ARBOR NETWORKS

The Arbor ATLAS Initiative, Under the Hood

May 2011

Darren Anstee
Solutions Architect

Introduction

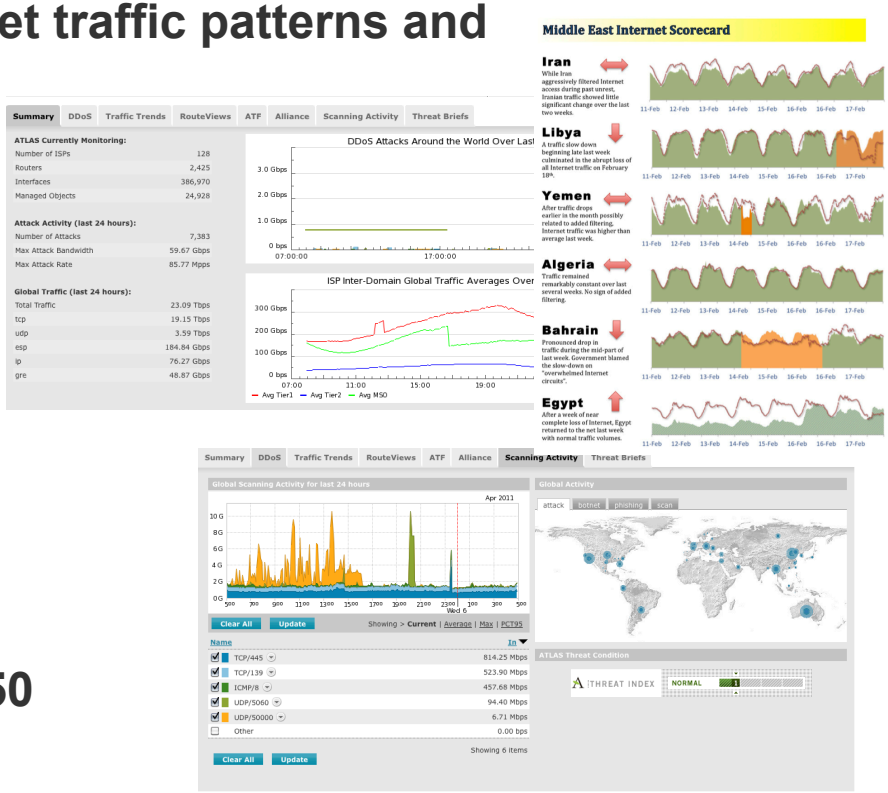
- Darren Anstee, EMEA Technical Specialist.
- 16+ years of experience in Networking and Security.
- 9 years at Arbor Network

ARBOR® NETWORKS
How networks grow™

- 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.

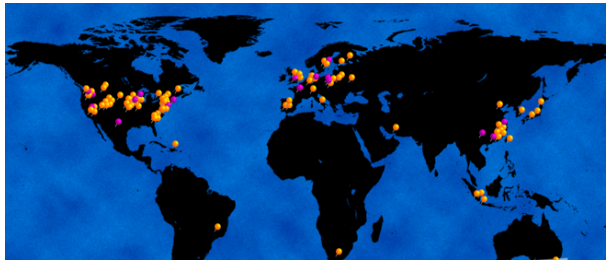
The Arbor ATLAS Initiative

- **What is it?**
  - **A**ctive **T**hreat **L**evel **A**nalysis **S**ystem
  - **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

- **100+ ISPs sharing real-time data - > ATLAS Internet Trends**
  - Automated hourly export of XML file to Arbor server (HTTPS)
  - File is anonymous, only tagged with
    - User Specified Region e.g. Europe
    - Provider Type (self categorized) e.g. Tier 1
- **Data derived from Flow / BGP / SNMP correlation**
  - Arbor Peakflow SP product
    - Correlates Sampled Flow / BGP in real-time
    - Distributed in nature
    - Network / Router / Interface etc. Traffic Reporting
    - Threat Detection (DDoS / infected sub)
      - Multiple detection mechanisms

