ARBOR NETWORKS
The Security Division of NETSCOUT

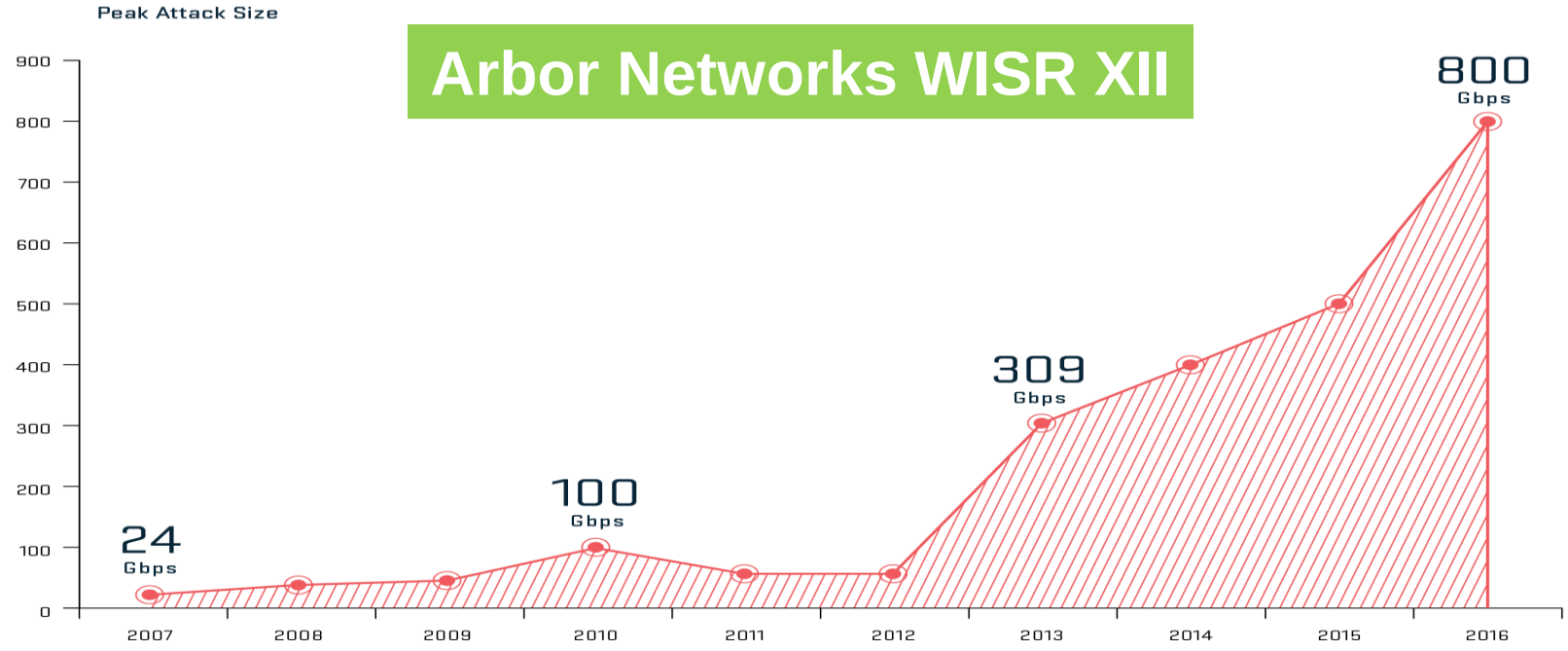
IoT - Next Wave of DDoS?

IoT Sourced DDoS Attacks

A Focus on Mirai Botnet and Best Practices in DDoS Defense

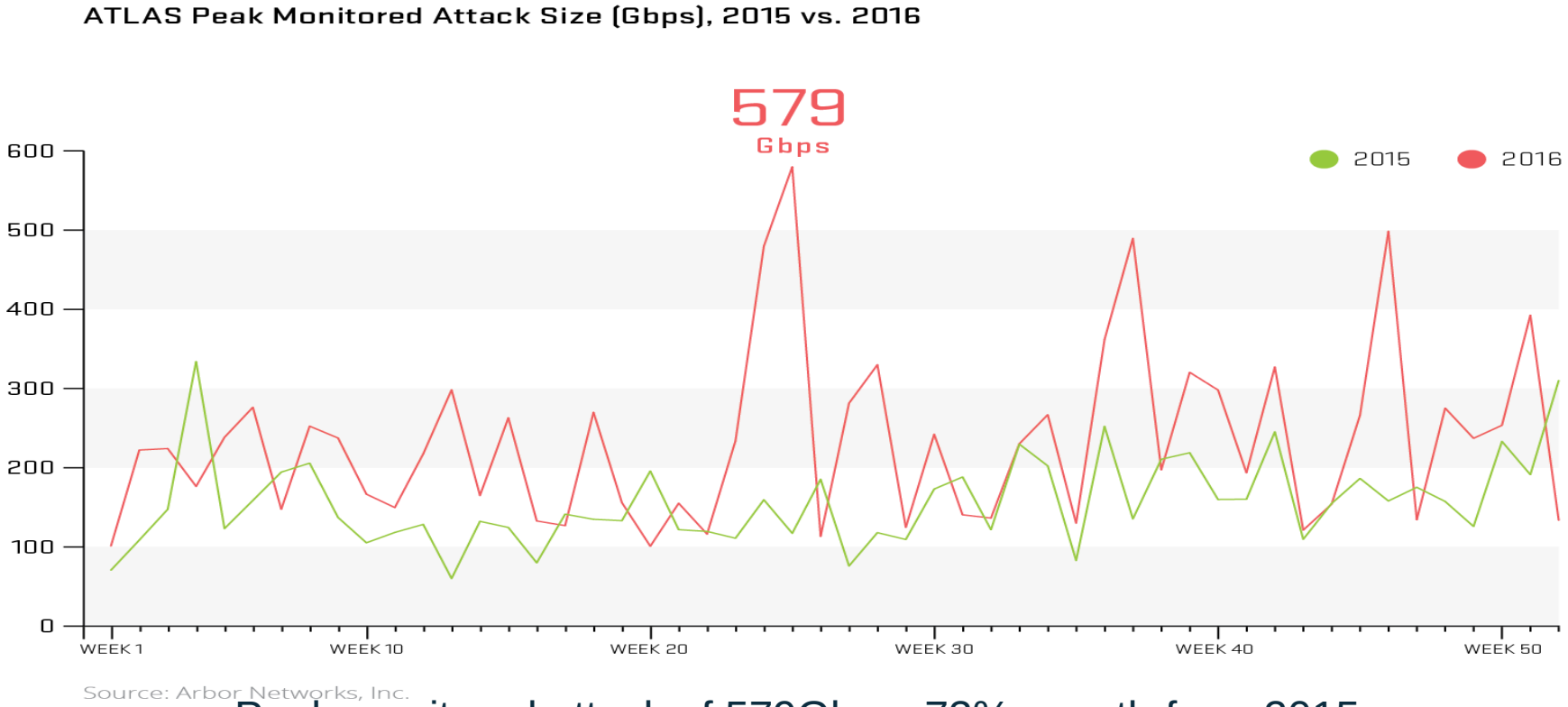
DDoS Attacks Increasing in Size, Frequency & Complexity

Arbor Networks WISR XII



- Largest attack reported was 800 Gbps with other respondents reporting attacks of 600 Gbps, 550 Gbps, and 500 Gbps
- One third of respondents report peak attacks over 100Gbps
- 41% of EGE respondents and 61% of data-center operators reported attacks exceeding their total Internet capacity

