHINA IN COMPARISON TO TOTAL



When looking at the other countries in the top 10 attacker list, no other country surpassed 10% of total traffic volume, with the exception of Russia, which was responsible for 12% of November's traffic. The top 10 attacking countries accounted for 78% of the total traffic.

That means 22% of the attack traffic came in small chunks (position 10 hovers between 1% and 2%) from dozens of different countries, indicating a global problem with compromised IoT devices that, once infected, are being directed to launch attacks.

TABLE 2

TOP 10 ATTACK SOURCE COUNTRIES

JULY		AUGUST		SEPTEMBER		OCTOBER		NOVEMBER		DECEMBER	
China	**56%**	**China**	**56%**	**China**	**41%**	**China**	**39%**	**China**	**35%**	**China**	**34%**
U.S.	6%	U.S.	5%	U.S.	7%	U.S.	8%	Russia	12%	Russia	7%
France	3%	Argentina	3%	France	7%	Ukraine	7%	U.S.	6%	U.S.	6%
Argentina	3%	France	3%	Brazil	5%	Russia	6%	Ukraine	5%	Japan	5%
Czech Republic	3%	Russia	3%	Russia	5%	France	4%	Japan	4%	France	4%
India	3%	Brazil	2%	India	4%	Brazil	4%	France	4%	Brazil	4%
Brazil	3%	India	2%	Vietnam	3%	India	3%	Brazil	3%	Ukraine	4%
Russia	2%	Czech Republic	2%	Germany	2%	Vietnam	2%	India	3%	South Korea	3%
Vietnam	2%	Vietnam	2%	Netherlands	2%	Italy	2%	Argentina	2%	Colombia	2%
South Korea	2%	Ukraine	1%	South Korea	2%	South Korea	2%	Vietnam	2%	Poland	2%
TOTAL	**81%**		**80%**		**76%**		**79%**		**77%**		**72%**

TOP 10 ATTACK DESTINATION COUNTRIES

There is no standout destination for IoT attacks. Each country on the top 10 list took a small portion of the total, with the exception of Spain, which took 22% of December's attacks. At most, the top 10 countries received 44% of the total number of attacks; 24% at least. That means vulnerable IoT devices are widely dispersed around the globe. Countries that are missing on the total attack destination list are likely those without significant infrastructure and deployed IoT devices, as there is no such thing as a country with a secure IoT infrastructure.

TABLE 3

TOP 10 ATTACK DESTINATION COUNTRIES

JULY		AUGUST		SEPTEMBER		OCTOBER		NOVEMBER		DECEMBER	
U.S.	5%	Hungary	4%	Spain	9%	Spain	9%	Spain	16%	Spain	22%
Singapore	4%	Singapore	3%	Hungary	8%	Hungary	4%	Hungary	5%	Hungary	5%
Hungary	3%	Spain	3%	France	4%	Singapore	3%	France	4%	U.S.	4%
Italy	3%	France	3%	U.S.	3%	France	3%	Italy	3%	France	3%
Spain	2%	U.S.	2%	Singapore	3%	Canada	3%	Singapore	3%	Singapore	3%
UK	2%	UK	2%	Canada	2%	U.S.	2%	U.S.	3%	Canada	3%
Norway	2%	Norway	2%	Italy	2%	Italy	2%	Finland	2%	Norway	1%
Bulgaria	2%	Bulgaria	2%	Norway	2%	Norway	2%	Canada	2%	Italy	1%
Canada	1%	Italy	2%	Bulgaria	1%	UK	1%	Norway	2%	Russia	1%
Denmark	1%	Canada	1%	UK	1%	Russia	1%	UK	1%	UK	1%
TOTAL	25%		24%		35%		31%		40%		44%

It is interesting to see Spain as a top attack destination after being the top source (attacking) country from January through June 2017. We would expect to see destination traffic become source traffic as attackers use compromised devices to attack and grow their thingbots, but the opposite was true with Spain.

Singapore is continuously in the top 5 destination countries, which is significant when you consider the size of the country in relation to the U.S., Canada, and European countries. This indicates they have a sizable—and vulnerable—IoT deployment.

Since China is the primary attacker, we checked to see if there was a pattern of who they were attacking, and the answer was no, which reinforces the trend of widely dispersed attacks without a clear bias. Their top target was Spain, which received 1% more of China's attacks than the U.S. did, followed by Singapore, Italy, and Hungary. The top 5 destinations collectively only received 27% of China's attacks; the other 73% were globally dispersed to countries that didn't account for more than 1% of the total attack volume.

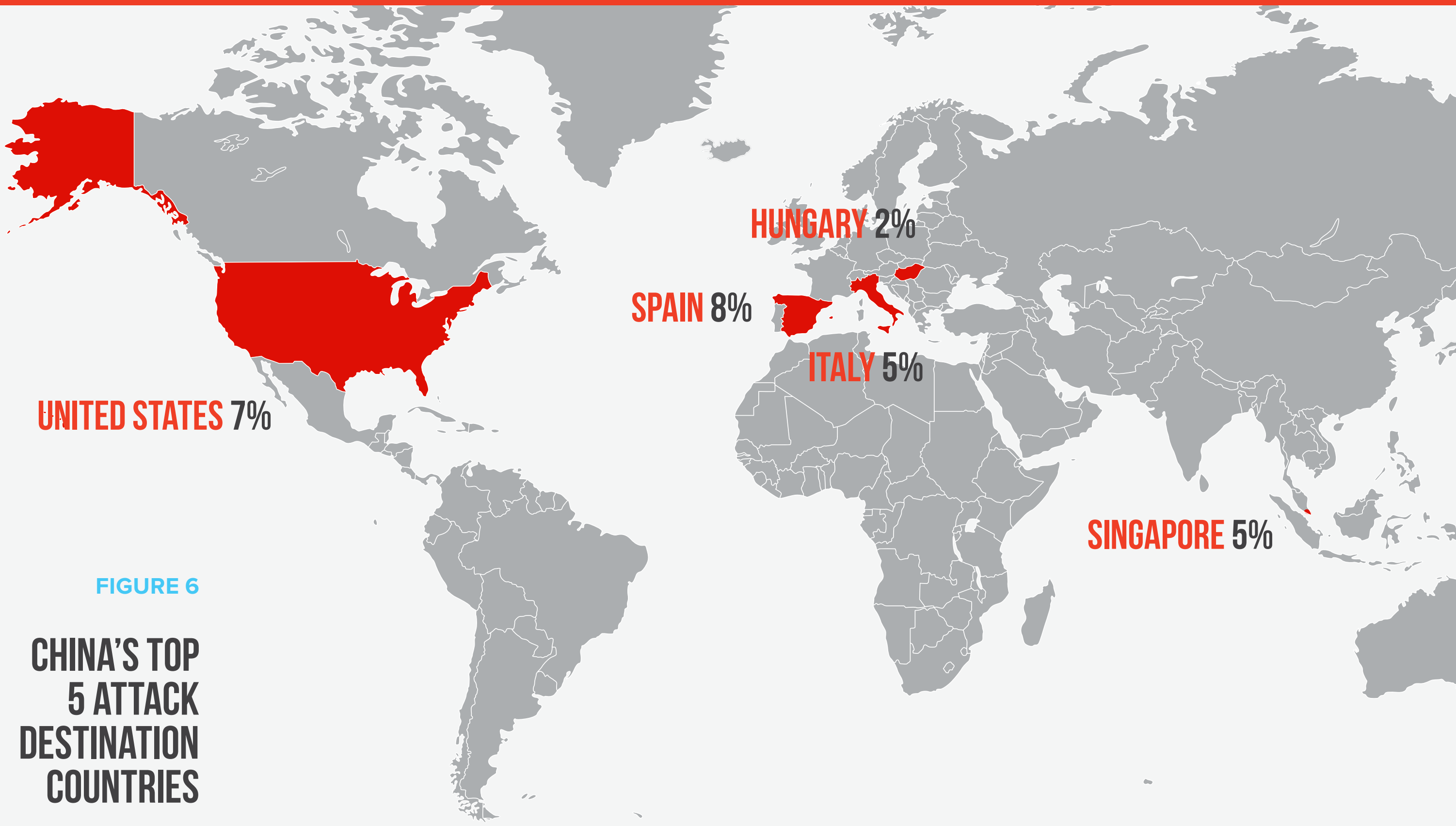


FIGURE 6

CHINA'S TOP 5 ATTACK DESTINATION COUNTRIES

TOP 50 ATTACKING NETWORKS

The list of top 50 attacking networks gives us a slightly different view of the primary threat actors by focusing on the networks from which attacks are launched. Few threat actors would launch a large number of attacks from one IP address because they could easily be caught. Instead, crafty threat actors spread out their attacks across a lot of IP addresses and systems, potentially in the same ASN. This is why we look at top IP addresses and top ASNs. When looking at the top ASNs, we see much more diversity in the number of countries and businesses (ASNs) than in the top IP addresses list.