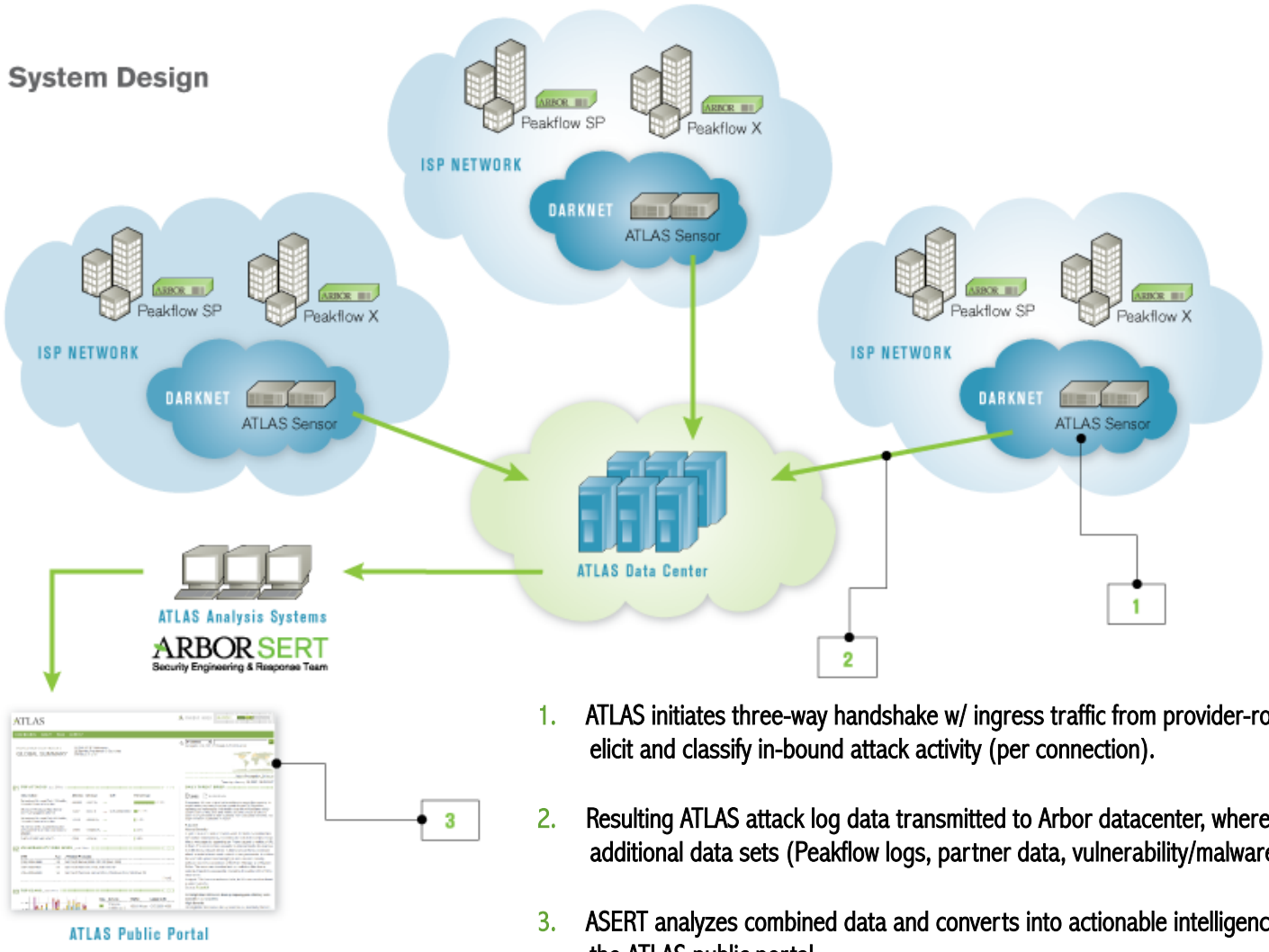
The Arbor ATLAS Initiative: Internet Trends

- **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

The Arbor ATLAS Initiative : Sensor Network



1. ATLAS initiates three-way handshake w/ ingress traffic from provider-routed dark IPs to elicit and classify in-bound attack activity (per connection).

