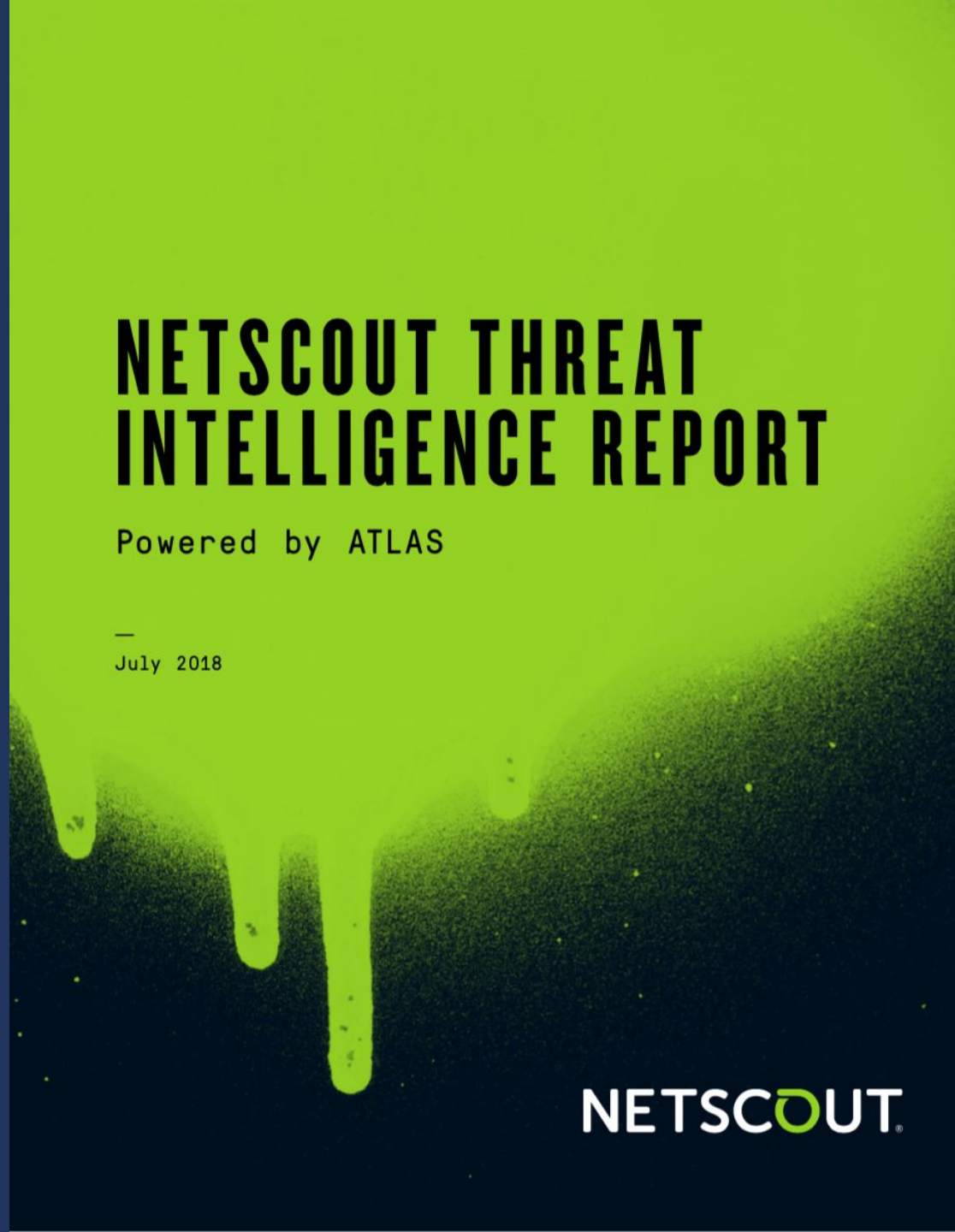
NETSCOUT

DDoS Threat Landscape

The NETSCOUT Threat Intelligence report for 1H 2018

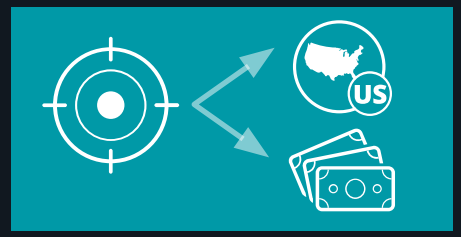
https://www.netscout.com/threatreport



Key Findings

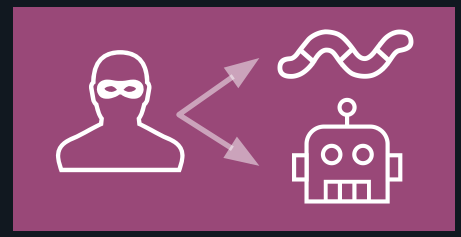
An Accelerating Internet Scale Threat Paradigm

- Big jump in frequency of very large DDoS attacks since Memcached.



- Countries and verticals can be highly targeted.

- More nation states adding APT to their statecraft.



