



DDoS Trend Analysis through 2010, Infrastructure Security Report & ATLAS Initiative

Yaroslav Rosomakho
Senior Consulting Engineer, EMEA

Introduction



- Yaroslav Rosomakho, Senior CE, EMEA.
- 10+ years of experience in Networking and Security.
- 4xCCIE (R&S, Voice, Security, SP)

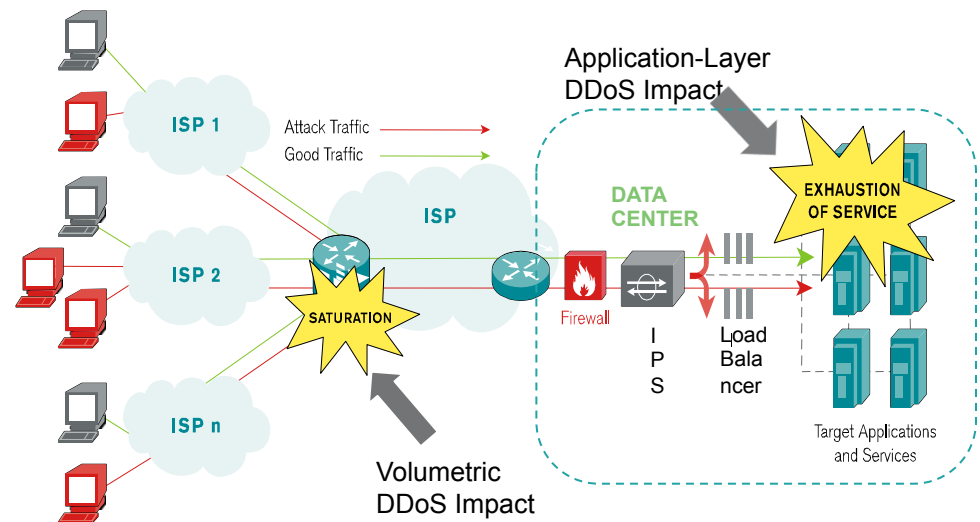
- 300+ employees in 20+ countries
- 300+ customers
 - 90%+ of Tier1 providers,
 - 60%+ of Tier2 providers, 11 of 13 of NA MSOs.
 - Privileged relationships with majority of world's ISPs
 - ATLAS / ASERT thought leadership.



DDoS Primer

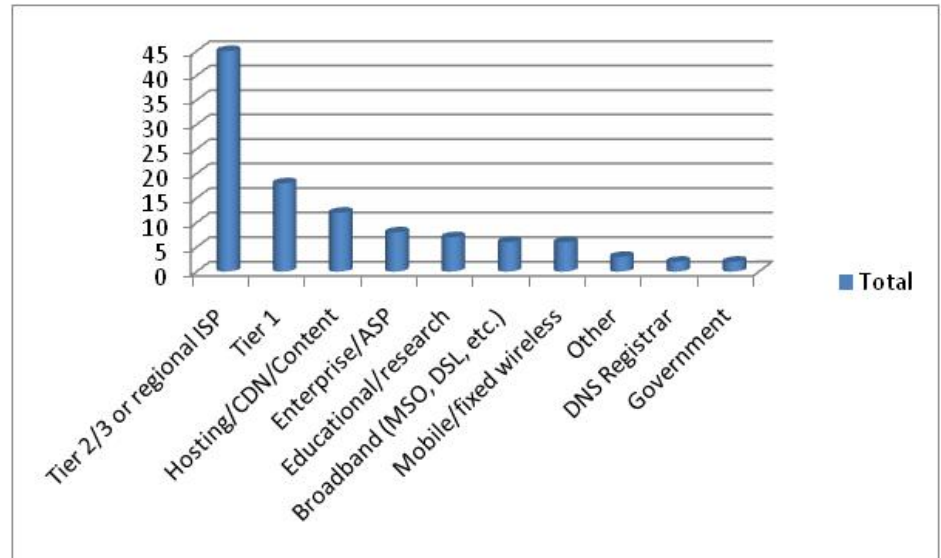
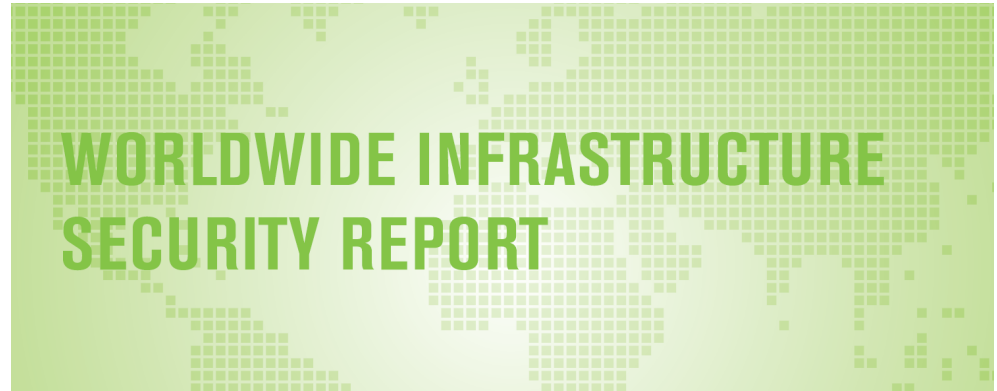
What is a Denial of Service attack?

- An attempt to consume finite resources, exploit weaknesses in software design or implementation, or exploit lack of infrastructure capacity
- Effects the availability and utility of computing and network resources
- Attacks can be *distributed* for even more significant effect
- The *collateral damage* caused by an attack can be as bad, if not worse, than the attack itself