2. Resulting ATLAS attack log data transmitted to Arbor datacenter, where it is combined with additional data sets (Peakflow logs, partner data, vulnerability/malware databases).

3. ASERT analyzes combined data and converts into actionable intelligence which is posted on the ATLAS public portal.

The Arbor ATLAS Initiative : Malware Analysis

- **2k – 5k Malware samples analysed automatically per day.**
- **Malware samples are analysed in virtualised 'sandbox' environment**
- **Samples are categorized into threat types:**
  - Spam
  - Virus
  - Botnet
  - DDoS Botnet
- Further analysis carried out for latter 2 (our area of expertise)
  - CnC mechanism / location
  - Attack vectors / Attack fingerprints etc..
- **Samples are compared to existing database of 5M malware signatures**
  - Approx 10% new per day.

The Arbor ATLAS Initiative : Malicious Link & Fastflux Analysis

- Automated tracking of Malicious Links and FasFlux domain names based on Spam email link / Phishing site data mining.
- Domain names / links are tracked along with associated IPs , ASNs and GeoIP data.

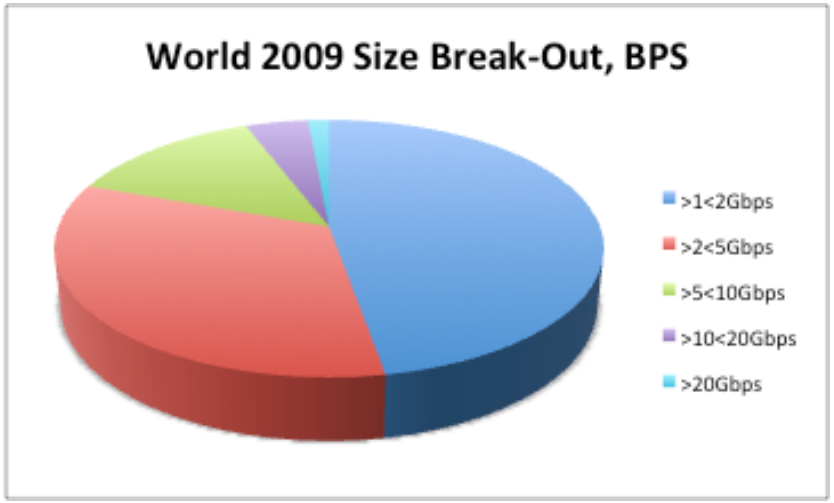
- So, what do we do with all of this stuff……

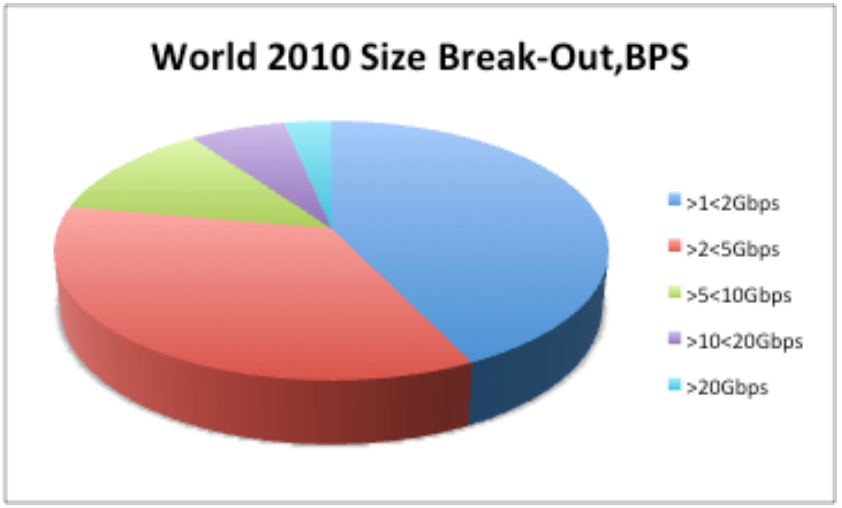
2010 ATLAS Initiative : DDoS Trends 2009 - 2010

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.