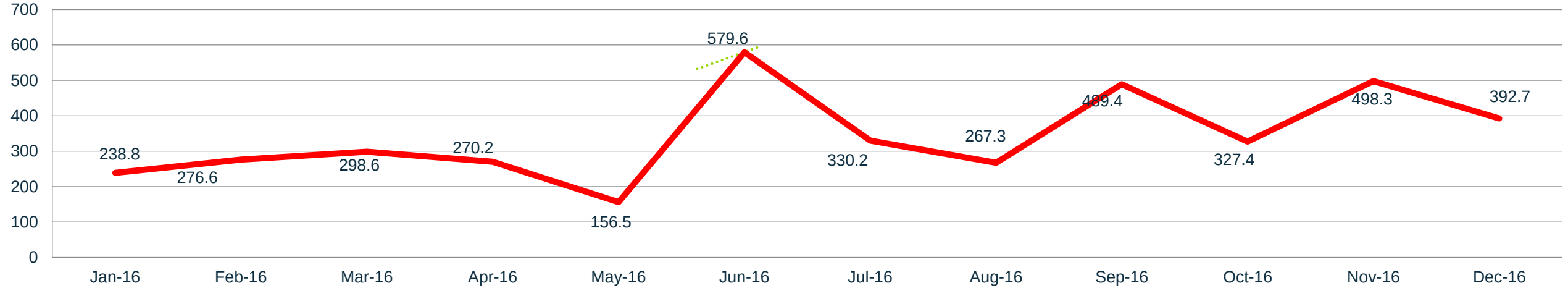
Arbor Networks ATLAS DDoS statistics



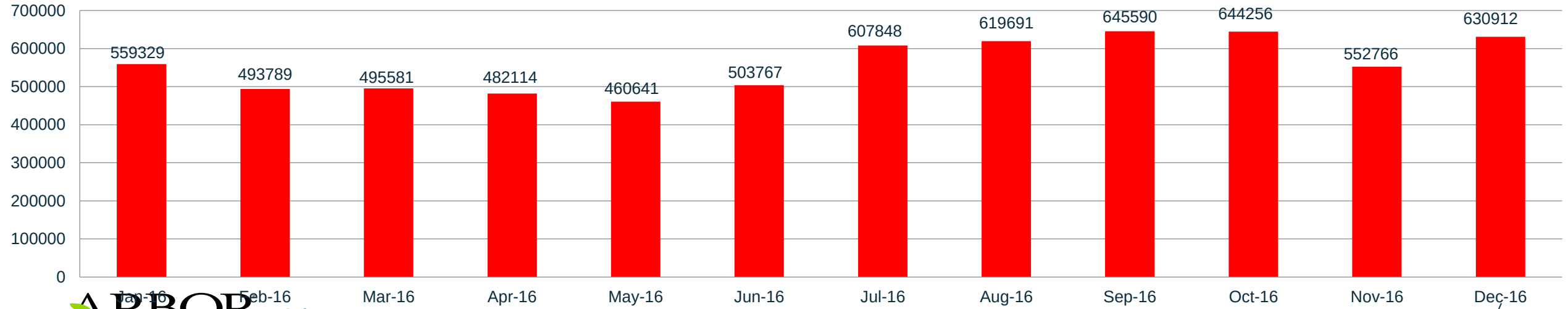
- Peak monitored attack of 579Gbps, 73% growth from 2015
- 558 attacks over 100Gbps, 87 over 200Gbps
  - Compared to 223 and 16 in 2015
- 20% of attacks over 1Gbps, as opposed to 16% in 2015
- Average attacks size now 931Mbps, up from 760Mbps, a 23% increase

DDoS Attack Trends

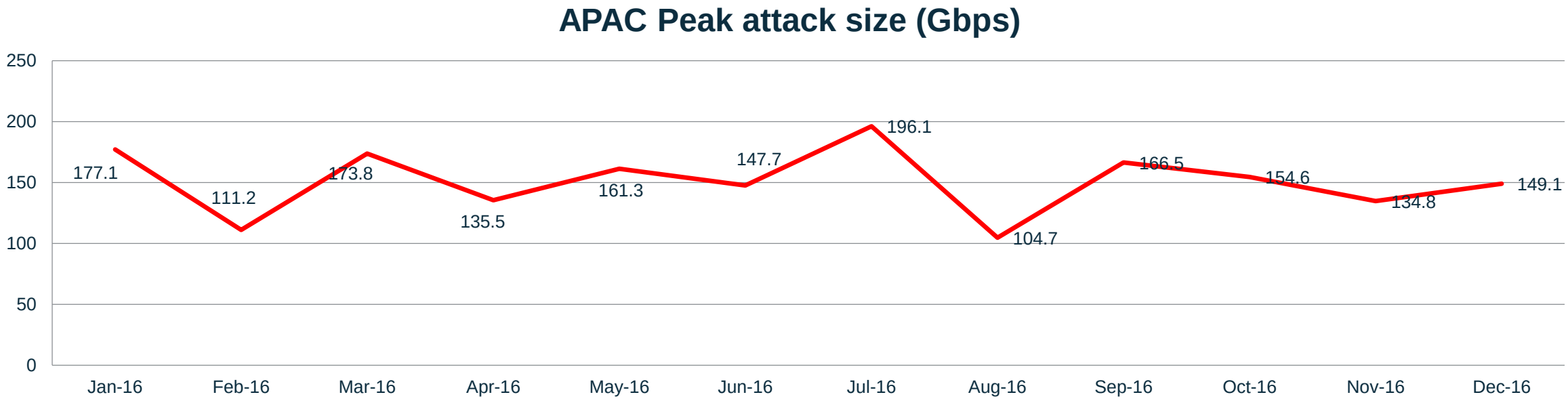
Worldwide Peak attack size (Gbps)



no of DDoS attacks

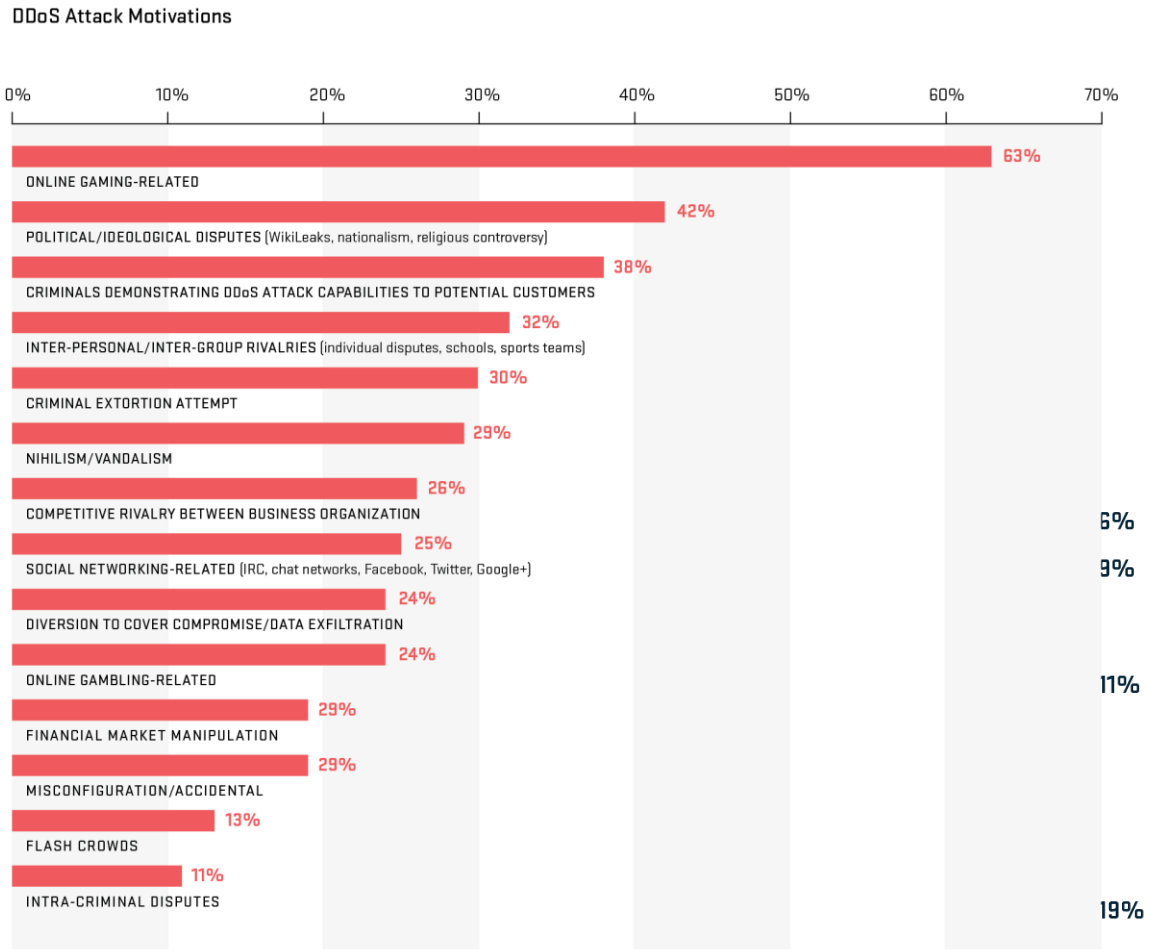


DDoS Attack Trends



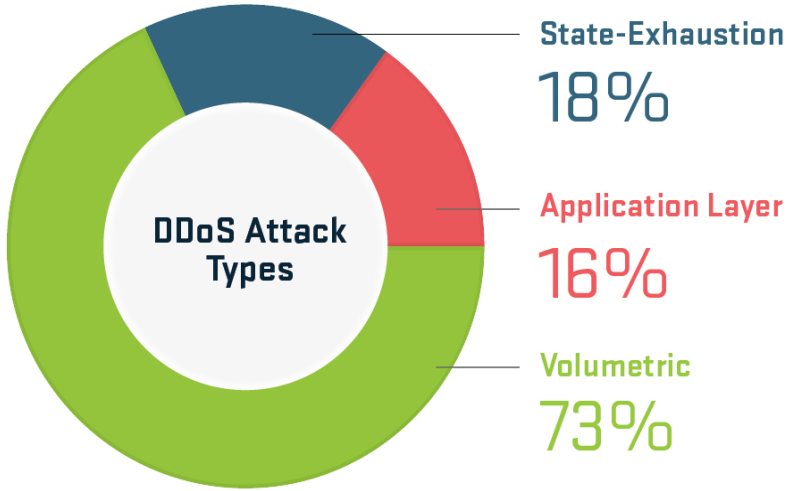
Year 2016	Global	APAC
Peak attack size	579.59 Gbps	196.06 Gbps
Average attack size	931.24 Mbps	623.82 Mbps
Average duration	55 min 20 sec	45 min 6 sec
Attack dest port	TCP/80	TCP/80
Top reflection attack type	DNS	DNS

