NEXUSGUARD®

Are Hong Kong networks ready to withstand evolving DDoS Attack?

Donny Chong
Product & Marketing Director, Nexusguard
September 6, 2019

NEXUSGUARD®

INFORMATION MANAGEMENT 2018 AWARDS

Best Security-As-A-Service Information Management Awards 2018

Quadrant Knowledge Solutions

Key player in DDoS Mitigation Global Market 2017

FROST & SULLIVAN

Global DDoS Mitigation Entrepreneurial Company of the Year Award 2016

FORRESTER®

The Forrester Wave™ DDoS Mitigation Solutions 2017

10+

Years experience fighting DDoS

15

Global DDoS Scrubbing Centers

2.24

Tbps Scrubbing Capacity

24x7

Security Operation Center

facebook ThreatExchange

PCI DSS COMPLIANT

bsi. ISO/IEC 27001 Information Security Management

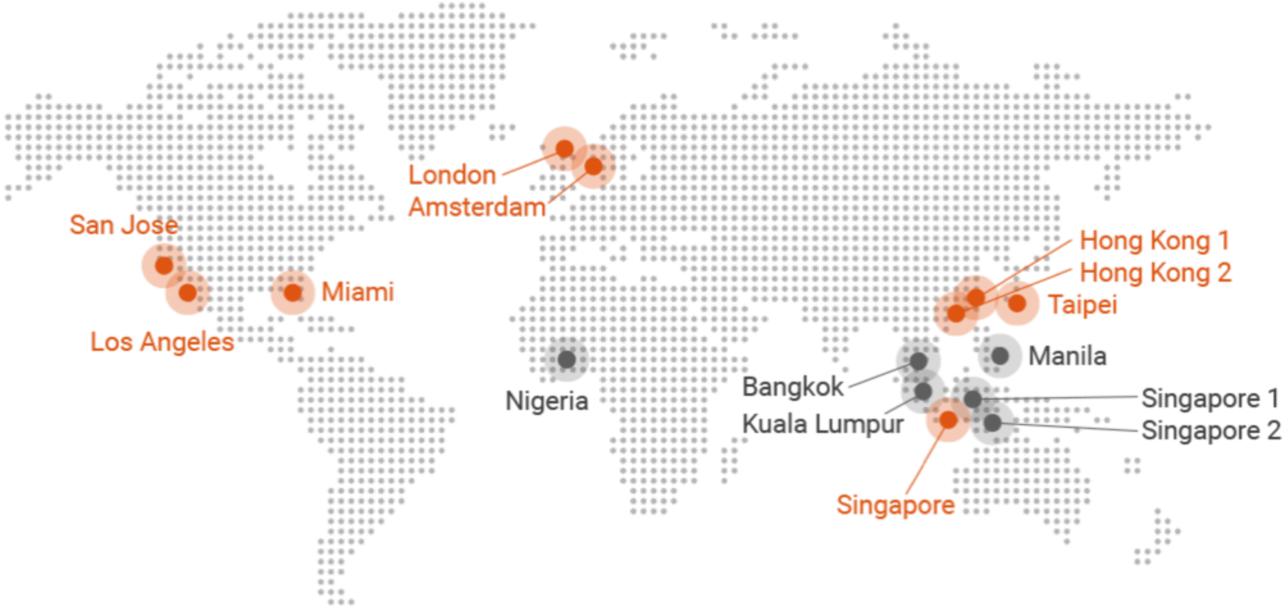
IS 655990

CUSTOMER SERVICE QUALITY STANDARD AP CSC CSQS CERTIFIED CUSTOMER SERVICE

NEXUSGUARD®

Global Scrubbing Network

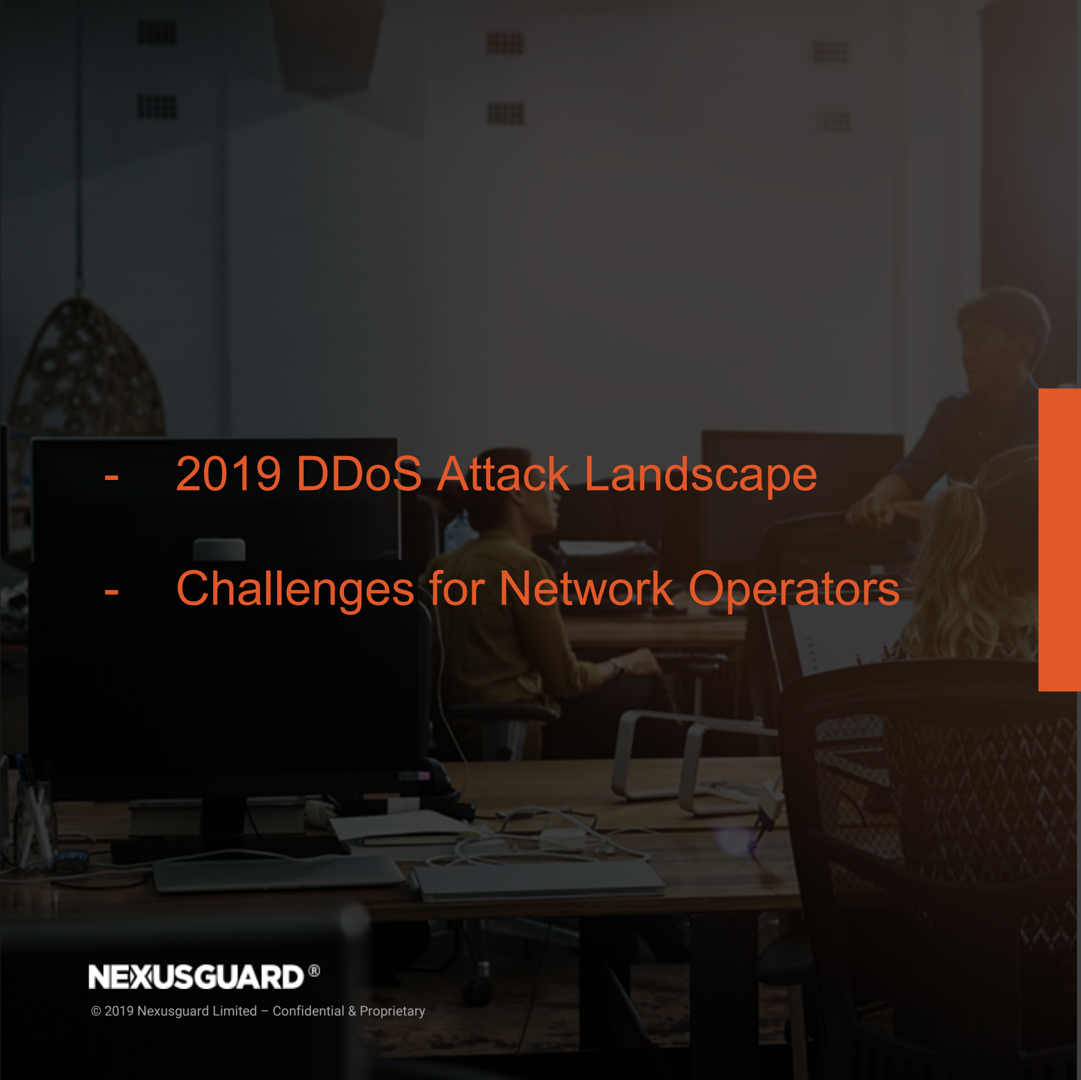
15 PoPs



● Nexusguard PoP

● Nexusguard Registered Partner PoP

Agenda



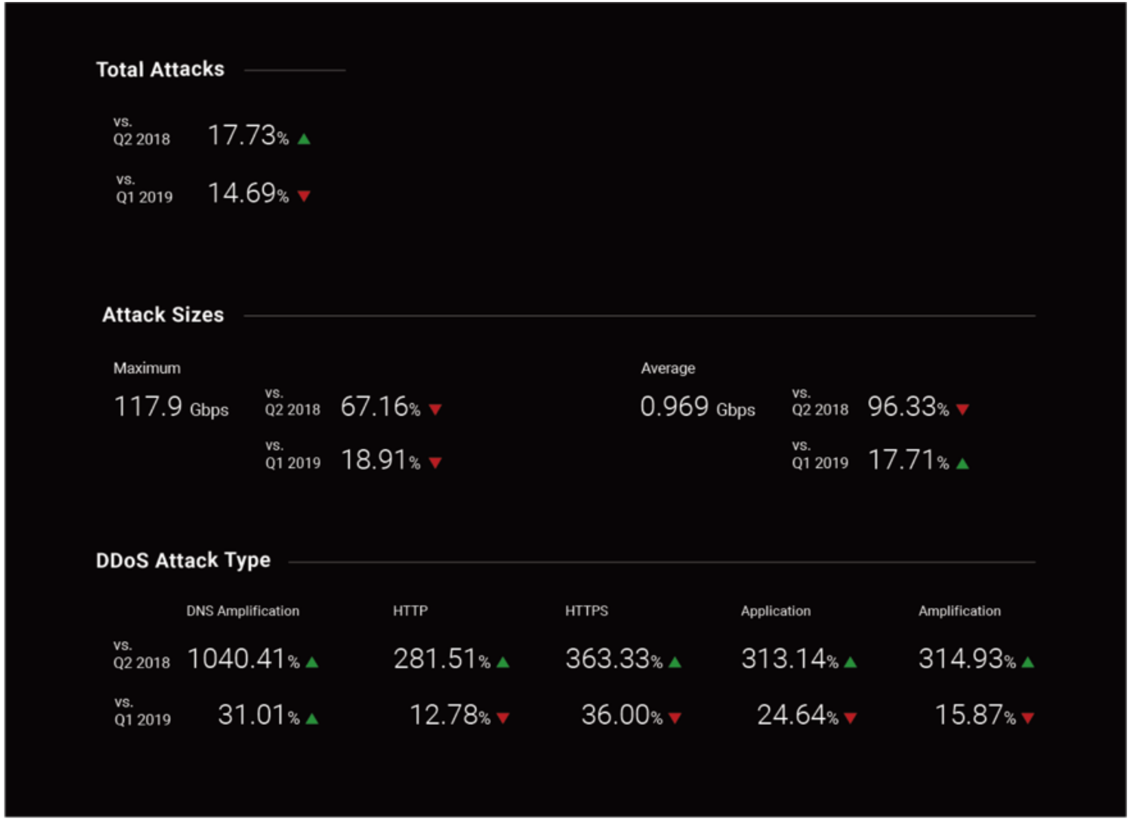
- 2019 DDoS Attack Landscape