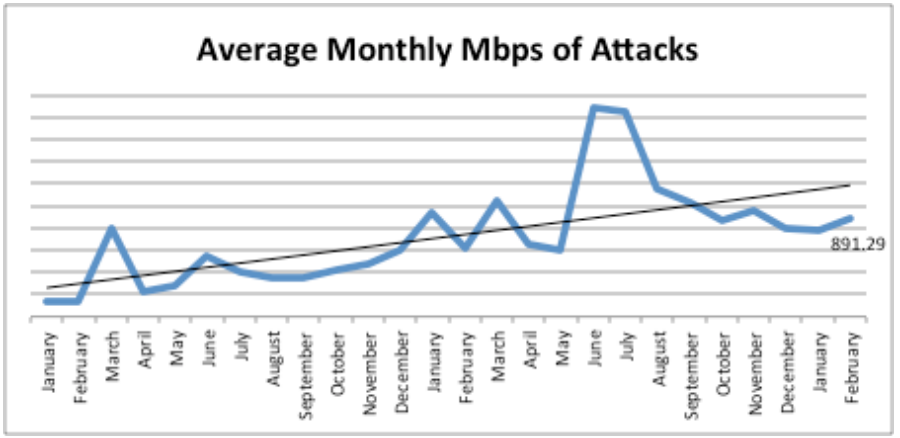


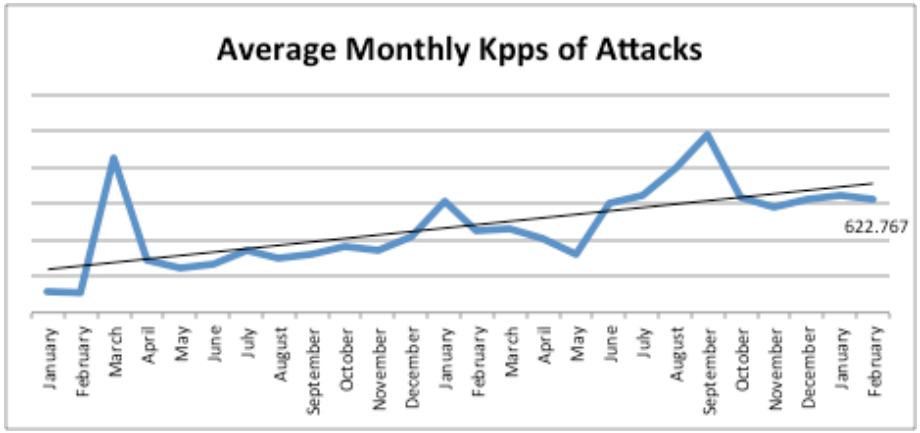


2010 ATLAS Initiative: DDoS Trends 2009 - 2010

Attack Growth trend in Mbps and Kpps

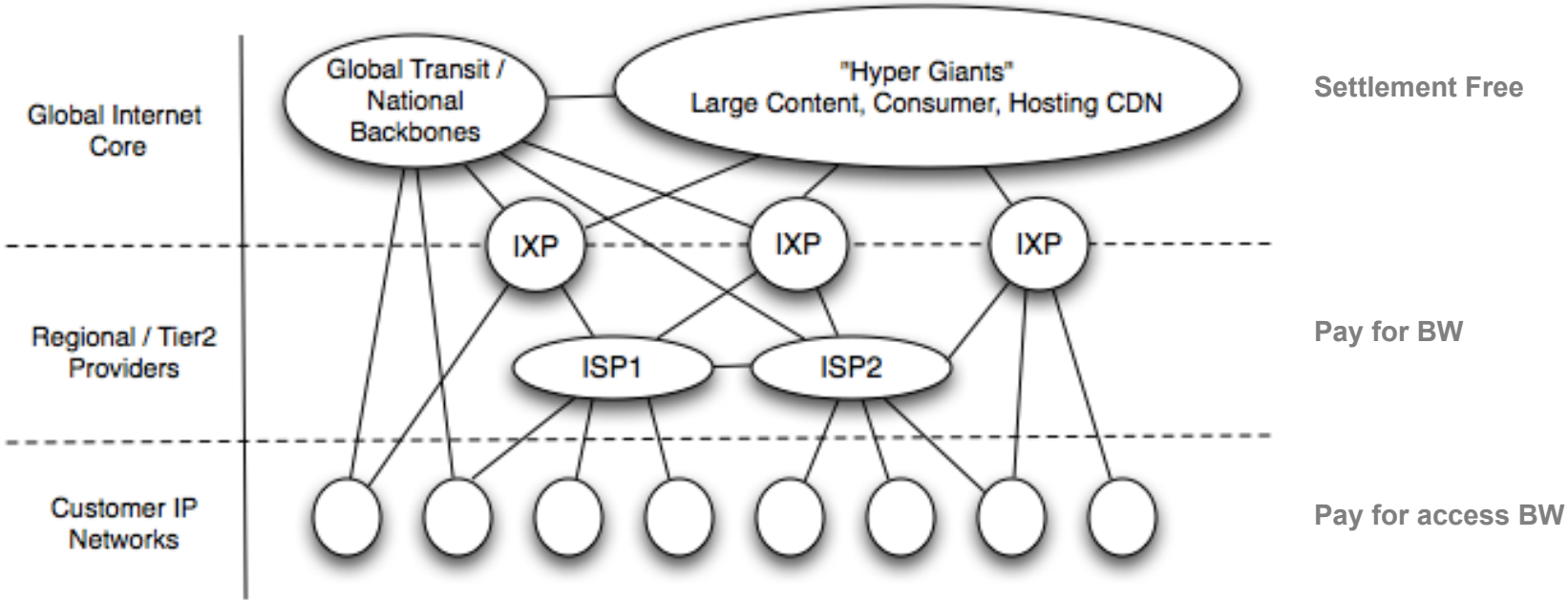
- Average monthly attack size since start of 2009.