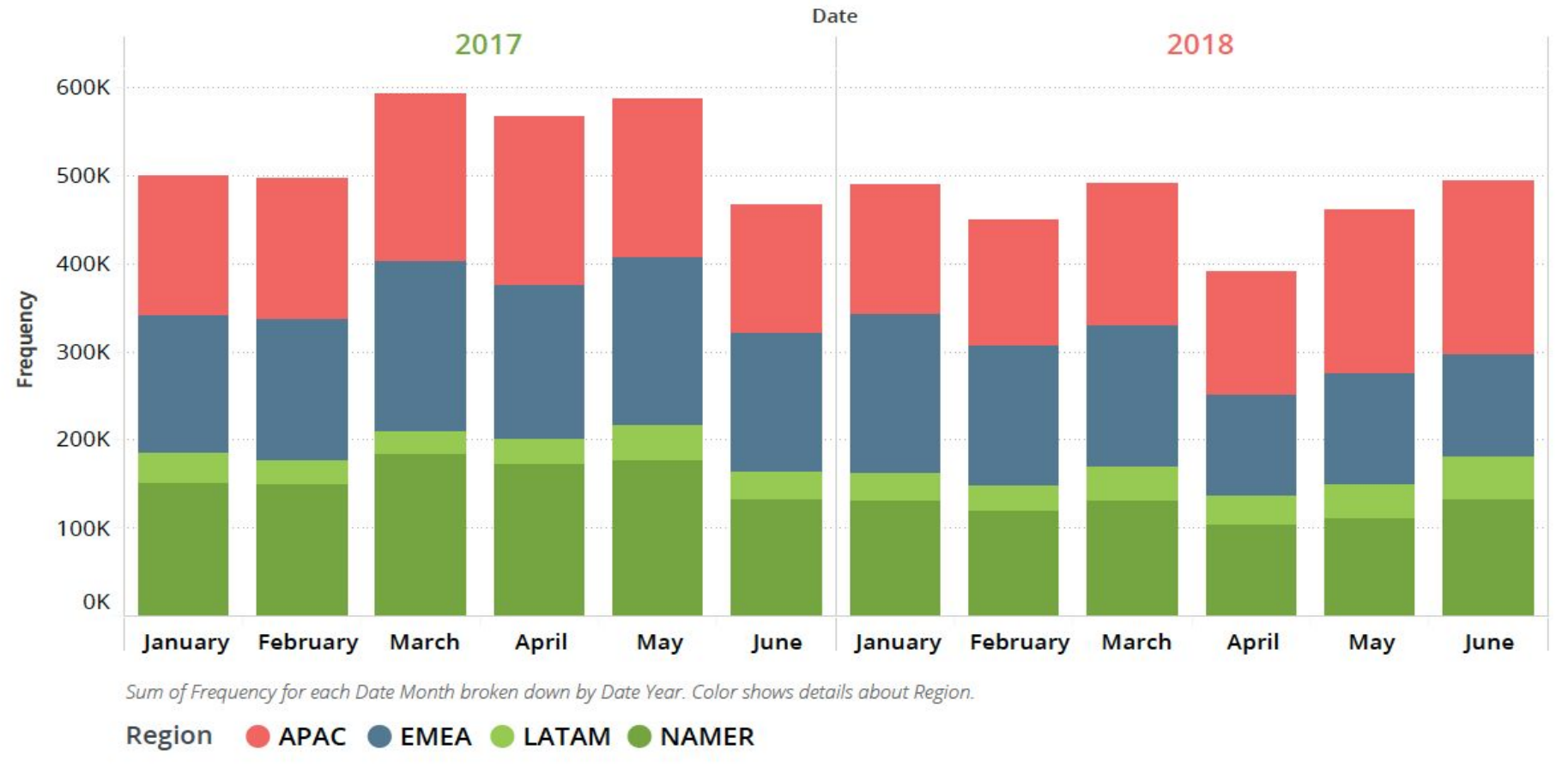
- DDoS tactics being used for internal intrusions. Crimeware and espionage adding Internet Scale techniques (worms, botnets for mass malware distribution)

Global DDoS trends - highlights

- Max attack size has increased by 174% (from 665 Gbps to 1.72 Tbps) and the average attack size has increased 24%.
- Attack frequency has decreased 13% but global attack volume is up 8%.