2010 Infrastructure Security Survey

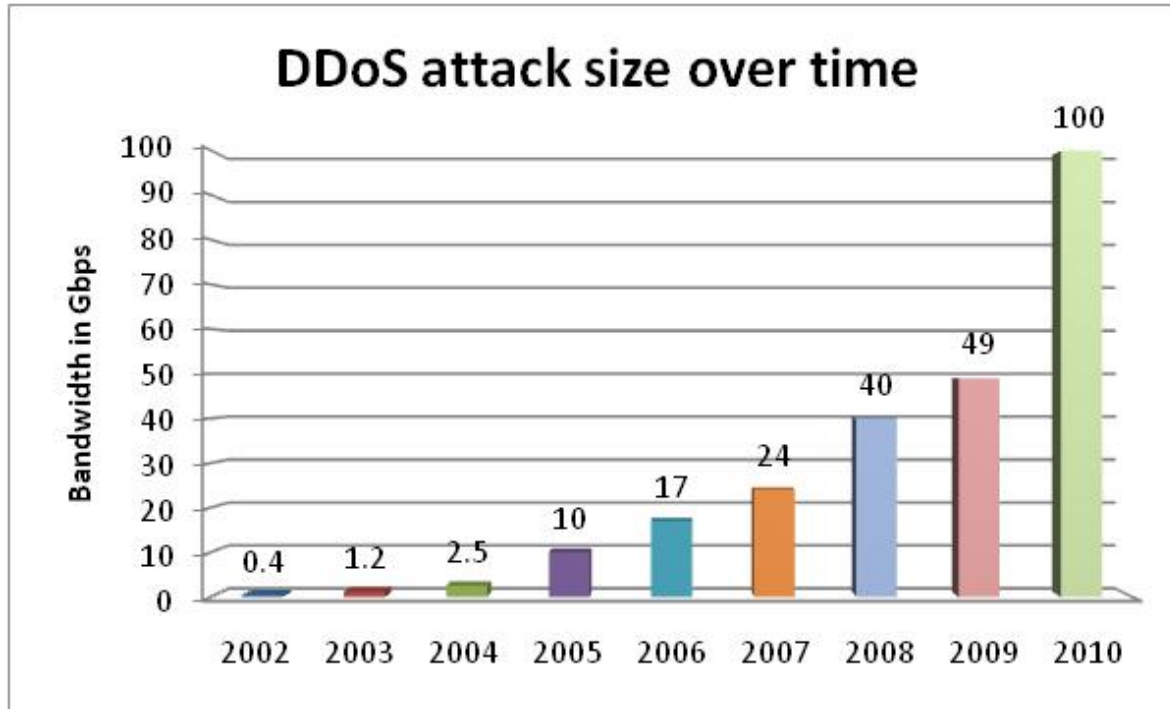
- 6th Annual Survey
- Survey conducted in September – October 2010
- 111 total respondents contributed
 - Service providers
 - Content/ASPs
 - Enterprises
 - Broadband
 - Mobile
 - DNS
 - Educational



Key Findings of the Survey

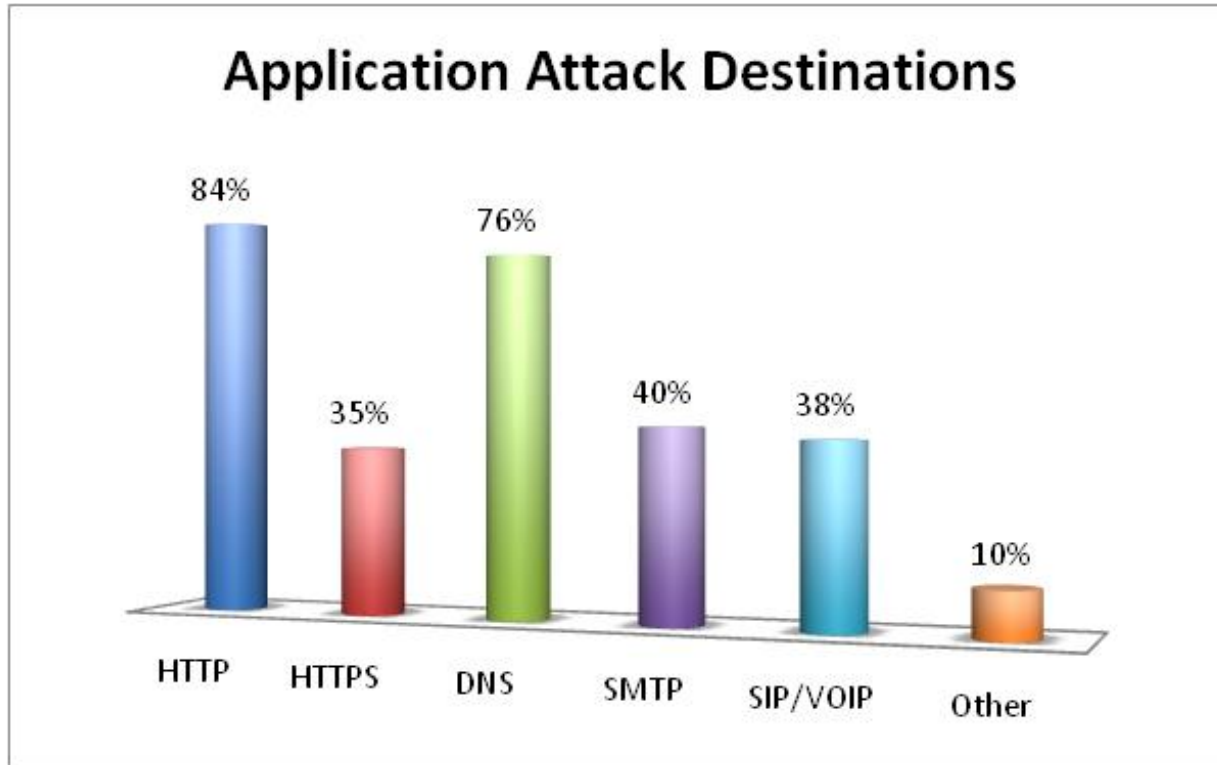
- **Threat severity and complexity continue to increase**
 - Attack size increases dramatically, impacting underlying network infrastructure
 - 102% increase in attack size YOY
 - Broke 100Gbps barrier for first time
 - Up 1000% since first Arbor's first WISR in 2005
 - Application layer attacks continue with some new applications being targeted more frequently.
 - HTTP and DNS remain the top targets but HTTPS, SMTP and SIP/VOIP attacks are becoming more common
 - **The Threat-to-Defense gap is the widest observed to date**
 - DDoS attack capabilities of miscreants are outpacing the defensive measures taken by network service providers
- **Firewall and IPS equipment represents critical points of failure during DDoS attacks**
 - These products are commonly the targets of DDoS attacks

