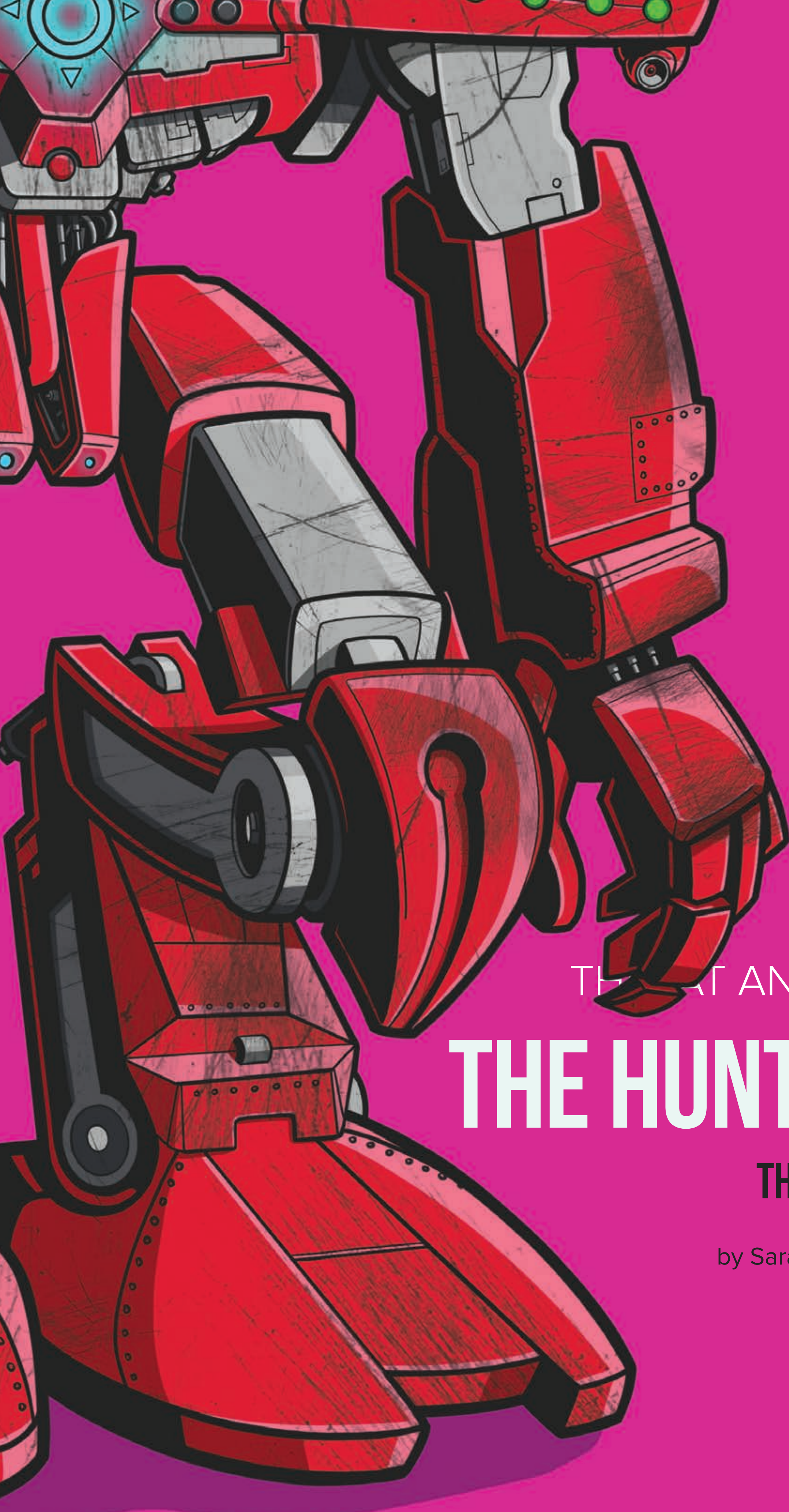


THREAT ANALYSIS REPORT

THE HUNT FOR IOT

THE RISE OF THINGBOTS

by Sara Boddy and Justin Shattuck

VOLUME 3
July 2017

TABLE OF CONTENTS

TABLE OF FIGURES

EXECUTIVE SUMMARY

The Internet of Things (IoT) and, specifically, the hunt for exploitable IoT devices by attackers, has been a primary area of research for F5 Labs for over a year now—and with good reason. IoT devices are becoming the "cyberweapon delivery system of choice" by today's botnet-building attackers. And, why not? There are literally billions of them in the world, most of which are readily accessible (via Telnet) and easily hacked (due to lack of security controls). Why would attackers rent expensive resources in hosting environments to build their botnets when so many devices are "free" for the taking?

Across all of our research, every indication is that today's botnets, or "thingbots" (built exclusively from IoT devices) will become the infrastructure for a future darknet.[1]

In our third semi-annual report on this topic, we continue to track Telnet attack activity and, through a series of global maps showing infected systems, we track the progression of Mirai, as well as a new thingbot called Persirai. We also include a list of the administrative credentials attackers most frequently use when launching brute force attacks against IoT devices.

Here are the key findings based on analysis of data collected between January 1 through June 30, 2017:

- Telnet attack activity grew 280% from the previous period, which included massive growth due to the Mirai malware and subsequent attacks.
- The level of attacking activity at the time of publishing doesn't equate to the current size of Mirai or Persirai, indicating there are other thingbots being built that we don't yet know about. Since there haven't been any massive attacks post Mirai, it's likely these thingbots are just ready and waiting to unleash their next round of attacks.
- 93% of this period's attacks occurred in January and February while activity significantly declined in March through June. This could mean that the attacker "recon" phase has ended and that the "build only" phase has begun. Or, it could just be that attackers were momentarily distracted (enticed) by the Shadow Brokers' release of EternalBlue.[2]
- The top attacking country in this reporting period was Spain, launching 83% of all attacks, while activity from China, the top attacking country from the prior two periods, dropped off significantly, contributing less than 1% to the total attack volume. (Has China cleaned up compromised IoT systems?)
- The top 10 attacking IP addresses all came from one hosting provider network in Spain: SoloGigabit.
  - SoloGigabit was the source of all attacks coming from Spain in this period. Given that SoloGigabit is a hosting provider with a "bullet proof" reputation, we assume this was direct threat actor traffic rather than compromised IoT devices being forced by their thingbot master to attack.

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

[2] https://f5.com/labs/articles/threat-intelligence/cyber-security/nsa-cia-leaks-provide-a-roadmap-to-stealthier-faster-more-powerful-malware-like-sambacry-and-notpetya

- The top 50 attacking IP addresses resolve to ISP/telecom companies, and hosting providers. While there were more ISPs and telecom IP addresses on the top 50 list, when looking at volume of attacks by industry, the overwhelming number came from hosting providers.
- Although IoT devices are known for launching DDoS attacks, they're also being used in vigilante thingbots to take out vulnerable IoT infrastructure before they are used in attacks[3] and to host banking trojan infrastructure.[4] IoT devices have also been subject to hacktivism attacks,[5] and are the target of nation-state cyber warfare attacks.[6]
- As we see in this report with Persirai, attackers are now building thingbots based on specific disclosed vulnerabilities[7] rather than having to launch a large recon scan followed by brute forcing credentials.

From a manufacturing and security perspective, the state of IoT devices hasn't changed, nor did we expect it to. In the short term, IoT devices will continue to be one of the most highly exploitable tools in attackers' cyber arsenals. We will continue to see massive thingbots being built until IoT manufacturers are forced to secure these devices, recall products, or bow to pressure from buyers who simply refuse to purchase vulnerable devices.

In the meantime, responsible organizations can do their best to protect themselves by having a DDoS strategy in place, ensuring redundancy for critical services, implementing credential stuffing solutions, and continually educating employees about the potential dangers of IoT devices and how to use them safely.

---

[3] https://arstechnica.com/security/2017/04/brickerbot-the-permanent-denial-of-service-botnet-is-back-with-a-vengeance/

[4] https://f5.com/labs/articles/threat-intelligence/malware/marcher-gets-close-to-users-by-targeting-mobile-banking-android-apps-social-media-and-email-26004

[5] http://www.businessinsider.com/hackers-attacking-vietnam-airports-2016-7

[6] https://motherboard.vice.com/en_us/article/bmvkn4/ukrainian-power-station-hacking-december-2016-report

[7] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8224

INTRODUCTION

It's hard to believe that just three years ago, 87% of consumers said they hadn't heard of the "Internet of Things" (IoT).[8] Today, they still might not recognize the term, but they've overwhelmingly embraced it. Many could name a half-dozen ways they use it daily, whether they're commanding Alexa to set an alarm, play music, or create a To Do list; remote-controlling their home's lighting, door locks, and thermostat; uploading health stats (like blood pressure or blood sugar data) directly to their doctor from a fitness app; scanning empty grocery items to automatically reorder online, or (gasp) watching security camera video feeds in real time as their homes are being burglarized.

From the innocence of the first Internet-connected device—a toaster (built in response to a half-serious challenge posed at Interop 1989[9])—to today's sensors that control our most critical infrastructure, the IoT represents one of the most sweeping technological (and some would argue, social and political) disrupters of our time, connecting the physical world to the virtual world. It is reshaping business and manufacturing as well as the way we, as consumers, approach life, work, and play.

MILLIONS OF ATTACKS

BILLIONS OF DEVICES

Today, there are already an estimated 8.4 billion IoT devices in use, and that number is expected to reach over 20 billion by 2020.[10] This inexorable march we're making toward a fully device-connected world (see Figure 1), not just an Internet-connected world, is proving to be as dangerous as it is enticing. Many consumers would be shocked to learn that some of their own IoT devices—IP cameras, DVRs, and home routers—might already be compromised. They could conceivably have been used as pawns in large botnets like Mirai, which took down hosting provider Dyn, and ultimately web giants like Twitter, Netflix, the Guardian, Reddit, and CNN in late 2016.[11]

---

[8] https://www.accenture.com/t20150624T211456__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Technology_9/Accenture-Internet-Things.pdf

[9] http://www.livinginternet.com/i/ia_myths_toast.htm

[10] http://www.gartner.com/newsroom/id/3598917

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

INTERNET "THINGS" CONNECT THE WORLD AROUND US

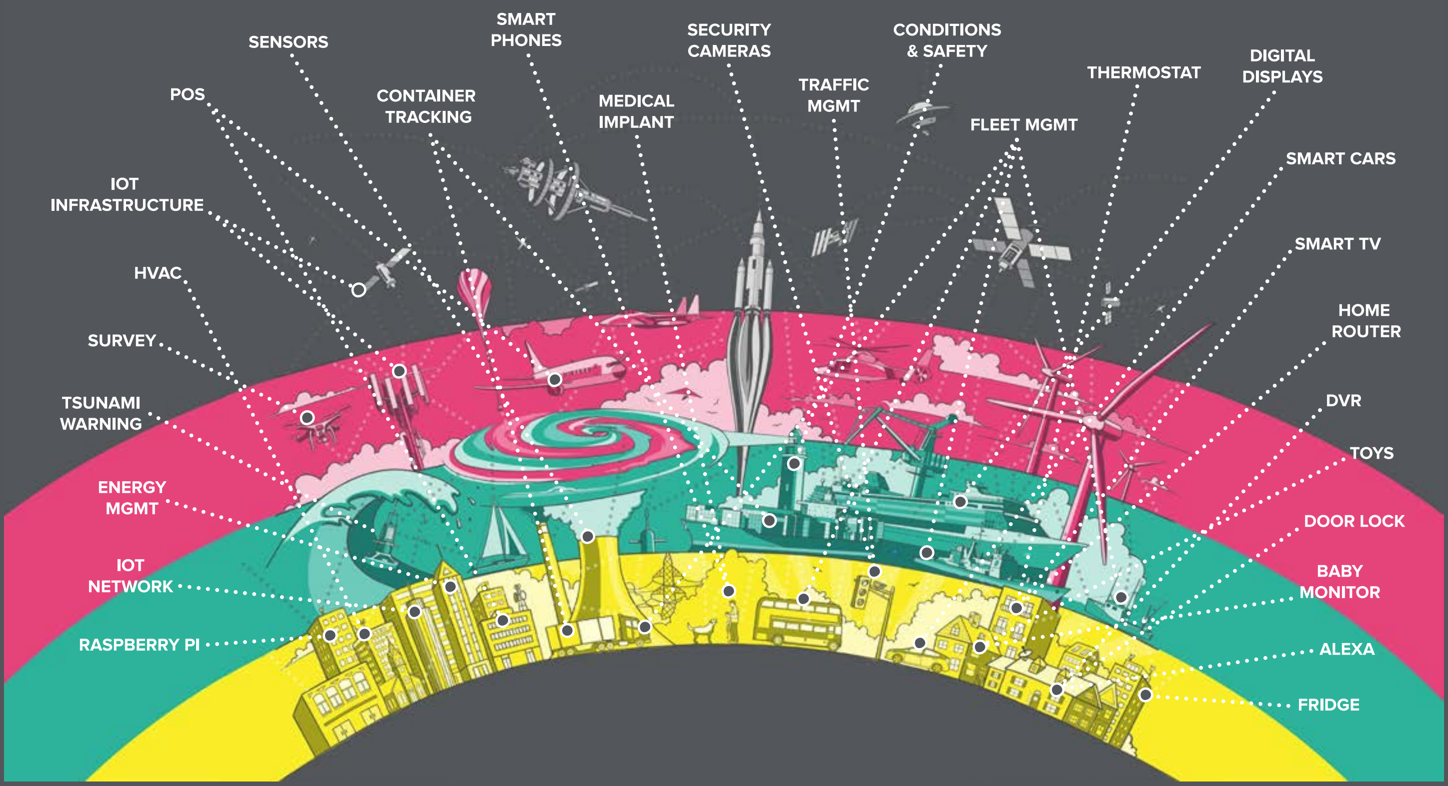


Figure 1: Internet "things" connect the world around us and power our modern way of life

Here are a few more sobering IoT facts:

- Attackers can leverage smart TVs for everything from spying[12] to relay attacks.
- Man-in-the-middle attacks on home routers can collect personal data and user credentials for online accounts and corporate networks.
- Medical implants such as cardiac pacemakers and defibrillators can be hacked, potentially endangering the lives of their human recipients.[13]
- Experts have warned for years that most cars manufactured today are vulnerable to complete remote control by attackers.[14]
- Major modes of transportation like subways, trains, airplanes, and ships rely on a variety of IoT sensors that, if tampered with, could cause catastrophic damage or loss of life.