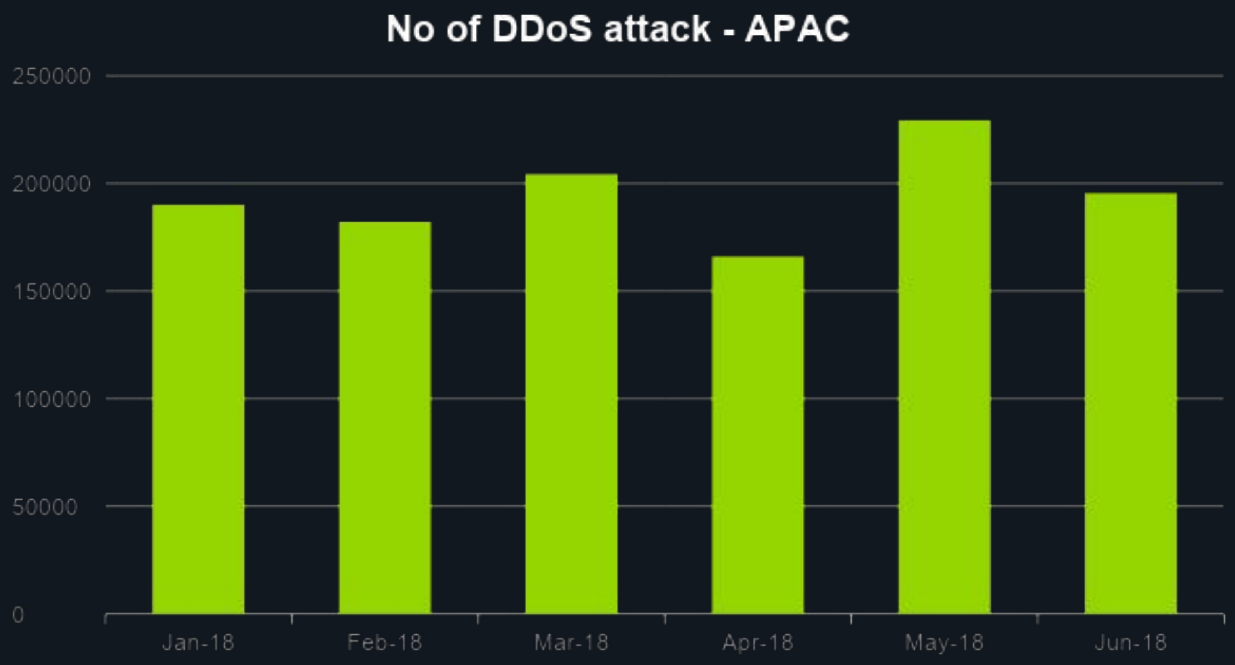
- Attacks are harder hitting, in the first half of 2018 there were 47 attacks greater than 300 Gbps compared to 7 in 1H 2017. This is a 571% increase!
- Memcached is one explanation for this but the real issue is the rapid weaponization of new harder-hitting attacks. For example it only took 1 week to weaponize memcached attacks.

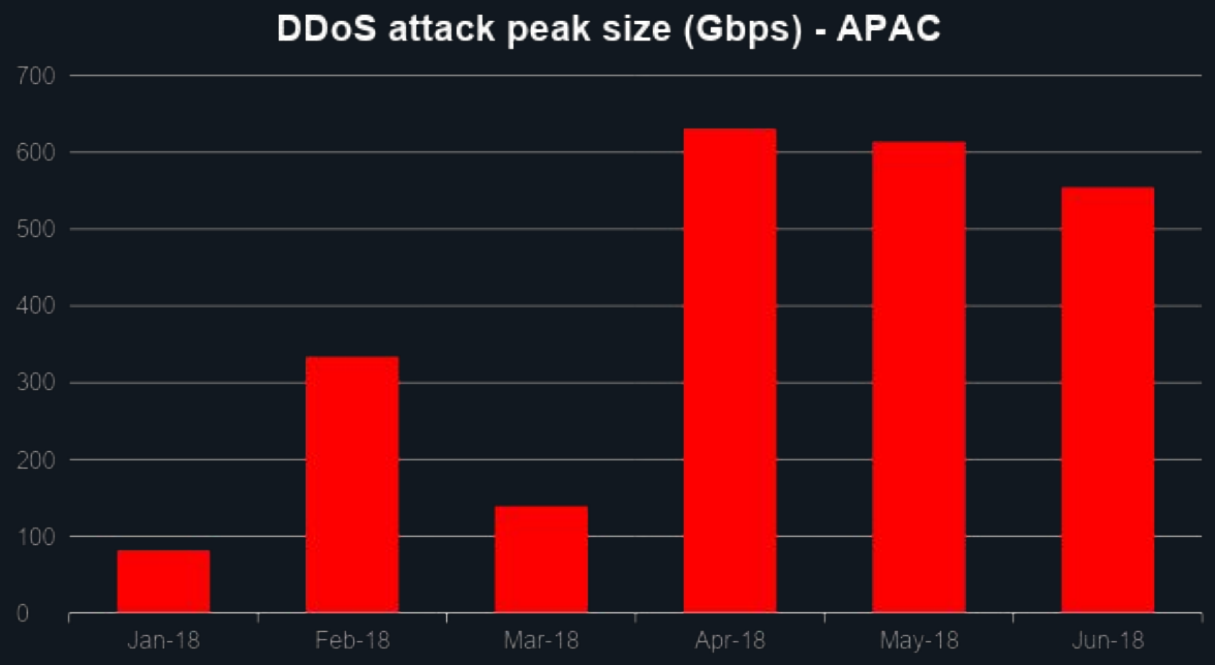
Regional Attacks Trend



- Dip in attack frequency across regions
- Asia Pacific sees increase in attacks greater than 300 Gbps 5 in 2017 H1 to **35** in 2018 H1
- Overall an increase in attack size and scale