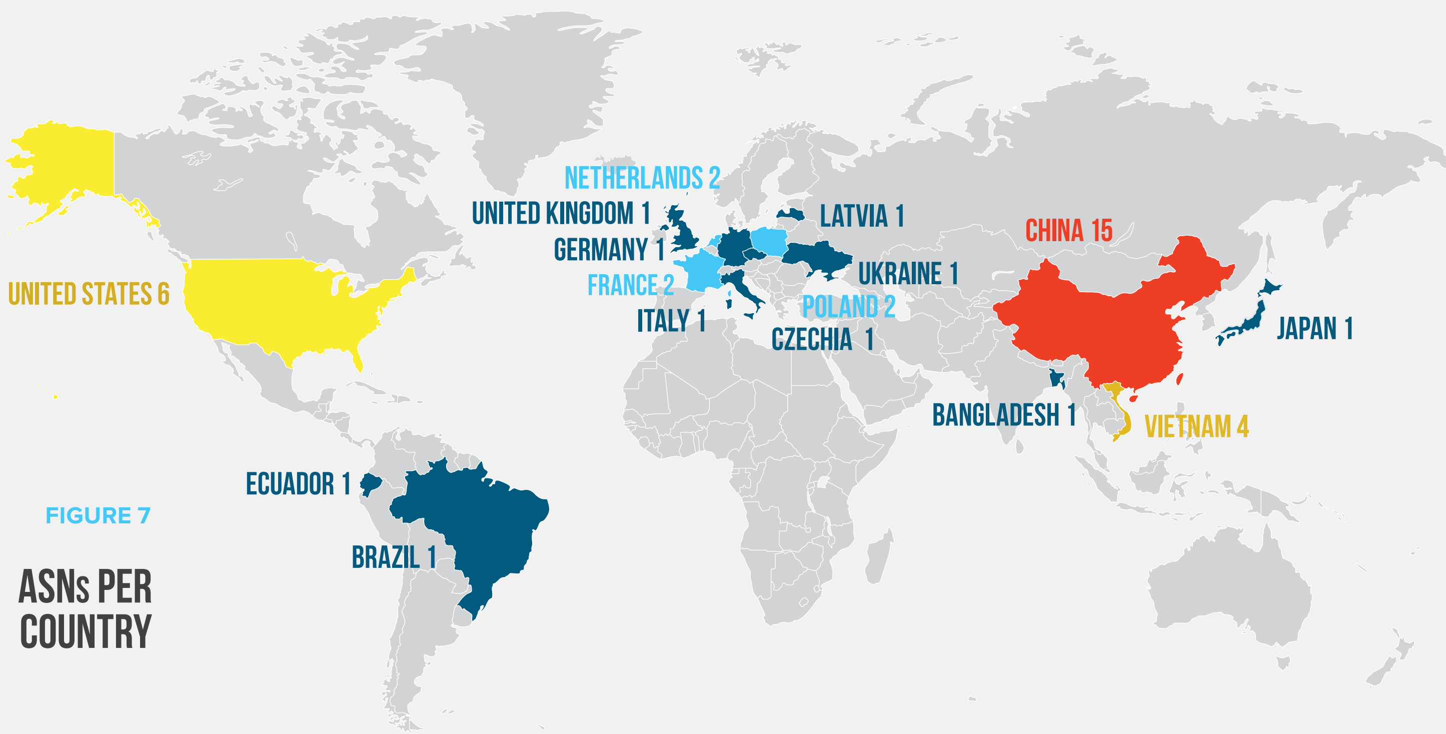


FIGURE 7

ASNs PER COUNTRY

Fifteen of the top attacking networks are from China, 60% of which are new networks, which means that we didn't see them on the top attacking ASN list in prior reporting periods.

FIGURE 8

COUNTRY CONTRIBUTION OF ATTACK VOLUME BY TOP 50 ATTACKING NETWORKS

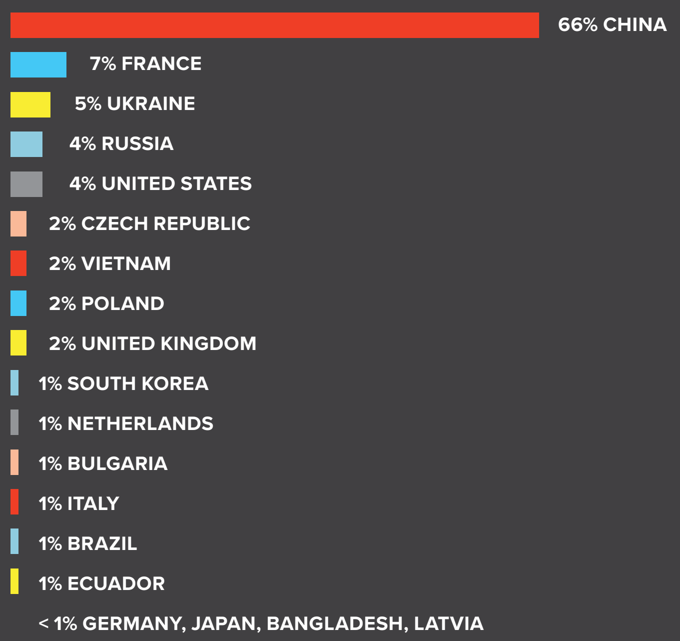
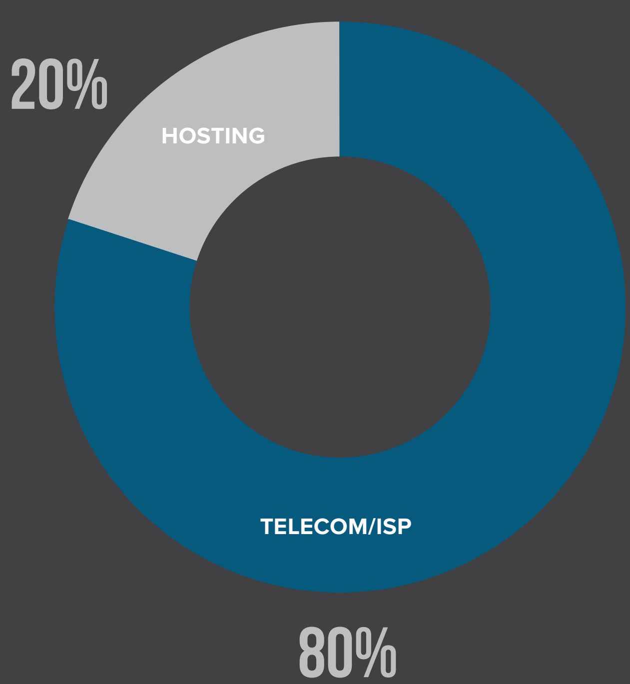


FIGURE 9

TOP 50 ATTACKING ASNs BY INDUSTRY



When looking at the attack volume generated from the top 50 networks, Chinese networks are responsible for the majority of the attacks at 66%. France comes in at number two with 7% of the attacks launched from the top 50 networks. Ukraine and Russia are not far behind at 5% and 4% respectively.

TOP ASNs BY INDUSTRY

Eighty percent of the attacks launched from the top 50 ASNs were from telecom companies and service providers (ISPs). We assume these are infected IoT devices controlled by a thingbot, launching scans for more vulnerable devices and infecting them with malware that grows the thingbot. The other 20% of attacks from the top 50 networks came from hosting companies.

In volume 3 of *The Hunt for IoT: Rise of Thingbots*, we talked about how we view the hosting provider's role in the effort to compromise and control IoT devices. We still attribute direct threat actor activity to hosting provider traffic because they use either their own rented server space, or servers they compromised in that space, to launch their recon scans, beginning the thingbot development process. Once the attacker infects the IoT device, they use it to scan and distribute the malware to other IoT devices, until eventually the compromised IoT devices are taking over the attack volume coming out of telecoms or ISPs, as shown in Figure 7. Many thingbots use this IoT distribution model, including Mirai, Hajime, Persirai, Reaper, Satori, Masuta, and PureMasuta.

TABLE 4

TOP 50 ATTACKING ASNs

Table 4 lists the top 50 ASNs from which telnet brute force attacks are launched, as well as their industry and their country.

We also indicate whether these ASNs are new to the list, or are networks we have been tracking in prior IoT reports.

No.	Network	Industry	Country	ASN	New?
1	ChinaNet	Telco/ISP	China	AS4134	IoT v1, 2, 3
2	ChinaNet Guangdong Province Network	Telco/ISP	China	AS134764	IoT v3
3	China Unicom China169 Backbone	Telco/ISP	China	AS4837	IoT v1, 2, 3
4	OVH SAS	Hosting	France	AS16276	IoT v2
5	PE Tetyana Mysyk	Hosting	Ukraine	AS25092	New
6	Petersburg Internet Network ltd.	Telco/ISP	Russia	AS58222	New
7	Global Layer B.V.	Hosting	Czech Republic	AS57172	New
8	Online S.A.S.	Hosting	France	AS12876	New
9	Planet Telecom Ltd.	Telco/ISP	UK	AS43715	New
10	Microsoft Corporation (Azure)	Hosting	U.S.	AS8075	New
11	Sprint S.A.	Telco/ISP	Poland	AS197226	New
12	ChinaNet Jiangxi Province IDC Network	Telco/ISP	China	AS134238	IoT v1
13	China Unicom Beijing Province Network	Telco/ISP	China	AS4808	IoT v1, 2
14	Aruba S.p.A.	Hosting	Italy	AS31034	New
15	Digital Ocean, Inc.	Hosting	U.S.	AS14061	IoT v2
16	TELEFÔNICA BRASIL S.A.	Telco/ISP	Brazil	AS18881	IoT v1
17	Comcast	Telco/ISP	U.S.	AS7922	IoT v1
18	Guangdong Mobile Communication Co., Ltd.	Telco/ISP	China	AS980	New
19	Hangzhou Alibaba Advertising Co., Ltd.	Hosting	China	AS37963	New
20	China Telecom (Group)	Telco/ISP	China	AS4812	New
21	Beijing Baidu Netcom Science and Technology	Telco/ISP	China	AS38365	New
22	DATALABS Ltd	Hosting	Russia	AS58222	New
23	VNPT Corp	Telco/ISP	Vietnam	AS45899	New
24	Blizoo Media and Broadband	Telco/ISP	Bulgaria	AS13124	New
25	Corporacion Nacional de Telecomunicaciones	Telco/ISP	Ecuador	AS28006	New
26	Korea Telecom	Telco/ISP	South Korea	AS4766	IoT v1, 3
27	WorldStream B.V.	Telco/ISP	Netherlands	AS49981	New
28	Contabo GmbH	Hosting	Germany	AS51167	New
29	NTT Communications Corporation	Telco/ISP	Japan	AS4713	New
30	LG DACOM Corporation	Telco/ISP	South Korea	AS3789	New
31	IDC, China Telecommunications Corporation	Telco/ISP	China	AS23724	New
32	Viettel Corporation	Telco/ISP	Vietnam	AS7552	IoT v1
33	The Corp for Financing & Promoting Technology	Telco/ISP	Vietnam	AS18403	IoT v1
34	Hostkey B.v.	Hosting	Netherlands	AS57043	New
35	ChinaNet Jiangsu Province Network	Telco/ISP	China	AS23650	IoT v1, 2
36	PJSC Rostelecom	Telco/ISP	Russia	AS12389	IoT v1
37	China Education and Research Network Center	Telco/ISP	China	AS4538	New
38	DRAGONLAB	Manufacturing	China	AS24575	New
39	Online Data Services	Hosting	Vietnam	AS45538	IoT v1
40	Rackspace Hosting	Hosting	U.S.	AS19994	New
41	United Protection (UK) Security LIMITED	Hosting	Bulgaria	AS205280	New
42	ColoCrossing	Hosting	U.S.	AS36352	New
43	TralNet Pawel Cichocki	Telco/ISP	Poland	AS200642	New
44	Neterra Ltd.	Telco/ISP	Bulgaria	AS34224	New
45	China Mobile Communications Corporation	Telco/ISP	China	AS56048	New
46	WholeSale Internet, Inc.	Telco/ISP	U.S.	AS32097	New
47	Bangladesh Research and Education Network	Telco/ISP	Bangladesh	AS63961	New
48	SK Broadband Co Ltd	Telco/ISP	South Korea	AS9318	New
49	Beijing Kingsoft Cloud Internet Technology	Hosting	China	AS38365	New
50	DataClub S.A.	Hosting	Latvia	AS52048	New