- Challenges for Network Operators

DDoS Attack Landscape

DDoS Evolution over the last Decade

DDoS Attack	2008	2018	
Size	Avg 1 Gbps Max 40 Gbps	Avg 300 Gbps Max 1.35 Tbps	300X BIGGER
Duration	6 - 8 Hours	~19 Days	60X LONGER
Sophistication	1~2 Vectors	>10 Vectors	10X MORE COMPLEX

DDoS Attack Summary (2019 Q2)



Total Attacks

vs. Q2 2018	17.73% ▲
vs. Q1 2019	14.69% ▼

Attack Sizes

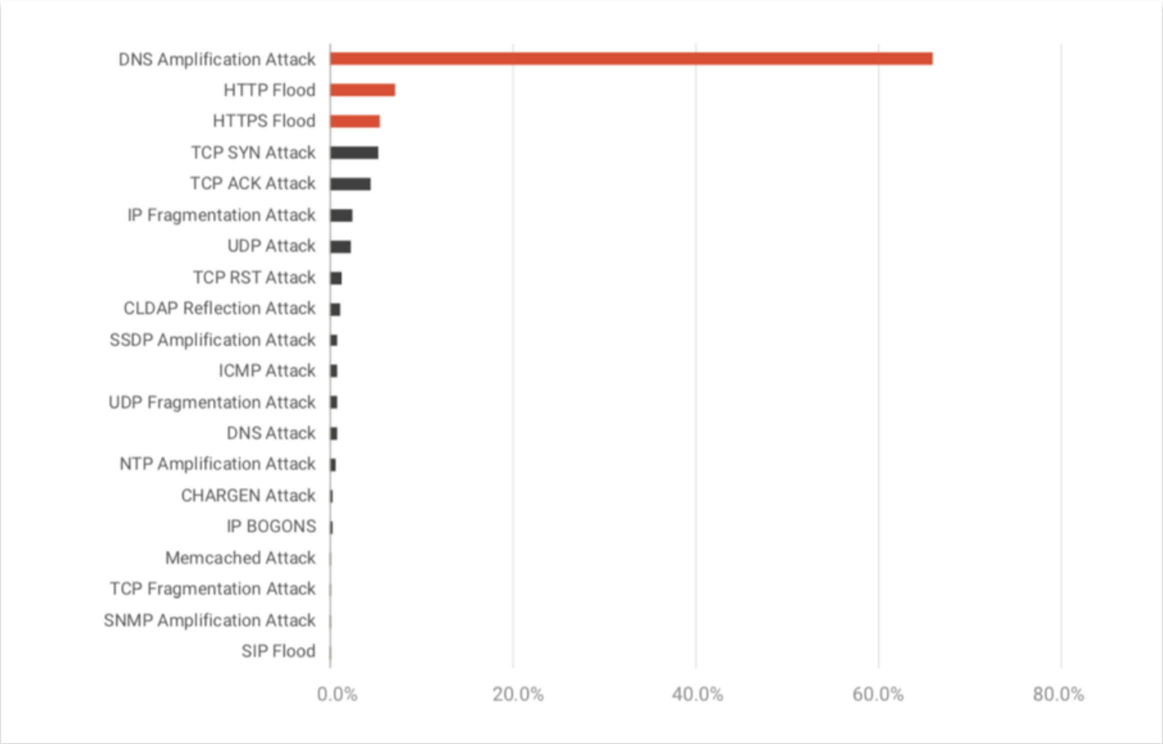
Maximum			Average		
117.9 Gbps	vs. Q2 2018	67.16% ▼	0.969 Gbps	vs. Q2 2018	96.33% ▼
	vs. Q1 2019	18.91% ▼		vs. Q1 2019	17.71% ▲