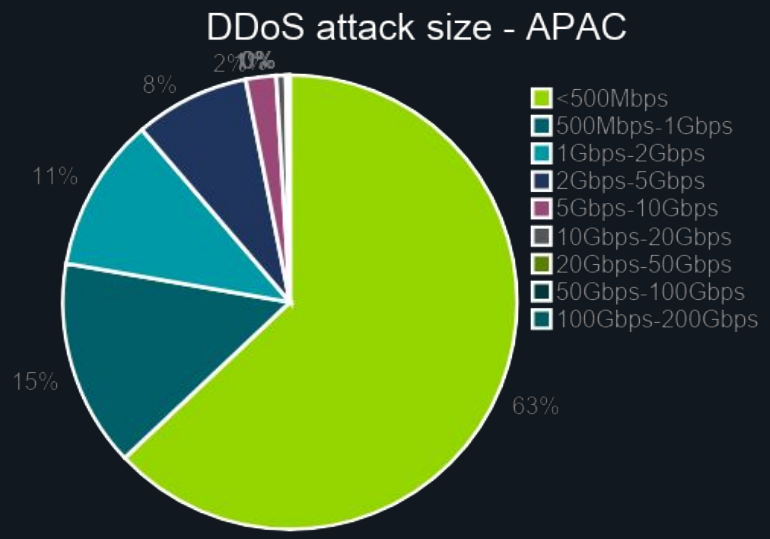
APAC 1H 2018 highlights

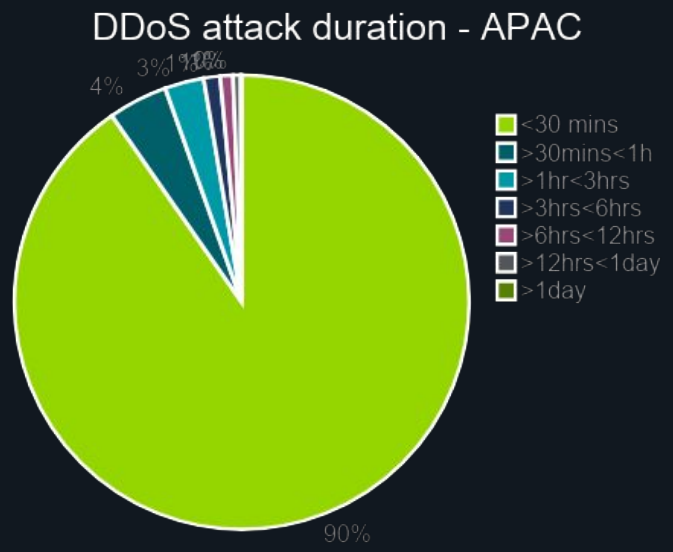


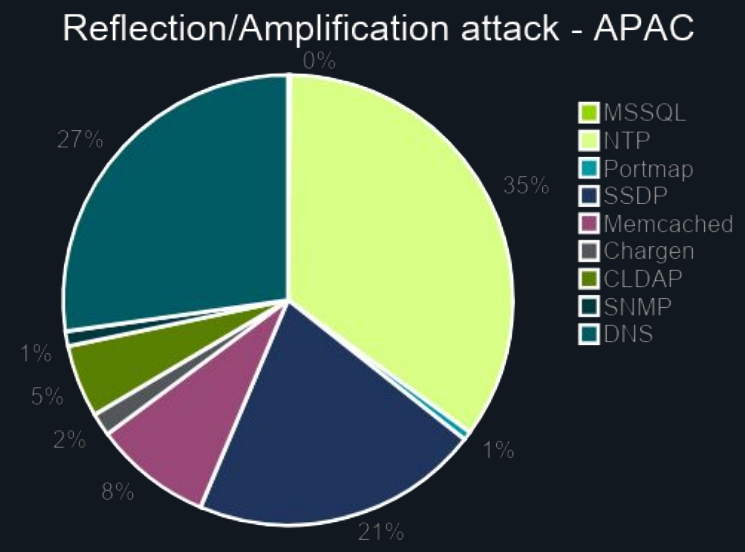


- For 1H 2018, ATLAS reports ~ 1.17M inbound attacks for APAC region with a peak attack size > 630 Gbps