WISR XII DDoS trend



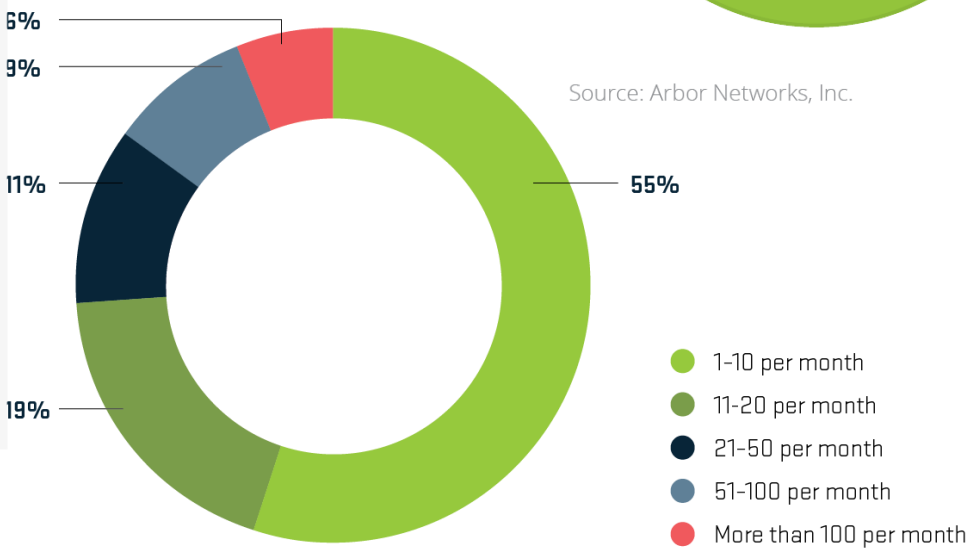
Source: Arbor Networks, Inc.

Service Provider Attack Types



Source: Arbor Networks, Inc.

DDoS Attack Frequency Per Month

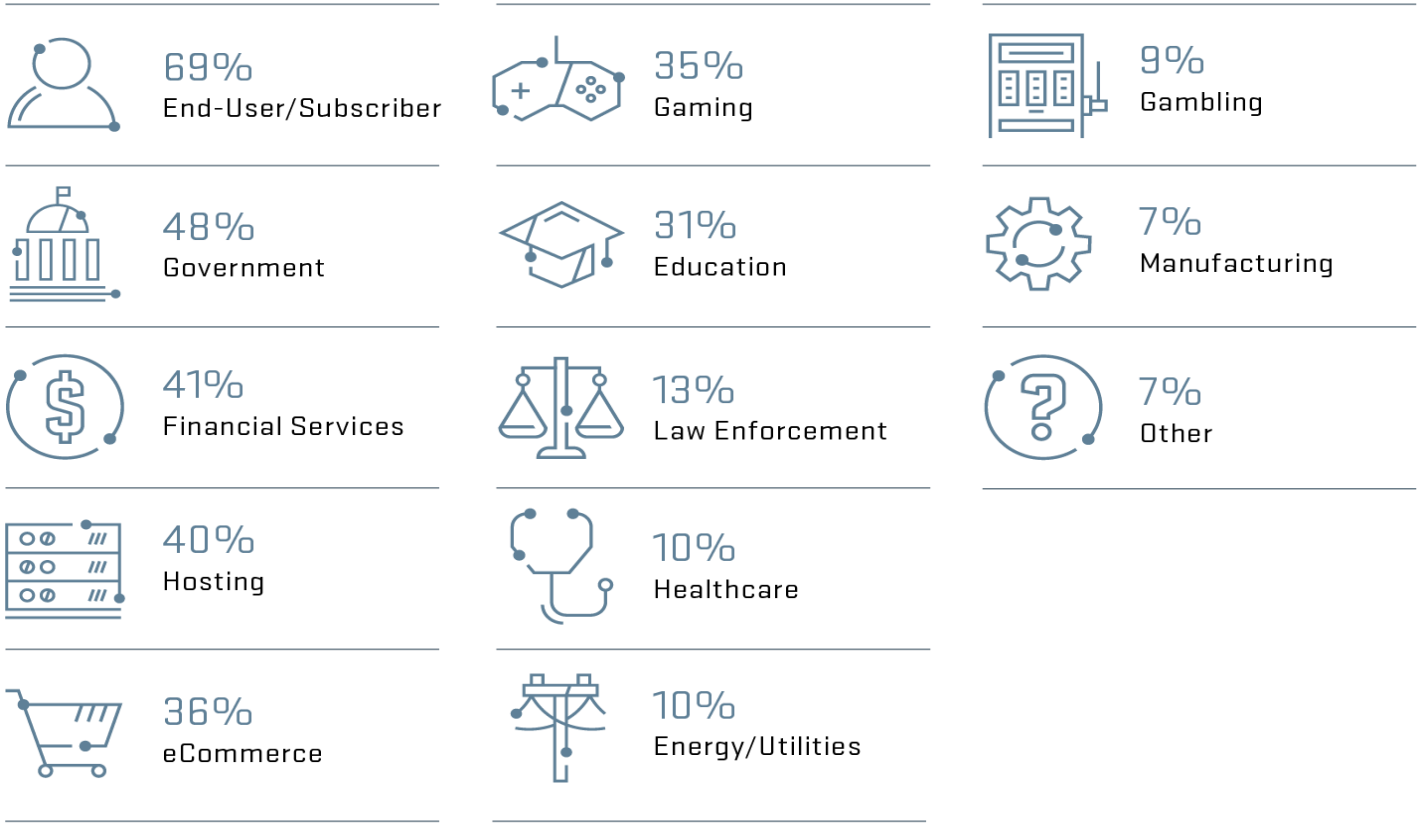


Source: Arbor Networks, Inc.

DDoS Targets

- SPs see Government, Finance and Hosting as top targets
- SPs seeing attacks on cloud services drops from one third to one quarter
- 42% of EGE respondents experienced an attack
  - 63% of finance, up from 45%
  - 53% of government, up from 43%

Attack Target Customer Verticals

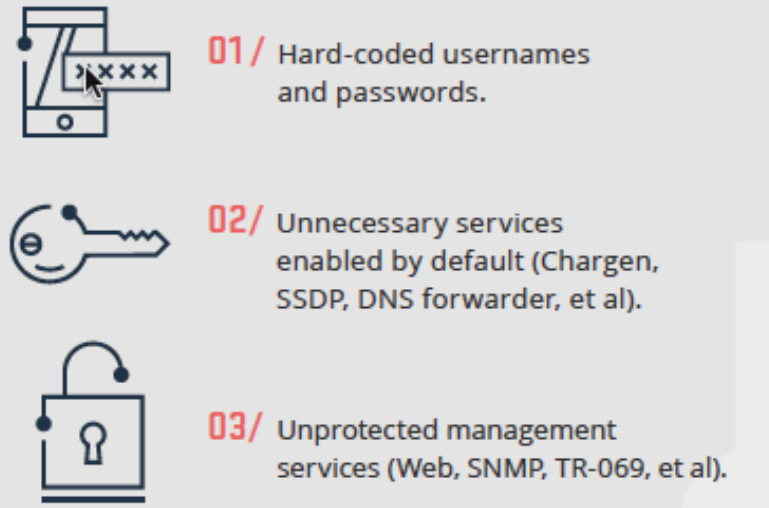


Source: Arbor Networks, Inc.