DDoS Attack Type

	DNS Amplification	HTTP	HTTPS	Application	Amplification
vs. Q2 2018	1040.41% ▲	281.51% ▲	363.33% ▲	313.14% ▲	314.93% ▲
vs. Q1 2019	31.01% ▲	12.78% ▼	36.00% ▼	24.64% ▼	15.87% ▼

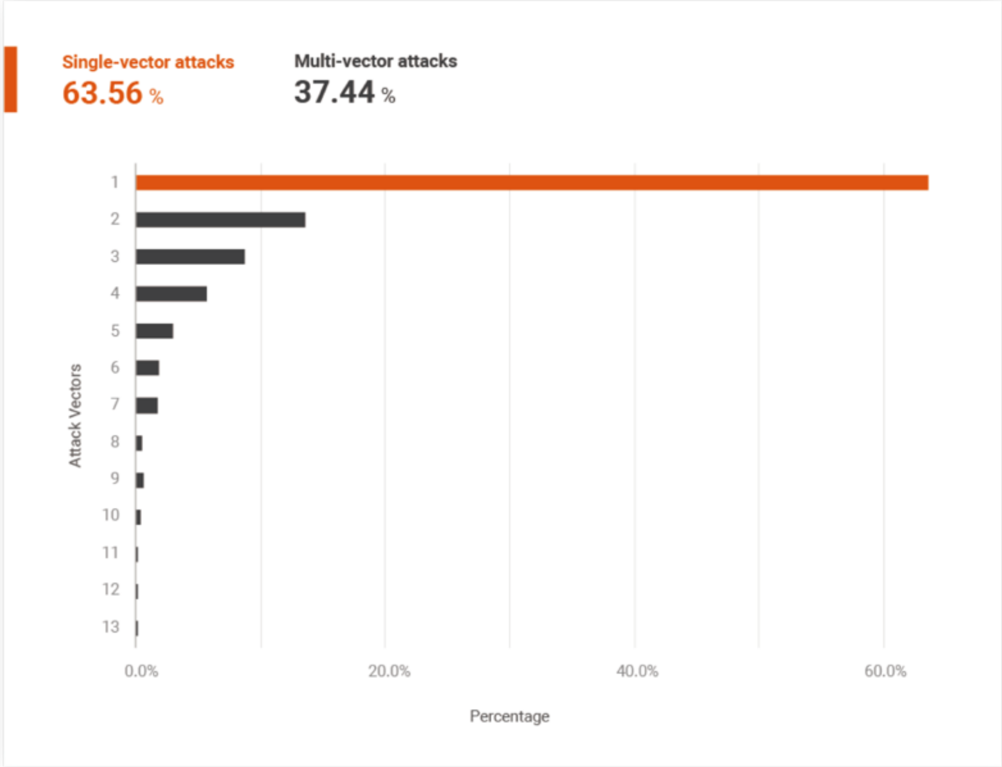
NEXUSGUARD®

Attack Vectors Distribution (2019 Q2)