APAC 1H 2018 highlights

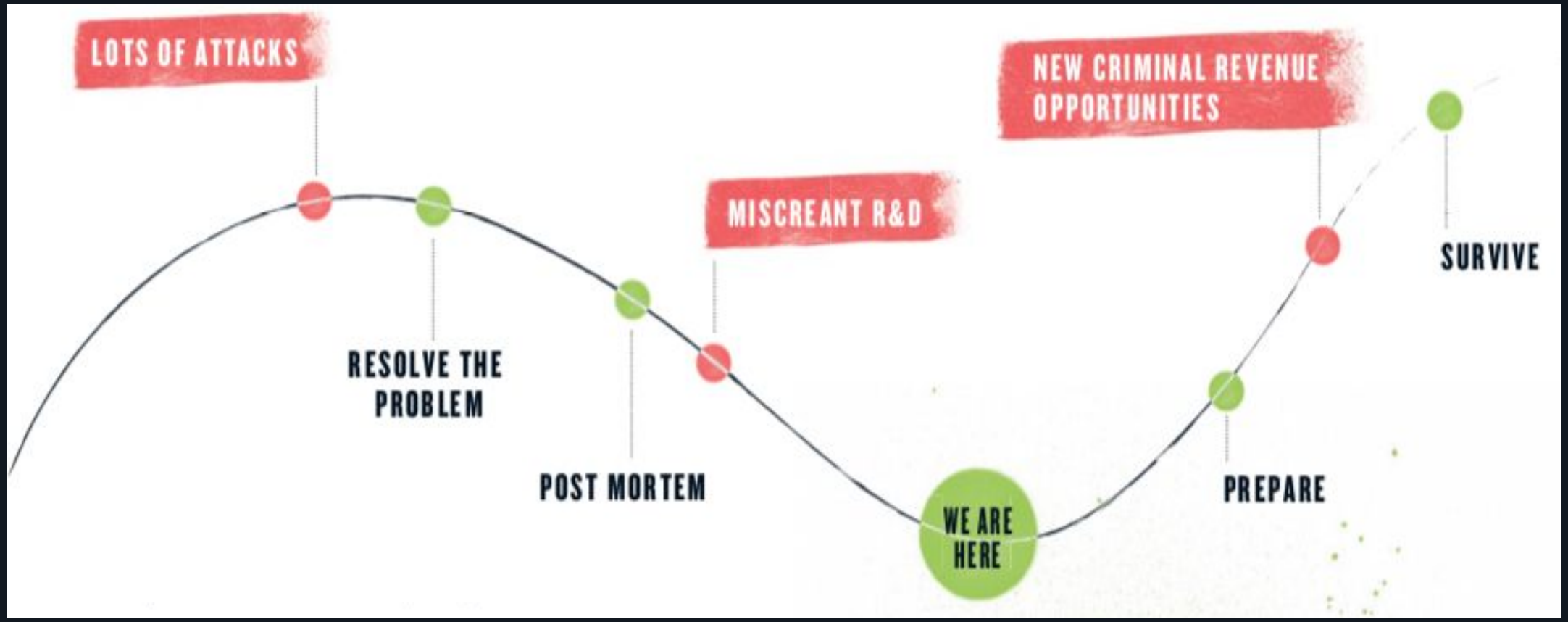




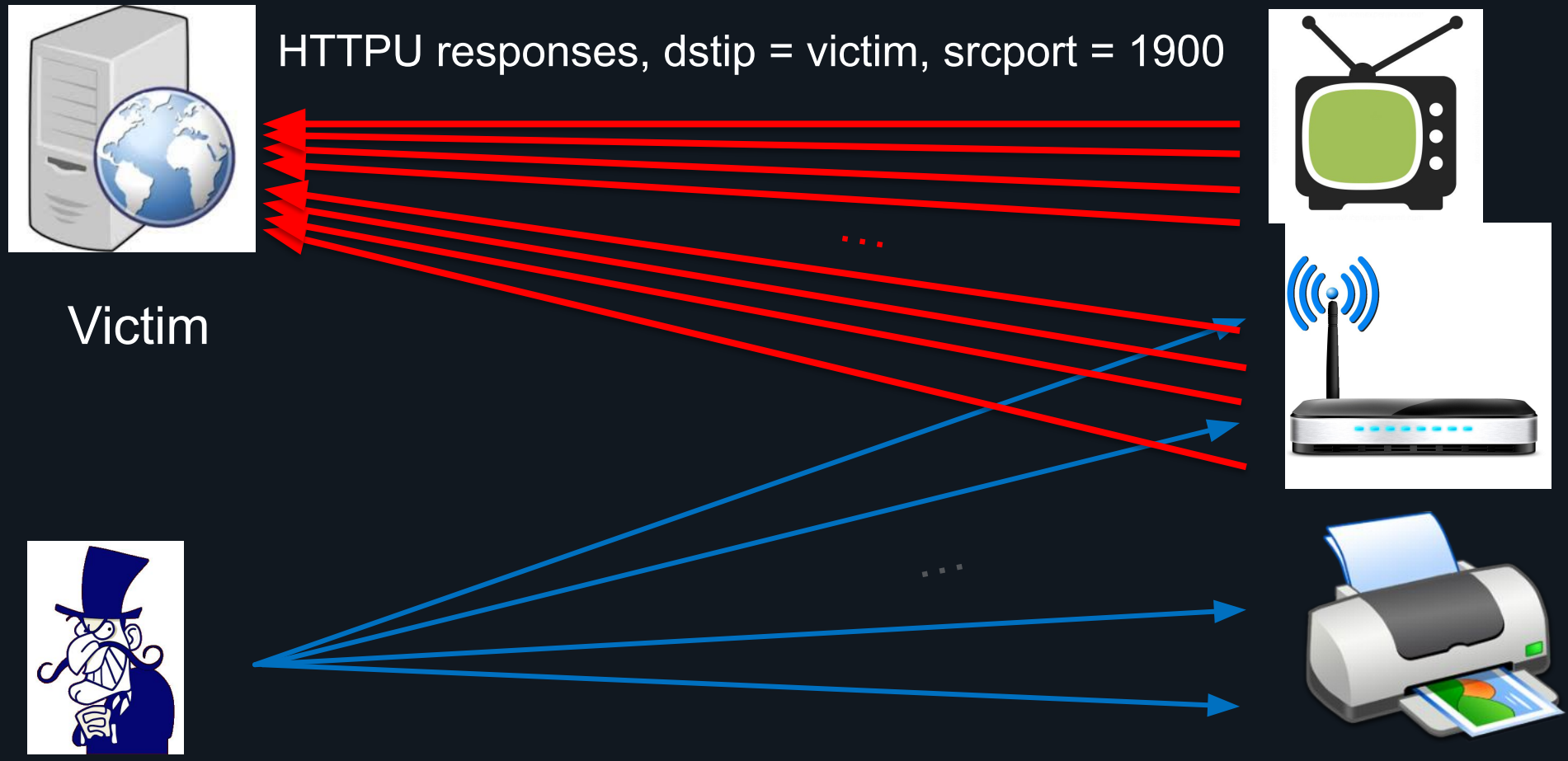


- For 1H 2018, 77% of the attacks seen in APAC is smaller than 1 Gbps
- Around 95% of the attacks last less than 1 hour