TOP ATTACKING IP ADDRESSES

We have been looking at the top 50 attacking IP addresses to get a narrower lens on the top threat actors since volume 2 of this report, *The Hunt for IoT: The Networks Building Death Star-Sized Botnets from IoT Minions.* The top 50 attacking IP addresses from July 1 through December 31, 2017, generated 26% of the period's total attack volume, compared to 84% in *The Hunt for IoT* volume 3 of this report (January 1 through June 30, 2017), and 30.5% in *The Hunt for IoT* volume 2 (July 1 through December 31, 2016).

The majority of IP addresses on the top 50 attacking list are in China; the 36 IP addresses in China were responsible for 80% of the attacks coming from the top 50 IP addresses, and all reside within state-owned telecom or ISP networks.

FIGURE 10

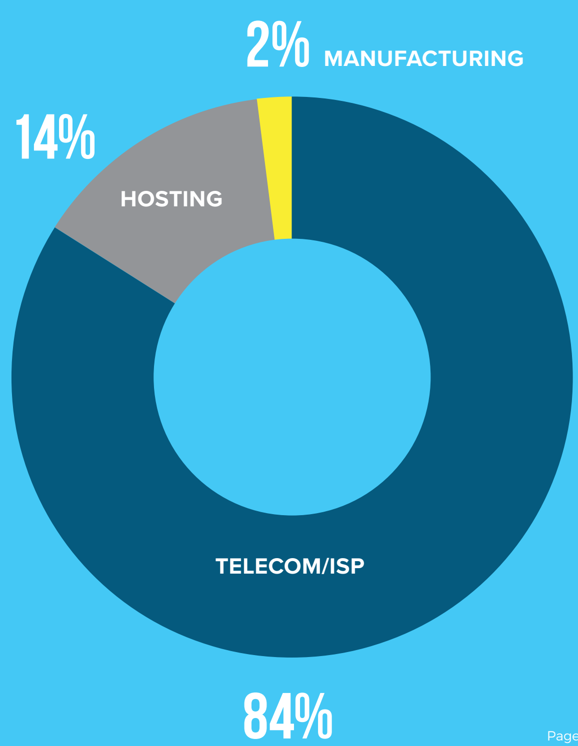
TOP 50 ATTACKING IP ADDRESSES BY COUNTRY

FIGURE 11

INDUSTRIES OF TOP 50 ATTACKING IP ADDRESSES

Figure 11 shows the industry breakdown of the top 50 attacking IP addresses, which, not surprisingly, is predominantly made up of telecom companies and ISPs where IoT devices primarily reside.

It's quite possible that rented servers in hosting provider environments are compromised and being used as pawns from which to launch attacks. But we also know that threat actors rent servers in these environments to start their thingbot development, so we associate this traffic with direct threat actor activity.



37 OF THE TOP 50 ATTACKING IP ADDRESSES HAVE CONSISTENTLY ENGAGED IN MALICIOUS ACTIVITY OVER LONG PERIODS OF TIME.

Eight of the top 10 attacking IP addresses were from ChinaNet. The other two were from hosting companies, PE Tetyana Mysyk in Ukraine, and China Unicom. 37 of the top 50 IP addresses have consistently engaged in malicious activity over the past two years. 42 of the 50 IP addresses attacked at high volumes for months in a row within this reporting period. Ideally, we would only see an IP address attacking for a short period of time before it was remediated by either the provider (suspended, disabled, or taken offline), or potentially by the device's owner. Because these attacking systems are not getting dealt with, we are disclosing the top 50 attacking IP addresses for the first time (see table 5).