DDoS driving factors - IoT

The Problem

- Almost every piece of technology we buy is ‘connected’
- Devices are designed to be easy to deploy and use, often resulting in limited security capabilities
- Software is very rarely upgraded. Some manufacturers don’t provide updates, or the ability to install updates



The Result

- First high-profile attack using IoT devices Christmas 2013, using CPE and webcams
- In 2016 Botnet owners started to recruit IoT devices en mass
- Attacks of 540Gbps against the Olympics, 620Gbps against Krebs, Dyn etc..

DDoS driving factors – DDoS as a service

Fact: It's Never Been Easier to Launch a DDoS Attack. DDoS attack tools and DDoS for Hire Services add to the weaponization of DDoS.

$5:$100sK

Cost of DDoS Service — Impact to Victim

DDoS Attacks Are The Great Equalizer…

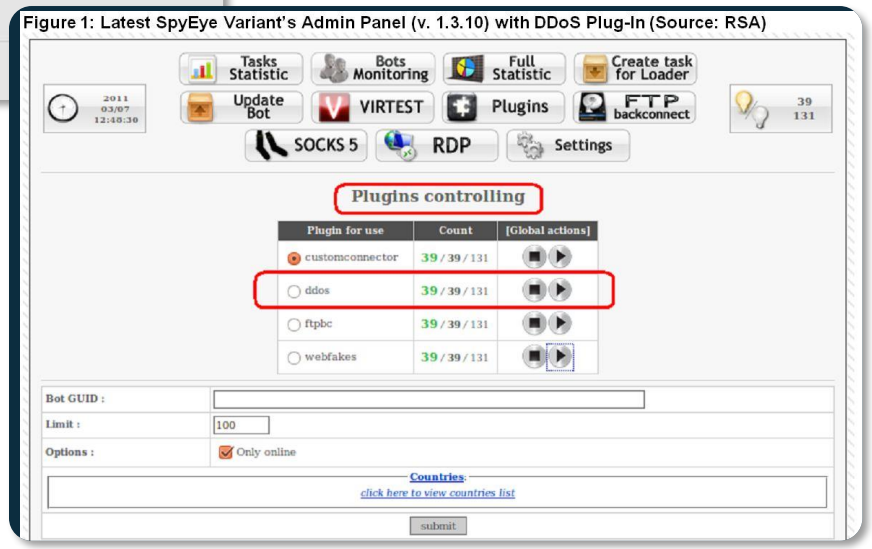
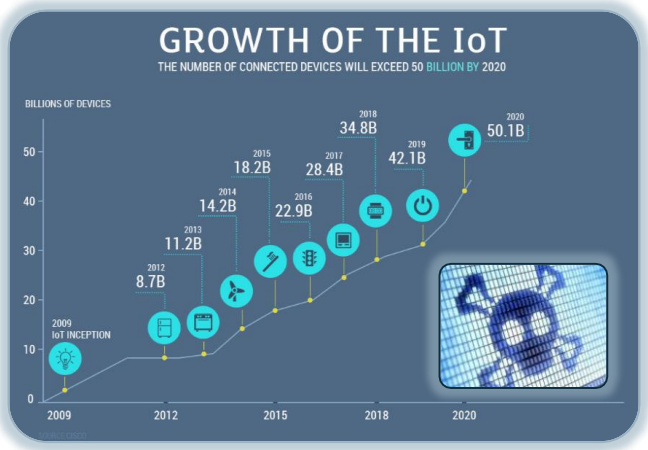


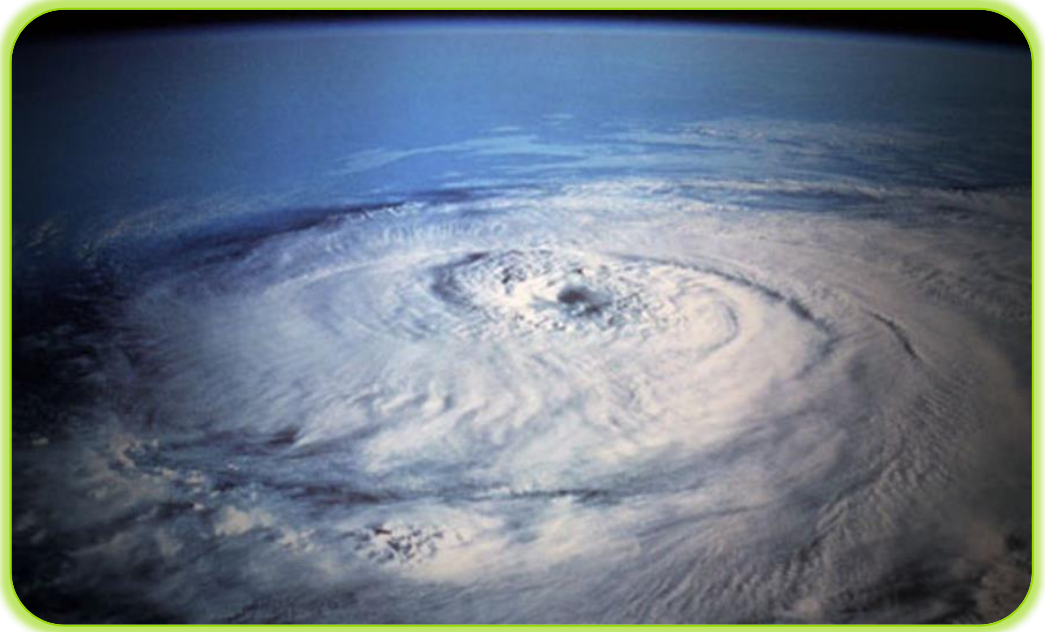
Figure 1: Latest SpyEye Variant's Admin Panel (v. 1.3.10) with DDoS Plug-In (Source: RSA)

Two Mega Trends Merging to Create “The Perfect Storm”?



Abusable IoT Devices

Weaponization and Ease of Attack



Rise in IoT-Based DDoS Attacks

Why IoT Devices?

- Embedded or stripped-down versions of Linux
- Easy to target a wide range of devices
- Limited security features

- Internet-accessible
- Unfettered outbound access

- **Market Dynamics**
- Extremely Low-margin Products not differentiated by security features
- Chip makers → ODM's → Brand Company → End User
  - No security expertise, No incentive for Security

- **Result**
- A large population of highly susceptible, high bandwidth devices that cannot or will not be patched or otherwise secured.

Default Crendentials for IoT Devices

https://krebsonsecurity.com/wp-content/uploads/2016/10/IoTbadpass-Sheet1.pdf

Username/Password	Manufacturer	Link to supporting evidence
admin/123456	ACTi IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/anko	ANKO Products DVR	http://www.cctvforum.com/viewtopic.php?f=3&t=44250
root/pass	Axis IP Camera, et. al	http://www.cleancss.com/router-default/Axis/0543-001
root/vizxv	Dahua Camera	http://www.cam-it.org/index.php?topic=5192.0
root/888888	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/666666	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/7ujMko0vizxv	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
root/7ujMko0admin	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
666666/666666	Dahua IP Camera	http://www.cleancss.com/router-default/Dahua/DH-IPC-HDW4300C
root/dreambox	Dreambox TV receiver	https://www.satellites.co.uk/forums/threads/reset-root-password-plugin.101146/
root/zlxx	EV ZLX Two-way Speaker?	?
root/juantech	Guangzhou Juan Optical	https://news.ycombinator.com/item?id=11114012
root/xc3511	H.264 - Chinese DVR	http://www.cctvforum.com/viewtopic.php?f=56&t=34930&start=15
root/hi3518	HiSilicon IP Camera	https://acassis.wordpress.com/2014/08/10/i-got-a-new-hi3518-ip-camera-modules/
root/klv123	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/klv1234	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/jvbzd	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/admin	IPX-DDK Network Camera	http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/
root/system	IQinVision Cameras, et. al	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/meinsm	Mobotix Network Camera	http://www.forum.use-ip.co.uk/threads/mobotix-default-password.76/

The Mirai Botnet

- Approximately 500,000 compromised IoT devices worldwide.
- Default user name and passwords enabled and open ports in firewalls (Telnet TCP 23/2323).

- IoT devices are subsumed into botnet by continuous, automated scanning by other compromised Mirai botnet IoT devices.
- Rebooting device removes malware, but its estimated that it will take less than 10 min to be rescanned and become part of botnet again.