---

[12] https://www.bleepingcomputer.com/news/security/about-90-percent-of-smart-tvs-vulnerable-to-remote-hacking-via-rogue-tv-signals

[13] http://money.cnn.com/2017/01/09/technology/fda-st-jude-cardiac-hack/index.html

[14] https://www.youtube.com/watch?v=MeXfCNwMG64

- IoT systems that control public infrastructure (such as water treatment facilities and power plants) have already been compromised.[15]
- Future candidates for IoT attacks include spam relay servers, click fraud (pay-per-click advertising), ad fraud (banner, video, and in-app ads), bitcoin mining, and darknet infrastructure.

And, as we move into uncharted territory with revolutionary uses for IoT devices, the potential for exploit only widens. Currently, specialized sensors used in the components of IoT-enabled devices track nearly 80 diverse "measured quantities," from body fat, heart rate, and weight to radioactivity, magnetic field strength, and electric resistance.[16] These components use different chipsets, all of which are potentially compromisable. The complexity grows as we begin to see layers and layers of components with diverse chipsets used in larger, IoT-controlled "objects" such as cars, where attackers can take over individual functions such as speed, braking, acceleration, steering, and so on.

There's no doubt that today's IoT threat landscape is massive, and the lax security posture that make these devices so easy to compromise has not improved—nor is it likely to anytime soon. (That would require immediate change to current product development practices, as well as firmware updates or product recalls for potentially billions of devices, neither of which are likely to happen without legislation.)

So, for the time being, the three-step attack plan (see Figure 2) remains incredibly simple: scan for vulnerable devices and brute-force them; install malware and auto-build a botnet; attack.

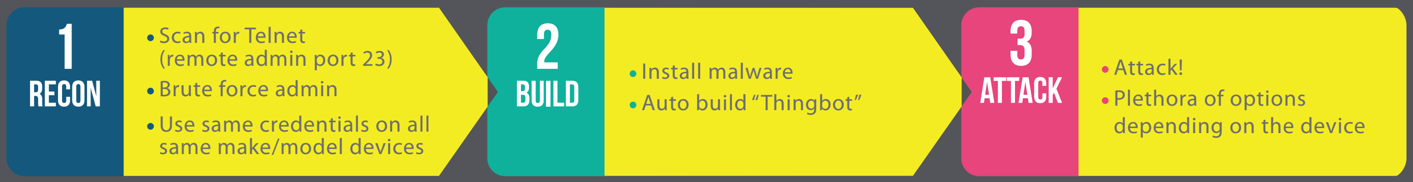


Figure 2: IoT attack plan—as easy as 1, 2, 3

The ease with which IoT devices can be compromised (and the impact of attacks) is why F5 Labs continues to research and report on this threat, tracking its progression in terms of size, specific attackers, targets, devices, and methods. Our first report on this topic[17] just scratched the surface and served as a wake-up call to alert consumers as well as the security community to the seriousness of the threat. In our second report,[18] we delved deeper into the IoT "iceberg," highlighting the huge growth rate (1,400% in 2016) in the hunt for vulnerable devices. We also called out the networks that were building Death Star-sized botnets capable of pulling off Mirai-sized (1 Tbps) DDoS attacks.

---

[15] https://motherboard.vice.com/en_us/article/bmvkn4/ukrainian-power-station-hacking-december-2016-report

[16] http://devices.wolfram.com/measured-quantities.html

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

[18] https://f5.com/labs/articles/threat-intelligence/ddos/the-hunt-for-iot-the-networks-building-death-star-sized-botnets-26796

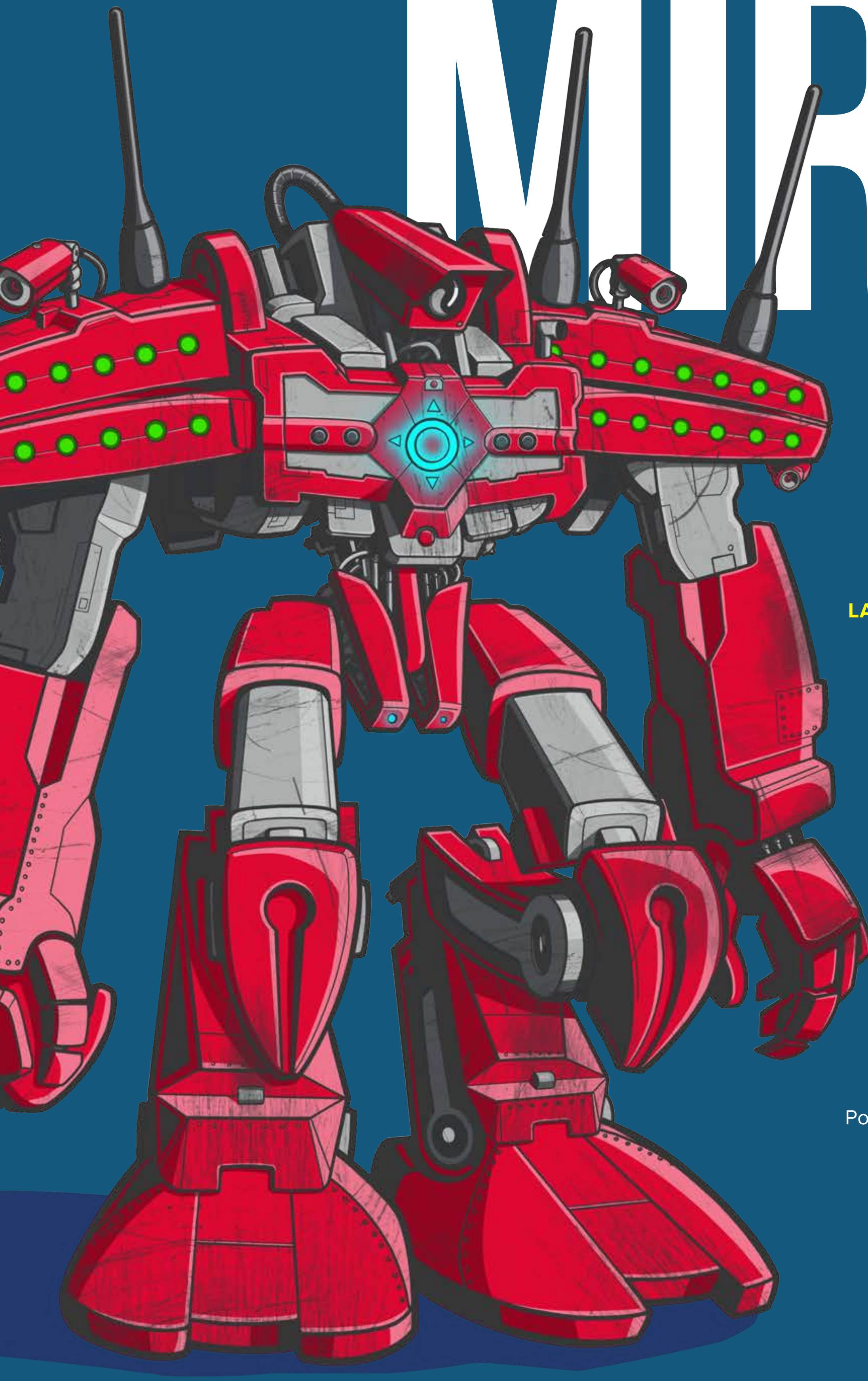
RISE OF THINGBOTS

The title of this report, *The Rise of Thingbots*, speaks to the evolving methods of attackers. In the past, massive botnets were built in hosting environments where resources (servers, memory, address space, bandwidth) were expensive. IoT devices have changed all that. Today, when attackers crack the admin credentials of a manufacturer's IoT device (say, a DVR), they have instant access to potentially thousands of units—all for a comparatively small amount of work and money. Why wouldn't attackers use these devices rather than costly hosting environments in which to build their botnets? With a virtually inexhaustible supply of IoT devices, we're seeing more and more botnets, or "thingbots," built exclusively out of IoT devices.

Let's look more closely now at attacker activity as of June 30 concerning the Mirai thingbot and Persirai, a new thingbot specifically targeting CVE-2017-8225, which was released on April 25, 2017.[19] We provide global maps of Mirai's scanners, loaders, and malware systems, as well as Persirai's infected cameras and command and control (C&C) locations.

[19] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8225

MIRAI



FIRST DISCOVERED:

August 2016

COMPOSED OF:

DVRs, routers, CCTV cameras

LAUNCHED THREE OF THE LARGEST DDOS ATTACKS IN HISTORY IN SEPT AND OCT 2016

- Krebs: 600 Gbps
- Dyn: 990 Gbps
- OVH: 1.2 Tbps

CORE COMPONENTS:

Loaders, scanners, and malware systems

CURRENT GROWTH:

Slowing

MALWARE ORIGIN:

Potentially Russian (hardcoded unicode strings in Russian).

SOURCE CODE:

Made public and adapted in other malware projects

GLOBAL MAPS OF MIRAI THINGBOT ACTIVITY

The following series of maps provide global views of Mirai's scanners, loaders, and malware systems that host the malware binary code as of June 2017. Scanner and loader systems are heavily concentrated in Europe, China, India, and the eastern US.

Mirai scanners (shown in red in Figure 3) search the Internet for vulnerable devices to compromise. Once found, scanners report the victim device's IP address, port number, and authentication credentials back to Mirai loader systems. Mirai scanners are heavily concentrated in Europe, China, India, and the eastern US.

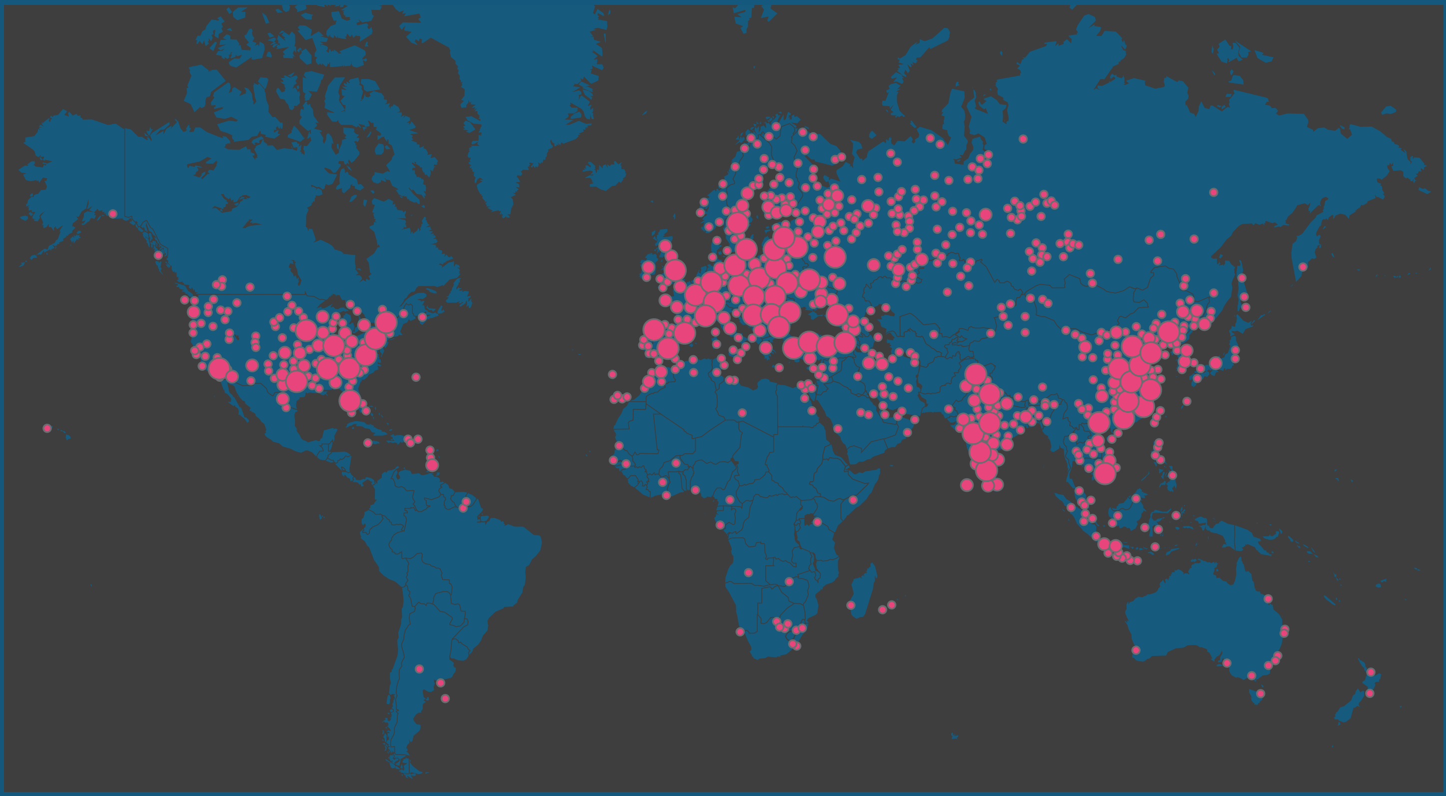


Figure 3: Mirai scanners, worldwide, June 2017

Mirai loaders are remote administration tools that push the bot binary code down to the devices found by scanners. Loader ports include:

- 32/TCP
- 1099/TCP
- 2222/TCP
- 2323/TCP
- 3232/TCP
- 5555/TCP
- 6789/TCP
- 7547/TCP
- 19058/TCP
- 23231/TCP

The highest concentration of loaders around the world exist in China, eastern Europe, and Brazil, as shown in green in Figure 4.

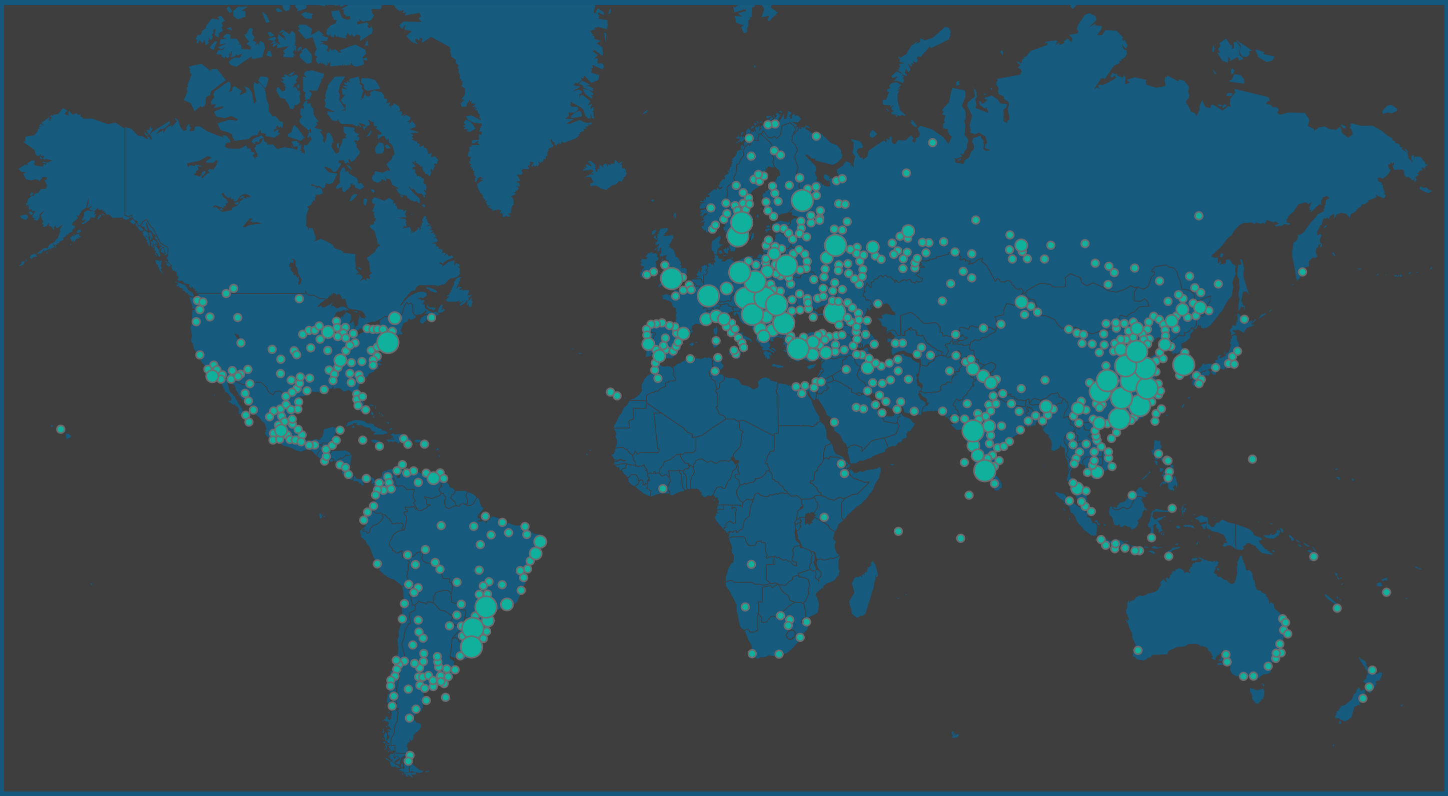


Figure 4: Mirai loaders, worldwide, June 2017

Mirai malware systems (shown in white in figure 5) host the malware binary code that is picked up by the loader systems and pushed down to the devices found by the scanners. There are limited malware systems across the globe; most are located in Europe and the US, and a smaller number in Asia.

Figure 5: Mirai malware binary hosts, worldwide, June 2017

Figure 6 provides a more detailed view of Mirai scanners (red), loaders (green), and malware systems (white) found in North America in June 2017. The highest concentration of both scanners and loaders is in New York, Los Angeles, San Francisco, and Seattle. Dallas, Atlanta, Tampa, Miami, and Washington D.C. also have large concentrations of scanners. Malware binary hosts in North America are primarily located in Seattle, San Francisco, and Los Angeles as well as the Midwest, Texas, and the eastern seaboard.

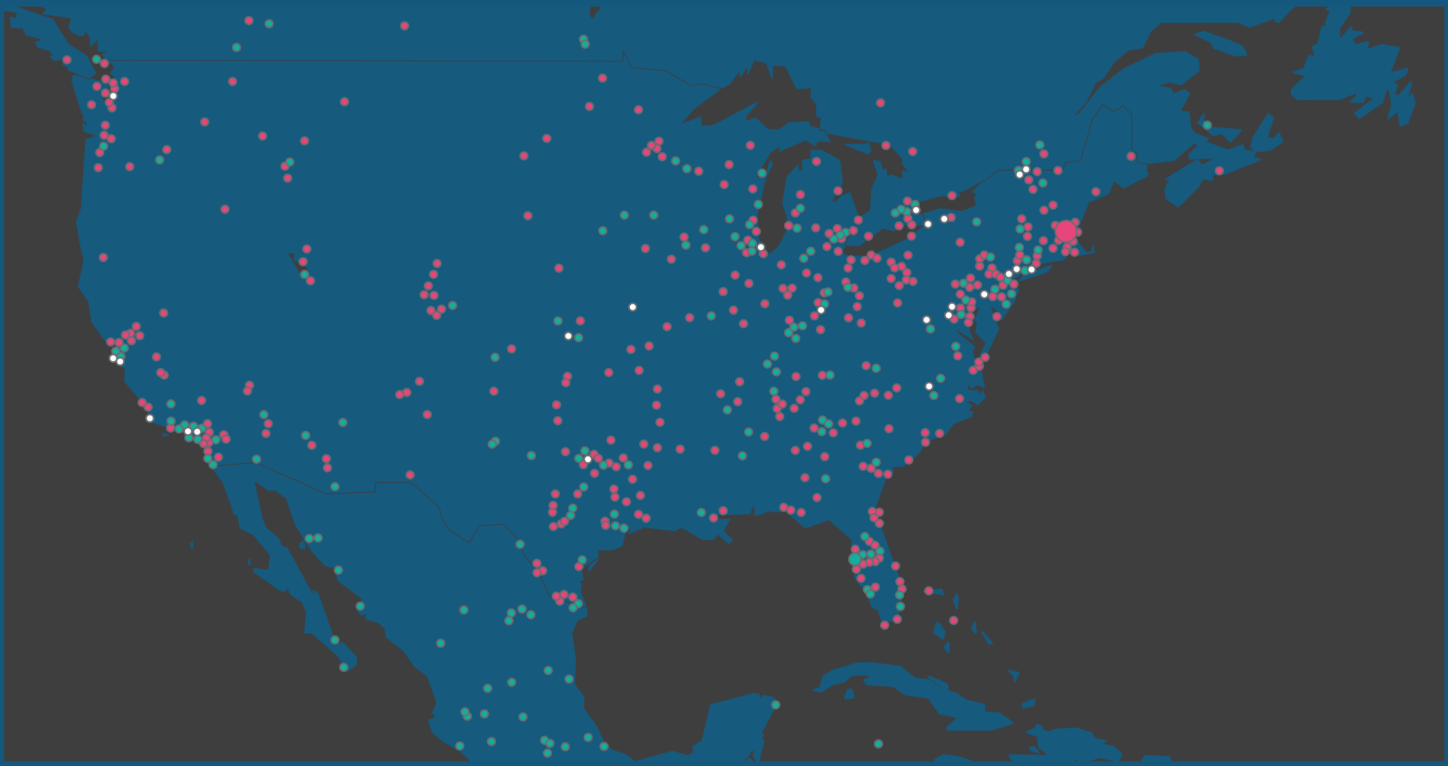
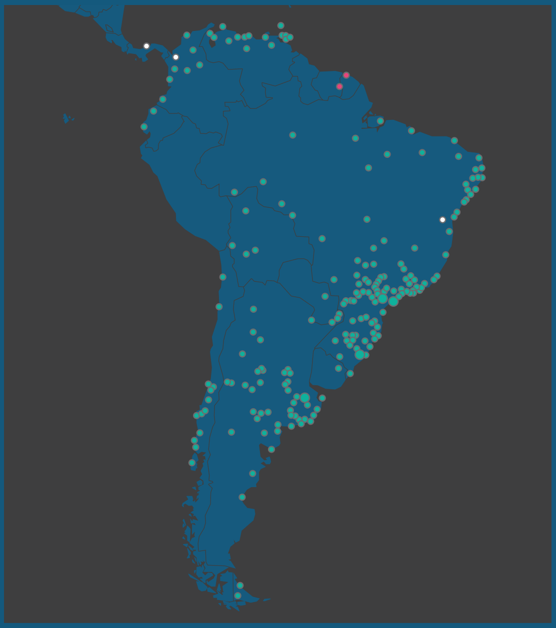


Figure 6: Consolidated view: Mirai scanners, loaders, and malware, North America, June 2017



Mirai activity in South America in June 2017 consisted mostly of loaders (shown in green in Figure 7), with the highest concentration in Brazil centered around São Paulo and Rio de Janeiro. Scanners also exist in French Guiana, Grenada, and Argentina (not visible in Figure 7 due to the concentration of loader dots). Only three malware binary hosts (white) exist in South America: in Brazil, Colombia, and Panama.

Figure 7: Consolidated view: Mirai scanners, loaders, and malware, South America, June 2017

Mirai loaders exist all over Europe, with the highest concentrations in the Netherlands, Czech Republic, and Romania (see Figure 8). Scanners also span all of Europe but are focused heavily in the UK, Italy, Poland, the Czech Republic, and Romania. The Netherlands is a hot spot for all three system types and has the highest concentration of malware binary hosts (white) in the world.