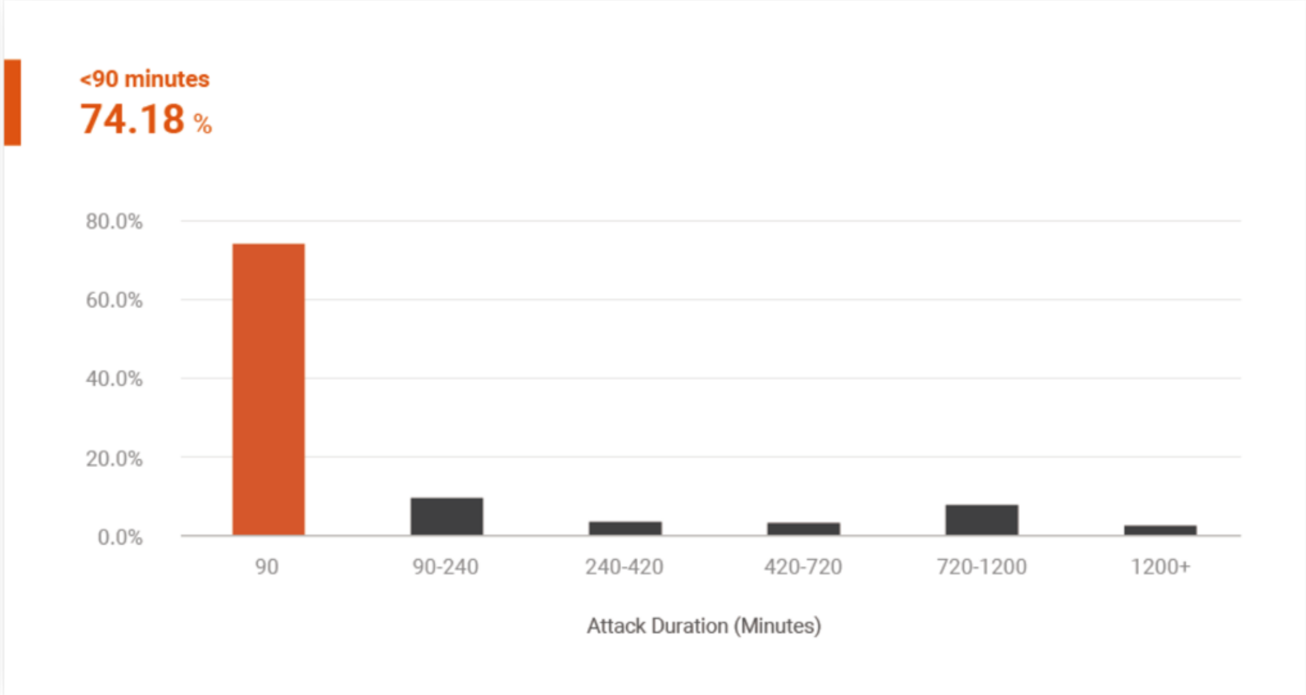


NEXUSGUARD®

Quantity of Attack Vectors (2019 Q2)



