



# .ASIA AGM 2017

February 26, 2017

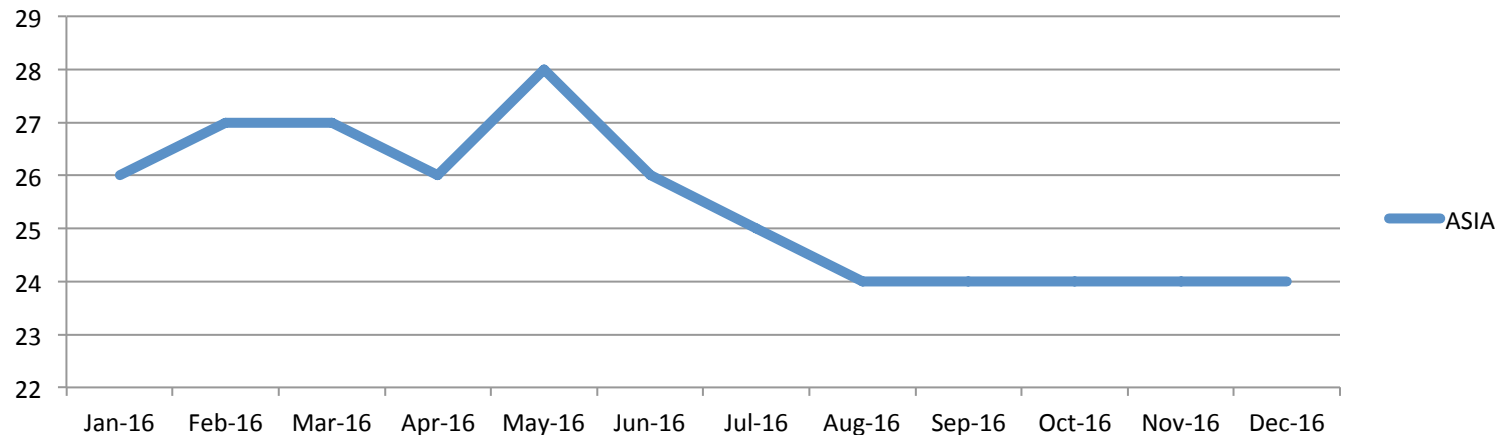
Joseph Yee  
[yyee@afilias.info](mailto:yyee@afilias.info)

- .Asia in 2016 Review
- System Update: Registry, WHOIS, DNS, Registrars
- Security Enhancement
- Hosting Enhancement
- Compliance
- Anti-Abuse highlight
- Operation Avalanche
- Plan in 2017

- Congratulations to DotAsia on your 9 year anniversary in 2016! Afilias is honored to be your technical service provider and a part of your exciting journey.
- There is no unplanned outage in 2016
- Great uptake on new registrars (71 in total) in 2016, all utilize Afilias' onboarding platform ORMS
- Successful promotion in 2016
- Worked together to achieve great success on anti-abuse front (Operation Avalanche), and continue the joint effort with DotAsia on anti-abuse
- Upgrade in .ASIA hosting environment

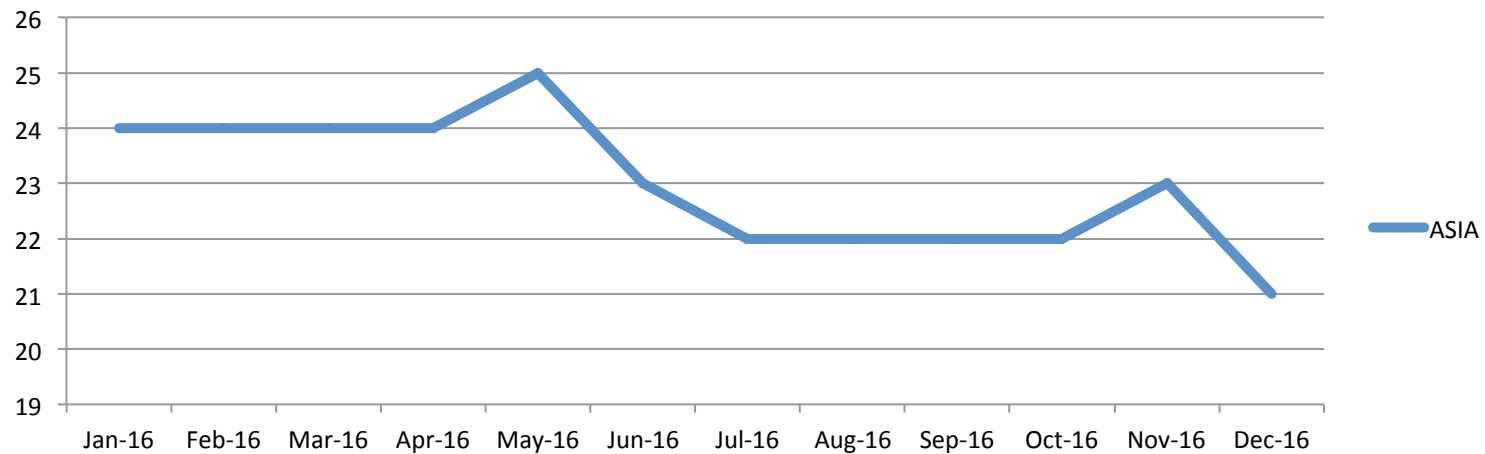
- Systems for .ASIA Stay Nimble & Scalable