DDoS Attack Sizes Over Time



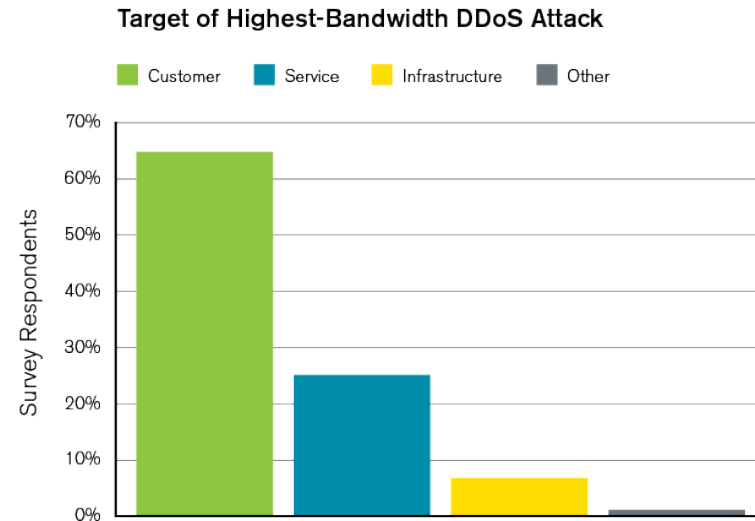
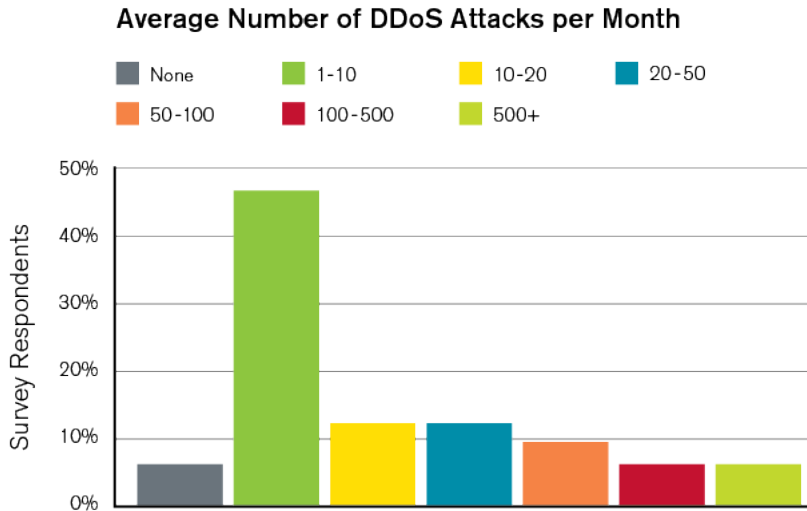
- Over 102% increase YOY in attack size shows resurgence of brute force and volumetric attack techniques
- Internet providers have focused on application threats so miscreants turned back towards attacking network capacity

Application Layer Attacks



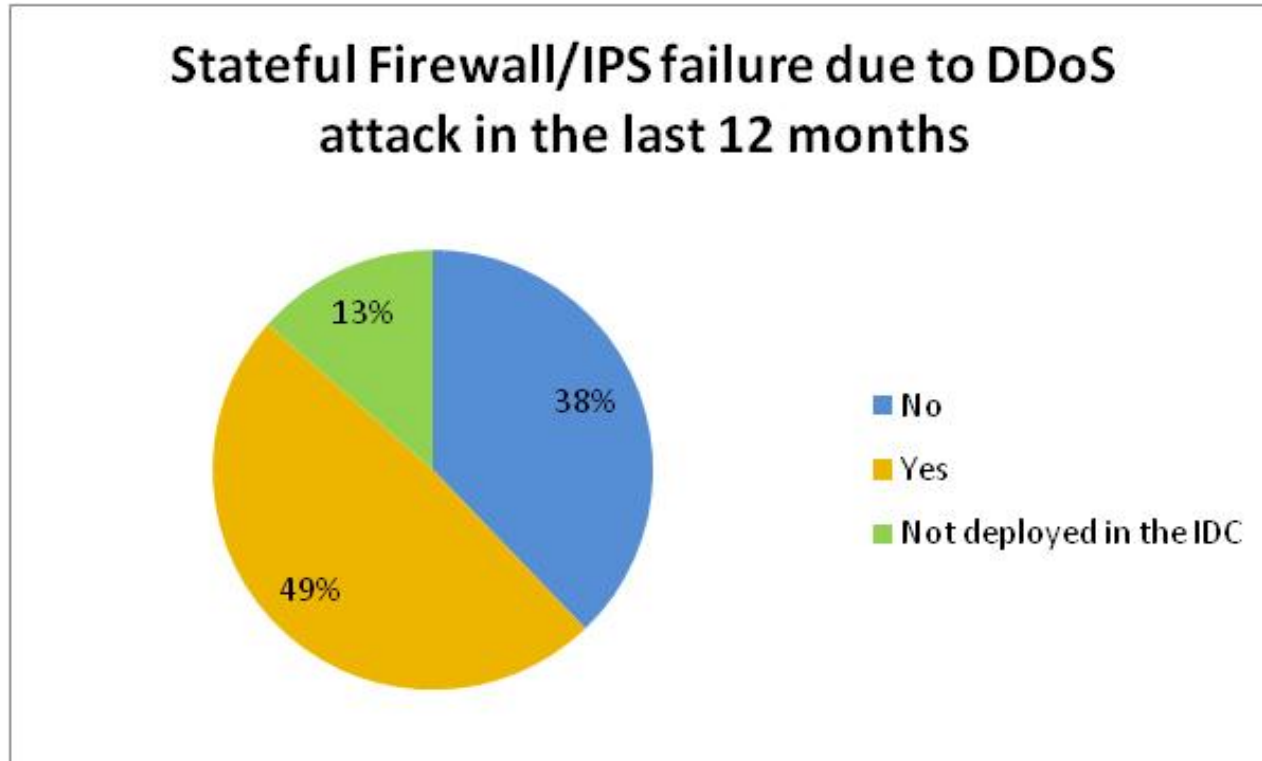
- **Application layer attacks are becoming common place**
 - 77% of respondents reported application layer attacks against critical services
 - Lynchpin service infrastructure remain top targets
 - Application attacks are advancing to more sophisticated services

Attack Frequency and Targets



- **Attack frequency is increasing**
 - 94% of respondents see at least 1 DDoS attack per month
 - 35% of respondents see 10 or more DDoS attacks per month compared to 18% in 2009
- **Customers or services comprise 87% of targeted victims**
 - Major collateral events are less common, but drive greater impact

Firewall and IPS are not designed for availability



- Nearly half of all respondents have experienced a failure of their firewalls or IPS due to DDoS attack