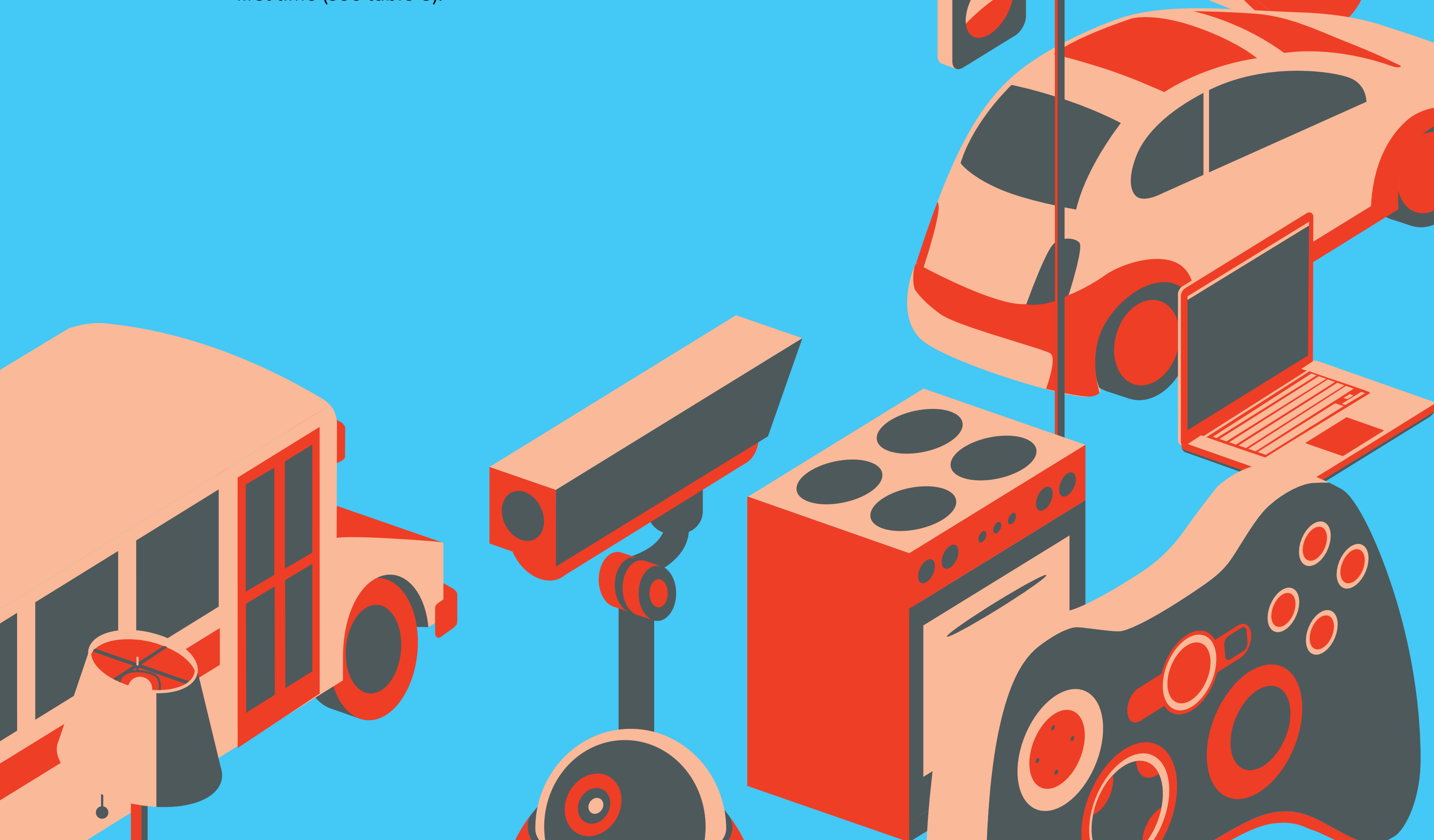


TABLE 5 TOP 50 ATTACKING IP ADDRESSES

No.	IP	IP Owner	Industry	Country	ASN	Attacked multiple months?	New?
1	116.31.116.21	ChinaNet Guangdong Province Network	Telco/ISP	China	AS134764	Yes	IoT v1,2,3
2	58.218.198.160	ChinaNet	Telco/ISP	China	AS4134	Yes	IoT v1,2,3
3	58.218.198.162	ChinaNet	Telco/ISP	China	AS4134	Yes	IoT v1,2,3
4	193.201.224.109	PE Tetyana Mysyk	Hosting	Ukraine	AS25092	Yes	New
5	58.218.198.161	ChinaNet	Telco/ISP	China	AS4134	Yes	IoT v1,2,3
6	218.65.30.156	ChinaNet	Telco/ISP	China	AS4134	Yes	IoT v1,2,3
7	58.218.198.156	ChinaNet	Telco/ISP	China	AS4134	Yes	IoT v1,2,3
8	113.195.145.52	China Unicom China169 Backbone	Telco/ISP	China	AS4837	Yes	IoT v1,2,3
9	116.31.116.7	ChinaNet Guangdong Province Network	Telco/ISP	China	AS134764	Yes	IoT v1,2,3
10	58.218.198.155	ChinaNet	Telco/ISP	China	AS4134	Yes	IoT v1,2,3
11	58.218.198.145	ChinaNet	Telco/ISP	China	AS4134	Yes	IoT v1,2,3
12	116.31.116.41	ChinaNet Guangdong Province Network	Telco/ISP	China	AS134764	Yes	IoT v1,2,3
13	116.31.116.17	ChinaNet Guangdong Province Network	Telco/ISP	China	AS134764	Yes	IoT v1,2,3
14	182.100.67.252	ChinaNet	Telco/ISP	China	AS4134	Yes	IoT v1,2,3
15	58.218.198.169	ChinaNet	Telco/ISP	China	AS4134	Yes	IoT v1,2,3
16	113.195.145.21	China Unicom China169 Backbone	Telco/ISP	China	AS4837	Yes	IoT v1,2,3
17	91.195.103.188	Global Layer B.V.	Hosting	Czechia	AS57172	Yes	New
18	116.31.116.18	ChinaNet Guangdong Province Network	Telco/ISP	China	AS134764	Yes	IoT v1,2,3
19	193.201.224.232	PE Tetyana Mysyk	Hosting	Ukraine	AS25092	Yes	New
20	91.195.103.189	Global Layer B.V.	Hosting	Czechia	AS57172	Yes	New
21	58.242.83.9	China Unicom China169 Backbone	Telco/ISP	China	AS4837	Yes	IoT v1
22	91.197.232.109	Planet Telecom Ltd.	Telco/ISP	UK	AS43715	Yes	New
23	123.249.24.199	ChinaNet	Telco/ISP	China	AS4134	Yes	IoT v1,2,3
24	61.177.172.60	ChinaNet	Telco/ISP	China	AS4134	Yes	IoT v1,2,3
25	116.31.116.33	ChinaNet Guangdong Province Network	Telco/ISP	China	AS134764	Yes	IoT v1,2,3
26	116.31.116.27	ChinaNet Guangdong Province Network	Telco/ISP	China	AS134764	Yes	IoT v1,2,3
27	58.242.83.8	China Unicom China169 Backbone	Telco/ISP	China	AS4837	Yes	IoT v1,
28	195.22.127.83	Sprint S.A.	Telco/ISP	Poland	AS197226	Yes	New
29	58.218.198.148	ChinaNet	Telco/ISP	China	AS4134	Yes	IoT v1,2,3
30	58.218.198.165	ChinaNet	Telco/ISP	China	AS4134	Yes	IoT v1,2,3
31	61.177.172.66	ChinaNet	Telco/ISP	China	AS4134	Yes	IoT v1,2,3
32	107.0.106.213	Comcast Cable Communications	Telco/ISP	U.S.	AS7922	No	IoT v1
33	59.45.175.4	ChinaNet	Telco/ISP	China	AS4134	No	IoT v1,2,3
34	58.57.65.113	ChinaNet	Telco/ISP	China	AS4134	No	IoT v1,2,3
35	217.9.237.9	Blizoo Media and Broadband	Telco/ISP	Bulgaria	AS13124	Yes	New
36	58.218.198.175	ChinaNet	Telco/ISP	China	AS4134	Yes	IoT v1,2,3
37	91.197.232.107	Planet Telecom Ltd.	Telco/ISP	UK	AS43715	Yes	New
38	190.214.22.242	Corporacion Nacional de Telecomunicaciones	Telco/ISP	Ecuador	AS28006	No	New
39	58.218.198.150	ChinaNet	Telco/ISP	China	AS4134	Yes	IoT v1,2,3
40	58.218.198.170	ChinaNet	Telco/ISP	China	AS4134	Yes	IoT v1,2,3
41	51.254.34.30	OVH SAS	Hosting	France	AS16276	Yes	IoT v2
42	123.249.24.160	ChinaNet	Telco/ISP	China	AS4134	No	IoT v1,2,3
43	58.218.198.172	ChinaNet	Telco/ISP	China	AS4134	Yes	IoT v1,2,3
44	58.218.198.141	ChinaNet	Telco/ISP	China	AS4134	Yes	IoT v1,2,3
45	46.37.24.118	Aruba S.p.A.	Hosting	Italy	AS31034	No	New
46	58.57.65.114	ChinaNet	Telco/ISP	China	AS4134	Yes	IoT v1,2,3
47	203.91.121.73	DRAGONLAB	Manufacturing	China	AS24575	No	New
48	155.133.16.246	TralNet Pawel Cichocki	Telco/ISP	Poland	AS200642	Yes	New
49	58.218.198.158	ChinaNet	Telco/ISP	China	AS4134	No	IoT v1,2,3
50	184.106.219.63	Rackspace Hosting	Hosting	U.S.	AS19994	Yes	New

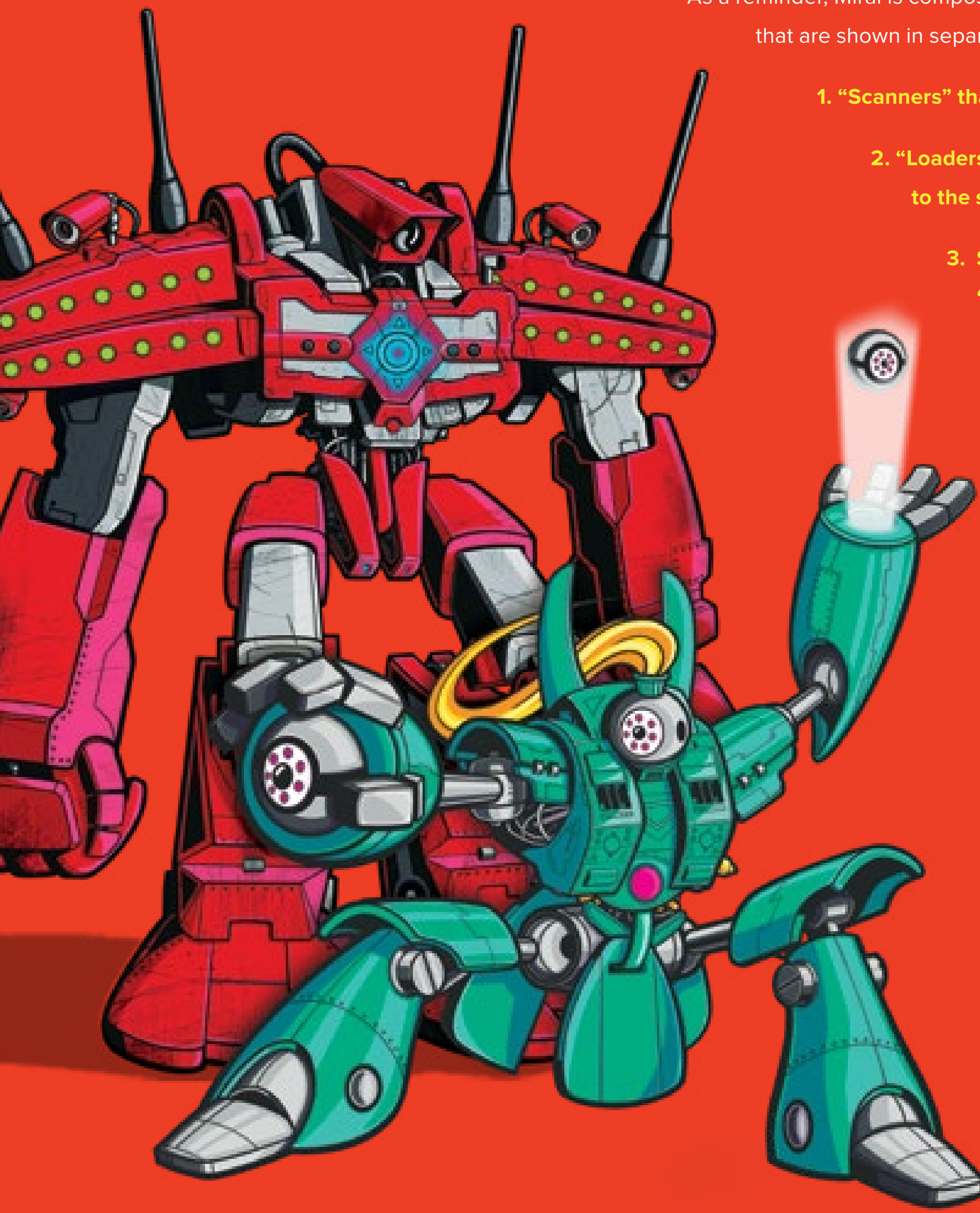
THINGBOT MAPS

We profiled the Mirai and Persirai thingbots in the volume 3 of *The Hunt for IoT*, and we're showing you their global stature again as they aren't going away. In fact, they are growing. Mirai has been forked several times, is the core of at least four other thingbots, and was seen attacking as recently as January 2018. Because of this, F5 Labs released Mirai's command-and-control servers in a blog post in January 2018.

As a reminder, Mirai is composed of three different system types that are shown in separate global maps in Figures 10–15:

1. **"Scanners" that search for vulnerable devices**
2. **"Loaders" that push the malware down to the systems found by the scanners**
3. **Systems that host the latest "malware" for the loaders**

The Persirai maps include all Persirai-infected IP cameras.



MIRAI GROWTH IN 2017

We actively monitor Mirai scanner systems throughout the world. During the six-month period between June 2017 (see Figure 12) and December 2017 (see Figure 13), the number of Mirai scanners grew significantly in Latin America, and slightly in the western United States, Canada, Africa, and Australia.