**Average Domain Create**



- Average: 25ms ICANN nTLD Requirement: 4000ms (0.625%)

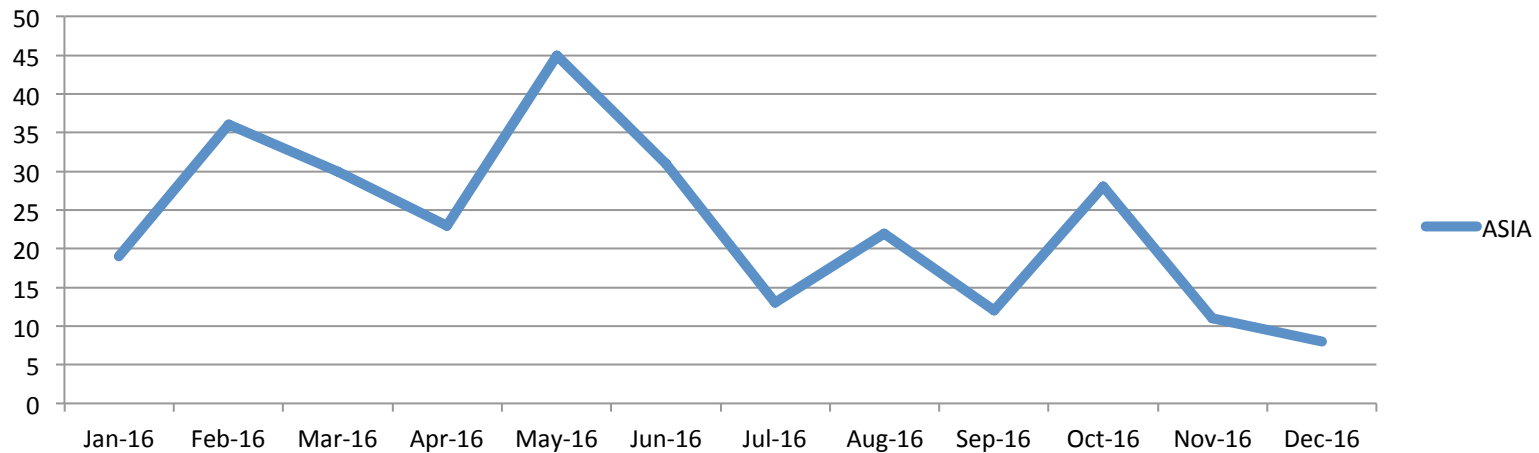
### Average Domain Delete



- Average: 23ms ICANN nTLD Requirement: 4000ms (0.575%)

- WHOIS is fast!

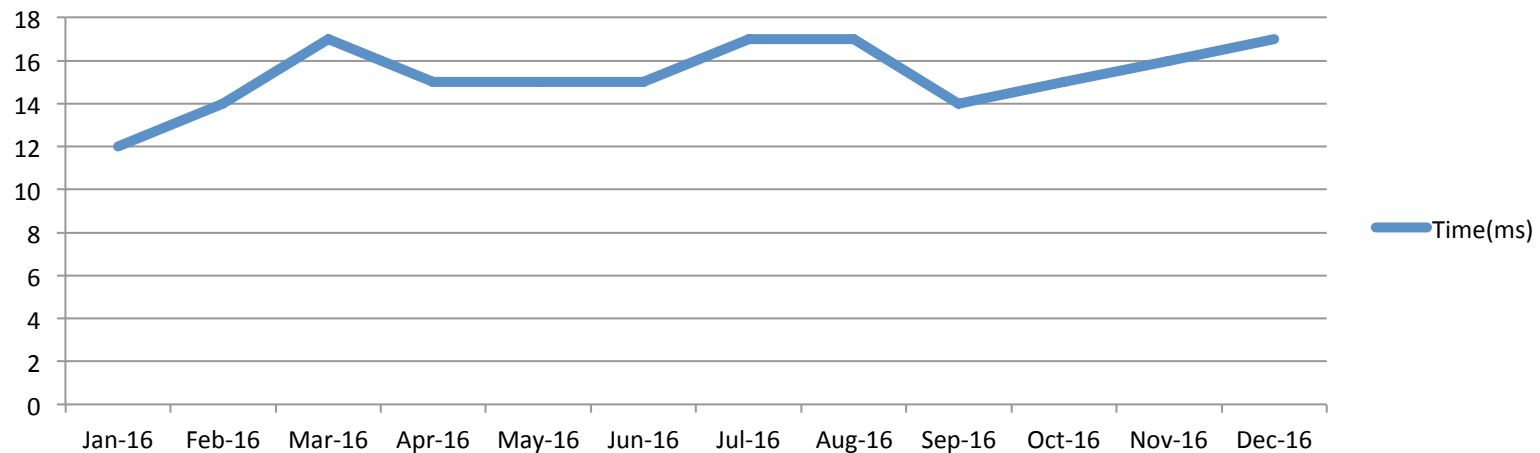
**WHOIS Response Time**



- Average: 23.16ms ICANN Requirement: 1500ms (1.5%)