The Arbor ATLAS Initiative

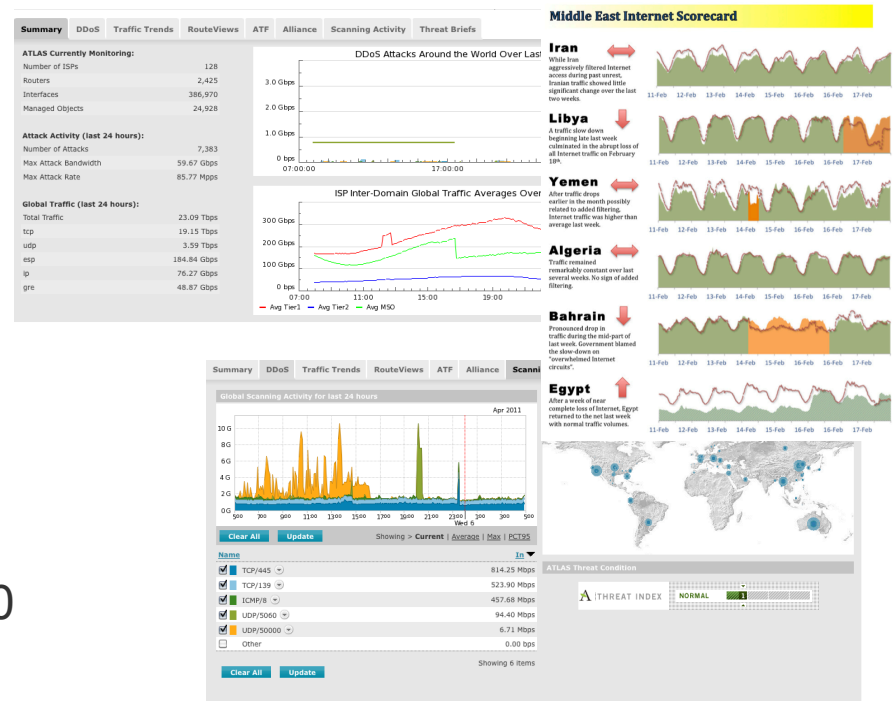
- What is it?
 - Active Threat Level Analysis System
 - A set of tools to model internet traffic patterns and Internet threat evolution

- How is it used?

- Within Arbor Products
- Atlas.arbor.net site / Blog
- Various Presentations
 - Trends in Internet Traffic Patterns – NANOG 47 / MENOG
 - Botnet, DDoS and Ground Truth – NANOG 50
- Broader Security Community

- What is it for?

- Broaden our understanding of the Internet



The Arbor ATLAS Initiative

Three Primary Direct Data Sources

- 100+ ISPs sharing real-time data
 - A cross section of global tier-1, national tier-2 carriers and the largest content providers; covering 20+ countries
 - Automated XML export from Arbor Peakflow SP deployments
 - ONLY where enabled by the customer
- **ATLAS Sensor Network**
 - Network of honey-pots over 4 continents
 - Route coverage includes North America, South America, Europe & Japan
 - 1 – 1.5 million unique IPv4 Internet addresses
- **30+ ISPs sharing full real-time routing data**



The Arbor ATLAS Initiative: Internet Trends

- Exported XML contains:
 - Traffic Reporting data for:
 - Whole Network breakouts for ASNs, Protocol, TCP / UDP Ports, Application and Geo IP stats and total traffic.
 - Anonymised data for Medium / High detected threats
 - Attack sources and destinations within the contributing service provider are obfuscated (X.X.1.1)
 - Data is stored centrally by Arbor and analysed using scripts
 - Inter-ASN traffic data
 - Internet Connectivity
 - Port / Protocol mix
 - GeoIP Country stats
 - DDoS threat evolution

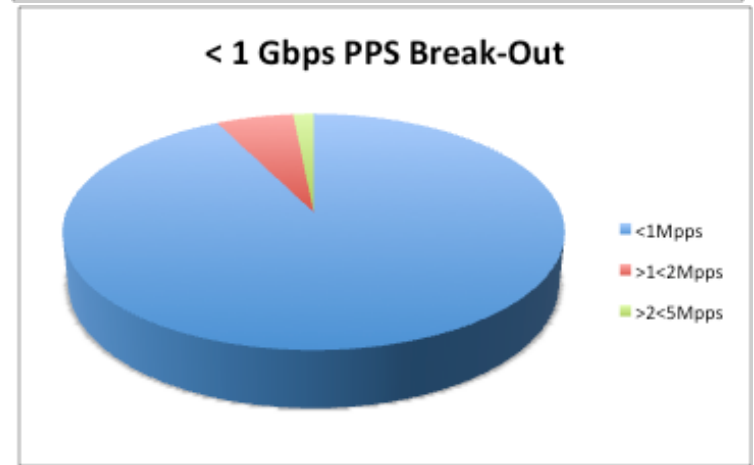
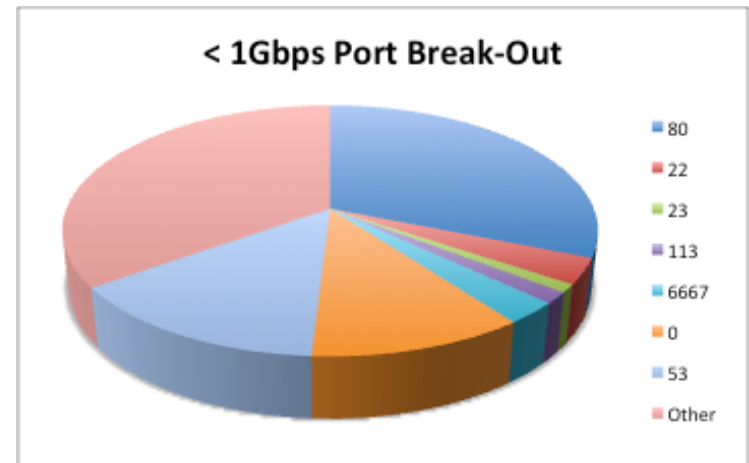
The Arbor ATLAS Initiative : Sensor Network

- Probes allocated dark IP space within carrier networks.
- Globally routable and allocated IPs that should not contain **ANY** active servers or hosts
- Multiple darknet use cases
 1. Flow collection
 2. Backscatter detection
 3. Packet sniffing
 4. Reconnaissance identification
- No legitimate packets should **EVER** be destined to these IPs
 - **Packets seen in dark IPs usually sourced by malware & botnets (spam, phishing, DoS, exploit scanning, etc.)**
- Since nearly all traffic is illegitimate, darknet analysis incurs low false positive rates
- Used to collect scan and attack / exploit data
 - All data is collected / analysed automatically