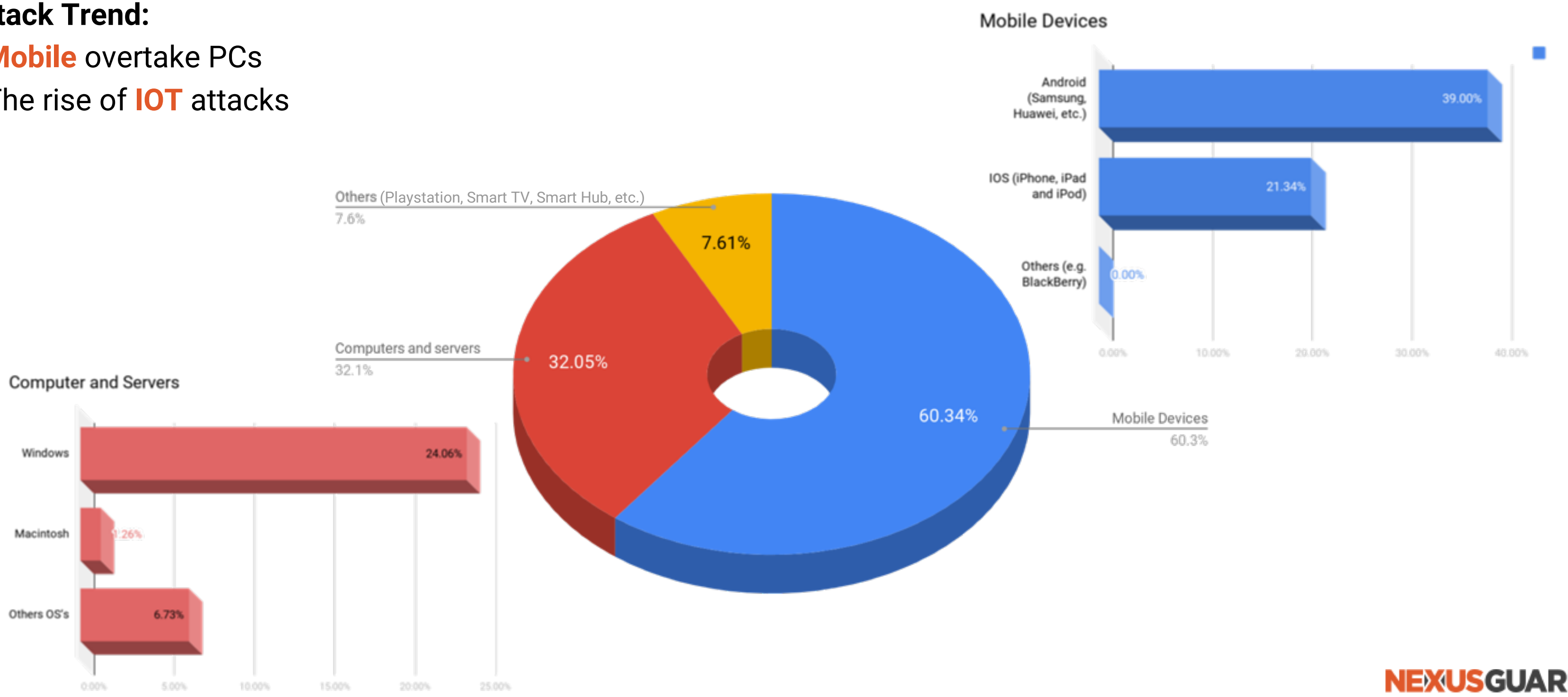
Attack Durations (2019 Q2)