- DNS stays up 100%

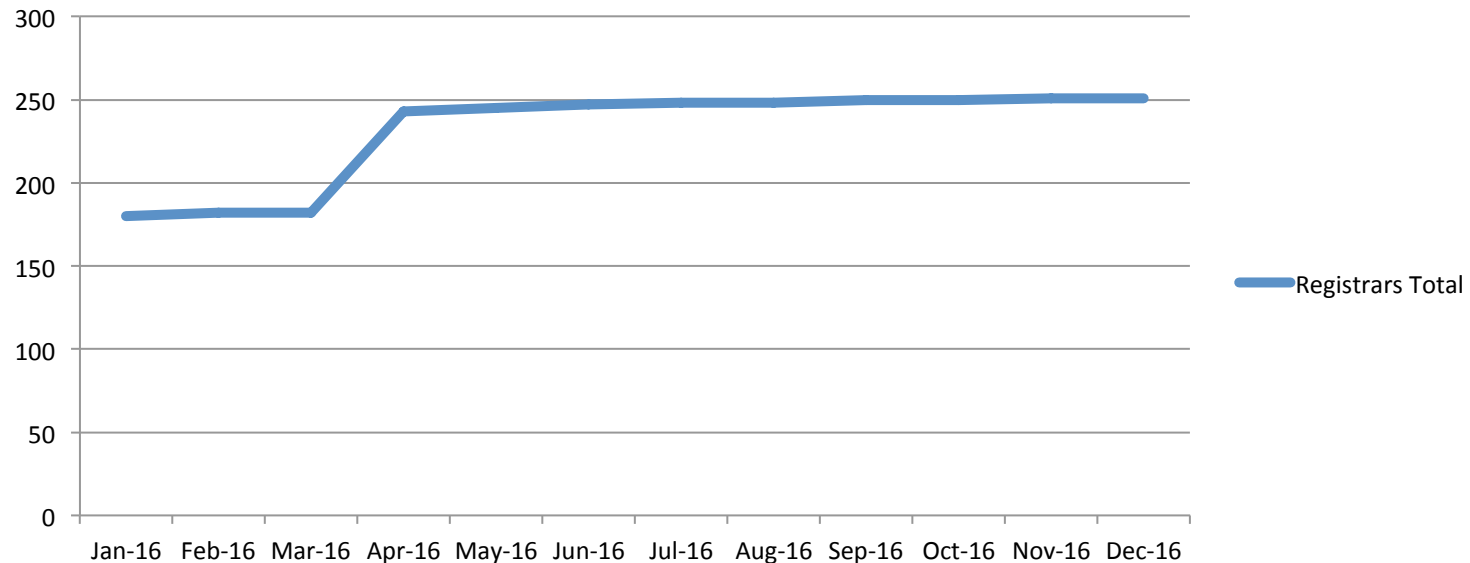
**DNS Queries Response Time**



- Average: 15.33ms ICANN requirement on UDP DNS: 500ms (3%)

- 71 new registrars in 2016, 45 in pipeline. There are 61 new registrars from March to April, and our onboard systems ORMS manage it without any impact to .ASIA.

## Registrars Total





- Prioritize the security and stability of the .asia registry system
- We worked together with .ASIA registrars proactively on Root Certificate update with minimum interruption to registrars
- The Root Certificate update enhance security, also helps registrars to confirm they are connecting to the right system

- In 2016, We worked with DotASIA team to move DotASIA's hosting environment to new home
- The new home has significant enhancement in hardware, security, monitoring & bandwidth

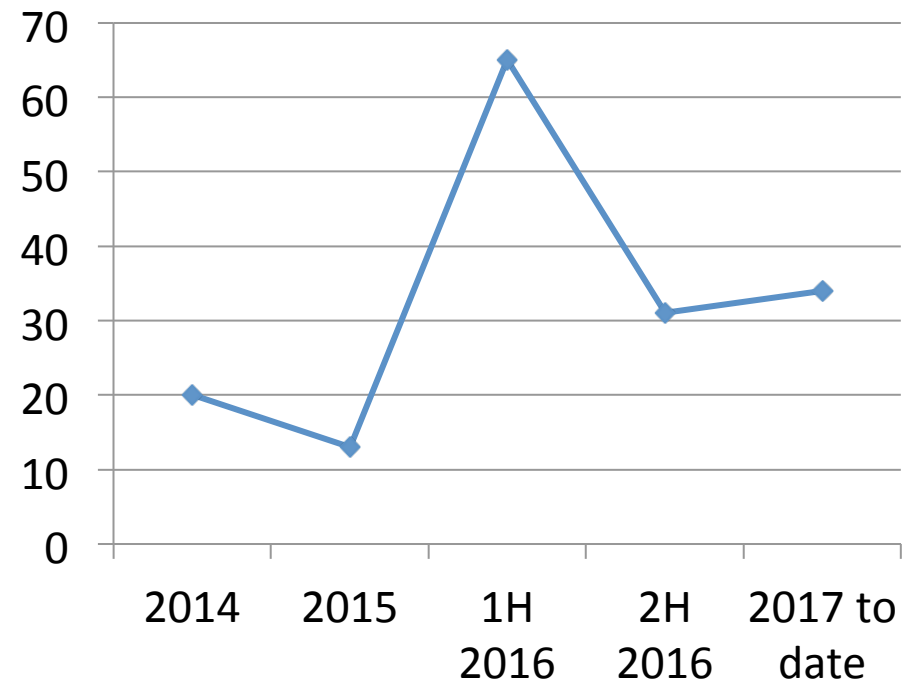
- Ensure compliant registry system for .asia TLD
- ICANN did not issue any compliance notice to .ASIA in 2016.
- In June, Afilias worked together with DotASIA & ICANN to upgrade its monthly report to new format, and to automate the submission process