- Average attack is 891Mbps / 622.7Kpps, Feb 2011





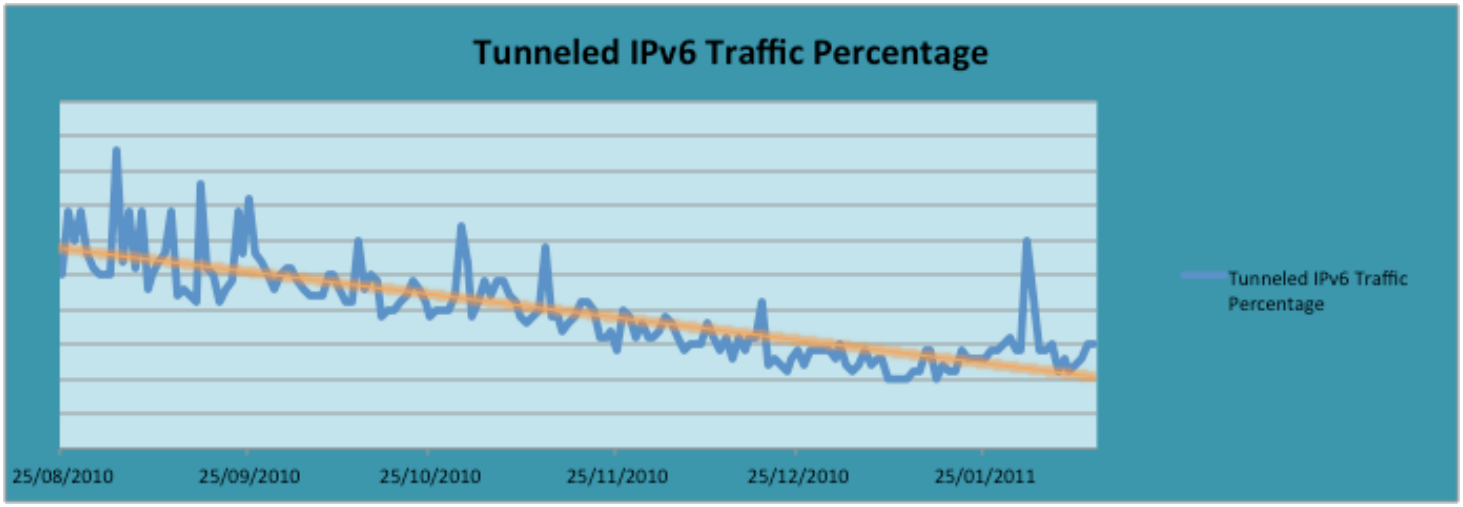
- Average attacks sizes have grown by 576% / 447% since start of 2009
- Spike in average BPS / PPS in late summer 2010