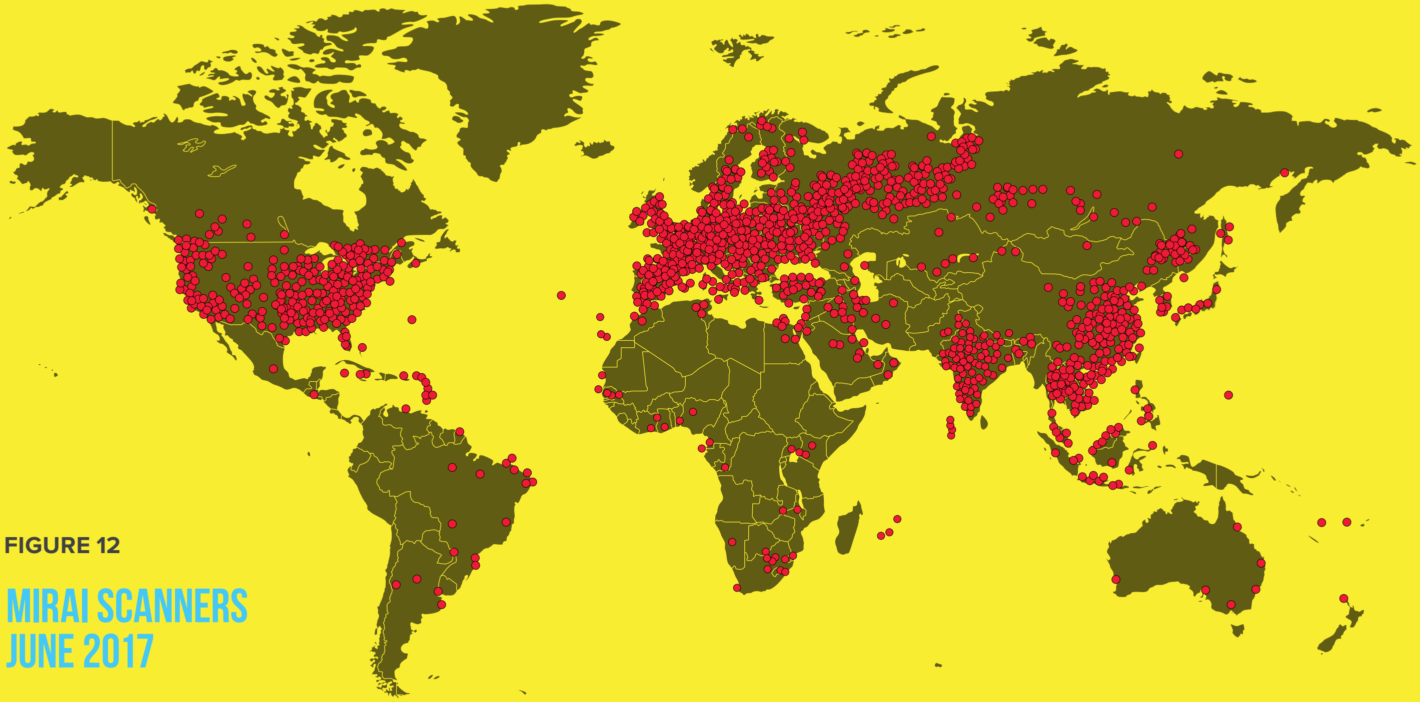


FIGURE 12

MIRAI SCANNERS JUNE 2017

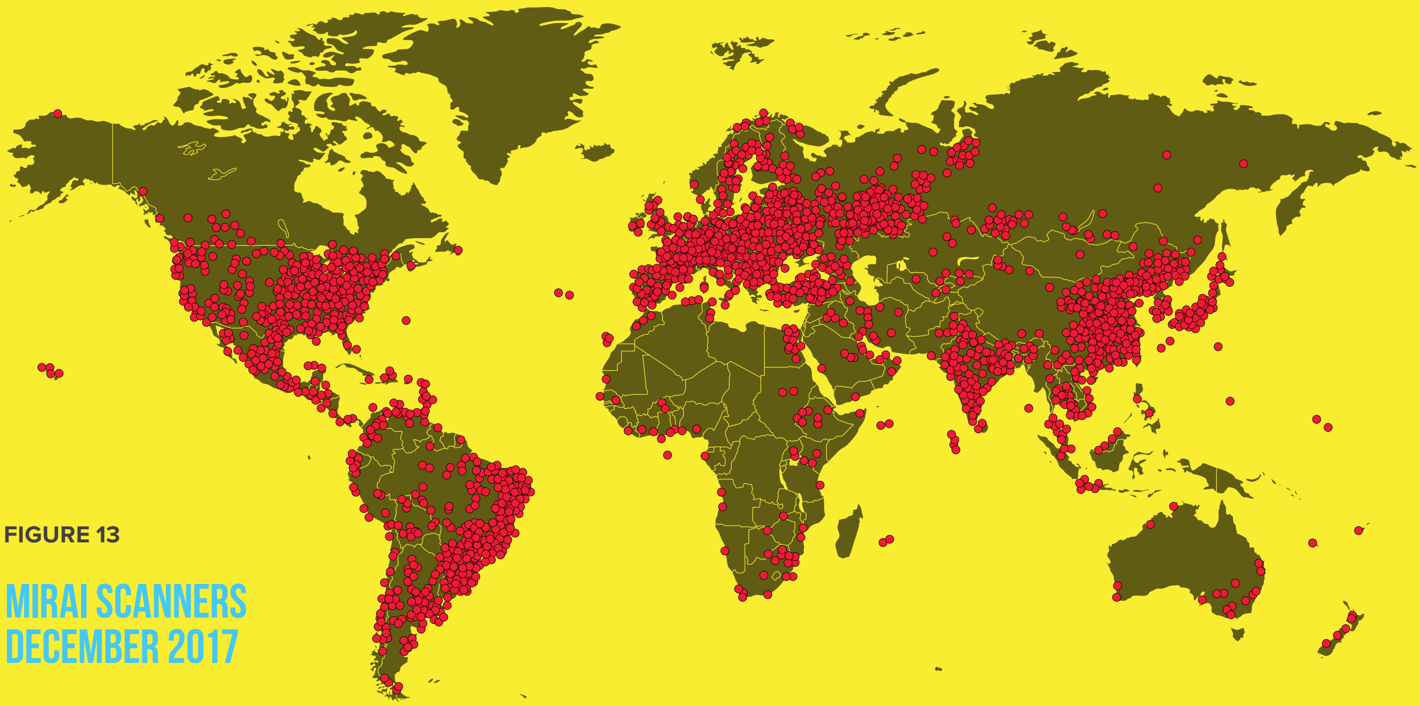


FIGURE 13

MIRAI SCANNERS DECEMBER 2017

Figure 14 shows Mirai loaders in June 2017, while Figure 15 details Mirai loaders in December 2017. There was a significant growth in loader systems in Japan, and slight growth in northern Europe.

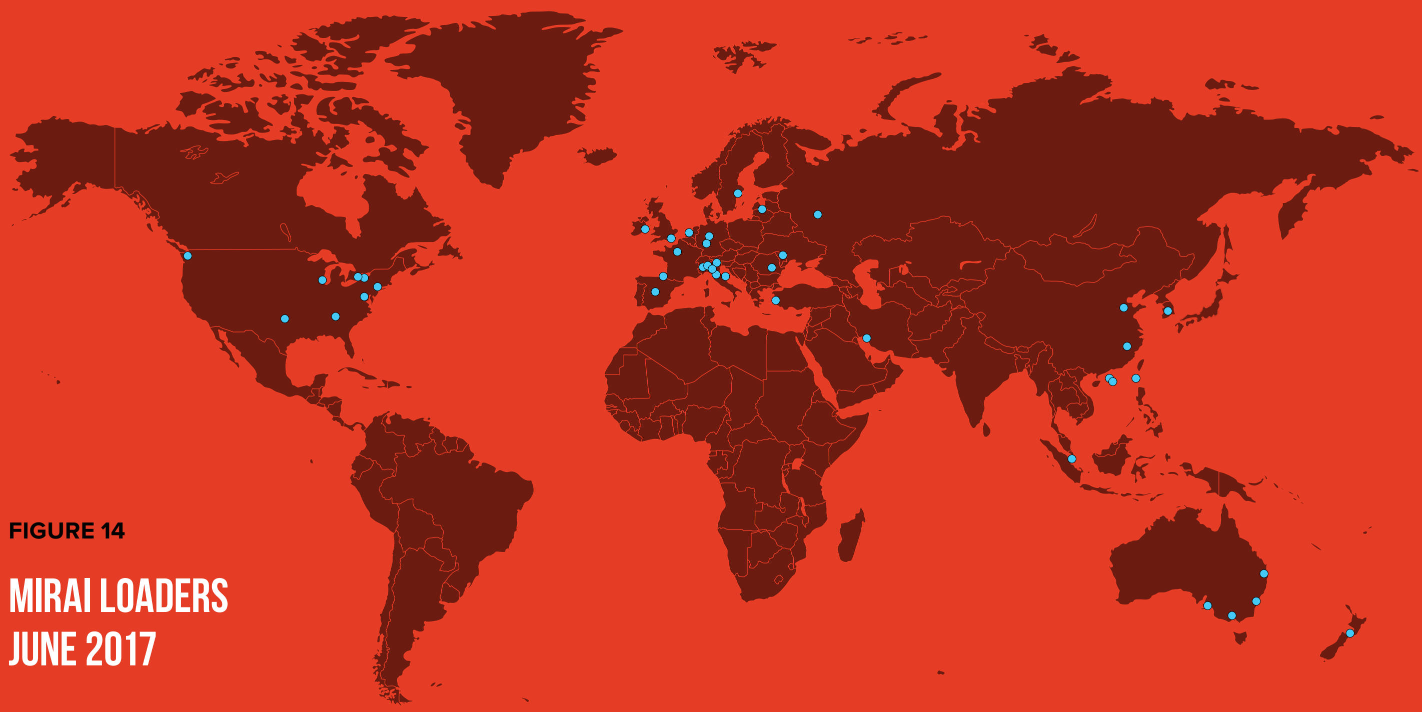


FIGURE 14

MIRAI LOADERS JUNE 2017

FIGURE 15

MIRAI LOADERS DECEMBER 2017

Figure 16 shows Mirai malware systems in June 2017, and Figure 17 shows Mirai malware systems in December 2017. Because there are significantly fewer malware systems compared to Mirai scanner and loader systems, it's easier to see which systems have remained in place, and which systems are gone. The Chinese malware systems are gone, and there are new malware systems in South Korea.