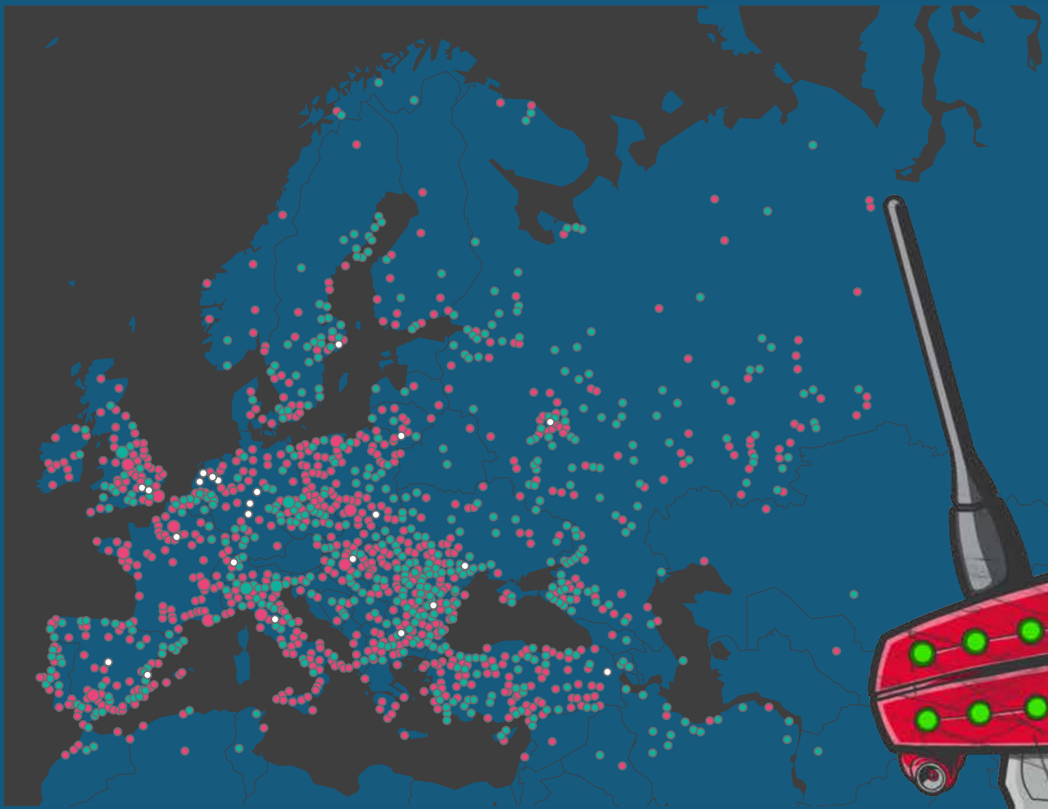
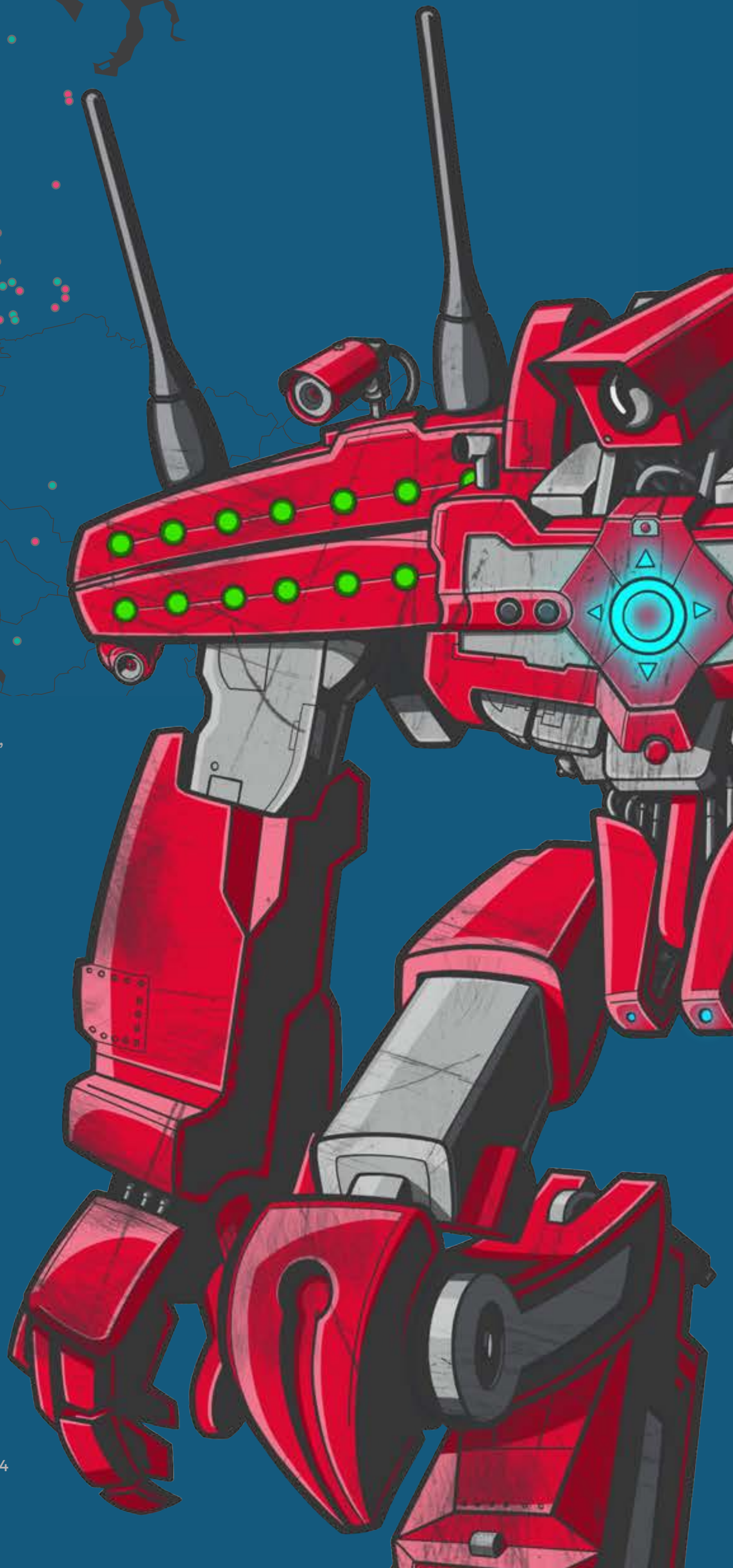


Figure 8: Consolidated view: Mirai scanners, loaders, and malware, Europe, June 2017



THE NETHERLANDS IS A HOT SPOT FOR ALL THREE SYSTEM TYPES

Loaders and scanners throughout Asia primarily exist in China, South Korea, Vietnam, Taiwan, and India. Indonesia and the Philippines also have concentrated spots of loaders and scanners (see Figure 9). Asian Mirai binary hosts are limited to Hong Kong, China (Beijing and Degen), South Korea (Seoul & Busan), Taipei, Taiwan, Japan (Tokyo and Fukuoka), Ho Chi Minh City, Vietnam, Singapore, Bangkok, Thailand and Bengaluru, India.

Figure 9: Consolidated view: Mirai scanners, loaders, and malware, Asia, June 2017

Although the continent of Africa has limited Mirai activity, it's worth mentioning where we saw activity in June 2017. Scanners make up the largest number of systems in Africa, mainly existing in coastal cities throughout the continent and focused in the Canary Islands, Morocco, Egypt, and South Africa. Loaders in Africa also exist primarily within coastal cities in Morocco, Egypt, South Africa, and the Canary Islands. There were only two malware binary hosts in Africa, in Namibia, and the Seychelles.

PERSIRAI

COMPOSED OF:

IP Cameras

- Exploits CVE-2017-8225, released 4/25/2017
- Chinese manufacturer of a Wireless IP Camera (P2P) WIFICAM that allows for remote streaming

SCOPE:

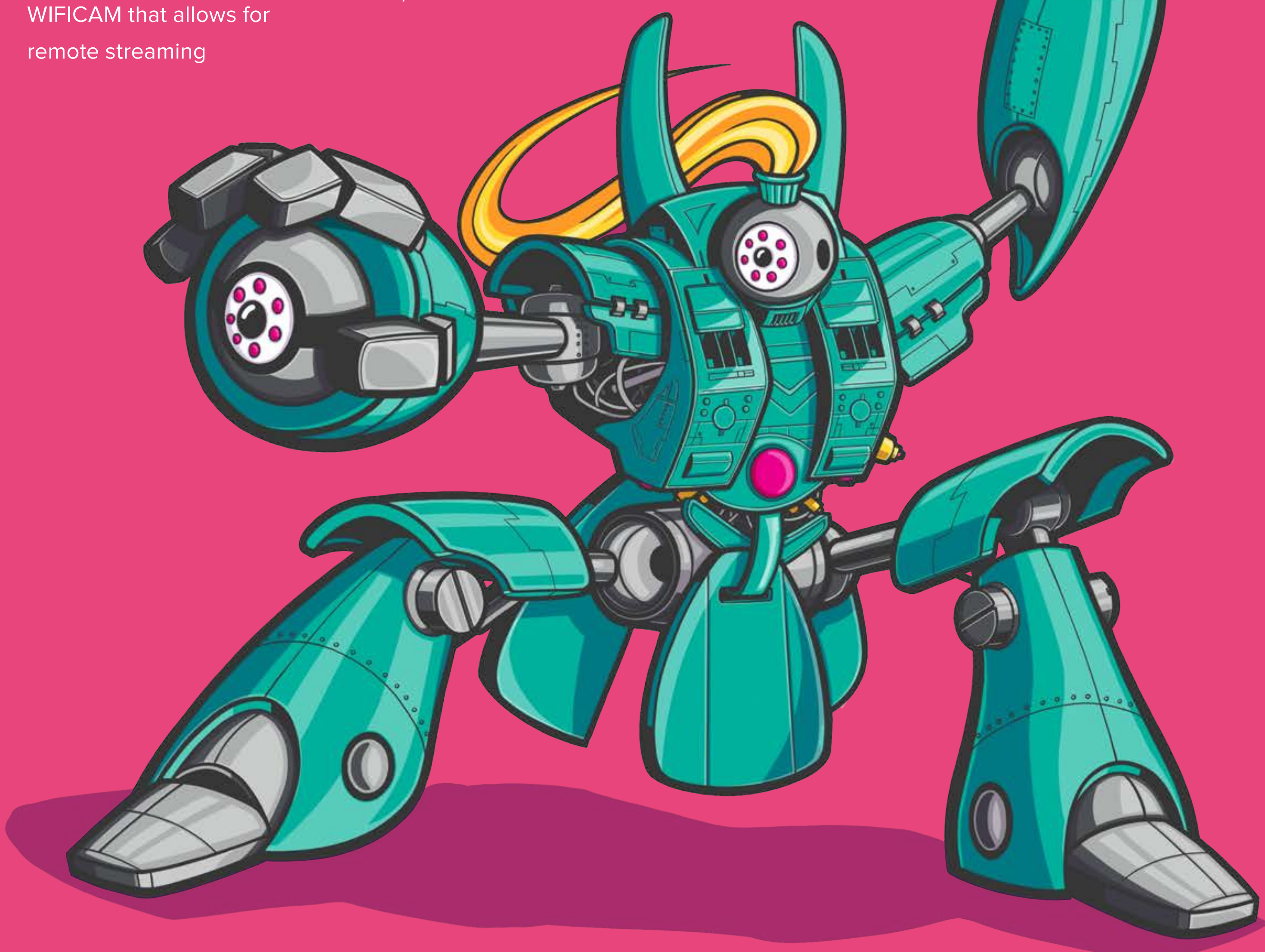
At least 1,250 IP camera models affected

INFECTED HOSTS AS OF 06/30/2017:

600,000

SHARES:

- Mirai code (scanning for growth techniques)
- Mirai C&Cs



GLOBAL MAPS OF PERSIRAI THINGBOT ACTIVITY

The following maps display the location of Persirai-infected systems (that is, IP-based cameras), (shown in green) and their controlling C&C servers (shown in yellow). As with Mirai, this data is based on latitude and longitude coordinates of systems, so the map locations are precise.

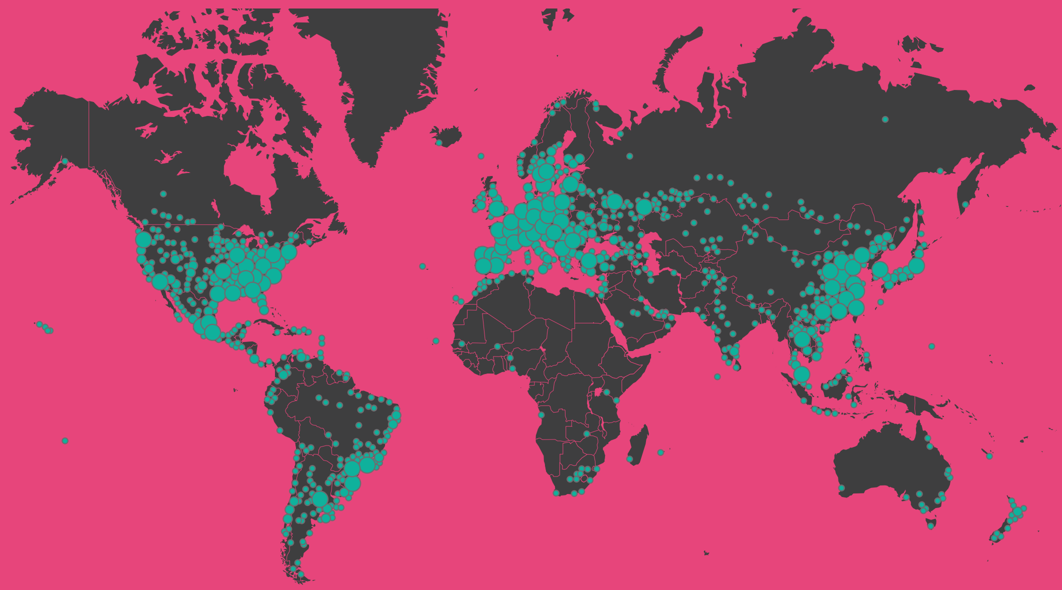


Figure 10: Persirai-infected IP cameras, June 2017

Figure 10 shows the heaviest concentration of infected systems (IP-based cameras) in the US, Europe, and southeast Asia.