- In 2016, there are 762 domains confirmed
  - Spam: 711
  - Malware: 20
  - Phishing: 25
  - Botnet C&C: 6
- Significant spam cases dropped, with effort from Security Team, .ASIA, and .ASIA registrars
- But sophisticated attack utilizing .ASIA domains increases (Malware, Phishing, Botnet all increases compared to 2015)

# Anti-Abuse Highlight

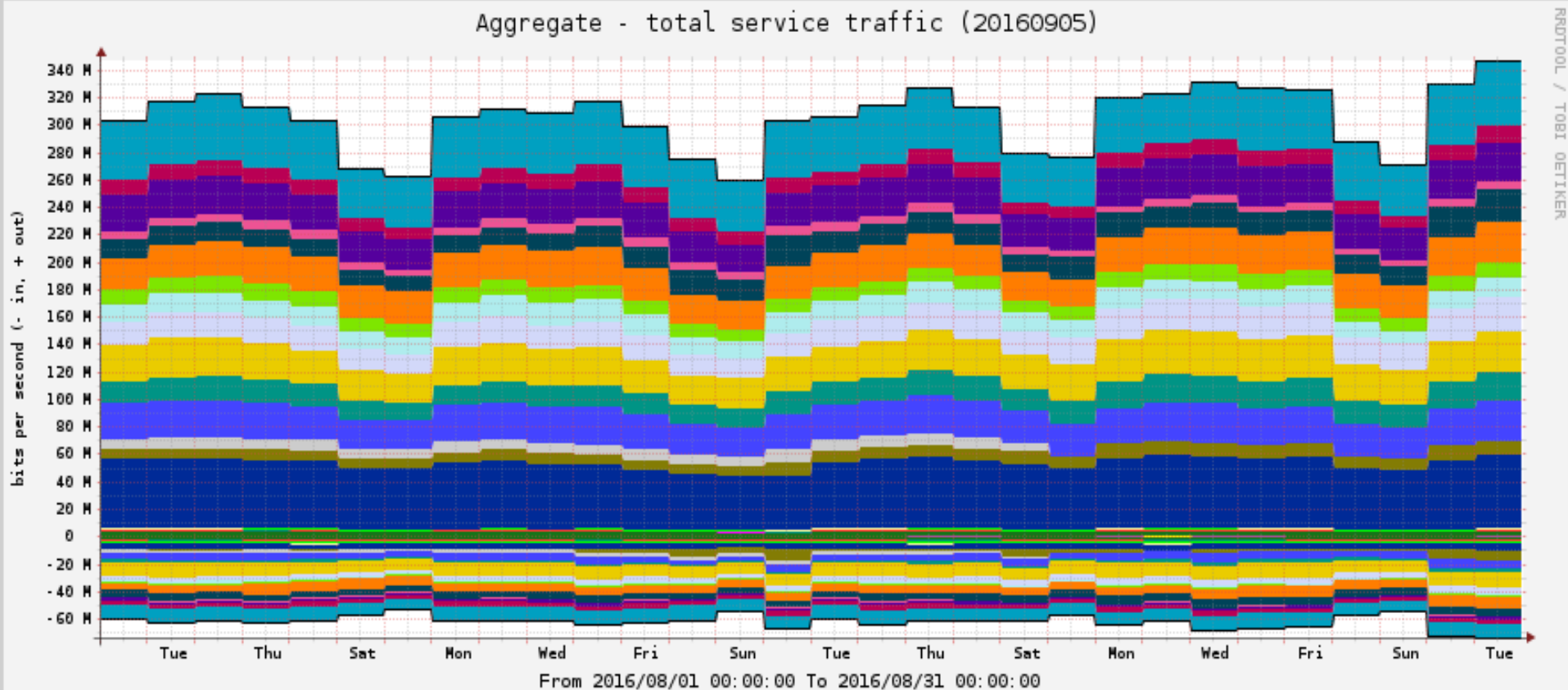
- By end of 2016, .ASIA was 31<sup>st</sup> most used TLD for spam.
- Change in rank due to spammers buying .asia domains but not activating them immediately.
- Large number of domains activated for spam in 2H2016.
- Our Security Team continues to work with third parties like Apple & Paypal on threat intelligence and act swiftly on malicious domains.