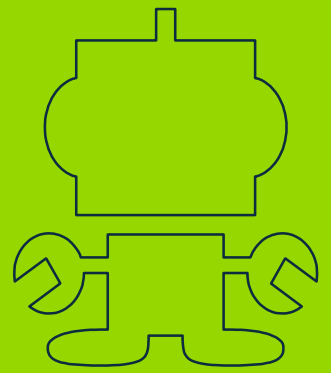
The Mirai Botnet *(cont'd)*

- Segmented command-and-control.
- Capable of launching simultaneous DDoS attacks against multiple targets.
- Non-spoofed traffic. (could change in future)
- Code has been released to wild…already seeing signs of alteration.

Mirai is NOT Just a DNS Attack

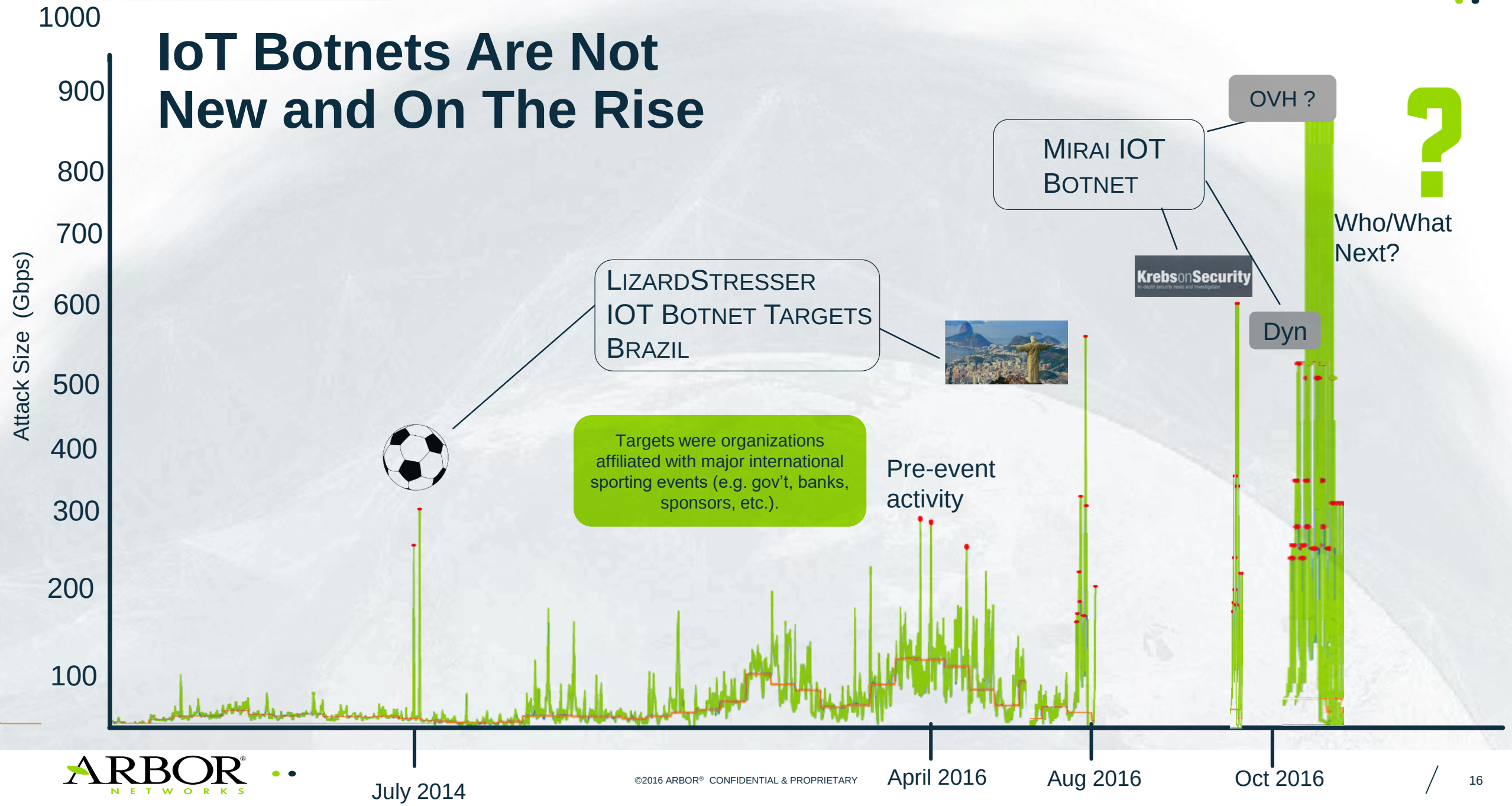
Attack Vectors:

- SYN-flooding
- ACK-flooding
- UDP flooding
- Valve Source Engine (VSE) query-flooding
- GRE-flooding
- Pseudo-random DNS label-prepending attacks (also known as DNS ‘Water Torture’ attacks)
- HTTP GET, POST and HEAD attacks.



The Mirai Botnet is capable of launching complex, multi-vector attacks.