Persirai C&C servers exist across the globe (see Figure 11), with the heaviest concentrations in the UK, Italy, and Turkey, as well as southeastern Australia and Brazil.

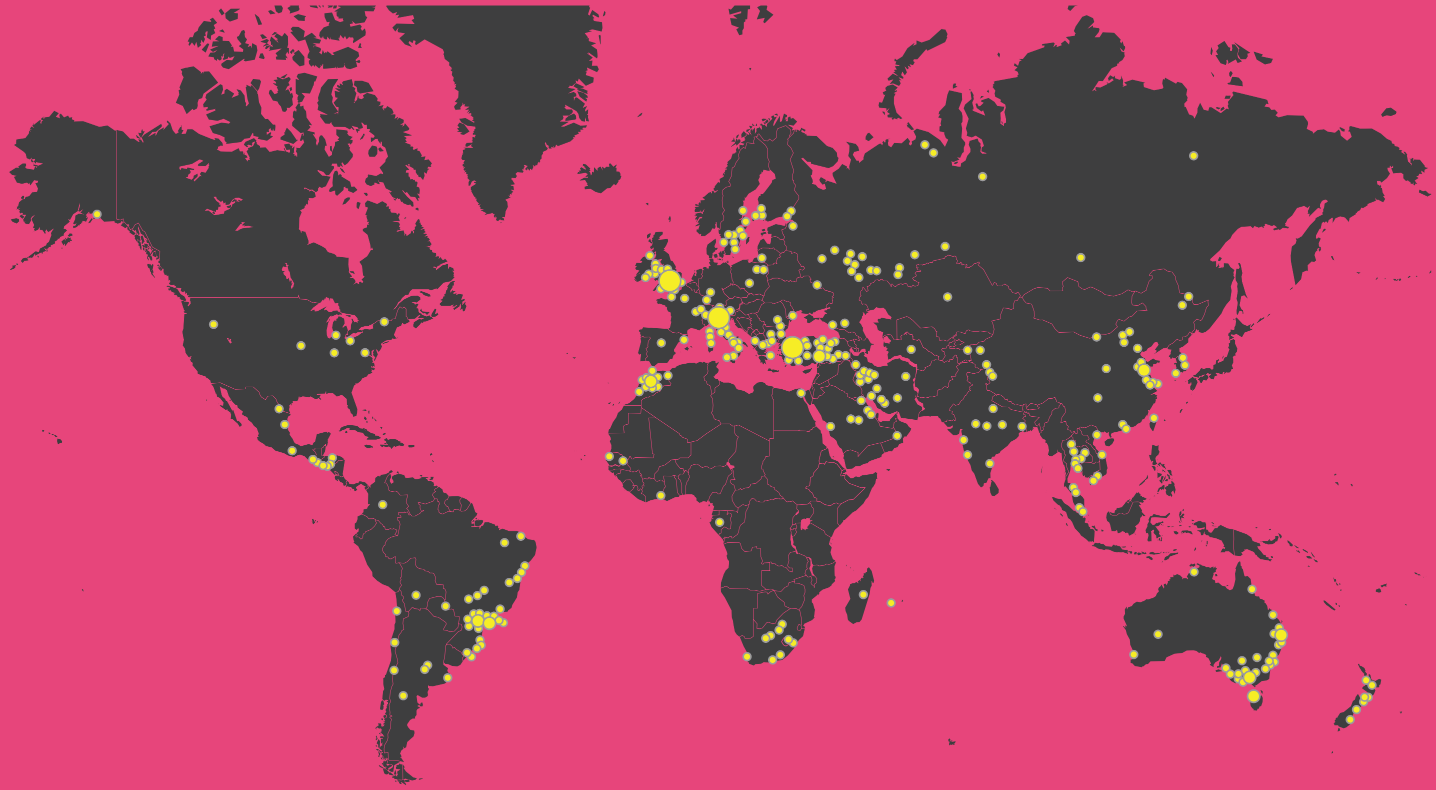


Figure 11: Persirai C&C servers, June 2017

Persirai's presence in North America is primarily seen in infected IP-based cameras (shown in green in Figure 12), however, there are also nine C&C servers (shown in yellow) in the US, four in Mexico, two in Guatemala, two in El Salvador, and two in Honduras.

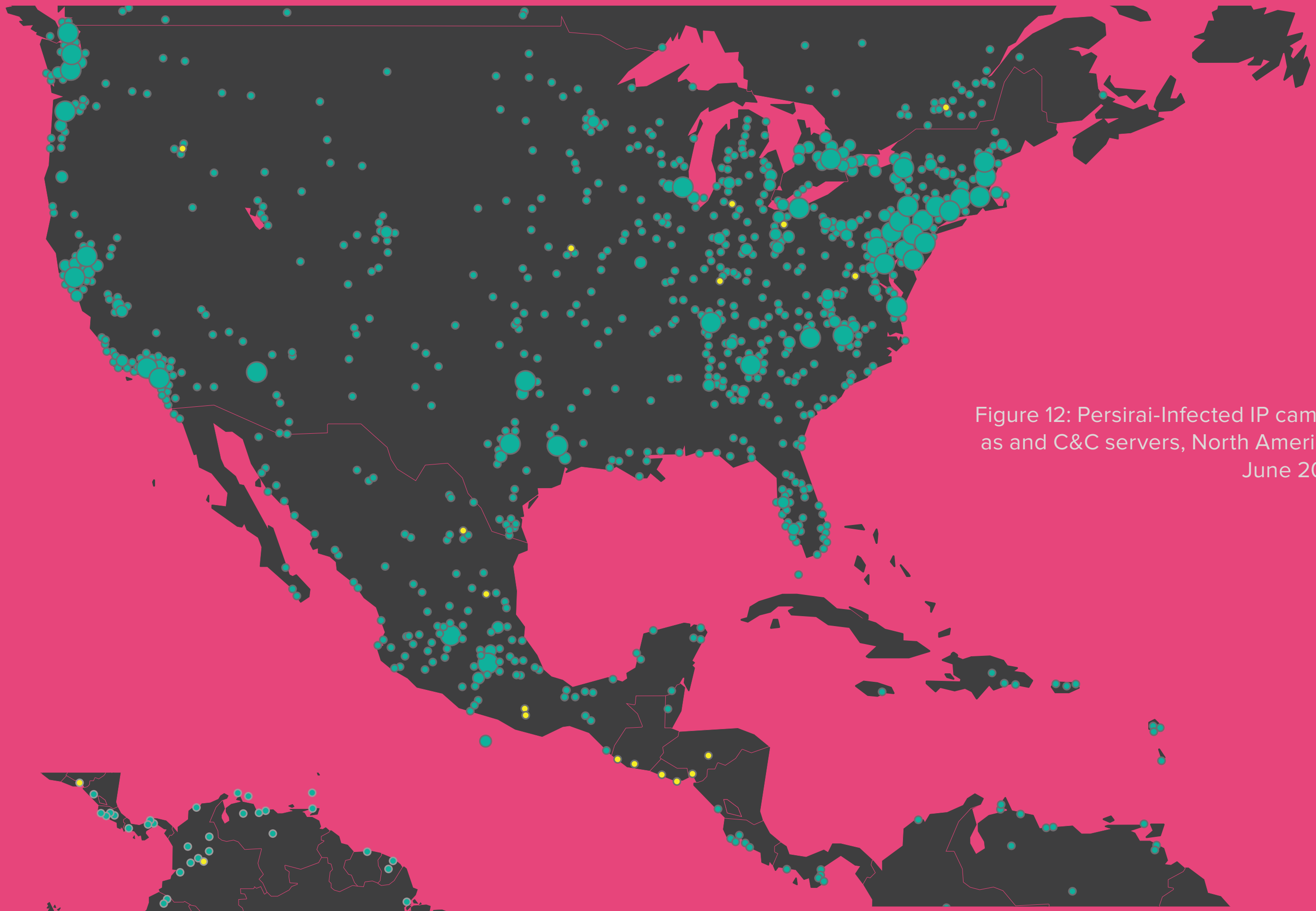
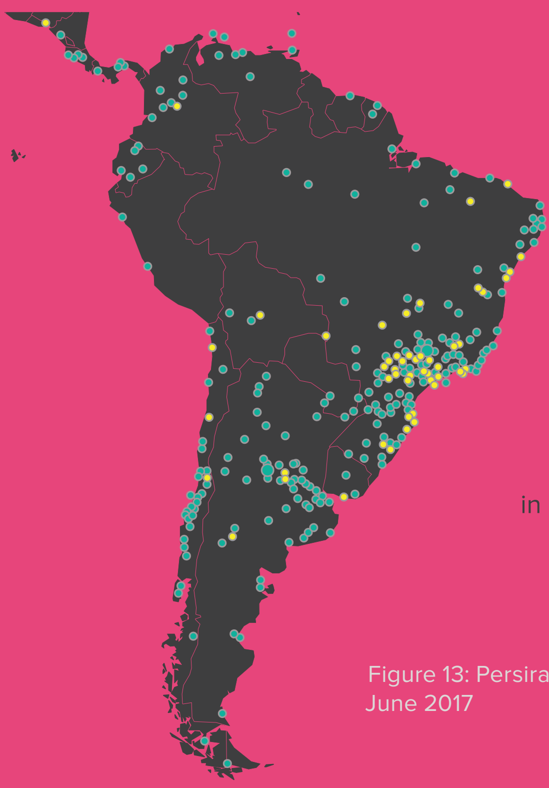


Figure 12: Persirai-Infected IP cameras and C&C servers, North America, June 2017



South American Persirai infections (shown in green in Figure 13) are heavily concentrated in Chile and the São Paulo and Rio De Janeiro municipalities of Brazil. Most C&C servers (shown in yellow) in South America are in São Paulo.

Figure 13: Persirai-infected IP cameras and C&C servers, South America, June 2017

Europe has the most Persirai activity in the globe, with a heavy concentration of infected IP-based cameras (shown in green in Figure 14) across the UK, France, Belgium, Netherlands, Switzerland, Italy, Denmark, and Poland. C&C servers in Europe (shown in yellow) are most prevalent in the UK, Italy, and Turkey.

Figure 14: Persirai-infected IP cameras and C&C servers, Europe, June 2017

Persirai-infected IP cameras (shown in green) exist all across Asia with the heaviest concentrations in Thailand, China, South Korea, Japan, Taiwan and Malaysia (see Figure 15). C&C servers (shown in yellow) also exist across Asia, however most are in China, India, and Thailand.

Figure 15: Persirai-infected IP cameras and C&C servers, Asia, June 2017

TELNET BRUTE FORCE ATTACKS

As we've done in our previous two reports, we continue to monitor attackers' scans for devices that use Telnet as their remote administration method. Telnet is used by literally billions of IoT devices, so it's no surprise that attackers are scanning for them. From January 1 to June 30, 2017, 30.6 million IoT brute force attacks were launched (see Figure 16). That's a 280% increase in attacks over the prior period of July 1 through December 31, 2016, which was already bloated due to the launch of Mirai in September and October and the resulting growth activity.