## **.ASIA Spamhaus ranking**



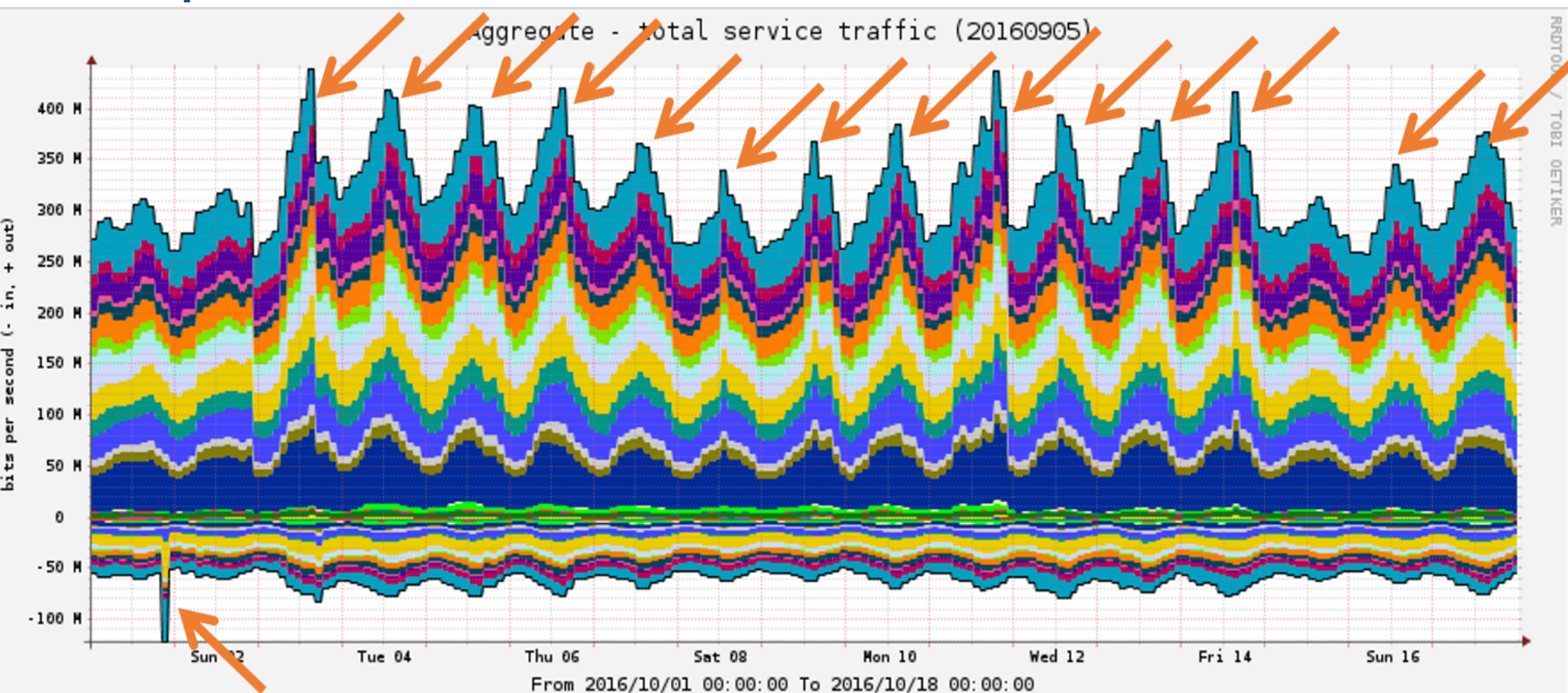
- DNS was being attacked constantly throughout 2016
- DNS provider Dyn was attacked in Oct 2016, many services were interrupted including Twitter, Amazon.com, CNN, Paypal, Reddit, etc.
- Afilias infrastructure faced attacks too, some samples of DNS traffic during relative normal time, constant small scale attacks, and mix of mid & small scale attacks