2010 ATLAS Initiative: Internet Trends

Small Attacks Continue to Make Up the Majority

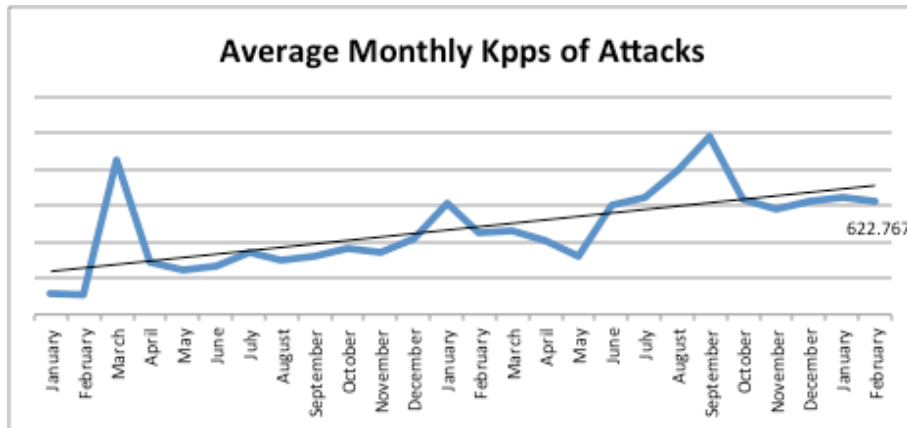
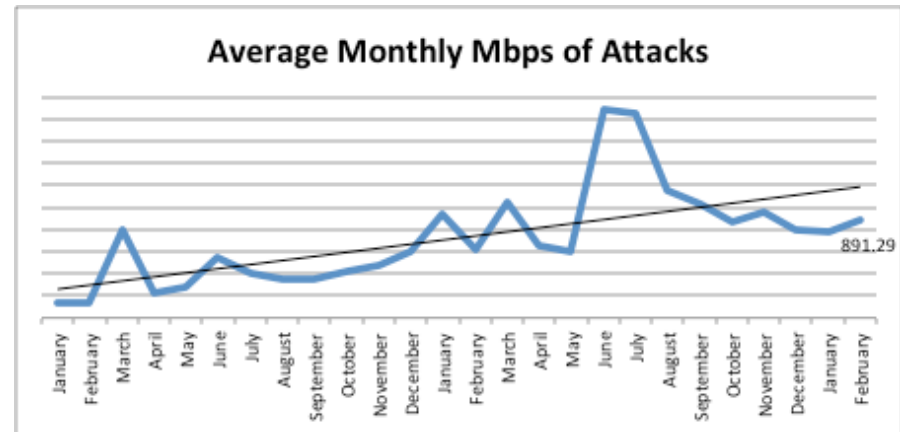
- In 2010 most attacks still small:
 - 79% less than 1Gb/sec (down from 93% in 2009)
 - 87% less than 1Mpps (down from 94% in 2009)
- Average BPS of attacks less than 1Gb/sec is 197.41Mbps
- Average PPS of attacks less than 1Gb/sec is 307.72Kpps
- Longest duration attack less than 1Gb/sec:
 - 17.94Mbps / 43.5Kpps
 - SYN Flood
 - 236 days, 22Hours, 26 mins



2010 ATLAS Initiative: Anonymous Stats

Attack Growth trend in Mbps and Kpps

- Average monthly attack size growing since start of 2009.
- Average attack is 891Mbps / 622.7Kpps, Feb 2011

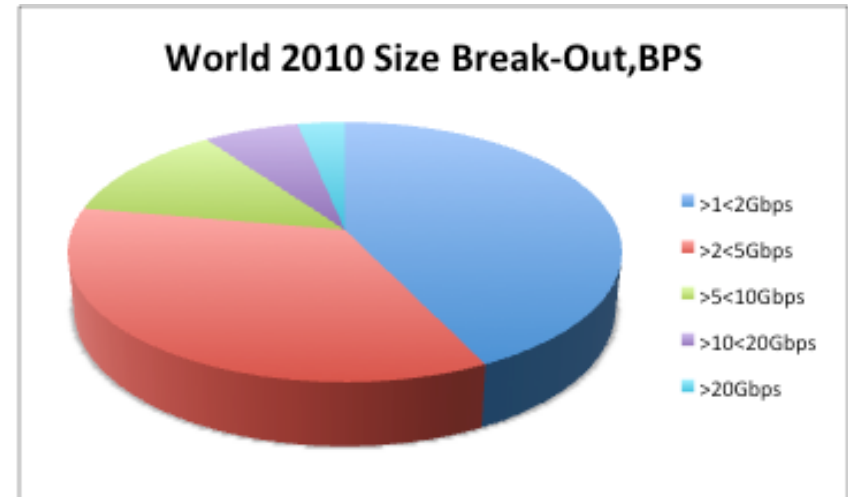
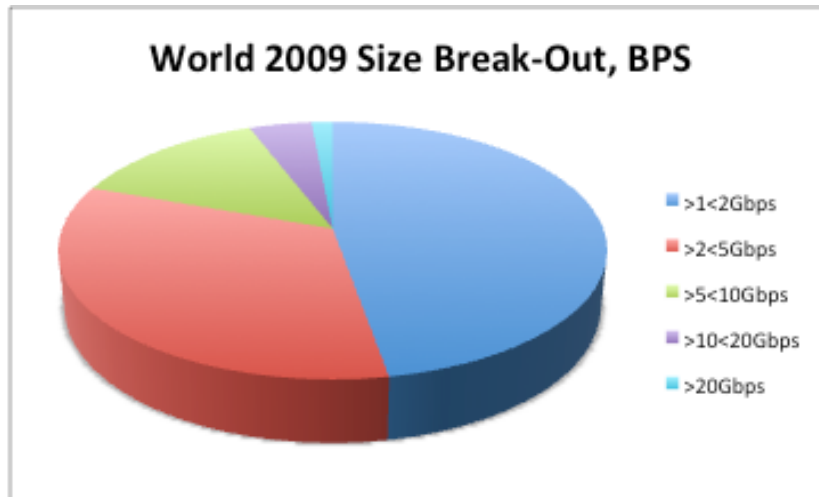


- Average attacks sizes have grown by 576% / 447% since start of 2009
- Spike in average BPS / PPS in late summer 2010

2010 ATLAS Initiative: Internet Trends

Attacks over 10Gb/sec on the rise!