IoT Botnets Are Not New and On The Rise

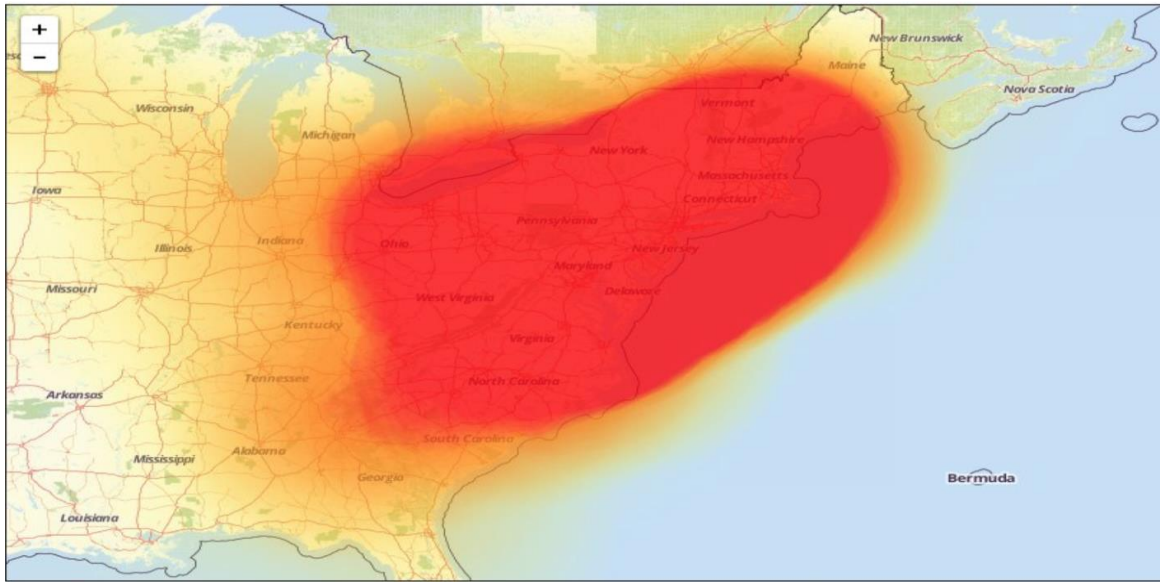


Recent Attacks

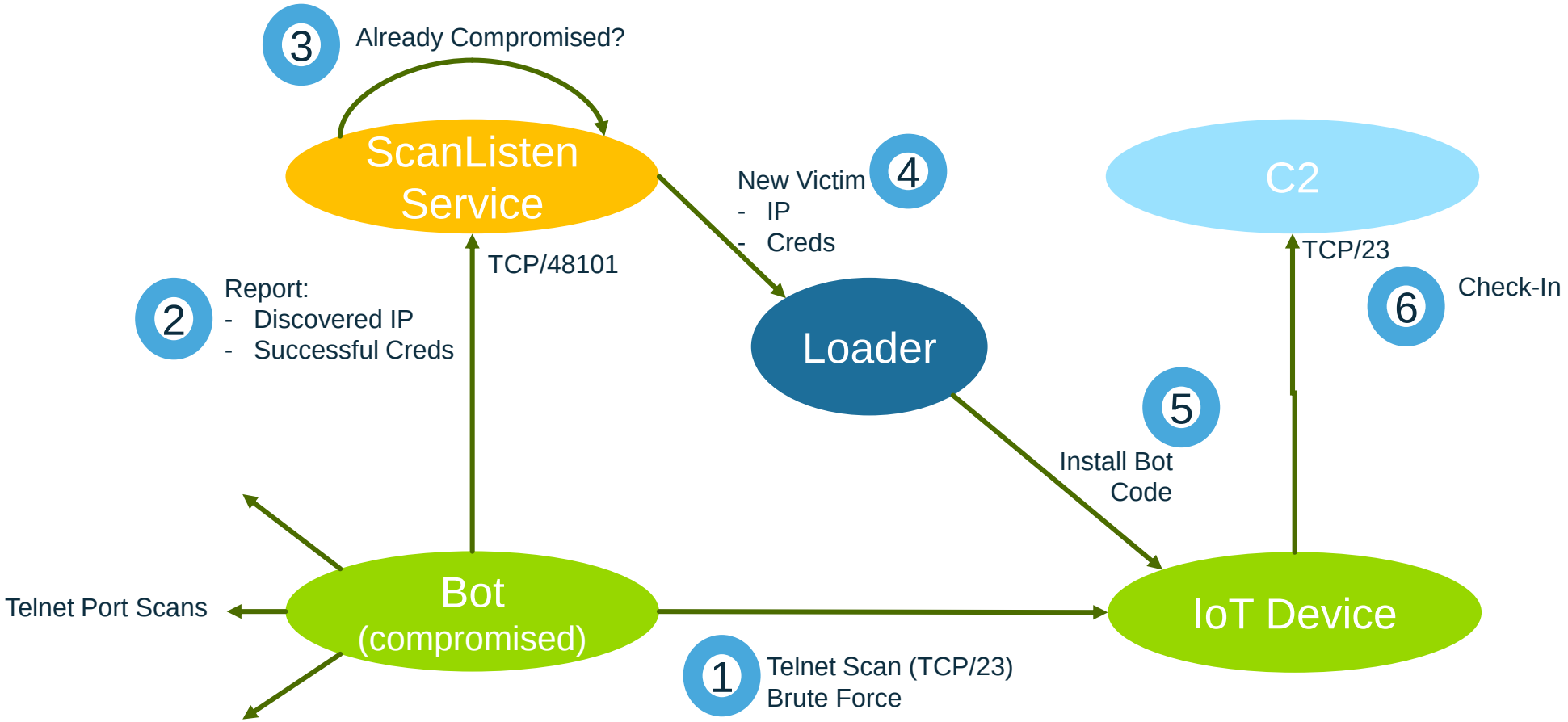
- Summer, 2016 – 540 Gbps attack on an organization associated with the Rio Olympics (Lizardstresser)
- September 20th – 620 Gbps attack targeting KrebsOnSecurity.com (Mirai)
- September 21st – 990 Gbps attack targeting OVH (Mirai)
- September 30th – Mirai source code leaked
- October 21st – Dyn's Managed DNS Infrastructure Targeted (Mirai)
- October 31st – 600 Gbps attack on Liberia (Mirai)

Dyn Attacks on October 21st

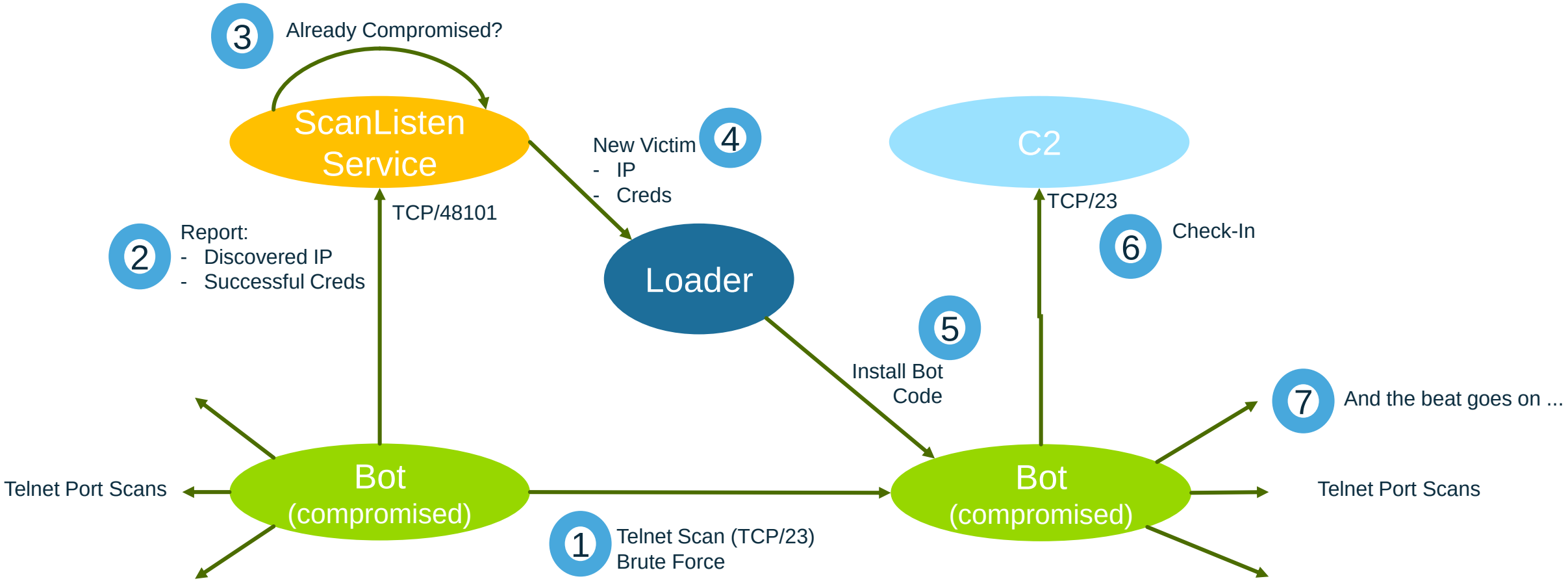
- Three Attacks Targeting Dyn's Managed DNS Infrastructure
- Dyn Customers include
- Netflix, Twitter, Reddit, Github, Spotify, PayPal, Airbnb, NYT, etc.
- Large-scale outages for Dyn Customers, even though the customers



Mirai – Propagation, Command and Control



Mirai – Propagation, Command and Control



ATLAS IoT Botnet tracking

- Network of honeypots setup to monitor IoT compromise activities
- Snapshots of activities from 29 Nov to 12 Dec 2016
- 1,027,543 login attempts from a total of 92,317 unique IP addresses
- Peak login attempts per hour is 18,054

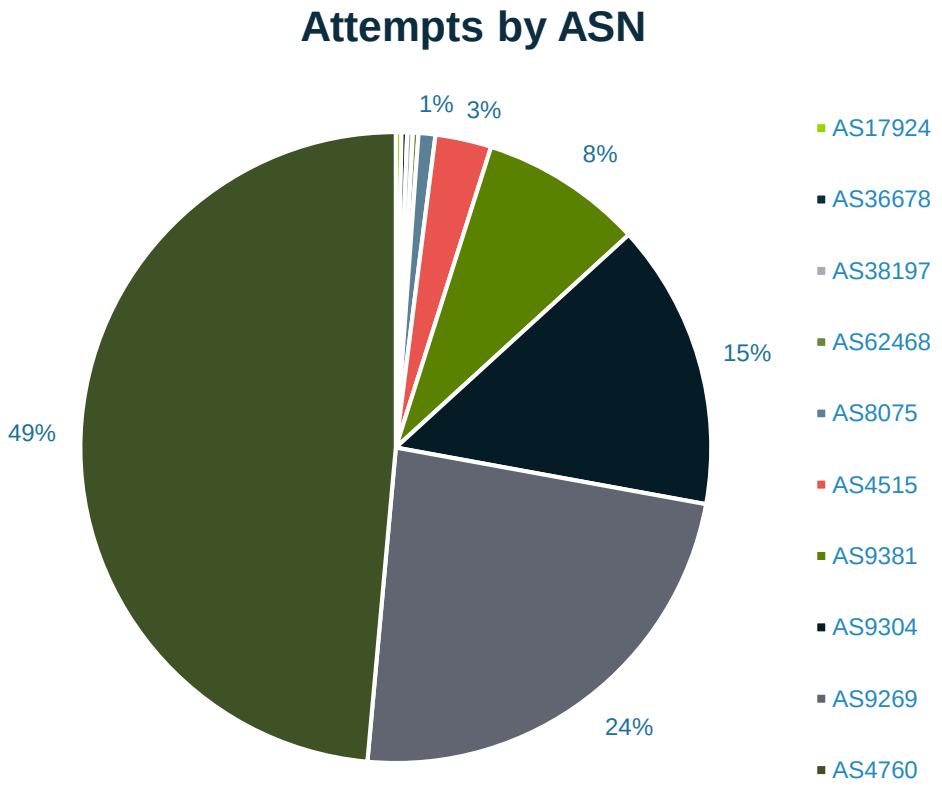
ATLAS IoT Botnet tracking

Source: Arbor Networks, Inc.