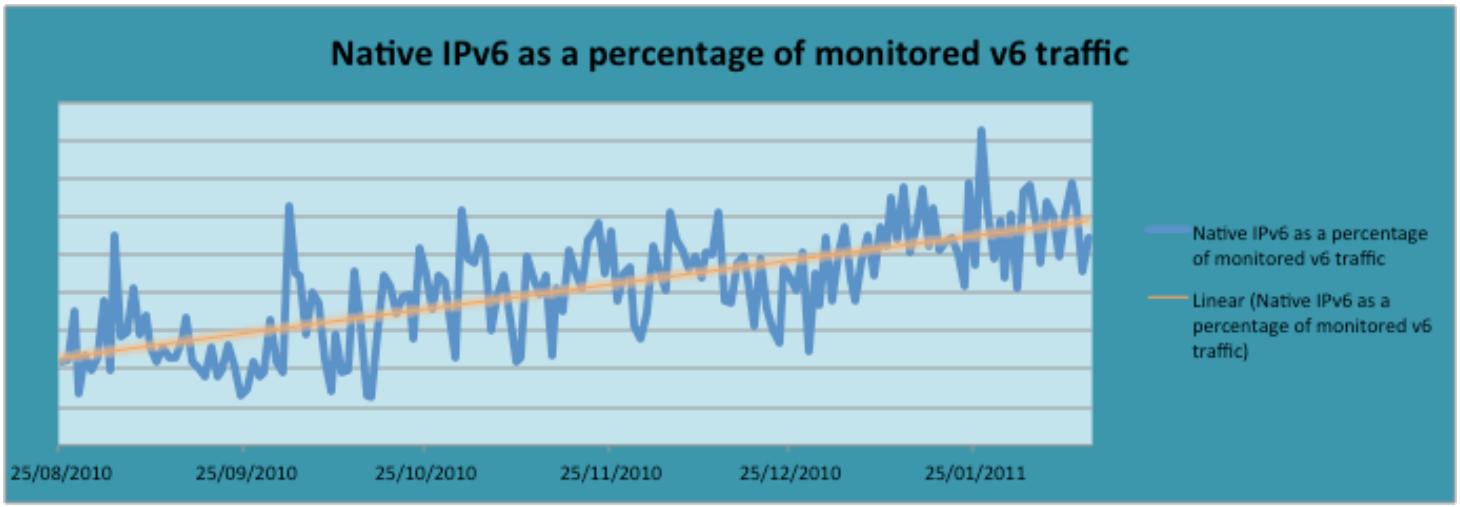
The New Internet – NANOG 47



- Flatter and much more densely interconnected Internet
  - Significant routing, traffic, security, economic, implications
- Disintermediation between content and eyeball networks
- New commercial models between content, consumer and transit

IPv6 Trends : Decline in Tunneled Traffic, Increase in Native traffic

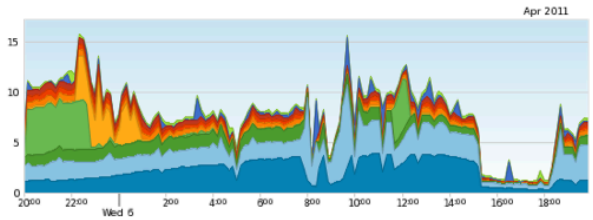




The ATLAS Initiative : Scans / Attacks Analysis

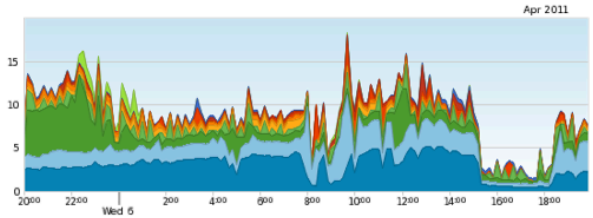
SUMMARY (past 24 hours)