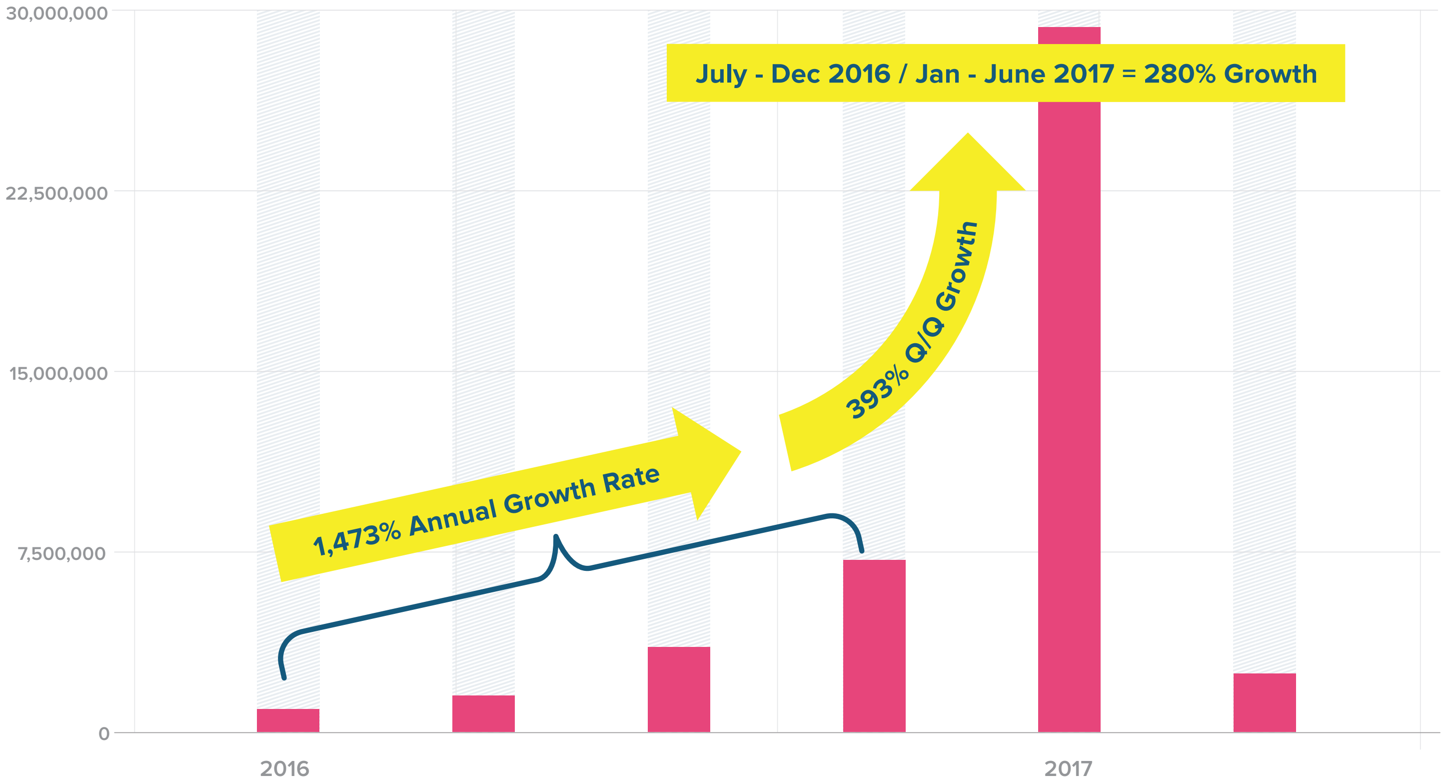


Figure 16: Historical view of IoT attack growth by quarter, January 2016 through June 2017

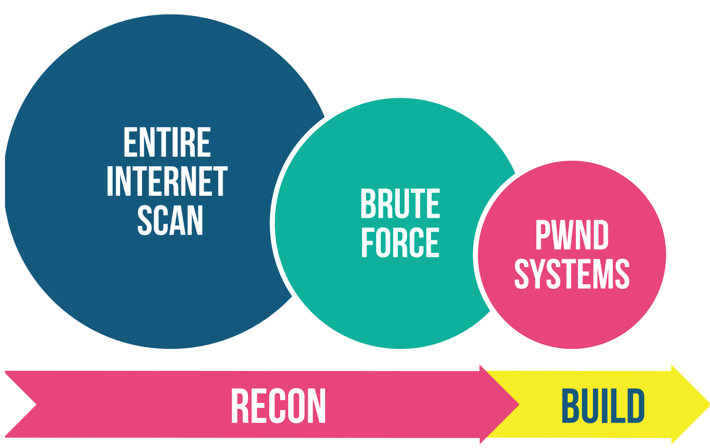


Figure 17: Typical bot-building attack phases

When looking at the attack volumes by month, we see an activity pattern that is typical of the attacker's reconnaissance phase: scanning large portions of the Internet (if not, the entire Internet) looking for vulnerable devices. These broad scans are followed by smaller, more precise scans, and ultimately, the brute forcing of credentials and installation of malware to build botnets. For simplicity, we break the typical bot-building attack phases down into recon and build (see Figure 17).

The expected pattern of attacker activity matched the attack activity we saw when looking at the Telnet attack volume by month (see Figure 18). Note that Mirai was built with a relative low level of activity compared to what we've seen since. This activity should be viewed as a precursor to attacks (as we warned pre-Mirai in our Volume 1 report, *DDoS's Newest Minions: IoT Devices*).[20] It indicates that one or more very large cyber weapon are being built, and since we haven't seen a large-scale attack since Mirai, it's likely a large thingbot (or potentially multiple thingbots) is already "loaded and ready to fire."

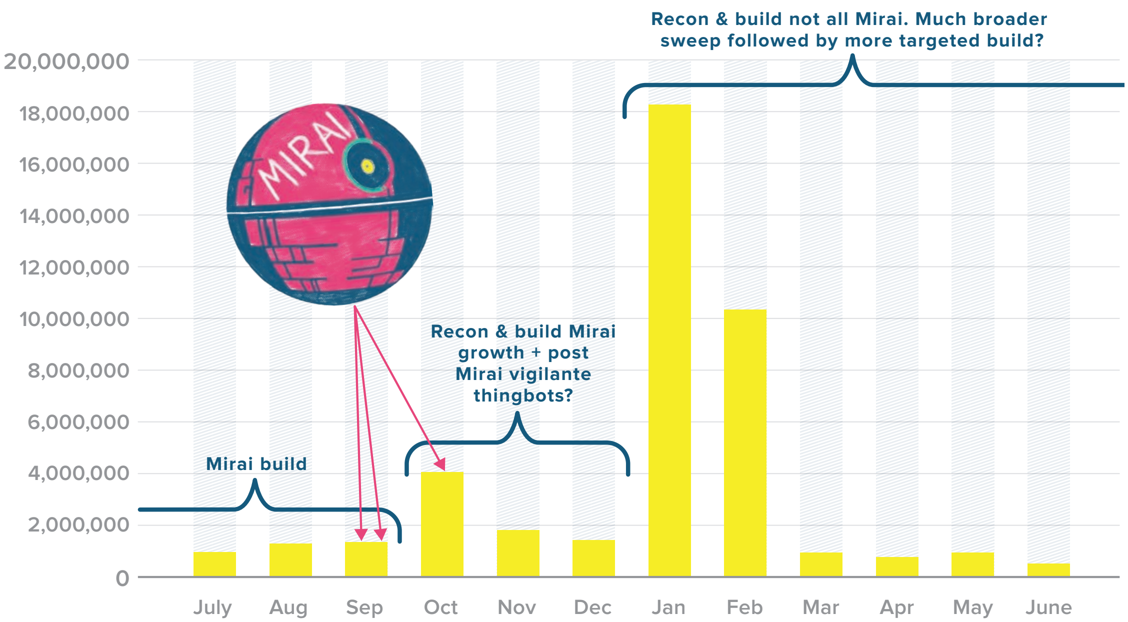


Figure 18: Pattern of IoT attacks by month

The so-called "vigilante" thingbots referenced in Figure 18 include those like Hajime or BrickerBot.[21] They were launched post-Mirai in a gray hat effort to take out IoT devices before they could be infected and weaponized by Mirai. BrickerBot is a Permanent Denial-of-Service (PDoS) thingbot that destroys the IoT device permanently. The device will no longer function, let alone become infected again. Hajime infects an IoT device and blocks it from a Mirai infection but, like Mirai, a simple reboot is all that's needed to reset the device to factory default settings, making it infectible again.

As researchers, we have been asking ourselves, why the recent lull in Telnet activity? It could be that attackers have finished their recon phase and have moved on to the build phase (as shown in Figure 17), or that the activity in March through June was all precise attacks that compromised devices. A third option is that attackers were simply distracted by the Shadow Brokers' release of EternalBlue and the resulting zero-day exploits.[22]

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

[21] https://arstechnica.com/security/2017/04/brickerbot-the-permanent-denial-of-service-botnet-is-back-with-a-vengeance

[22] https://f5.com/labs/articles/threat-intelligence/cyber-security/nsa-cia-leaks-provide-a-roadmap-to-stealthier-faster-more-powerful-malware-like-sambacry-and-notpetya

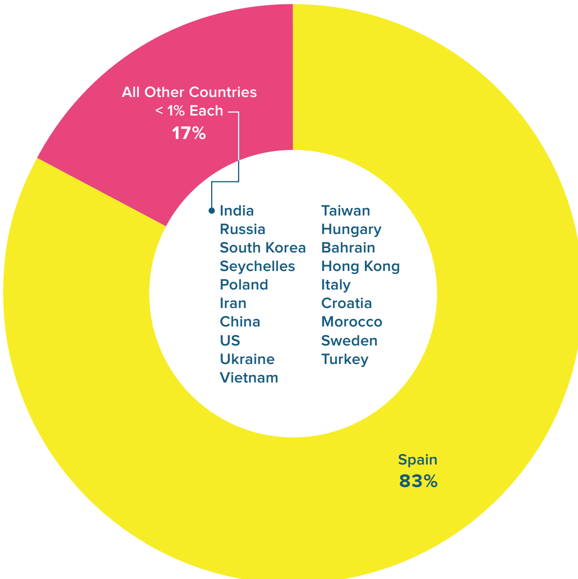


Figure 19: Top 20 threat actor source countries

TOP 20 THREAT ACTOR SOURCE COUNTRIES

Spain conducted 25.5 million attacks between January 1 and June 30, equating to 83% of the total attacks, all of which occurred over 15 days in late January to early February. Many other countries participated in attacks during the six-month period, however, none of their contributions to the total attack volume surpassed 1%.

The top 5 attacking countries were Spain, followed by India, Russia, South Korea, and the Seychelles. Most notable is China, which fell into the eighth position. Even with Spain launching such a massive amount of attacks and diluting the other countries' participation percentages, China still didn't launch anywhere close to the number of attacks it did in previous periods, leading us to wonder if China has been cleaning up infected IoT devices.

TOP 50 ATTACKERS BY IP ADDRESSES AND THEIR NETWORKS

A full 49 of the top 50 attacking IP addresses (based on count of attacks) from January 1 through June 30 were different than the those noted in the prior six-month period.[23] The fact that we are seeing "new" threat actors makes sense, given the large volume of (likely reconnaissance) scans that current threat actors would probably have completed already. The only consistent attacking IP and ASN (automated system number) in the top 50 list from the prior six-month period is Chinanet.

SOLOGIGABIT: STANDOUT THREAT ACTOR NETWORK

The standout threat actor in this period is a Spanish hosting provider called SoloGigabit (Figure 19). Ten SoloGigabit IP addresses accounted for 83% of the attacks launched from January 1 through June 30. Nine of the 10 IP addresses launched over one million attacks each, with the top IP owner launching over 5 million.

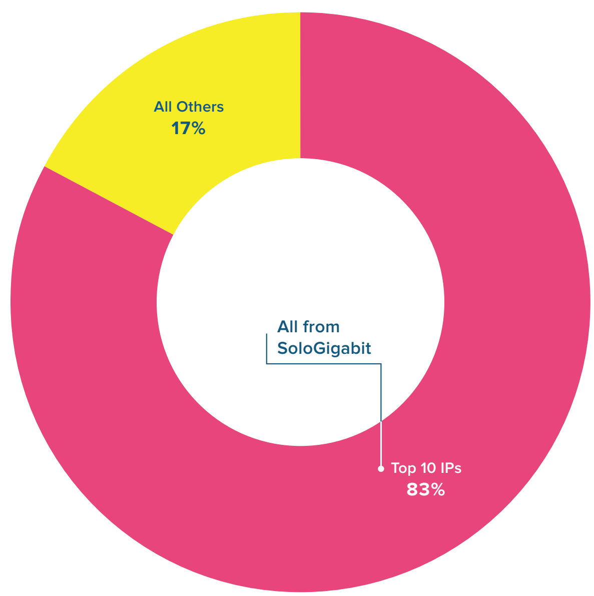


Figure 20: 10 SoloGigabit IP addresses launched 83% of attacks

[23] https://f5.com/labs/articles/threat-intelligence/ddos/the-hunt-for-iot-the-networks-building-death-star-sized-botnets-26796

Spain was a large destination country in the prior reporting period. We questioned whether this activity was infected devices that are now launching attacks themselves (thingbots build themselves through the devices they infect, so it's typical to see the attacked become the attacker). But, we would expect that type of activity to come from a telecom provider network with a large IoT installed base. Instead, SoloGigabit is a high speed—alleged bullet-proof—hosting provider network from which attackers might typically operate.

ATTACK PATTERNS AMONG THE TOP 10 ATTACKING IP ADDRESSES

We looked at the daily volume of attacks coming out of each of the top 10 IP addresses to see if there was a pattern. Each IP address began attacking on the same day—January 28—but all attacks ended on different days between January 29 and February 11. Each IP address followed a similar attack pattern, starting off small, peaking, and then trailing off (see Figure 20).