DDoS Attack Source (Q1 2019)

Attack Trend:

- **Mobile** overtake PCs
- The rise of **IOT** attacks



NEXUSGUARD®

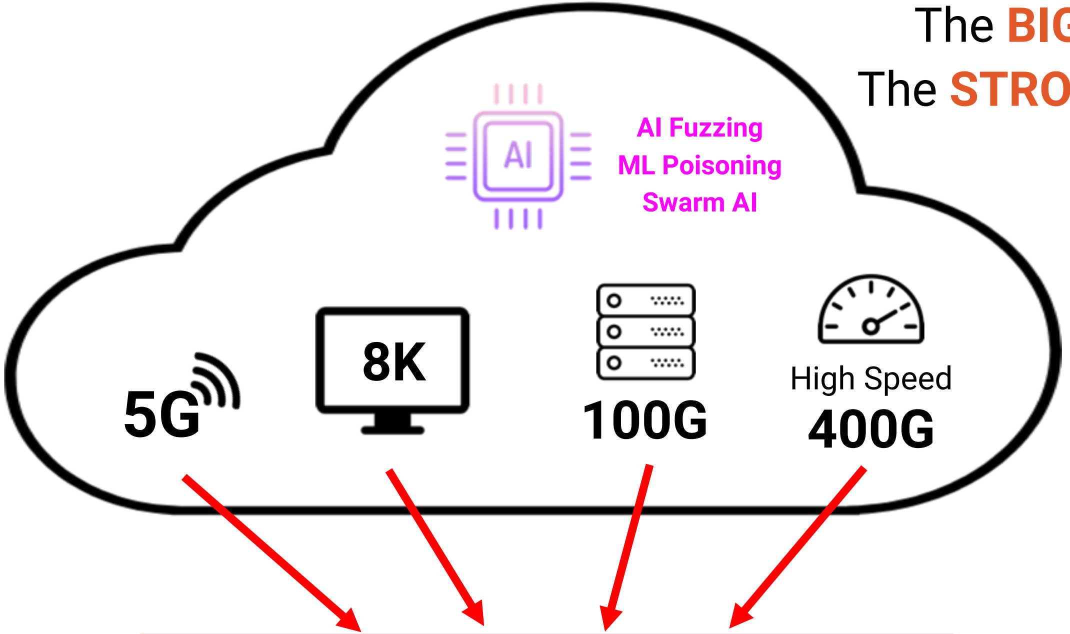
NEXUSGUARD®

DDoS Challenges for Network Operators

Larger, Longer, more Complex and SMARTER attack

The Rise of Terabits DDoS Attacks

The **BIGGER** the pipe
The **STRONGER** the threat

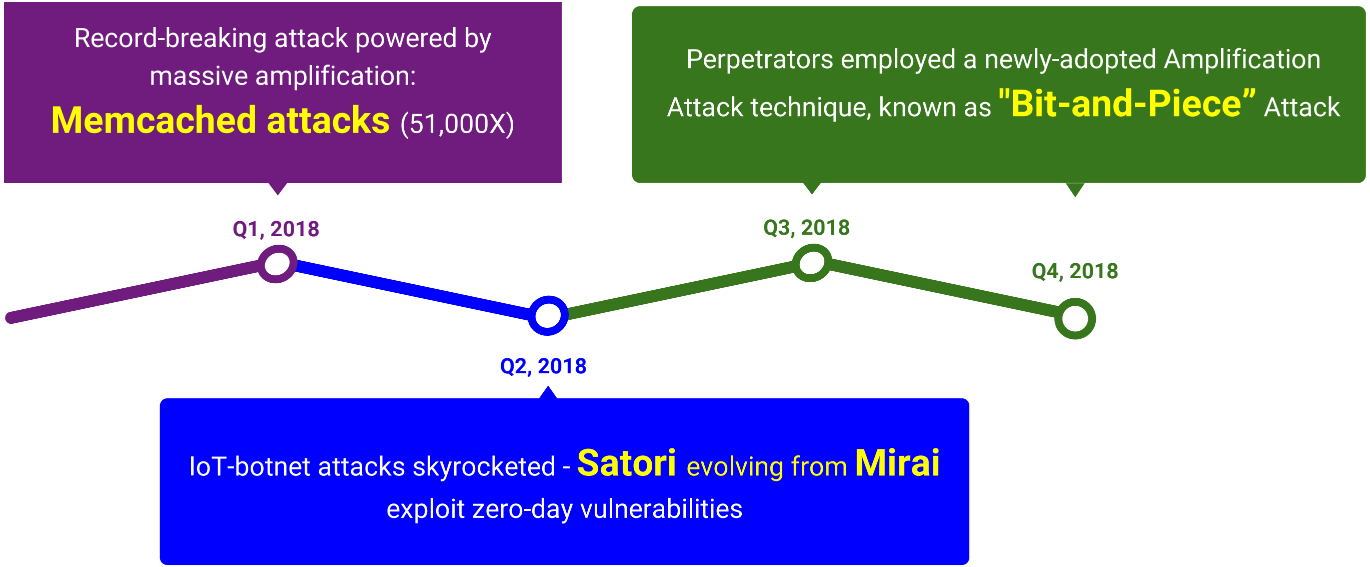


TERABITS DDoS Attack

Powered by Millions of large-bandwidth IOT devices

Significant DDoS Attacks events (2018)

37,728 attacks



Record-breaking attack powered by massive amplification: **Memcached attacks** (51,000X)

Q1, 2018

Q2, 2018

IoT-botnet attacks skyrocketed - **Satori** evolving from **Mirai** exploit zero-day vulnerabilities

Q3, 2018

Q4, 2018

Perpetrators employed a newly-adopted Amplification Attack technique, known as **"Bit-and-Piece"** Attack

New Type: "Bits-and-Pieces" Attack

In our quarterly threats report, we identified a new, sneaky attack technique whereby attackers launch attack towards a diverse pool of IP addresses across hundreds of IP prefixes (Distributed-IP: at least 159 ASN, 527 class C networks) with small-sized junk traffic.