## Quiet August – No Appreciable Attacks





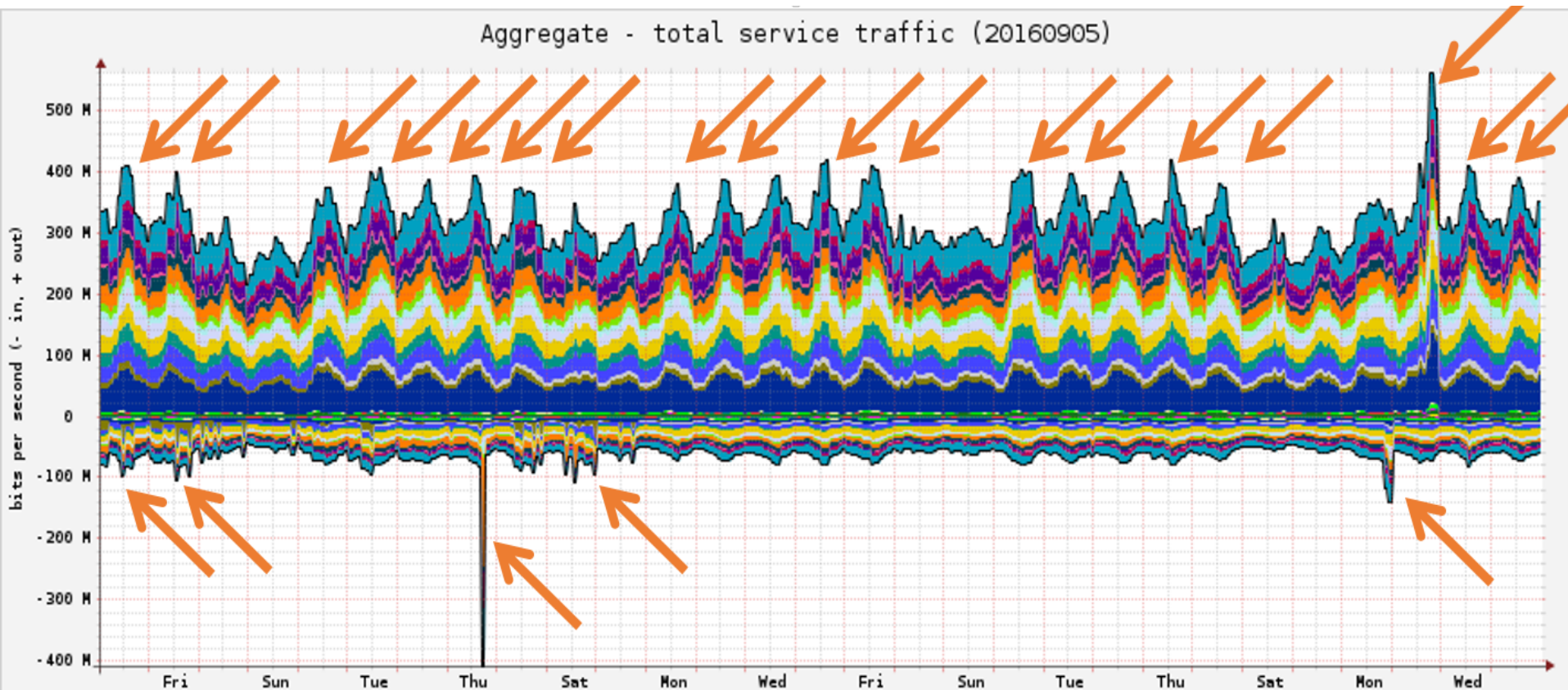
## September – 15 Small attacks

























# DNS Traffic and Attacks – 3 Very Different Months

- October – 1 Medium, 22 Small Attacks



# Sources of DDoS: China is largest source

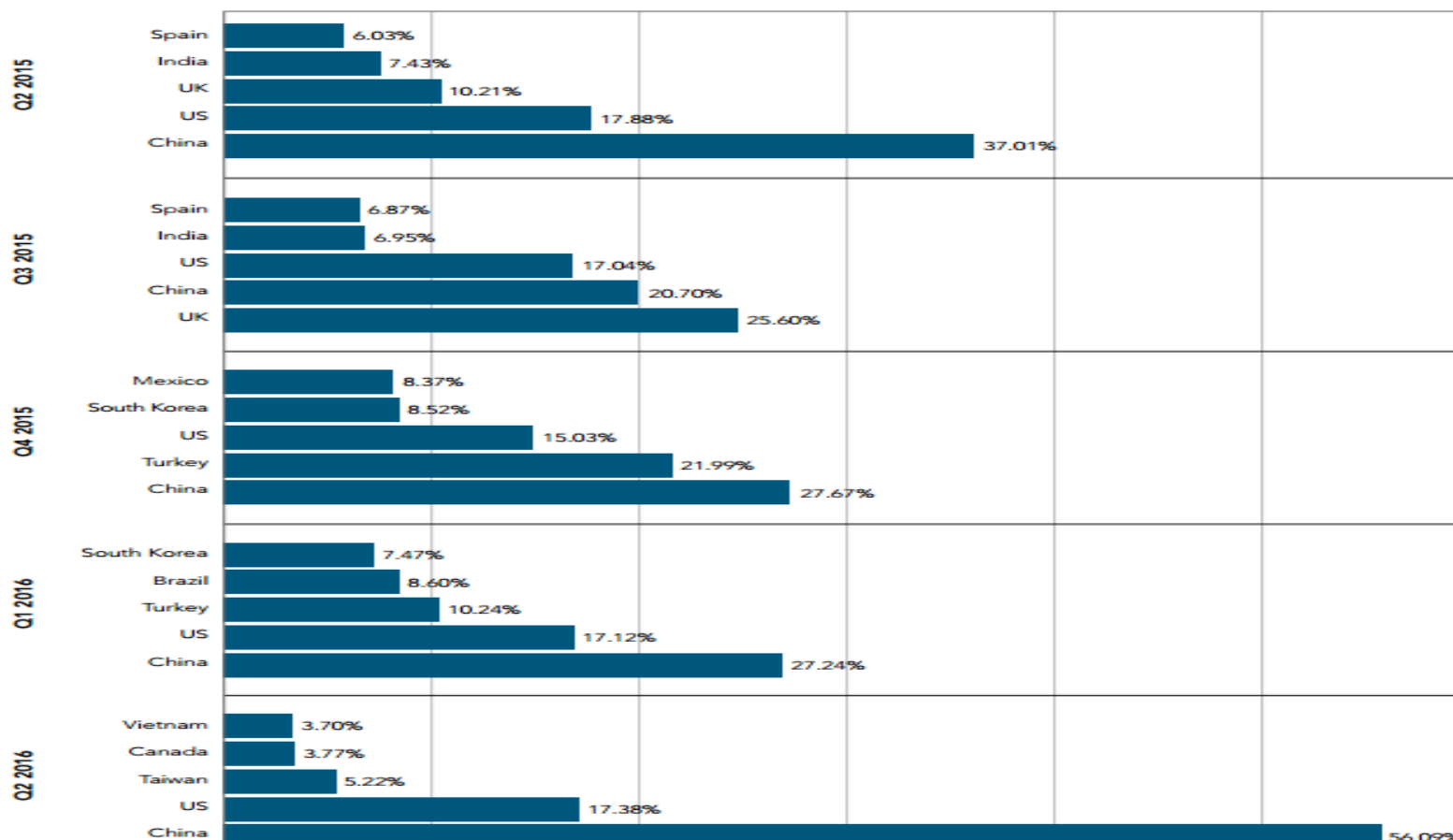
**Top 10 Source Countries for DDoS Attacks, Q2 2016**

	China	56.09%	
	US	17.38%	
	Taiwan	5.22%	
	Canada	3.77%	
	Vietnam	3.70%	
	Brazil	2.96%	
	Spain	2.94%	
	Singapore	2.90%	
	Italy	2.65%	
	UK	2.38%	