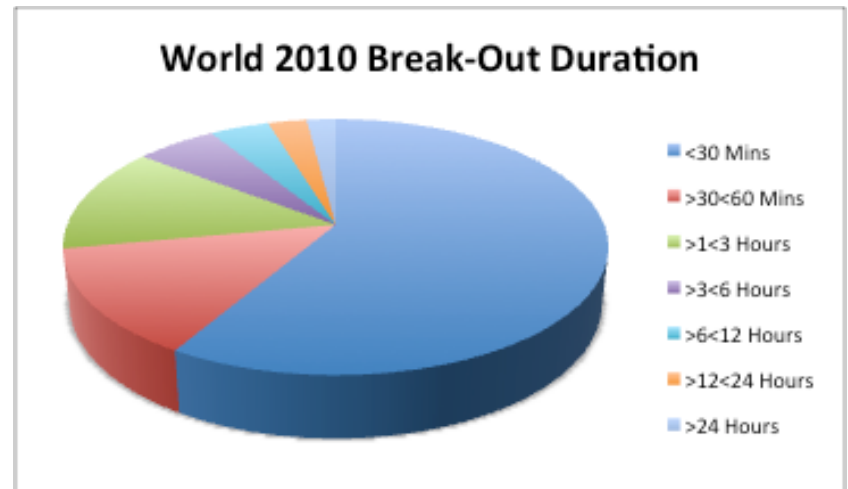
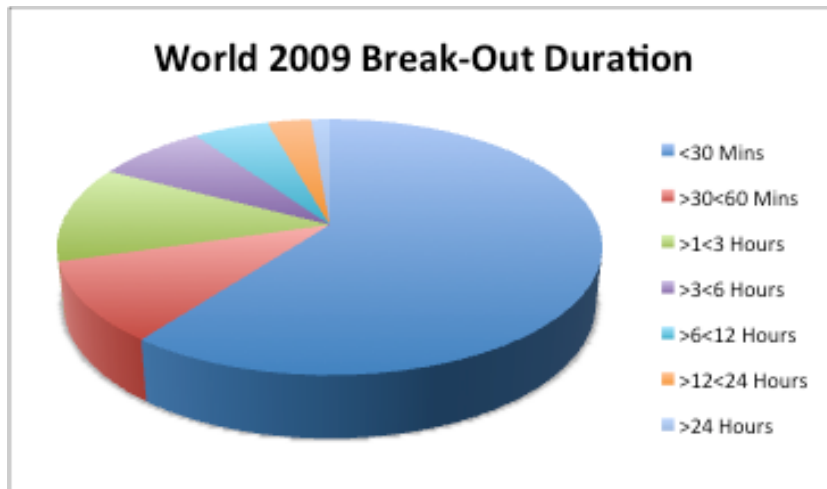
- Proportion of monitored attacks over 10Gb/sec has grown by 470% from 2009
- Monitoring > 10Gb/sec attack approx every 6.5 hours
- Increase in large bps / pps attacks year on year:
 - 319% increase in number of monitored attacks > 10Gbps from 2009 – 2010.
 - 45% growth in number of attacks > 10Mpps.



2010 ATLAS Initiative : Internet Trends

Attack Duration Mix Almost Constant

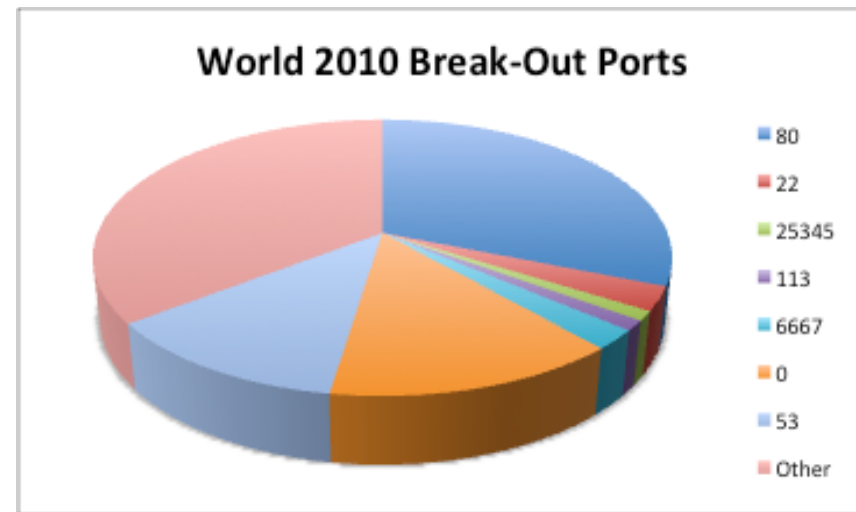
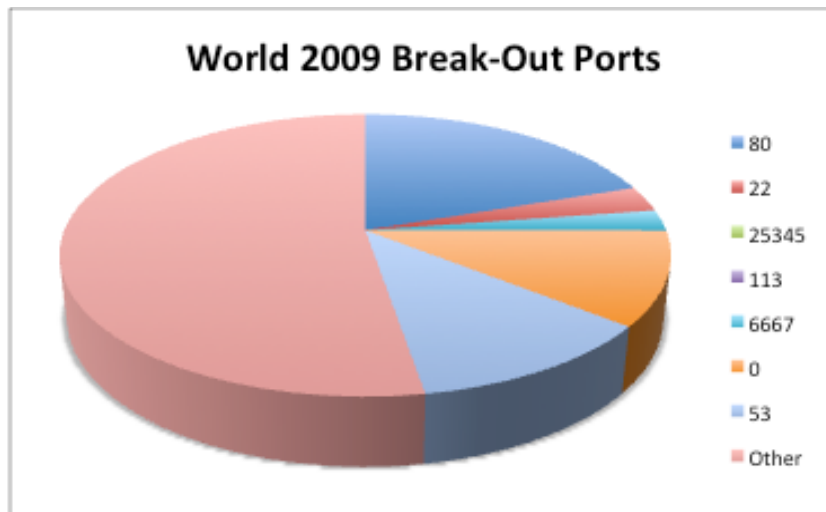
- Majority of attacks short-lived.
- Approx 70% less than 1 hour
- Number of attacks lasting longer than 24 hours up by 54.9%
 - But, still only 2% of total number of attacks