TOP ATTACKS



Key	Description	Attacks per subnet	Change from yesterday	CVE	Percentage
	POLICY Reserved IP Space Traffic - Bogon Nets 1	305.01	-9.5 %		21.3%
	SCAN Sipvicious Scan	300.77	+163.1 %		21.0%
	POLICY Reserved IP Space Traffic - Bogon Nets 2	136.10	-10.2 %		9.5%
	Setup.php access	95.65	-62.9 %		6.7%

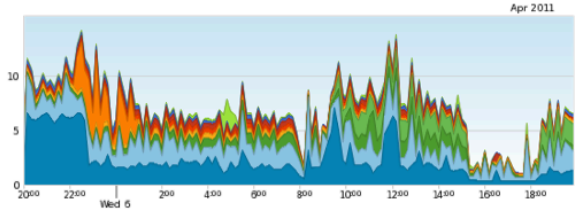
BY SERVICE



Key	Service	Attacks per subnet	Percentage
	TCP/445 (microsoft-ds)	429.51	29.9%
	UDP/5060	301.11	21.0%
	TCP/80 (http)	245.17	17.1%
	TCP/2967	95.93	6.7%
	UDP/49550	61.94	4.3%
	TCP/9988	48.38	3.4%
	TCP/22 (ssh)	42.94	3.0%
	TCP/5900	33.64	2.3%
	TCP/23 (telnet)	25.03	1.7%
	TCP/443 (https)	22.79	1.6%
	Other	128.78	9.0%

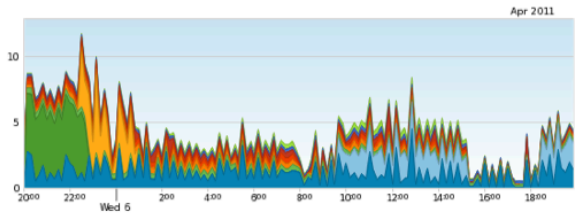
SOURCES (past 24 hours)

BY COUNTRY



Key	Country	Attacks per subnet	Percentage
	US (United States)	327.84	22.8%
	CN (China)	246.25	17.2%
	RU (Russian Federation)	106.06	7.4%
	CZ (Czech Republic)	76.81	5.4%
	EC (Ecuador)	48.52	3.4%
	MM (Myanmar)	46.22	3.2%
	ID (Indonesia)	44.32	3.1%
	IN (India)	40.10	2.8%
	IL (Israel)	36.09	2.5%
	TW (Taiwan)	30.17	2.1%
	Other	432.84	30.2%

BY ASN



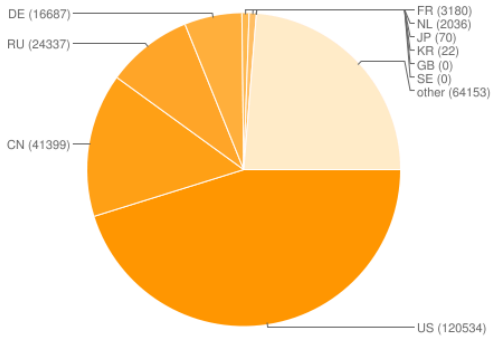
Key	ASN	Attacks per subnet	Percentage
	AS4134 (CHINANET-BACKBONE)	171.58	12.0%
	AS30764 (Unknown)	75.95	5.3%
	AS40676 (PSYCHZ)	74.49	5.2%
	AS19582 (GRUPO)	47.97	3.3%
	AS18399 (BAGAN-TRANSIT-AS)	42.83	3.0%
	AS23693 (TELKOMSEL-ASN-ID)	41.91	2.9%
	AS29802 (HVC-AS)	41.50	2.9%
	AS4837 (CHINA169-BACKBONE)	37.84	2.6%
	AS6621 (HNS-DIRECPC)	31.00	2.2%