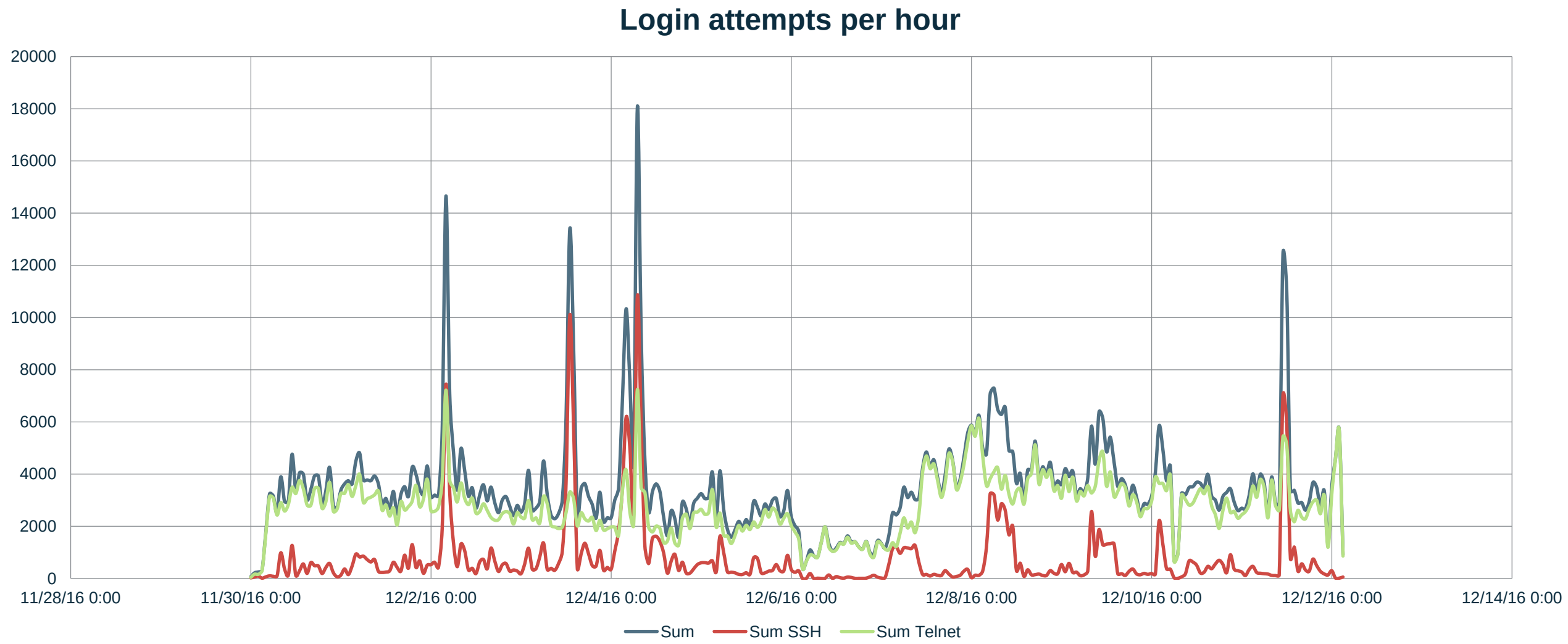
- Billions of IoT devices connected to the Internet
  - Estimates vary, 5B+, with millions added every day
- Arbor honeypot devices look for exploit activity on Telnet / SSH ports
- 1M login attempts from 11/29 to 12/12 from 92K unique IP addresses
- More than 1 attempt per minute in some regions

ATLAS IoT Botnet tracking

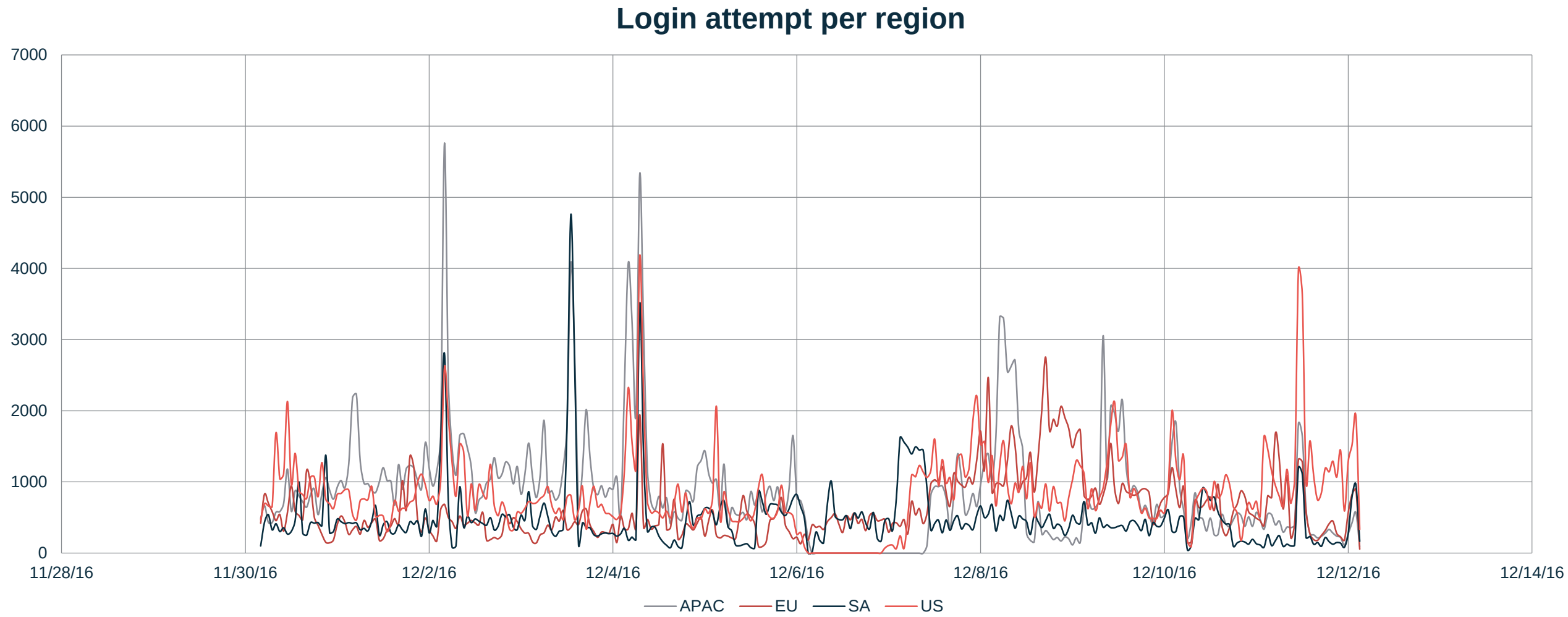
Country	Number of Attempts
China	102,975
Vietnam	26,573
Republic of Korea	19,465
USA	17,062
Brazil	16,609
Russia	13,378
Taiwan	11,697
Hong Kong	11,200
Turkey	10,190
Romania	9,856



ATLAS IoT Botnet tracking



ATLAS IoT Botnet tracking

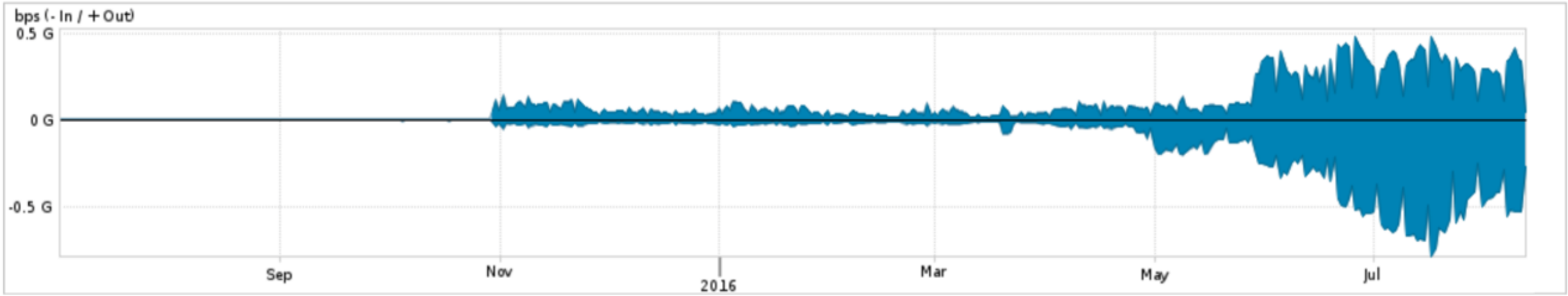


Attack Characteristic, Effects, and Mitigations

- Multiple Highly Distributed Attack Vectors
- Dyn originally reported ”10s of millions of IP addresses”
- Later corrected to an estimate of 100,000
- Cascading Effect
- 2nd Order Impact on Dyn customers
- DNS service disruption from original attack generates legitimate retry activity
  - This is, in part, what caused Dyn to overreport the number of attacking IP’s
- 3rd Order Impact on Broadband Operators
- Mitigations Performed by Dyn According to Dyn:
- Traffic shaping, Anycast Rebalancing, ACL Filtering, Scrubbing Services