- NTP is the most popular protocol used for Reflection/Amplification attack

The digital underground innovation cycle

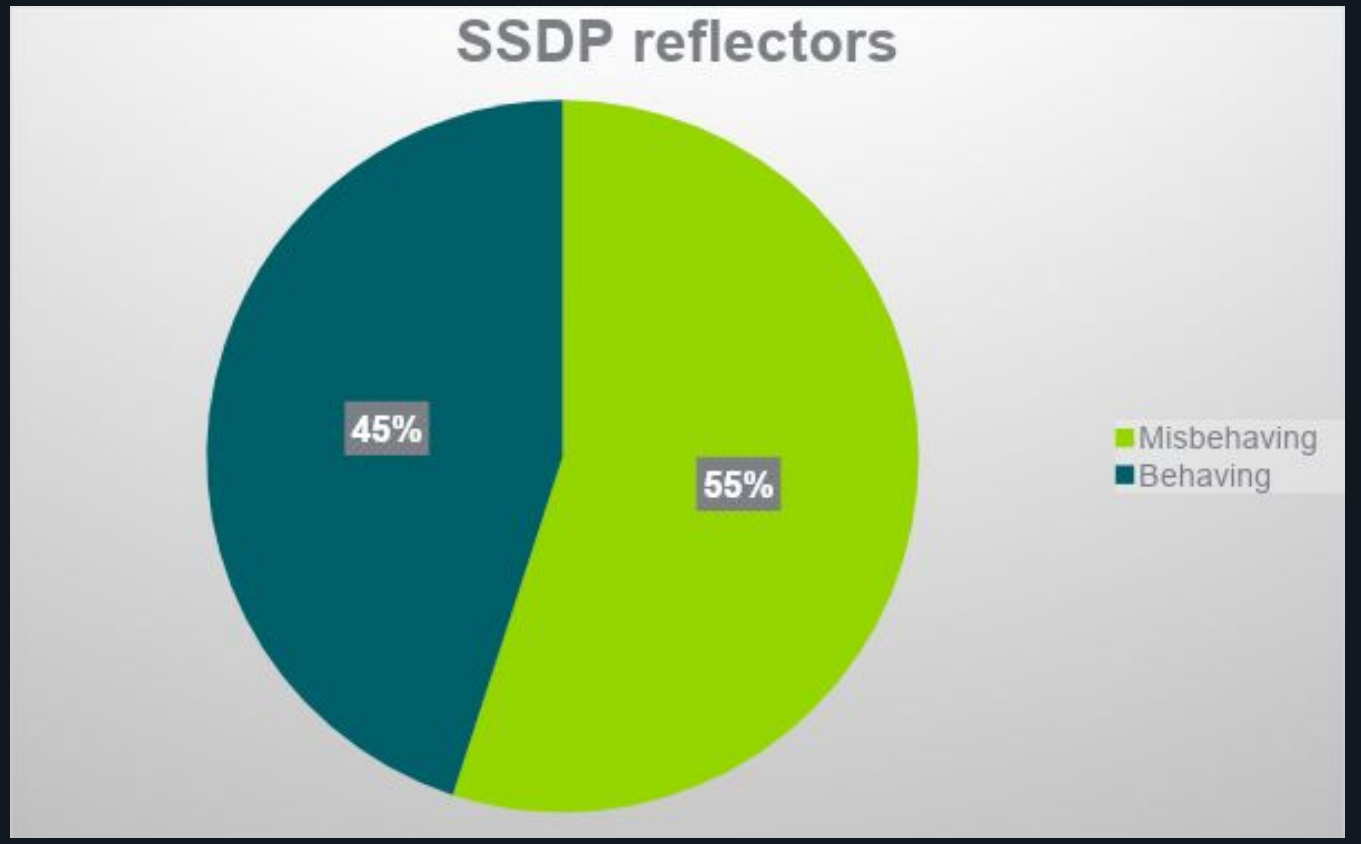


Reflection/Amplification (a new twist)