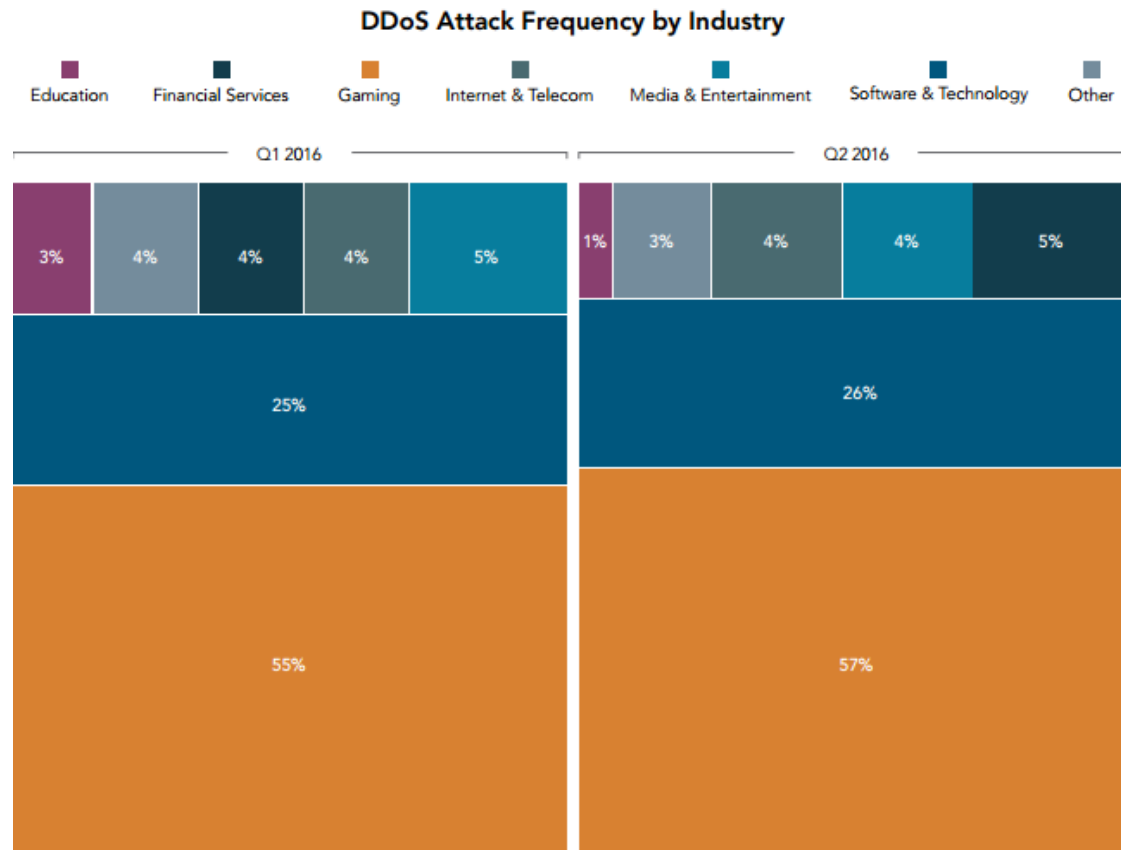
Source: <https://www.stateoftheinternet.com>