The ATLAS Initiative: Malware Analysis

DOS BOTNET ACTIVITY IN REGION
GLOBAL RANK BY COUNTRY
Active C&C servers by country

Country	Rank
RU	4
FR	11
NL	13
CN	2
DE	5
JP	20
US	1
KR	24
GB	NA
SE	NA

C&C DoS command activity by country



GLOBAL BOTNETS

View: Port Summary | C&C Servers
Output: Print | XML | CSV

PORT SUMMARY (past 24 hours)

Server Port	Number of Servers	Percentage
6667	1041	41.6%
1234	74	3.0%
81	66	2.6%
7000	61	2.4%
6668	59	2.4%
2345	40	1.6%
80	38	1.5%
51987	34	1.4%
6669	32	1.3%
6567	32	1.3%
other	1023	40.9%

C&C SERVERS (past 24 hours)
BY COUNTRY

Country	Number of servers	Percentage
US (United States)	1015	40.6%
DE (Germany)	185	7.4%
NL (Netherlands)	153	6.1%
GB (Great Britain)	139	5.6%
FR (France)	136	5.4%
RU (Russian Federation)	105	4.2%
CA (Canada)	75	3.0%
TR (Turkey)	72	2.9%
CN (China)	56	2.2%
UA (Ukraine)	48	1.9%
Other	516	20.6%

- **Attack Fingerprinting used to determine detection / mitigation mechanisms.**
  - **Included in product data-feeds**

The ATLAS Initiative : Blog Posts

JKDDOS: DDoS bot with an interest in the mining industry?

by Jeff Edwards

Today we document JKDDOS, the moniker we have been using for yet another malware family that specializes in DDoS attacks. Looking back through our malware zoo, we observed our first JKDDOS sample as early as September 2009. Since then, we have analyzed almost 50 unique JKDDOS samples, the most recent of which we acquired in December 2010. Based on its recent history of attacks, the operators of this family appear to have an axe to grind against several relatively large international holding companies that have connections to the mining industry.

Malcode Properties

The JKDDOS malware is distributed in the form of a relatively small executable that tends to vary widely in size across different samples; we have seen specimens as small as 17,408 bytes and as large as 240,997 bytes. The most common size for a JKDDOS sample is approximately 33.5 KB; recently, the JKDDOS samples we have analyzed have usually been packed whereas earlier samples were not.

Example MD5 hashes for the JKDDOS samples we have analyzed to date are as follows:

Skunkx DDoS Bot Analysis

by Jose Nazario

Lest you think all of the DDoS bots we focus on come only from China, we found one that appears to be from the US. We're calling this bot "Skunkx". We have not yet seen the bot's attacks in the wild, however, and so we do not know its favored victim profiles. We also do not know how big this botnet is at this time.

The bot's capabilities include:

- Perform DDoS attacks: UDP floods, SYN floods, HTTP floods, and Slowloris attacks
- Detect some analyst tools (Commview, TCPView, and Wireshark) and platforms (QEMU, VMWare, VirtualPC)
- Spread over USB, MSN, YahooMessenger
- "Visit" sites, speedtest
- Download and install, update, and remove arbitrary software
- Detect and stop DDoSer, Blackshades, Metus and IRC bots on the box; it apparently can speak "DDoSer" too
- Spread as a torrent file
- Steal logins stored in the SQLite DB by Mozilla

We have not seen source or the control panel of the bot. The author appears to like the "JoinVPS" service, however. His servers that he has used go back to "Net-0x2a: Zharkov Mukola Mukolayovuch" in the Ukraine, and also "PIRADIUS" in Malaysia. This is someone familiar with underground hosting, it seems.

The ATLAS Initiative

- **A scalable way of getting near real-time visibility of Internet traffic / Threat data**
- **Can help us to better understand traffic / threat trends**
  - Coarse grained data – (primarily) from Flow.
  - Finer grained data – honeypots / malware analysis
- **Always looking for new areas to investigate in relation to traffic / threat trends**
  - Ideas Welcome

ARBOR NETWORKS

Thank You

Darren Anstee

darren@arbor.net