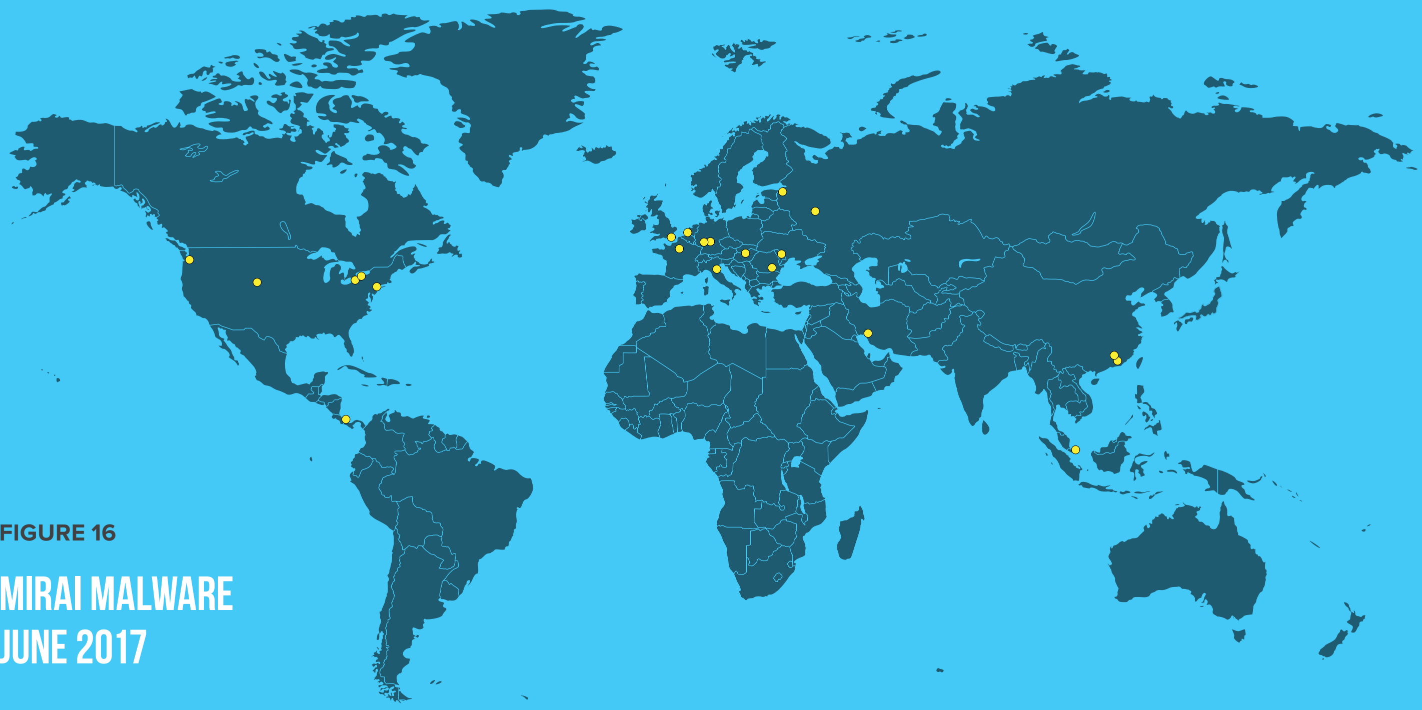


FIGURE 16

MIRAI MALWARE JUNE 2017

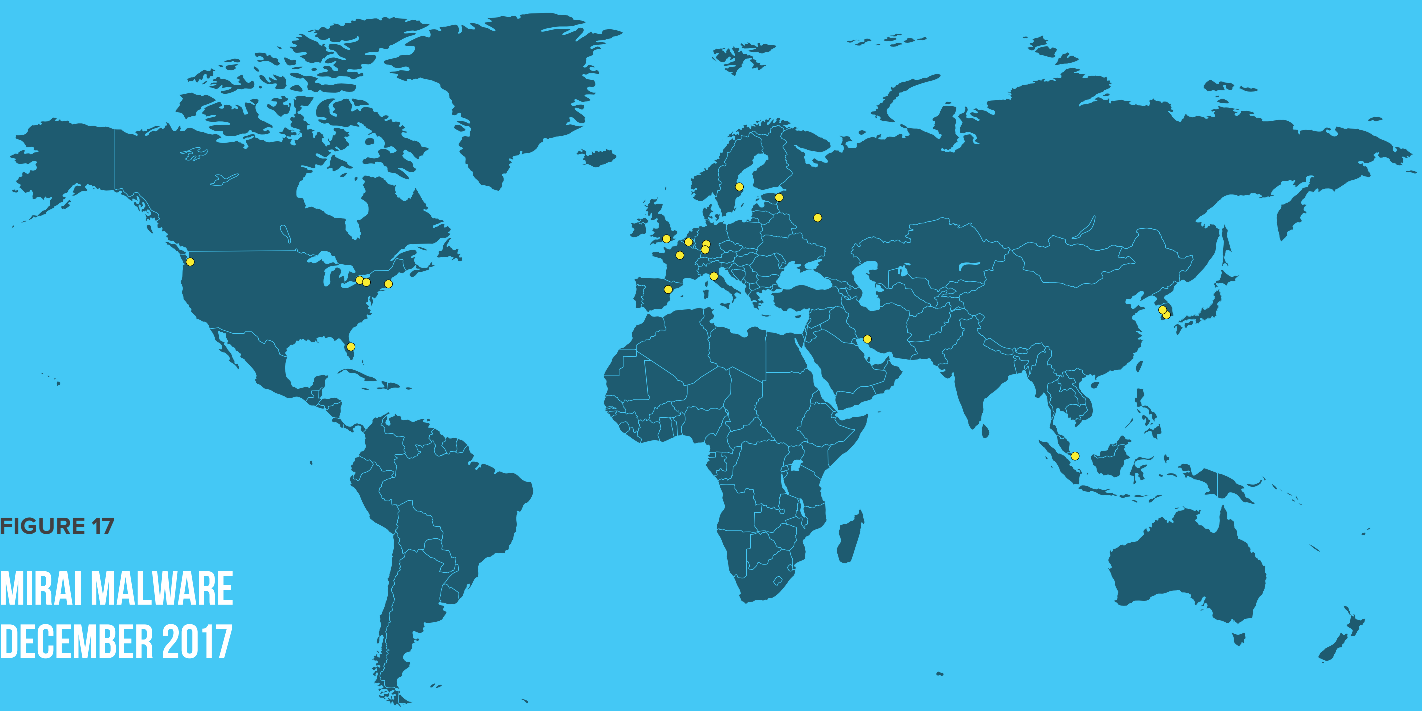


FIGURE 17

MIRAI MALWARE DECEMBER 2017

PERSIRAI MAINTAINS ITS POSTURE IN 2017

Persirai is a thingbot forked from Mirai's code that is composed of infected IP cameras. Figure 18 shows infections in June 2017, versus infections in December 2017 shown in Figure 19. Persirai has reduced its footprint over the last 6 months, most notably in India and central Asia.