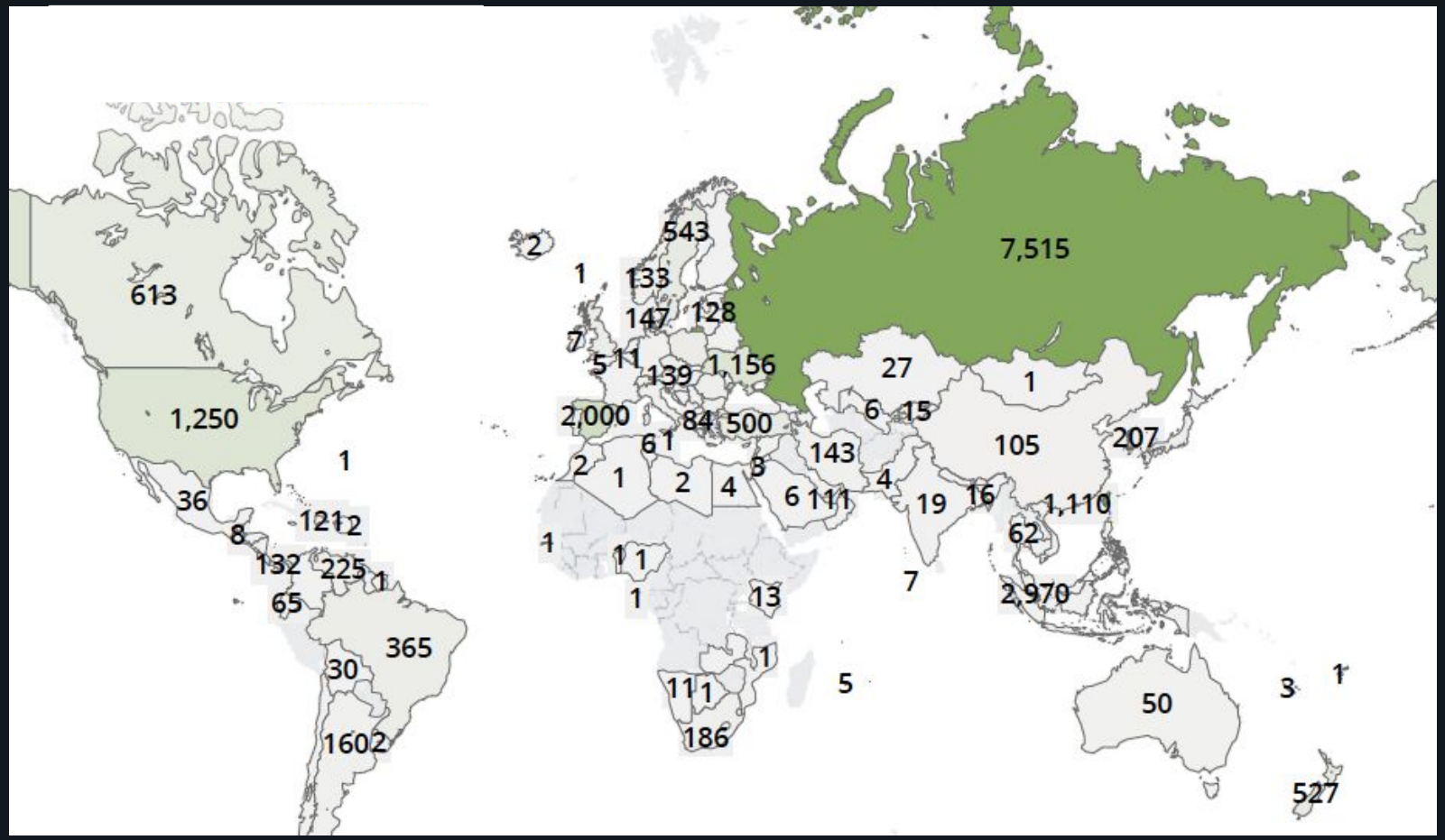
Scanning SSDP reflectors

- Behaving = src port 1900
- Misbehaving = src port NOT 1900
- 5M responses



The Culprit

Distribution of SSDP vulnerability



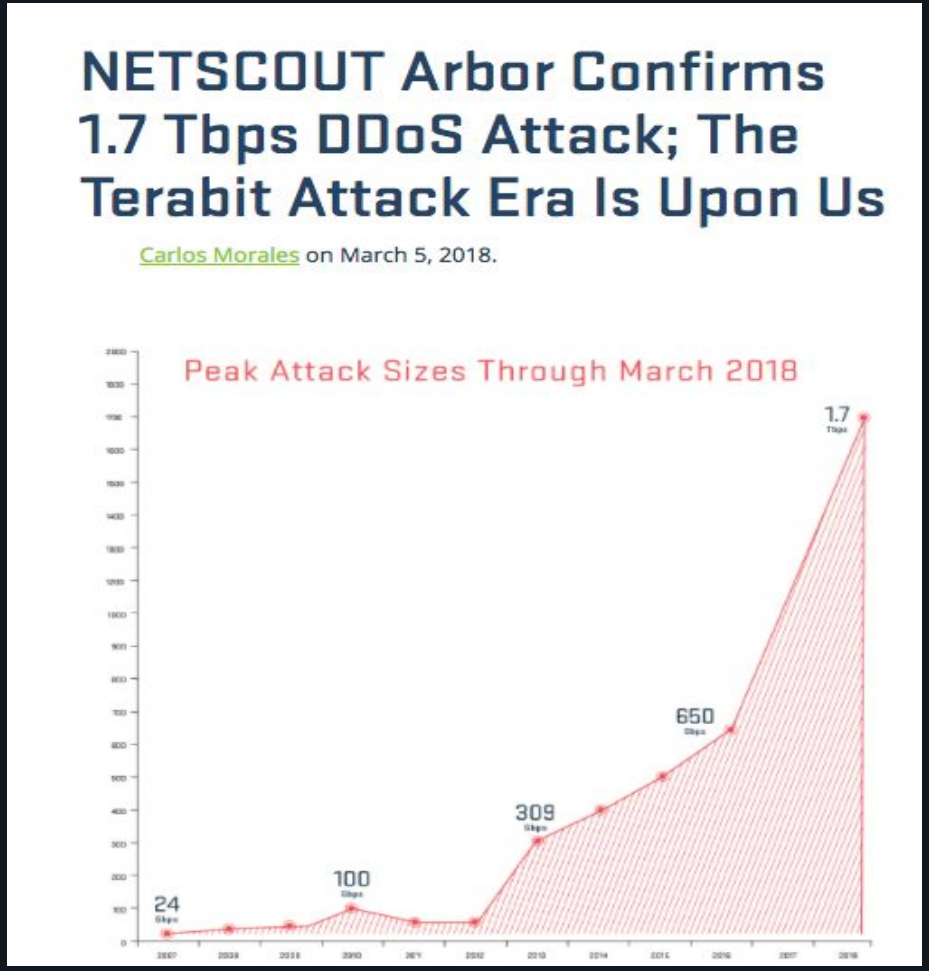
Linux SDK for UPnP Devices (libupnp)

An Open Source UPnP Development Kit

```
86  #ifndef X_USER_AGENT
87      /*! @name X_USER_AGENT
88       *  The {\tt X_USER_AGENT} constant specifies the value of the X-User-Agent:
89       *  HTTP header. The value "redsonic" is needed for the DSM-320. See
90       *  https://sourceforge.net/forum/message.php?msg_id=3166856 for more
91       * information
92       */
93      #define X_USER_AGENT "redsonic"
94  #endif
```

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 – request own key(s)

Attacker sends 1 packet

Reflector sends 536,302 packets = 6.2Gb

```
...n scapy.all import *
...ort binascii
...md = "get a a a a a a a a a a a a a a a a a a a a a a a a a a a … <729 times>"
...yload=binasc...                                                    612…   120…
...t=Ether()/IP...                                                    /pa…
endp(pkt, iface="eth1", loop=0,verbose=False)
```

Amplification factor of 1:500.000!

3	0.002366	10.1.138.170	172.17.10.103	QUIC	1513	Payload (Encrypted), Seq: 1
4	0.075723	172.17.10.103	10.1.138.170	QUIC	1442	Payload (Encrypted), Seq: 1
6	0.088618	172.17.10.103	10.1.138.170	QUIC	1442	Payload (Encrypted), Seq: 1