2010 ATLAS Initiative : Internet Trends

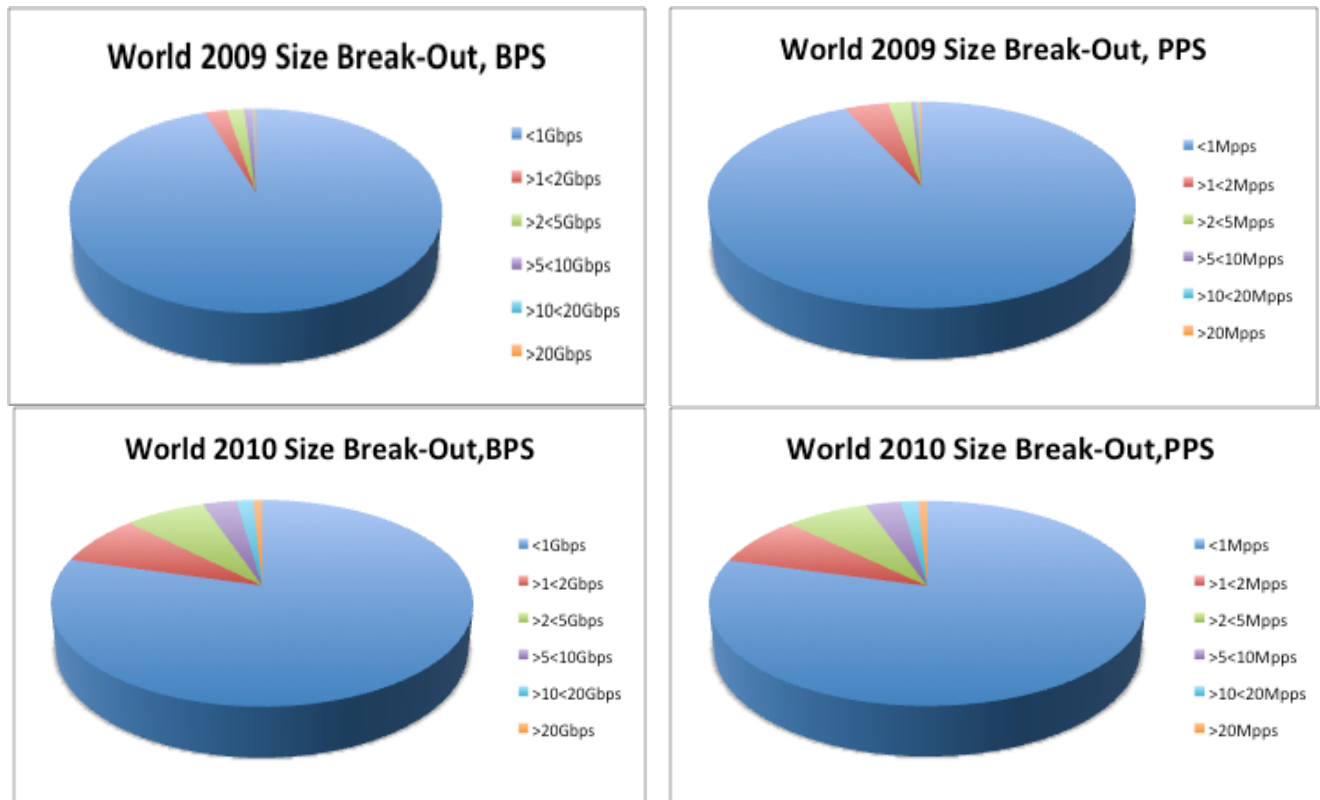
Proportion of Attacks Targeting Port 80 Increase

- In 2009, 19.6% of monitored attacks targeted port 80.
- In 2010 this had increased to 31%.
- Attacks targeting fewer ports
 - 80, 53 and Fragment
- Nearly 597% growth in number (474) of attacks over 10Gb/sec, targeting port 80.



2010 ATLAS Initiative : Internet Trends

Size of Attacks Targeting Port 80 Shifts UP



- 292% growth in proportion of attacks over 1Gbps.
- 500% growth in proportion of attacks over 10Gbps.
- 246% growth proportion of attacks over 1Mpps
- 398% growth proportion of attacks over 10Mpps

2010 ATLAS Initiative : Internet Trends

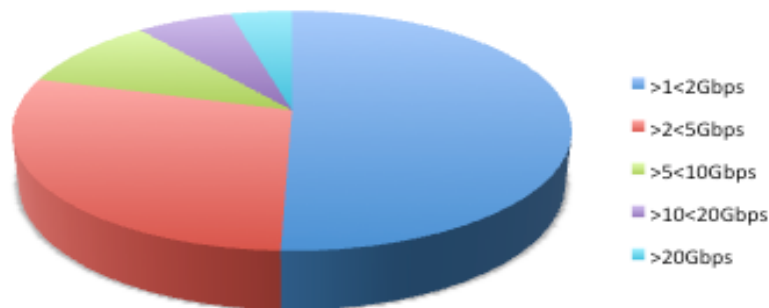
Size of Attacks Targeting Port 53 Increase

- Proportion of monitored attacks targeting port 53 stays roughly the same.
- 885% increase in number of attacks over 10Gb/sec

World 2009 Size Break-Out, BPS



World 2010 Size Break-Out, BPS

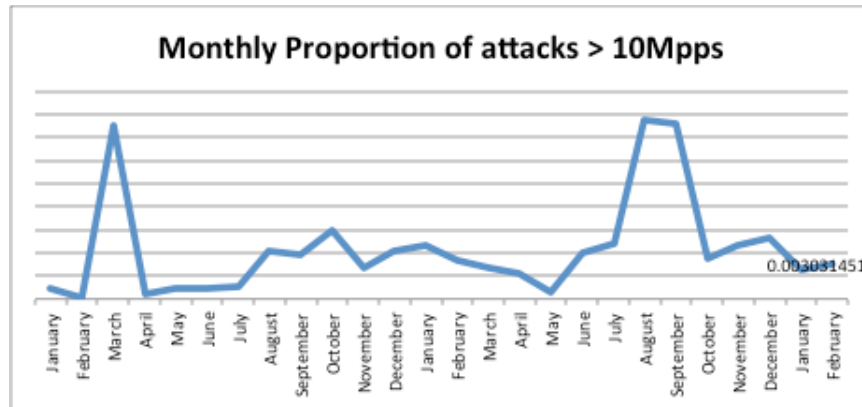
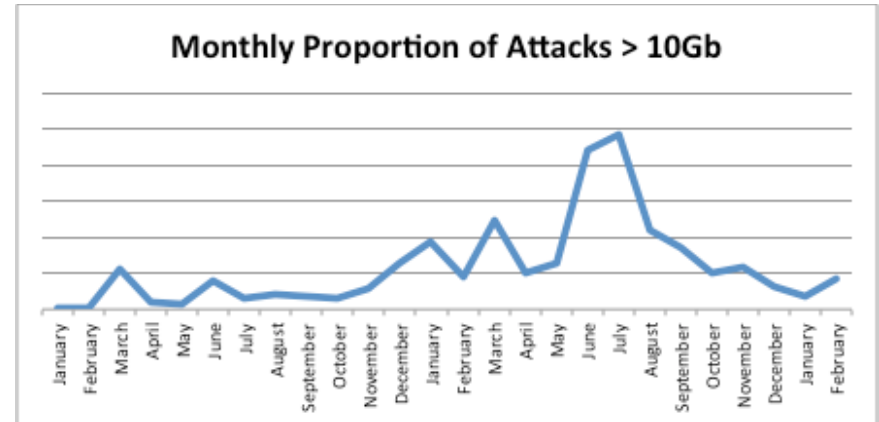


- 247% growth in number of attacks over 10Mpps.
- Multiple attacks monitored at over 40Gb/sec or 50Mpps.