Telnet Traffic – IoT botnet growing

2015 | 2016

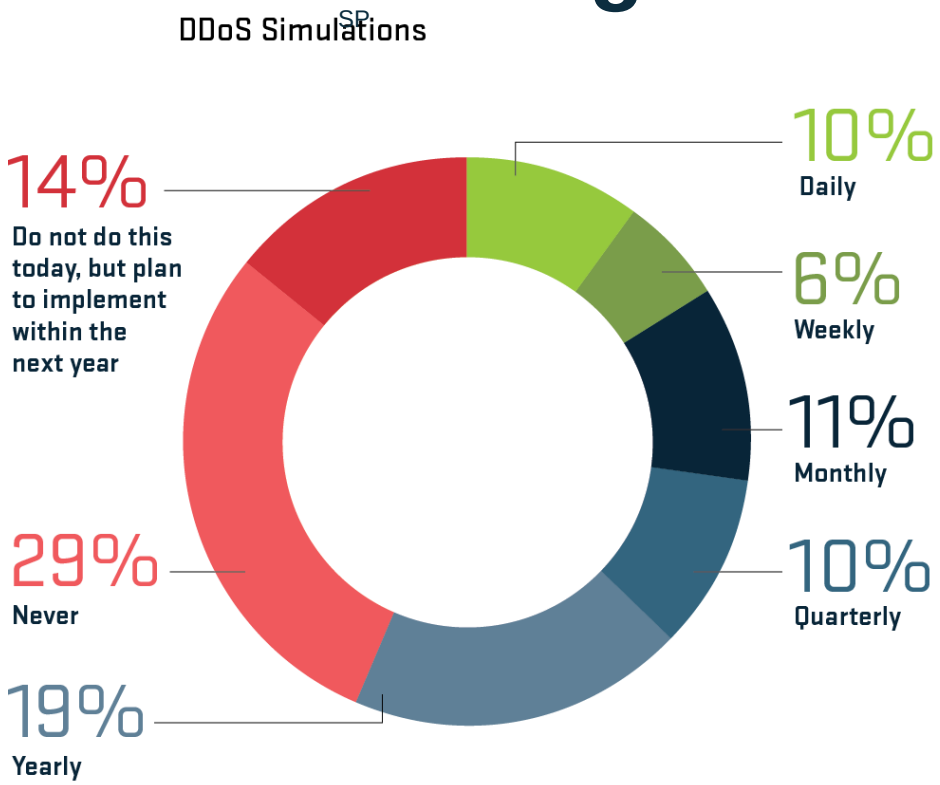


Bot infection is made logging in DVR/Cameras's Telnet, using hardcoded root credential.
Most of those boxes are embed with BusyBox Linux, and there're no patches available so far.

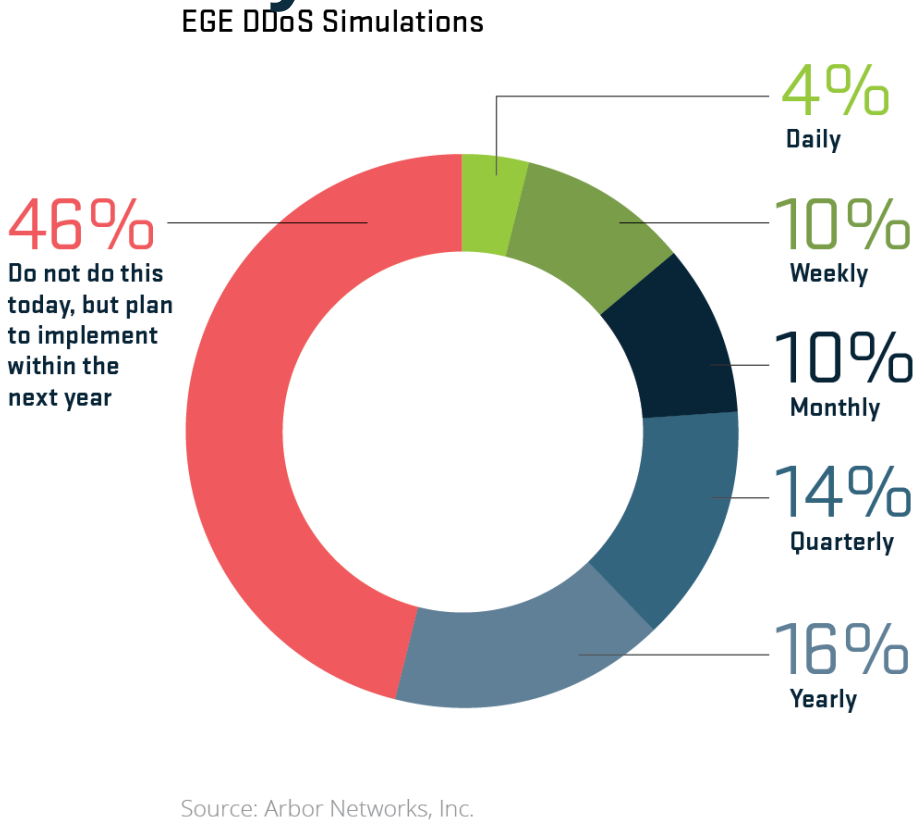
Telnet Traffic by Country – Matches Attack SRC

APPLICATION	COUNTRY	IN	OUT	TOTAL (IN + OUT)
X telnet	Korea, Republic of	671.93 Mbps	23.74 Mbps	695.67 Mbps
X telnet	United States	24.14 Mbps	160.09 Mbps	184.22 Mbps
X telnet	China	23.36 Mbps	52.95 Mbps	76.31 Mbps
X telnet	Japan	29.27 Mbps	32.55 Mbps	61.82 Mbps
X telnet	Brazil	14.40 Mbps	19.34 Mbps	33.74 Mbps

WISR XII – Organization Security



Source: Arbor Networks, Inc.



Source: Arbor Networks, Inc.

- Nearly half of SPs now implement anti-spoofing filters
- Rehearsing DDoS attack processes and procedures is key
  - 10% increase in SPs running simulations, 37% do this quarterly
  - EGE 55% now run simulations, 40% do this quarterly
- Difficulty in hiring and retaining personnel remains a key issue for both SP and EGE respondents

For More Information …

Mirai IoT Botnet Description and DDoS Attack Mitigation

By **Roland Dobbins** on 10/26/2016.

Rio Olympics Take the Gold for 540gb/sec Sustained DDoS Attacks!

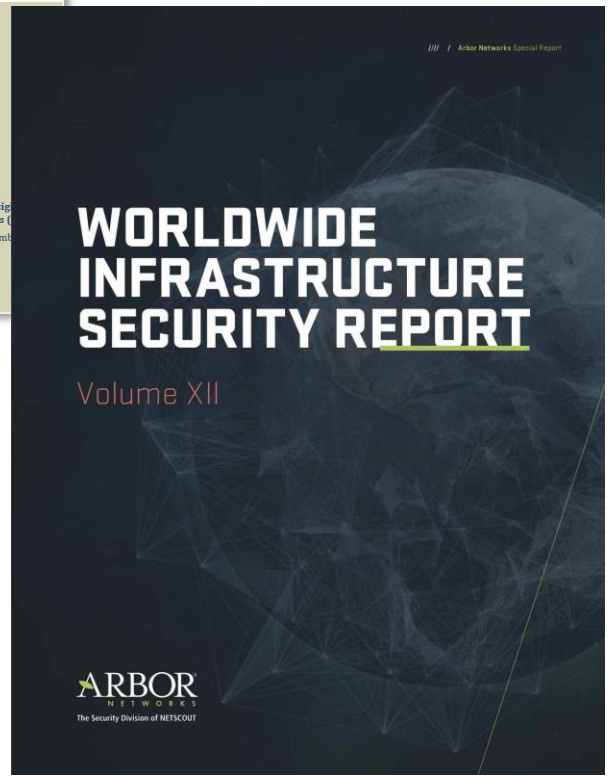
By **ASERT team** on 08/31/2016.

ASERT AUTHORS

by Roland Dobbins, Principal Engineer & Kleber Carriello, Senior

The Lizard Brain of LizardStresser

By **Matthew Bing** on 06/29/2016.



Thank You

ARBOR® NETWORKS
The Security Division of NETSCOUT