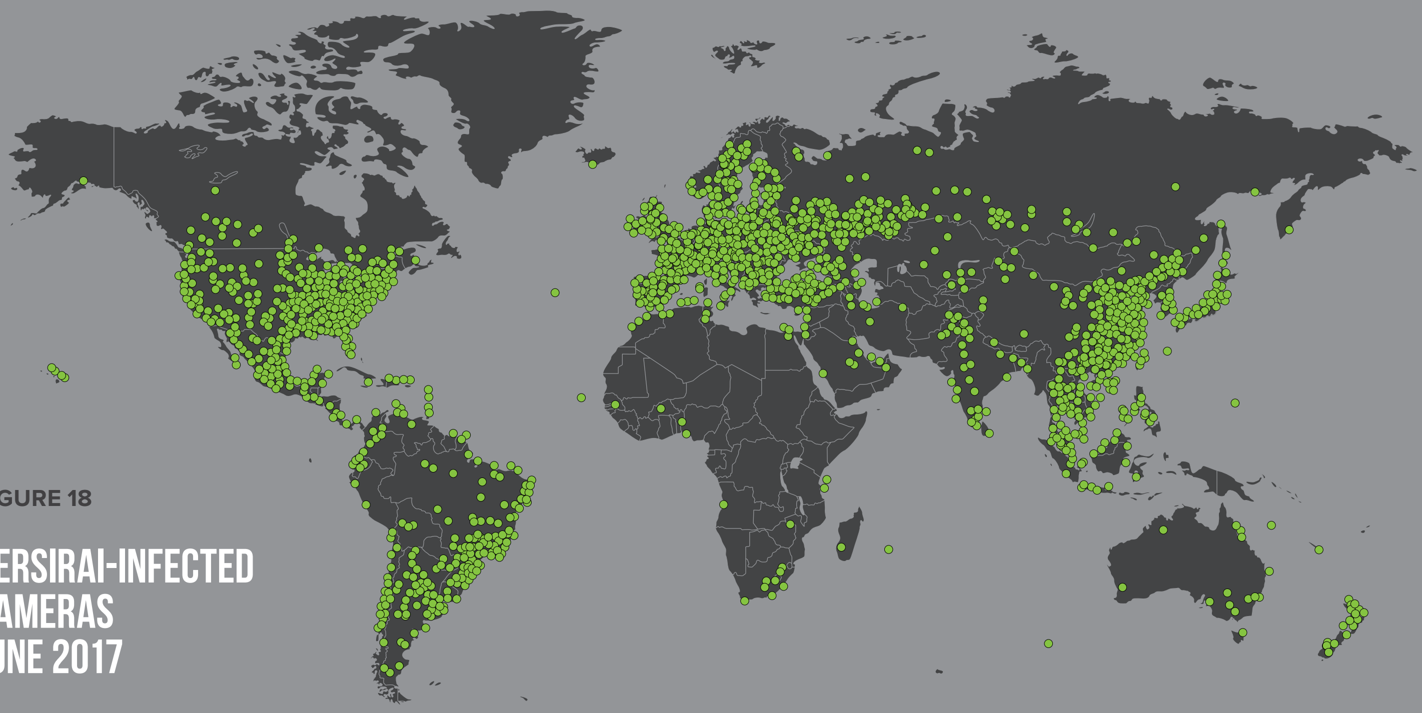


FIGURE 18

PERSIRAI-INFECTED CAMERAS JUNE 2017

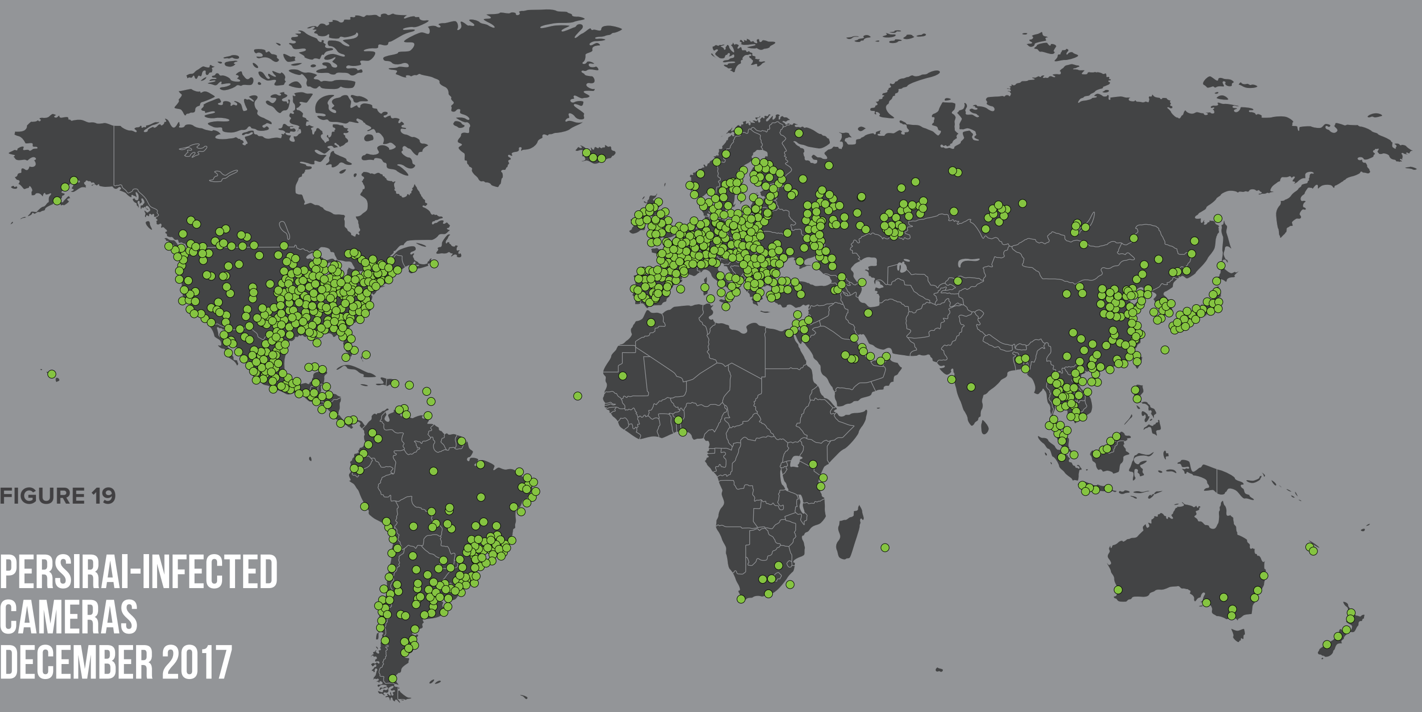


FIGURE 19

PERSIRAI-INFECTED CAMERAS DECEMBER 2017

TOP 50 ATTACKED ADMIN CREDENTIALS

The following tables include the top 50 most used admin credentials during SSH attacks (listed in order), that are also used in telnet attacks when brute forcing the admin login. **Do not use any of these usernames and passwords for any device, anywhere, ever.**

TABLE 6

TOP 50 ATTACKED ADMIN CREDENTIALS

Q3 2017

USERNAME	PASSWORD
support	support
root	root
admin	admin123
ubnt	ubnt
usuario	usuario
service	service
pi	raspberry
user	user
guest	guest
test	test
mother	f-cker
supervisor	supervisor
git	git
0	0
ftp	ftp
operator	operator
oracle	oracle
osmc	osmc
ubuntu	ubuntu
default	1
monitor	monitor
postgres	postgres
nagios	nagios
1111	1111
api	api
10101	10101
dbadmin	admin
butter	xuelp123
ftpuser	asteriskftp
PlcmSpIp	PlcmSpIp
tomcat	tomcat
hadoop	hadoop
mysql	mysql
vagrant	vagrant
jenkins	jenkins
www	www
a	a
apache	apache
minecraft	minecraft
testuser	testuser
ts3	ts3
backup	backup
vnc	vnc
deploy	deploy
odoo	odoo
user1	user1
alex	alex
zabbix	zabbix
server	server
bot	bot

Q4 2017

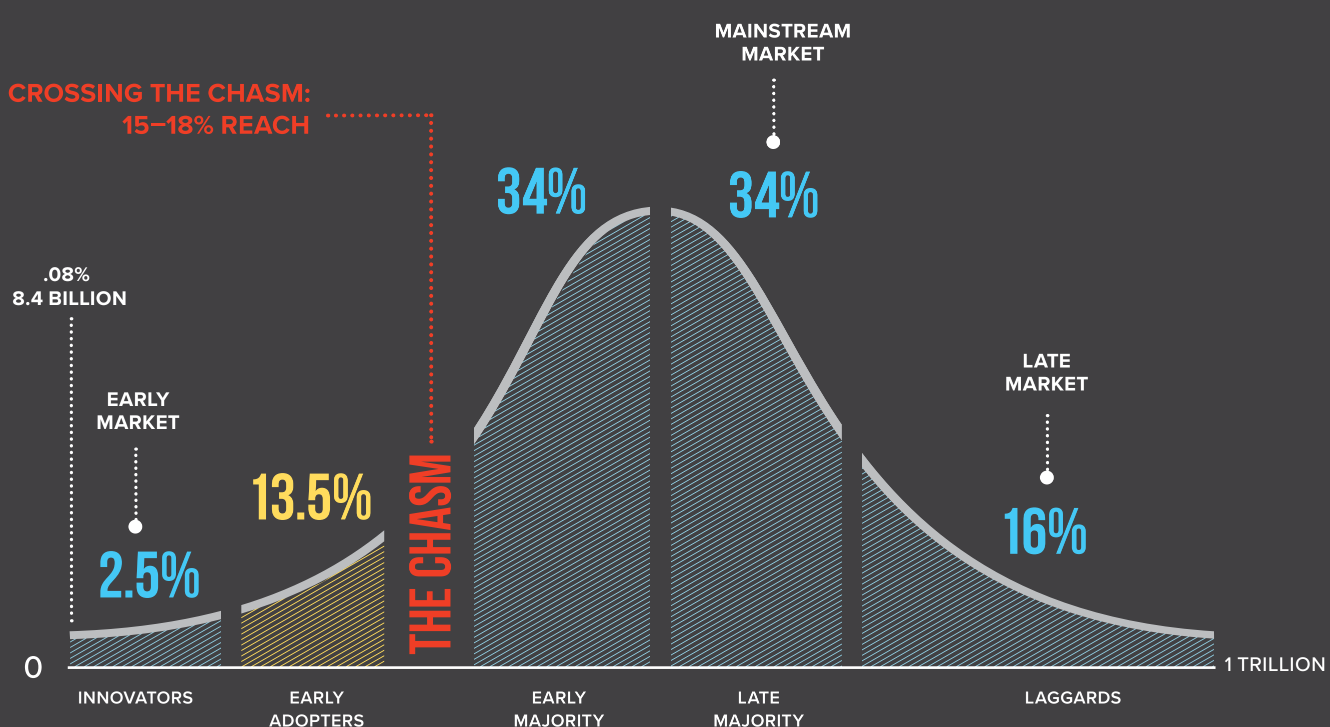
USERNAME	PASSWORD
root	root
support	support
admin	admin123
ubnt	ubnt
service	service
usuario	usuario
pi	raspberry
user	user
test	test
guest	guest
mother	fucker
oracle	oracle
operator	operator
supervisor	supervisor
ftp	ftp
git	git
ubuntu	ubuntu
nagios	nagios
postgres	postgres
uucp	uucp
Admin	admin
ftpuser	asteriskftp
Root	
1234	<Any Pass>
tomcat	tomcat
PlcmSpIp	PlcmSpIp
sshd	sshd
monitor	monitor
butter	xuelp123
mysql	mysql
hadoop	hadoop
user1	user1
cisco	cisco
vagrant	vagrant
101	101
ts3	ts3
FILTERC-NT	FILTERC-NT
apache	apache
telnet	telnet
jenkins	jenkins
Management	TestingR2
www	www
zabbix	zabbix
backup	backup
anonymous	any@
a	a
osmc	osmc
teamspeak	teamspeak
minecraft	minecraft