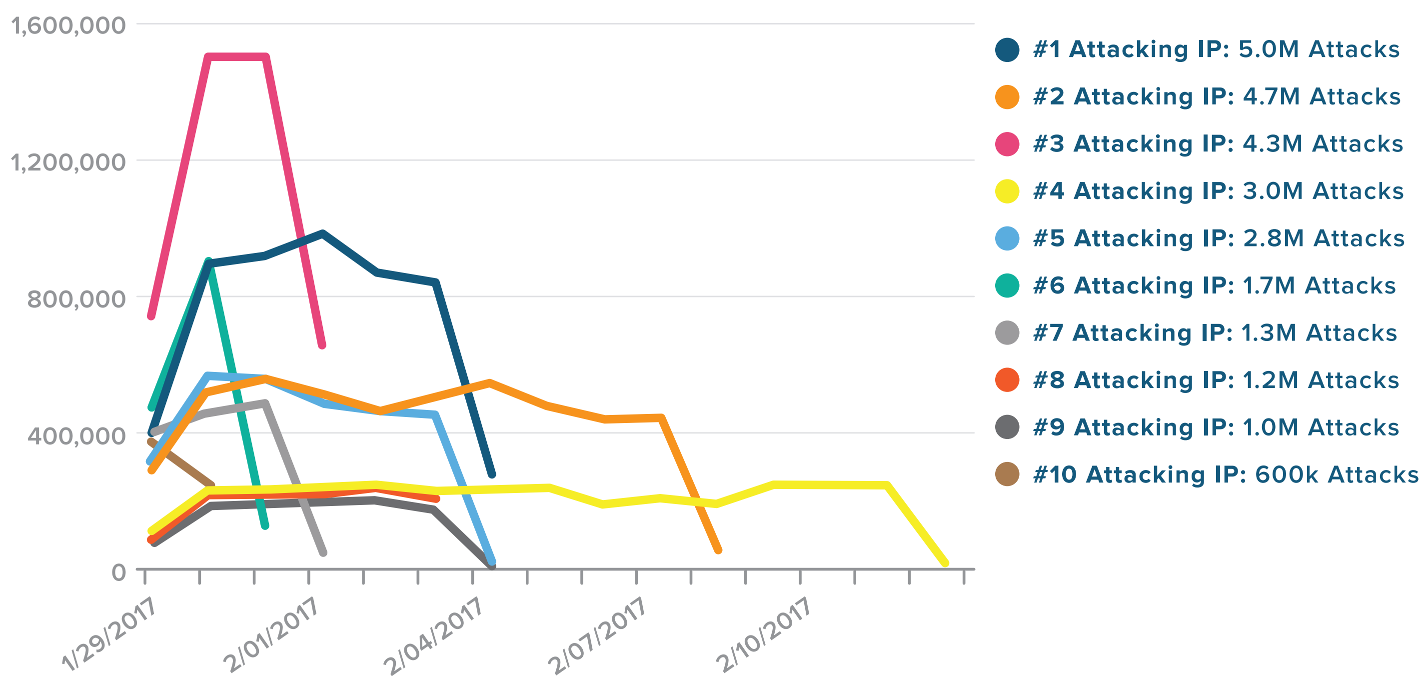


Figure 21: Attack patterns of top 10 IP addresses

COUNTRIES OF THE TOP 50 IP ADDRESSES

When looking at the number of IP addresses on the top 50 list by country, Russia had the most IP addresses on the top 50 list. This does not equate to count of attacks per IP address, however, because Spain launched 83% of the total attacks from 10 IP addresses. This is simply a count of IP addresses on the top 50 attackers list.

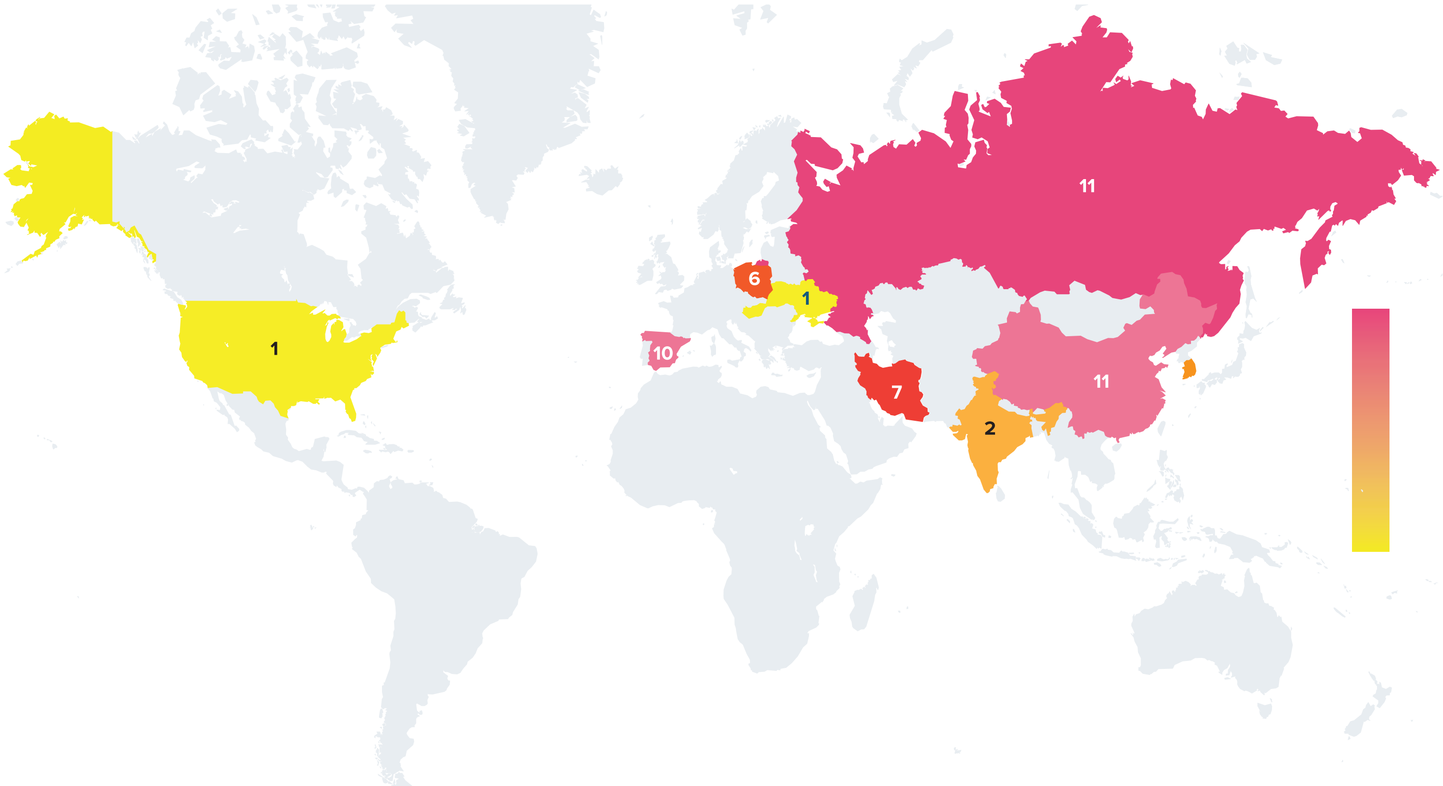


Figure 22: Countries where top 50 IP addresses reside

TOP 50 ATTACKING IP ADDRESSES AND ASNS

All IP addresses on the top 50 list outside of the top 10 contributed less than 1% to the total attack volume. Although insignificant to the overall attack volume, there were "new" threat actors in this reporting period, which is always a point of interest.

Tata Communications in India owns the #11 attacking IP address; Quasi Networks (also known as Ecatel, the notorious bulletproof hosting provider) that is now operating out of the Seychelles in Africa, owns the #12 attacking IP address; CityLine, an ISP in Russia owns the #13 IP address; and CariNet in the US owns the #14 attacking IP address. Integradesign in Poland owns 6 IP addresses on the top 50 list; Korea Telecom owns 4 IP addresses on the top 50 list; and Mobin Net in Iran, a WiMAX broadband operator, owns 7 IP addresses on the top 50 list. Together, these took the rest of the spots in the top 20.

Figure 23 below lists the top 50 attacking IP address owners as well as their respective ASNs, countries, and industries.

Position	ASN	ASN Owner	Country	Industry
1	AS56934	SoloGigabit, S.L.U.	Spain	Hosting
2	AS56934	SoloGigabit, S.L.U.	Spain	Hosting
3	AS56934	SoloGigabit, S.L.U.	Spain	Hosting
4	AS56934	SoloGigabit, S.L.U.	Spain	Hosting

Position	ASN	ASN Owner	Country	Industry
5	AS56934	SoloGigabit, S.L.U.	Spain	Hosting
6	AS56934	SoloGigabit, S.L.U.	Spain	Hosting
7	AS56934	SoloGigabit, S.L.U.	Spain	Hosting
8	AS56934	SoloGigabit, S.L.U.	Spain	Hosting
9	AS56934	SoloGigabit, S.L.U.	Spain	Hosting
10	AS56934	SoloGigabit, S.L.U.	Spain	Hosting
11	AS4755	TATA Communications	India	ISP/telecom
12	AS29073	Quasi Networks LTD (Ecatel)	Seychelles	Hosting
13	AS48909	CityLine	Russia	ISP/telecom
14	AS10439	CariNet, Inc.	US	Hosting
15	AS61154	Integra-design	Poland	Hosting
16	AS4766	Korea Telecom	South Korea	ISP/telecom
17	AS61154	Integra-design	Poland	Hosting
18	AS4766	Korea Telecom	South Korea	ISP/telecom
19	AS61154	Integra-design	Poland	Hosting
20	AS50810	Mobin Net	Iran	ISP/telecom
21	AS61154	Integra-design	Poland	Hosting
22	AS4766	Korea Telecom	South Korea	ISP/telecom
23	AS196739	Success Ltd	Russia	ISP/telecom
24	AS50810	Mobin Net	Iran	ISP/telecom
25	AS50810	Mobin Net	Iran	ISP/telecom
26	AS29124	Iskratelecom CJSC	Russia	ISP/telecom
27	AS50810	Mobin Net	Iran	ISP/telecom
28	AS4766	Korea Telecom	South Korea	ISP/telecom
29	AS29070	Morton-Telekom Ltd	Russia	ISP/telecom
30	AS45062	Netease Network	China	Hosting
31	AS50810	Mobin Net	Iran	ISP/telecom
32	AS61154	Integra-design	Poland	Hosting
33	AS3462	HINET-NET	Taiwan	ISP/telecom
34	AS51685	Micron-Media Ltd.	Russia	ISP/telecom
35	AS61154	Integra-design	Poland	Hosting
36	AS21228	Vinasterisk	Ukraine	ISP/telecom
37	AS42339	Chaika Telecom Petersburg Limited Company	Russia	Hosting
38	AS50810	Mobin Net	Iran	ISP/telecom
39	AS4816	Chinanet-Guangdong province network	China	ISP/telecom
40	AS56634	Fly-Tech Ltd.	Russia	ISP/telecom
41	AS4837	China Unicom Jilin province network	China	ISP/telecom
42	AS59533	Lukjanova Lydia Andreevna PE	Russia	ISP/telecom
43	AS58466	Chinanet	China	ISP/telecom
44	AS50810	Mobin Net	Iran	ISP/telecom
45	AS197112	Jacsa Net	Hungary	ISP/telecom

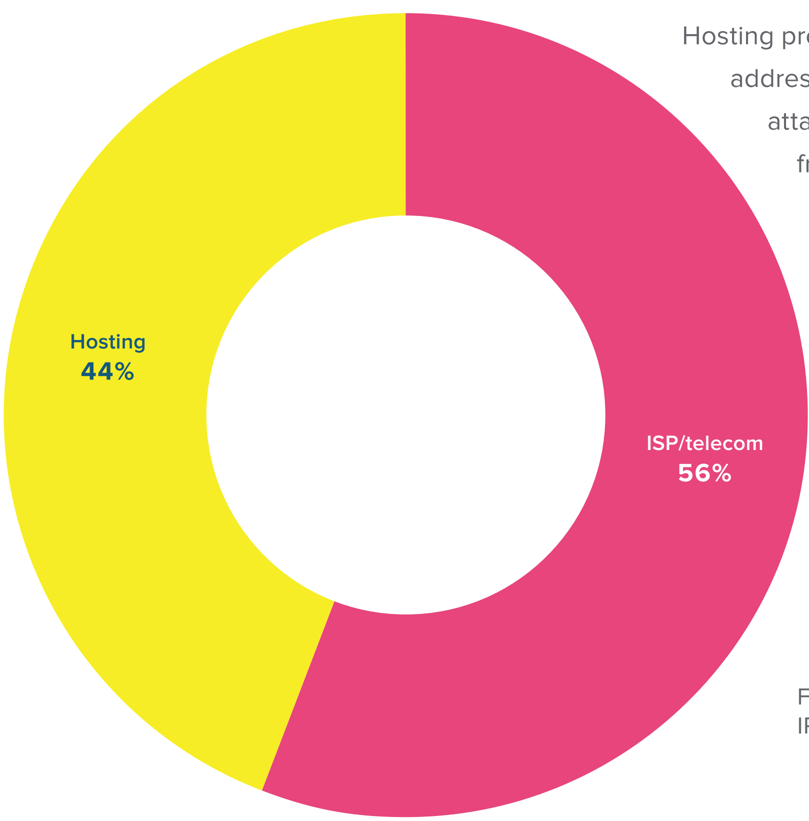
Position	ASN	ASN Owner	Country	Industry
46	AS197275	LINKTELECOM-NETWORK	Russia	ISP/telecom
47	AS45469	Elecon Information Technology Ltd	India	Hosting
48	AS29069	Morton-Telekom Ltd	Russia	ISP/telecom
49	AS39273	KALAAM TELECOM	Bahrain	ISP/telecom
50	AS39264	METROMAX-AS	Russia	Hosting

Figure 23: Top 50 attacking IP addresses, January 1 —June 30

Note: We will only disclose the source IP addresses to the network (ASN) owners.