# Source of DNS Trend

**Top 5 Source Countries for DDoS Attacks, Q2 2015 – Q2 2016**



# Who is being affected?



Source: <https://www.stateoftheinternet.com>

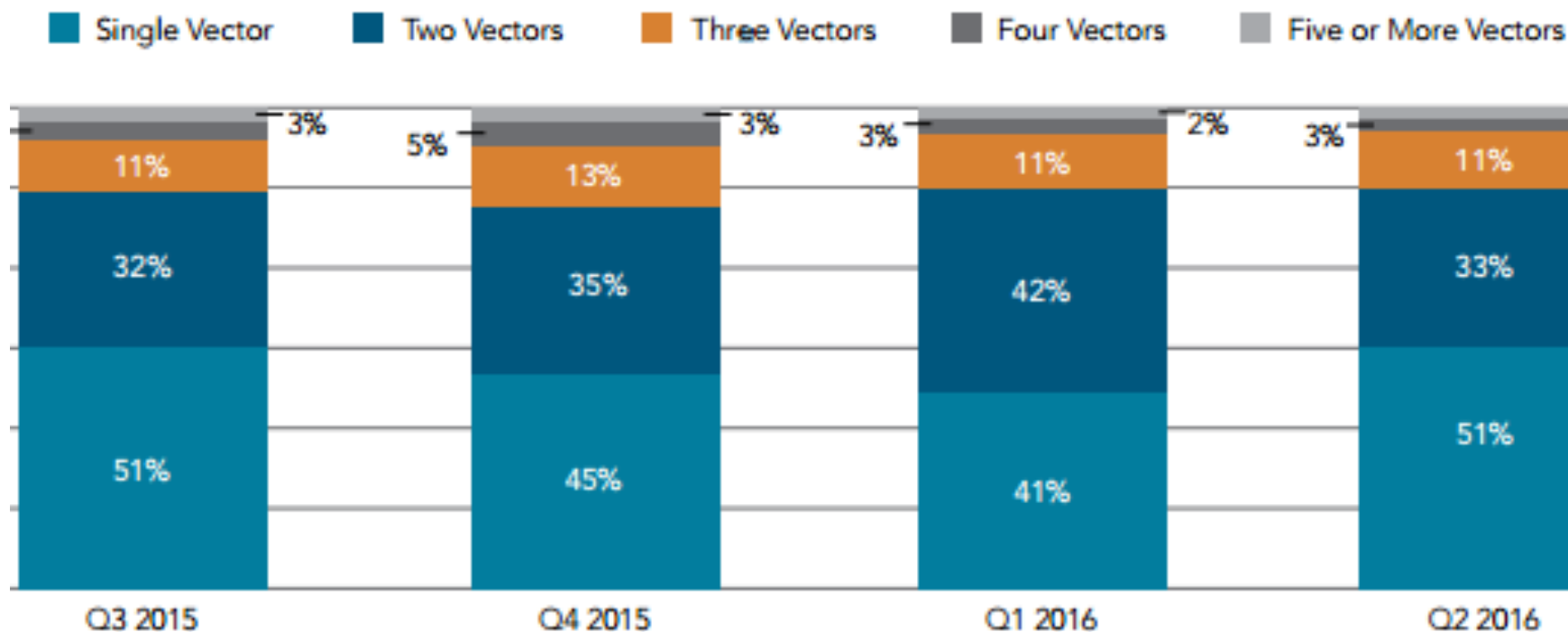
# DNS Attacks by the Numbers

- DDoS attacks, Q2 2016 vs. Q1 2016
  - 9% increase in total DDoS attacks
  - 10% increase in infrastructure layer (layers 3 & 4) attacks
  - 47% increase in UDP flood attacks
- DDoS attacks, Q2 2016 vs. Q2 2015
  - 129% increase in total DDoS attacks
  - 151% increase in infrastructure layer (layers 3 & 4) attacks
  - 276% increase in NTP reflection attacks (a record high)
  - 70% increase in UDP flood attacks
- New record DDoS attack: 363 Gbps in Q2 2016

Source: <https://www.stateoftheinternet.com>

# Multi-Vector DDoS Attacks

## Multi-Vector DDoS Attacks, Q3 2015–Q2 2016



Source: [www.akamai.com/StateOfTheInternet](http://www.akamai.com/StateOfTheInternet)

- 5 New algorithm and software upgrades to handle changing requirement characteristics
- 15 New DNS nodes (to 80+ nodes)
- 3 New nodes in South America
- 2 New nodes in Africa
- 4x Increase in global resiliency and node capacity

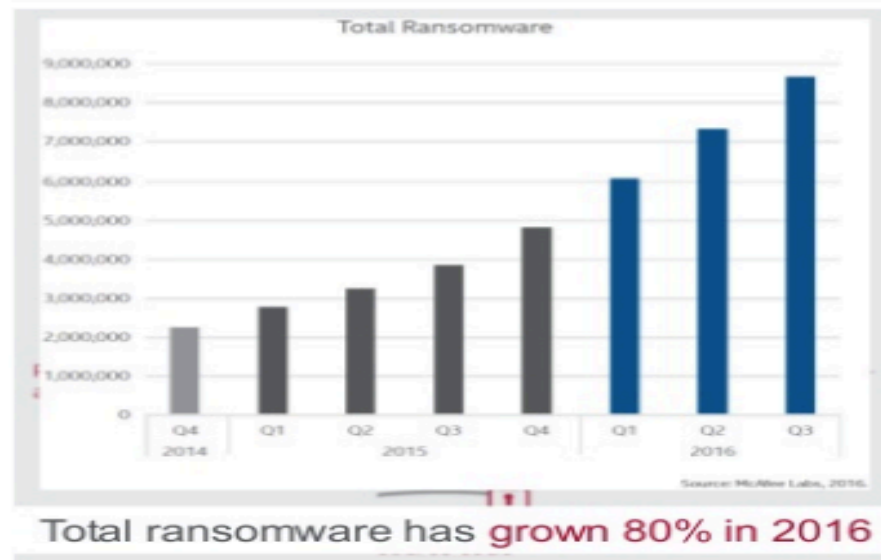


# Threats in 2017

- Beyond spam, two types of new threats stepped to forefront: Ransomware, Internet-of-Things (IoT) Botnets

## McAfee Labs 2017 Threats Predictions Ransomware

2016 – The year of ransomware



Continue the 2017 threat predictions discussion – tweet to: [#LabsPredictions](#)



# Operation Avalanche

- In November 2016, we worked together with DotASIA, ICANN, Registrar, Security Firm, Police Authority on taking down a large botnet used for mass global malware attacks and money mule recruiting campaigns
- We worked proactively with the security firm and registrar on their setup to ensure they can work on the .ASIA domains
- Only a handful of .ASIA domains involved, due to proactive effort from the past, but in order to take down botnet effectively, one can't allow any leak
- In the past, many bot-net will resurrect in 24-48 hours. So far, this bot-net is still down. It is not back live, especially not utilize .ASIA names.

# Plan in 2017

- Registry Excellence – continue to beat SLA
- DNS – 100% uptime despite continuous attack, no interruption to end user
- Anti-abuse: Drive abuse out with active monitoring and daily intervention
- Security: Constantly enhance system and user environment
- Partnership: sharing the cost of promotions to drive growth as we had in the past (promotion in progress in 2017)
- Planning in motion: to move .ASIA to a new platform when details of new Registry Agreement confirmed, with many enhancement and features for .ASIA registrars

Thank You!



***Questions?***



Thank you