2010 ATLAS Initiative : Anonymous Stats

So, what were the spikes?

- Spikes:
 - BPS Spike in June / July 2010.
 - PPS Spike in August / September 2010.
- Proportion of attacks over 10Gb / 10Mpps also shows spike

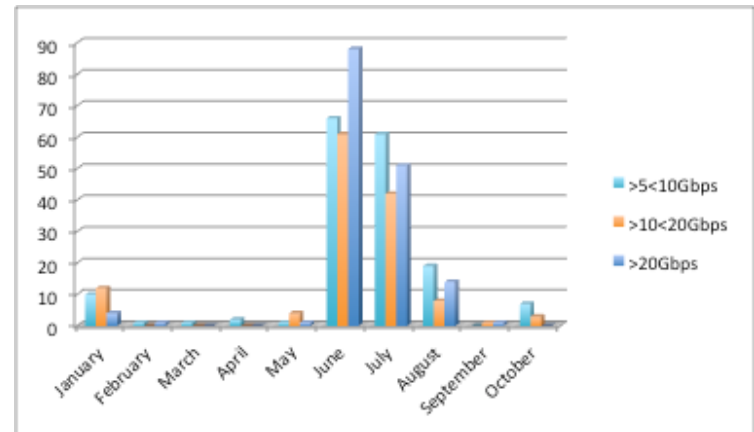
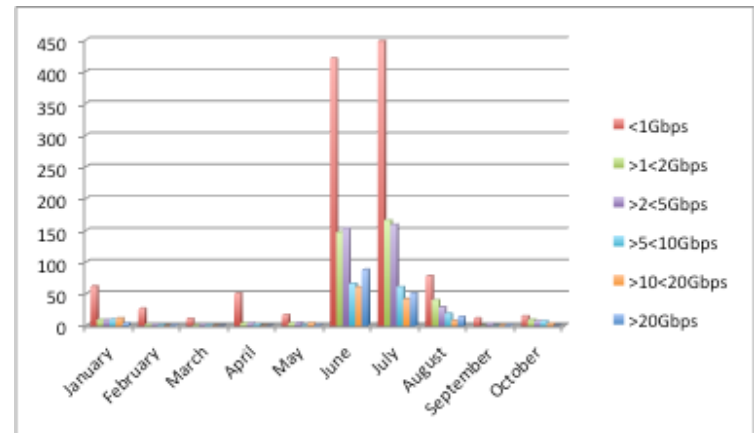


- BPS Spike largely due to intense activity targeting South Korea.
- PPS Spike due to increased attacks against US and China

2010 ATLAS Initiative : Anonymous Stats

Intense activity in South Korea in June & July 2010

- Huge Spike in number of large attacks
- 242 > 10Gbps attacks in June & July (16 in previous 5 months)
- 149 attacks greater than 20Gbps.
- Largest attack 49.73Gbps
 - Target port 6210
 - 16 mins 45 secs

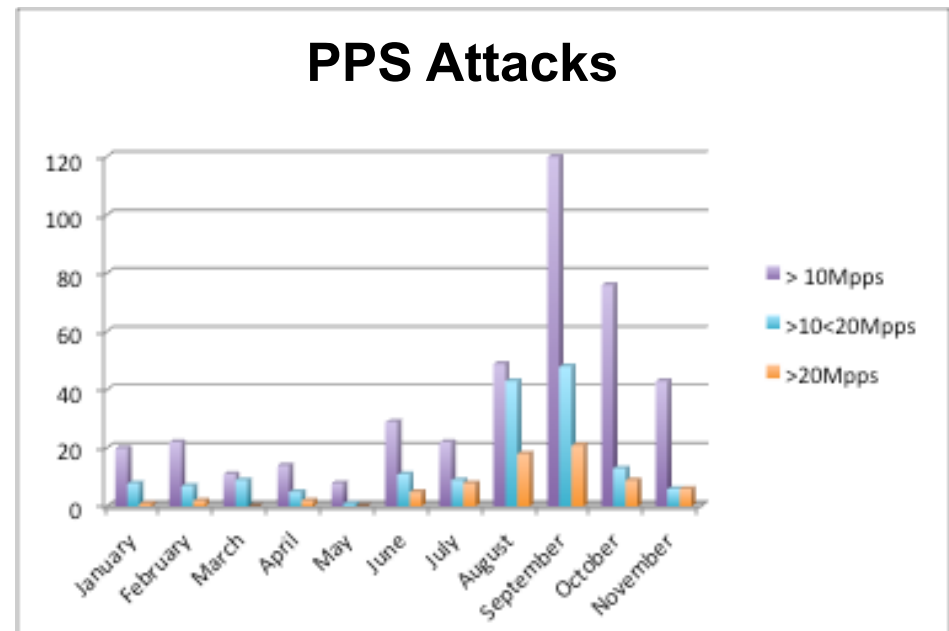


2010 ATLAS Initiative: Anonymous Stats

PPS Spike in August / September - USA

USA

- Spike in high PPS attacks, 130 in 2 month period – 68 in previous 7 months.
- Largest attack:
 - 66.2Gbps /108.89Mpps
 - 3d 14h 18mins
 - DNS
 - Hosting Provider
- Large attacks primarily targeted two hosting / IDC providers.
- Focus on ports 80 and 53



DDoS Trend Analysis : Key Points

- From ISR responses attack size, complexity and frequency are still increasing.
- From the Internet Observatory:
 - Average monitored attack size (Feb '11) 891Mbps / 622.7Kpps
 - This has been growing steadily since the start of 2009.
 - Majority of attacks are still small (< 1Gbps / < 1Mpps)
 - But rapid growth in number of large attacks seen.
 - (> 10Gb/sec or 10Mpps)
 - In 2010 more attacks targeting fewer ports + more large attacks targeting port 80 and 53.
 - Some spikes in growth due to clusters of attacks against
 - South Korea in June / July 2010
 - US Hosting Providers in August / September 2010.
- Internet Observatory and ISR results align pretty well



Thank You

Yaroslav Rosomakho

yaroslav@arbor.net

+74957224652