TOP 50 ATTACKING IP ADDRESSES BY INDUSTRY

Figure 23 is driven by the data from Figure 22 and shows the industry breakdown of the top 50 attacking IP addresses. Not surprising, it is a mix of ISP/telecom providers and hosting companies.



Hosting providers make up 44% of the top 50 attacking IP addresses, however, they make up most of the period's attack volume, considering that 83% of attacks came from hosting provider, SoloGigabit. It's a safe bet to say that this is direct threat actor traffic rather than the ISP/Telecom traffic that's likely generated from compromised IoT devices.

Figure 24: Industries of the top 50 attacking IP addresses

MOST COMMONLY ATTACKED ADMIN CREDENTIALS

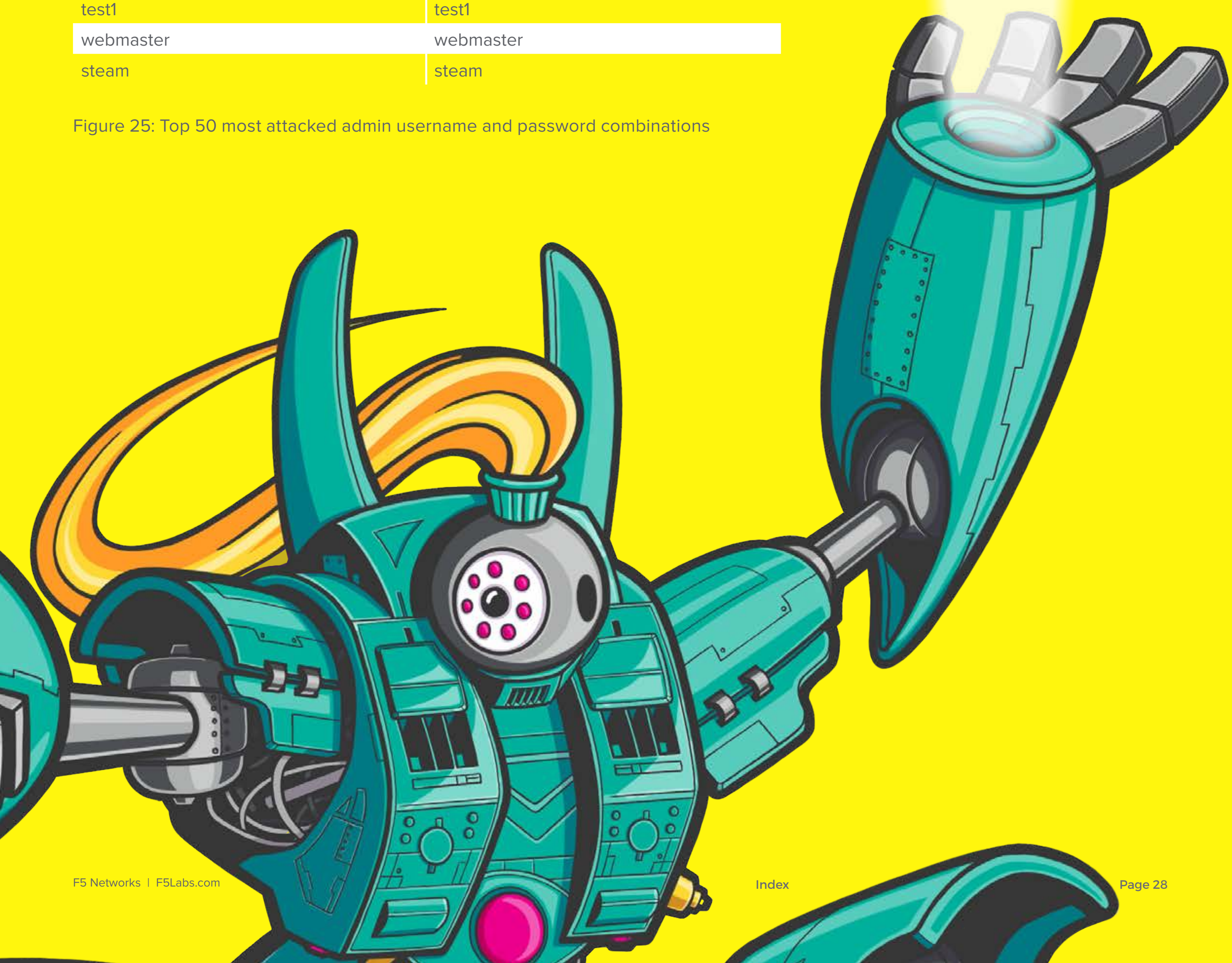
Due to the glaring access control challenges that need to be addressed within IoT devices—including their wide-open Telnet port access to the entire Internet, lack of brute force restrictions, and simple username and password "protections" for administrator access—we include the list of top 50 most attacked admin username and password combinations (see Figure 24). We are disclosing the top 50 list in hopes that IoT developers and manufacturers will start to change these utterly basic and easy-to-guess credentials (which all bad actors can easily obtain on the dark web, anyway), and never use them again.

Username	Password
support	support
root	root
admin	admin1
ubnt	ubnt
usuario	usuario
pi	raspberry
user	user
guest	guest
mother	f__ker
test	test
operator	operator
oracle	oracle
ftp	ftp
git	git
ftpuser	ftpuser
postgres	postgres
nagios	nagios
ubuntu	ubuntu
tomcat	tomcat
osmc	osmc
1234	1234
service	service
default	default
mysql	mysql
monitor	monitor
testuser	testuser
demo	demo
www	www
manager	manager
vagrant	vagrant
jenkins	jenkins
teamspeak	teamspeak

94%
SAME PASSWORD AS THE USERNAME

Username	Password
minecraft	minecraft
PlcmSplp	PlcmSplp
info	info
apache	apache
deploy	deploy
nobody	nobody
vnc	vnc
zabbix	zabbix
cisco	cisco
backup	backup
csgoserver	csgoserver
centos	centos
hadoop	hadoop
0	0
a	a
test1	test1
webmaster	webmaster
steam	steam

Figure 25: Top 50 most attacked admin username and password combinations



CONCLUSION

Gartner estimates 63% of in-use IoT devices in 2017 are consumer products, the "audience" that's least capable of doing something about a device's inherent vulnerabilities.[24] Even with proper instruction, most devices weren't designed to accept admin credential changes, so a responsible owner of a home-use IoT device couldn't do the right thing if they knew how.[25] Nevertheless, this IoT problem needs proper attention that certainly will not be solved in the short term. Product fixes and recalls can be extremely costly for IoT manufacturers and developers, and global legislation would require coordinated efforts on a scale the world has never seen. So, now is the time to act on behalf of your business before another Death Star-sized attack is launched. Our recommendations—some reiterated from previous reports—are still timely and relevant:

- **Have a DDoS strategy in place**, whether it's an on-premises, cloud-based, or hybrid solution.
- **Ensure critical services have redundancy.** You aren't always the direct target. Plan ahead for downstream impact if your service provider is attacked.
- **Purchase wisely**; money talks! Don't buy, deploy, or sell vulnerable IoT devices. They could become cyber weapons that turn around and attack businesses. Do your homework before you purchase. If you are conducting due diligence with your IoT manufacturers, use the checklist below when questioning their secure development practices.

Additionally, talk about the threat of IoT devices to your employees, both on a personal and business level. The more awareness consumers have about IoT threats in general, the less likely they are to buy known vulnerable devices, or become victims of attacks.

If you haven't already, look into implementing credential stuffing solutions. IoT hacks provide just one more way for attackers to collect users' business account credentials.

If you are developing IoT products, you should immediate begin doing the following:

1. Make security planning, design, and testing a required part of your software development lifecycle. Never assume your device won't be a hacking target. Follow the threat modeling frameworks and materials on OWASP.[26]
2. Do not allow basic credentials to be set for admin accounts.
3. Do not allow brute force attacks! Rate-limit connections or set account lockouts after failed login attempts.
4. If you must use Telnet for remote administration, restrict Telnet access to within your management network; never allow admin connections from any location on the Internet!

---

[24] http://www.gartner.com/newsroom/id/359891 7

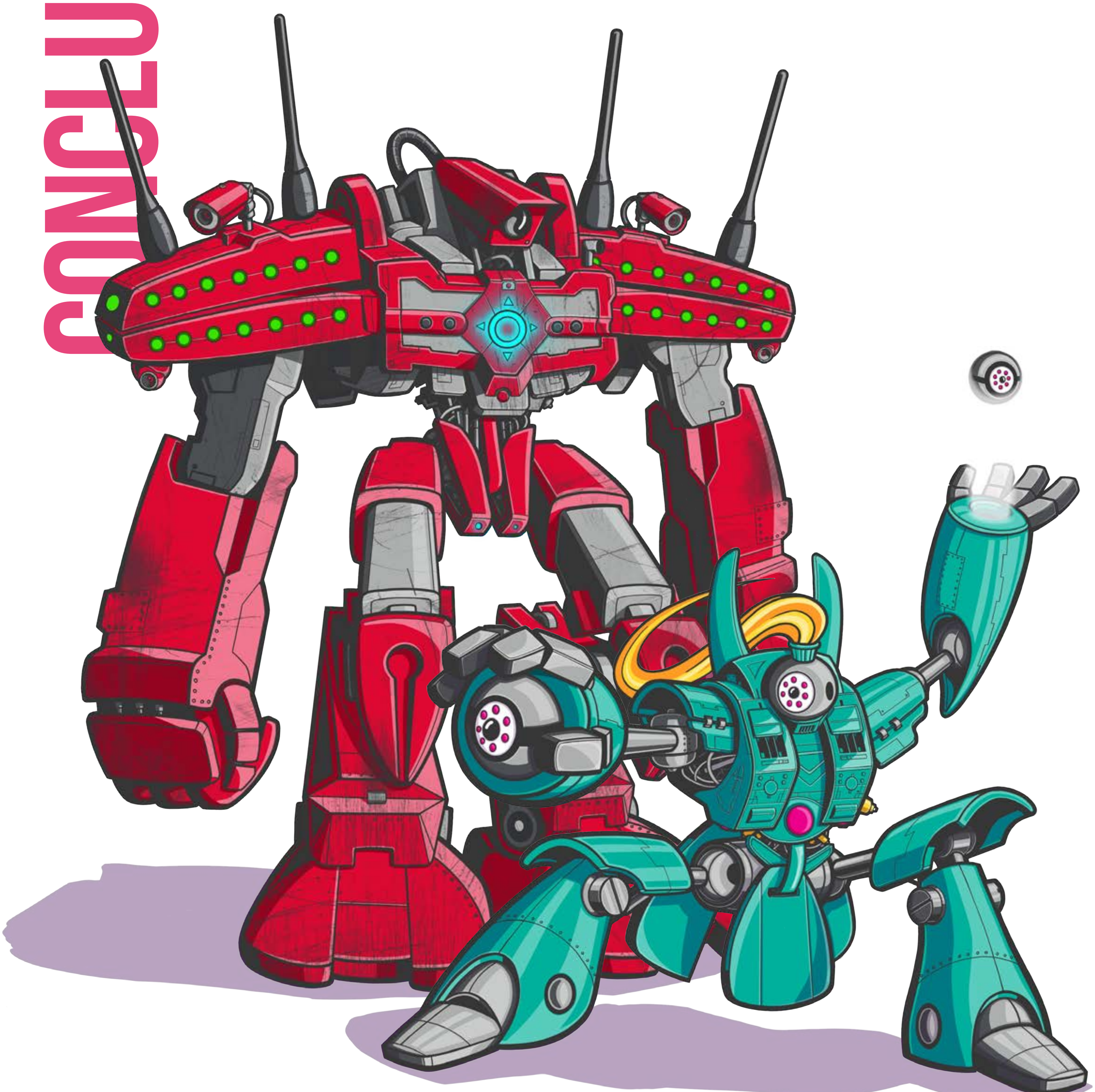
[25] https://f5.com/labs/articles/threat-intelligence/cyber-security/default-passwords-are-not-the-biggest-part-of-the-iot-botnet-problem

[26] https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

CONCLUSION

5. If possible, implement antivirus solutions on devices so they cannot be infected with common malware. This should be a must for devices that perform critical functions and also have high bandwidth capacity. These devices are highly valuable targets and are therefore more likely to be targeted.

6. Allow for firmware updates. Don't be caught unprepared when a vulnerability disclosure comes out and you have no way to fix it other than to recall the product.



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

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