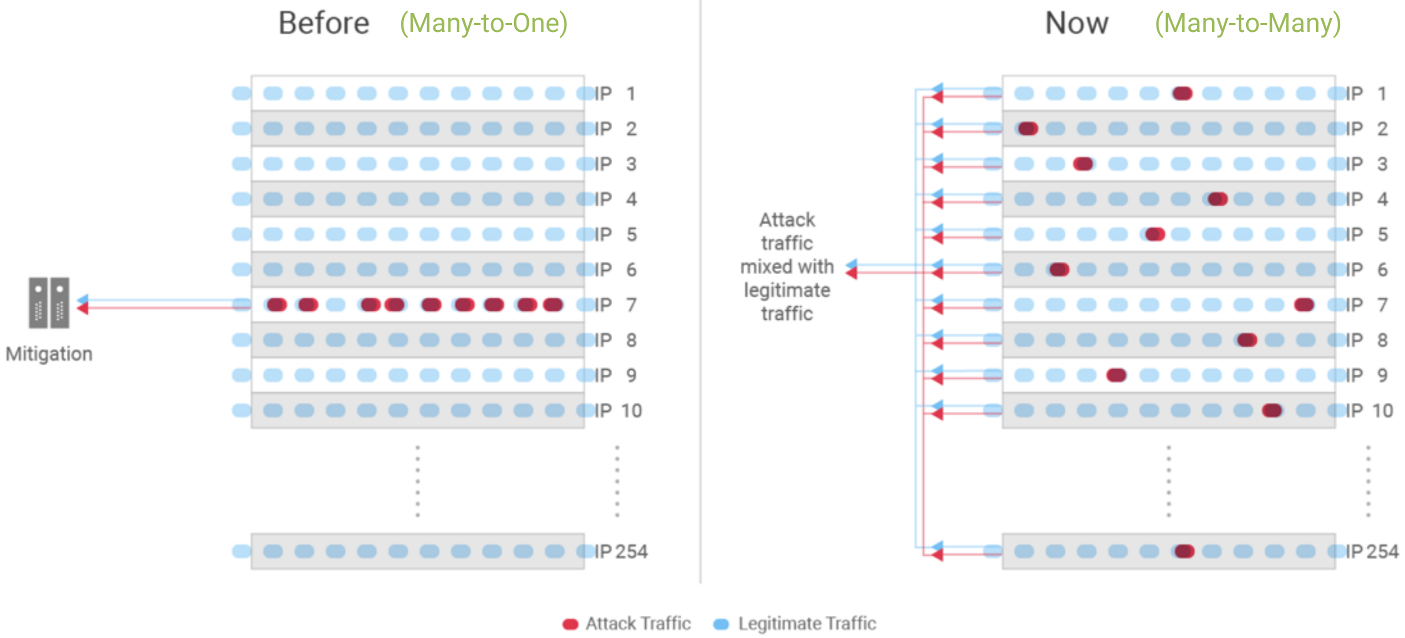
As a result, both the maximum and average attack sizes fell significantly from the same period a year ago.

NEXUSGUARD®

What is “Bits-and-Pieces” Attack?

Blackholing is no longer the solution

If attacker targeted at only a few IPs or domains, blackholing could be a way out.
But unfortunately, Blackholing entire IP prefix, especially those with legitimate traffic, would affect large portions of internet services.



Our Observation of “Bits-and-Pieces” Attack

Attack Summary

Targeted ASNs	159
Attack Types	SSDP amplification attack DNS amplification attack NTP amplification attack CHARGEN amplification attack
Targeted Geolocations	Attacks tended to target resources physically located within the same geolocation
Total IP Prefixes (Class C) under attack	527

Compare to Classical DDoS Attack

	Bit-and-piece	Classical DDoS Attack
No. of targeted IP addresses per IP prefix	49-252 IP addresses	1-3 IP addresses
Attack duration	5.12 - 1439.67 mins	2 - 8692mins
Attack size per IP	2.5Mbps - 300.1 Mbps	50 Mbps - 359Gbps
Attack size per IP prefix	285.4Mbps - 5.32 Gbps	50 Mbps - 359Gbps

Evolved “Bits-and-Pieces” Attack in Q2

No. of targeted ASNs	84	
Attack types	CHARGEN (58.76%) DNS Amplification Attack (23.26%), SSDP Amplification Attack (17.80.%), NTP Amplification Attack (0.18%)	
Targeted geolocations	Belgium, Brazil, Bulgaria, China, Czech Republic, France, Gabon, Germany, Hong Kong, Indonesia, Kazakhstan, Korea, Republic of, Latvia, Netherlands, Poland, Portugal, Romania, Russian Federation, Sweden, Taiwan, Turkey, Ukraine, United Kingdom, United States	
Total IP prefixes under attack (Class C)	No. of Prefix	315
	Total	460

NEXUSGUARD®

DDoS challenges for Network Operators

- Given their large attack surfaces and high profiles, carrier/ASN-level networks are attractive targets for DDoS attacks.
- But the legacy methods and/or hardware put together to mitigate the ever-growing, more complex DDoS attacks (e.g. bit-and-piece, among many emerging attacks) are not effective.
- Network Operators ought to step up efforts to ensure a clean, reliable Internet for customers in a win-win situation for the service provider and customers.

NEXUSGUARD®

CleanPipe as a Platform approach

Benefits

- Protect both the CSP’s own network as well as their downstream customers.
- Eliminate service outages and bandwidth loss due to attacks.
- Save the team a great deal of time/resources figuring out the root cause of outage.
- Generate incremental service revenues and annuities from customers.

NEXUSGUARD®

Key Takeaways

- Mobile and IOT based DDoS attacks will continue to grow
- Cloud and Service Providers become the prime targets
- The rise of Terabits attacks
- Cleanpipe-as-a-Platform (CaaP)

NEXUSGUARD®

Are you ready for the **Next-Gen massive DDoS Attack**?