7	0.088652	172.17.10.103	10.1.138.170	QUIC	1442	Payload (Encrypted), Seq: 1
8	0.088658	172.17.10.103	10.1.138.170	QUIC	1442	Payload (Encrypted), Seq: 1
9	0.088662	172.17.10.103	10.1.138.170	QUIC	1442	Payload (Encrypted), Seq: 1
10	0.088678	172.17.10.103	10.1.138.170	QUIC	1442	Payload (Encrypted), Seq: 1
11	0.088683	172.17.10.103	10.1.138.170	QUIC	1442	Payload (Encrypted), Seq: 1
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

IoT Botnet

- Mirai first utilized to launch high-profile, high-impact DDoS in 2016
- Mirai source code published Sept 2016
- Mirai variants developed
- OMG can pivot to private networks
- Wicked target Netgear routers and CCTV-DVR
- IoTrojan exploits router and includes DDoS function

CONNECTED DEVICES

VULNERABLE TO IOT BOTNETS

27 BILLION

IN 2017

▼

125 BILLION

BY 2030

MIRAI

SOURCE CODE PUBLISHED

9.30.2016

FIVE VARIANTS

DEVELOPED BY
IoT BOTNET AUTHORS

OMG

WICKED

JEN X

SATORI

IoTROJAN

Summary

- DDoS attacks have now entered the Terabit era.
- Attacks are now harder hitting, primarily due to the rapid weaponization of new attack vectors.
- Operators should follow Security Best Practices and protect their borders, both external and internal:
  - Scan your networks for known threats and vulnerable IoT devices.
  - Block/Rate limit known threats (”Exploitable port filters”)
  - Make VERY strict requirements of your vendors, especially the CPE vendors
- Take advantage of new information sources to see through the fog.