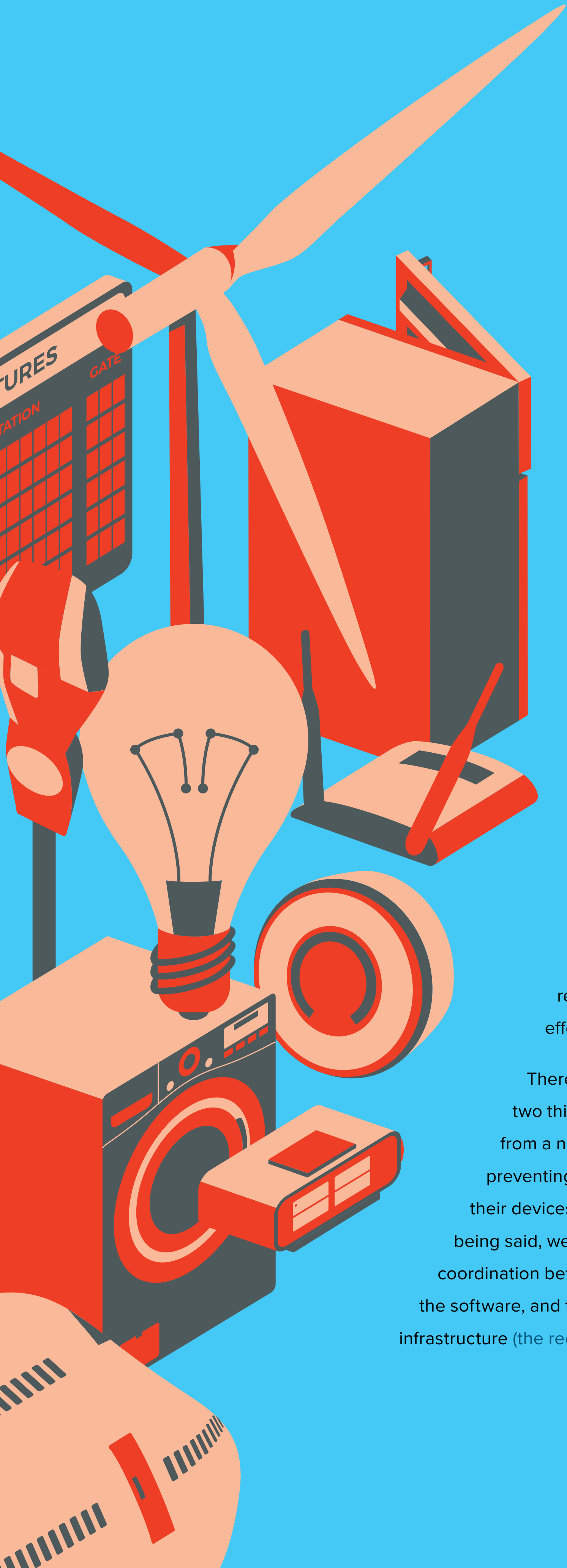
CONCLUSION

Modern life depends on properly functioning IoT devices that are ***available*** when you need them, have ***integrity*** so you can trust them, and are ***confidential*** so they aren't sharing critical data with the wrong (nefarious) people. These basic principles of security were overlooked in the development of most IoT devices, which paved the way for the world we now live in. Thanks to elementary security mistakes like allowing brute force attacks, default (sometimes hard-coded) admin credentials, and remote code execution over port 80, thingbot operators can choose to launch an attack that takes out global Internet infrastructure. Or they can fly under the radar launching mini-but-disruptive attacks, collecting data, and spying on large portions of the population or a singularly targeted business.

The world is just now catching on to how useful IoT devices are; the industry is in its startup phase, just scratching the surface of its future potential. If you follow the "diffusion of innovation" theory, and IoT market expectations exceeding 1 trillion devices, we haven't yet crossed the chasm of IoT potential, or mainstream global market adoption.

FIGURE 20 DIFFUSION OF INNOVATION THEORY





WITH GARTNER ESTIMATES OF 20.4 BILLION IOT DEVICES DEPLOYED BY 2020, THE SECURITY INDUSTRY NEEDS TO BE THE CHAMPION OF IMPLEMENTING SIMPLE SECURITY CONTROLS IN IOT DEVICES.

When the majority of the world is online, smart homes with dozens of Internet-enabled devices and smart cities will be everywhere instead of only in the hands of the early adopters. At that point, IoT thingbots could threaten global stability if we don't start doing something about it now.

With Gartner estimates of 20.4 billion IoT devices deployed by 2020, the security industry needs to be the champion of implementing simple security controls in IoT devices—with a greater sense of urgency than we are doing now. This effort is likely only possible on a go-forward basis. As we've said in prior reports, it's unlikely that we will see any remediation on the 8.7 billion currently deployed IoT devices. Recalls on even a small fraction of this number could have a massive economic impact, and we know that pushing security patches isn't feasible for a lot of IoT devices deployed (not to mention there are no global compliance requirements, Internet police, or global IT squad to assist us in that effort).

There are plenty of IoT hardware platforms that are capable of doing two things at once, such as recording video while blocking admin access from a non-management network IP address. There is nothing technically preventing developers of IoT products from implementing security policies on their devices and choosing to only develop on platforms that can be secured. That being said, we do not want to downplay the effort as it will not be easy. It will require coordination between the developers of different components, from the chipsets to the software, and that is a level of complexity we still haven't mastered in standard IT infrastructure (the recent Spectre and Meltdown vulnerabilities are a good example of this).

Below is a list of IoT security recommendations for personal use, businesses, and IoT manufacturers that we have been championing in each report. They are still applicable and worth continuing to publish.

TABLE 7

IOT SECURITY CHECKLIST

PERSONAL	BUSINESS/ GOVERNMENT	IOT MANUFACTURERS
Do not purchase or deploy IoT devices that are known to be compromised. Reset the administrative password on every IoT device you can. Encrypt your home wireless traffic. Leverage NAT so not all of your home IoT devices are on the public Internet, then secure your one public access point. Educate your friends and family about these efforts.	Have a DDoS strategy in place to keep your applications up and running under a thingbot attack. Ensure you have redundancy in place for critical services in case your service provider is targeted by a thingbot. Mitigate identity attacks as a result of stolen credentials with credential stuffing controls and multi-factor authentication. Implement decryption inside your network to catch malicious traffic hiding in encrypted traffic. Ensure IoT devices connecting to your network pass through your information security event prevention and detection systems (IPS/IDS). Re-evaluate VPN use if always-on tunnels are created for IoT devices. They need isolation. Conduct regular security audits of IoT devices. Conduct basic security tests on IoT products before you deploy them. Do not implement insecure IoT devices! Educate your employees on the threat of IoT and which IoT products/brands are vulnerable. Security awareness is critical to limiting the number of insecure IoT devices that get deployed.	Implement a secure software development lifecycle (SDLC) process. Do not use basic admin credentials for remote management, and do not hard-code the admin credentials. Require admin password resets upon deployment. Do not allow brute force attacks. Restrict remote administration to admin networks. Allow for IP tables and/or block lists. Allow for remote operating system upgrades and patches.

Furthermore, security professionals, as well as machine learning and artificial intelligence developers, should be working together to develop forward-thinking IoT security controls. IoT devices connect the physical world to the virtual world. The future needs IoT neural networks that mimic the way fungal networks keep ecological environments thriving.[vii] In the meantime, F5 Labs will continue to track the hunt for IoT as we have expanded our research into other IoT attack methods (disclosed and non-disclosed CVEs and exploits), and IoT device types beyond wireless.

i https://arstechnica.com/information-technology/2016/11/notorious-iot-botnets-weaponize-new-flaw-found-in-millions-of-home-routers/

ii https://www.idc.com/getdoc.jsp?containerId=prUS43295217

iii https://www.cyber.nj.gov/threat-profiles/botnet-variants/hide-n-seek

iv https://www.gartner.com/newsroom/id/3598917

v https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated

vi http://www.atma.es/

vii http://www.bbc.com/earth/story/20141111-plants-have-a-hidden-internet

ABOUT F5 LABS

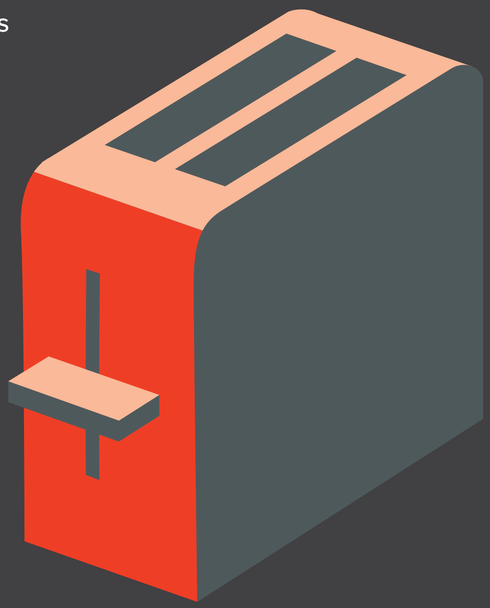
F5 Labs combines the threat intelligence data we collect with the expertise of our security researchers to provide actionable, global intelligence on current cyber threats—and to identify future trends. We look at everything from threat actors and the nature and source of attacks, to post-attack analysis of significant incidents in order 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 monitoring and investigating emerging attacks, advanced persistent threats, and the organizations and individuals responsible for them. The team also develops research tools to identify, investigate, and track ongoing attacks and emerging threats.

For more information, visit www.loryka.com.



APPLICATION THREAT INTELLIGENCE

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