Rethink Possible

Cybersecurity and AT&T

John C. Nagengast

nagengast@att.com

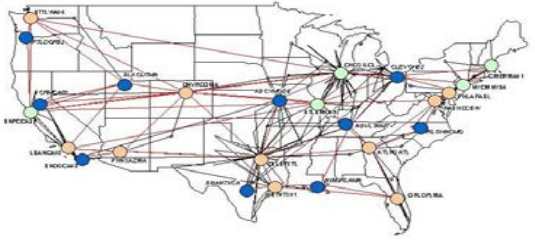
AT&T Global Security Operations

Global Sensor Grid

- Threat detection & analysis

Security Nodes

- Monitoring & Mitigation



Security Operations

- Configuration, Alerting, & Response

AT&T's Cyber Security Platform - AURORA

Alarm & Log Analysis
- FW logs
- IDS alarms
- VPN / Proxy / Etc.

Flood Flow Analysis
- Scan detection
- Worm detection
- Volumetric analysis
- Forensic investigation
- Algorithm research

Extended Netflow Systems
- Arbor alarms
- TAP Sampled flow data

Fathom
- Registry analysis
- Route analysis

Global Correlation & Analysis

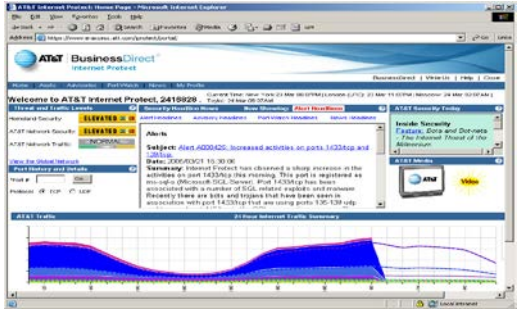
AURORA

Alerts

AT&T GNOC

Rapid Response

Customers



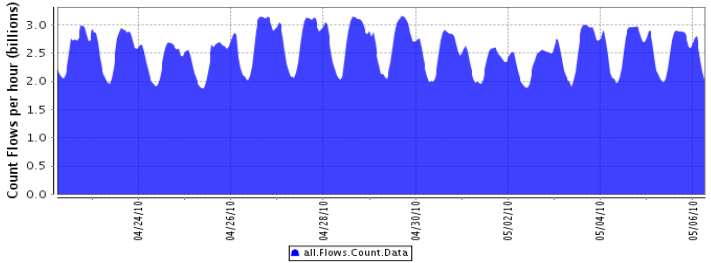
AT&T Internet Protect (SM)

Flow Record Analysis

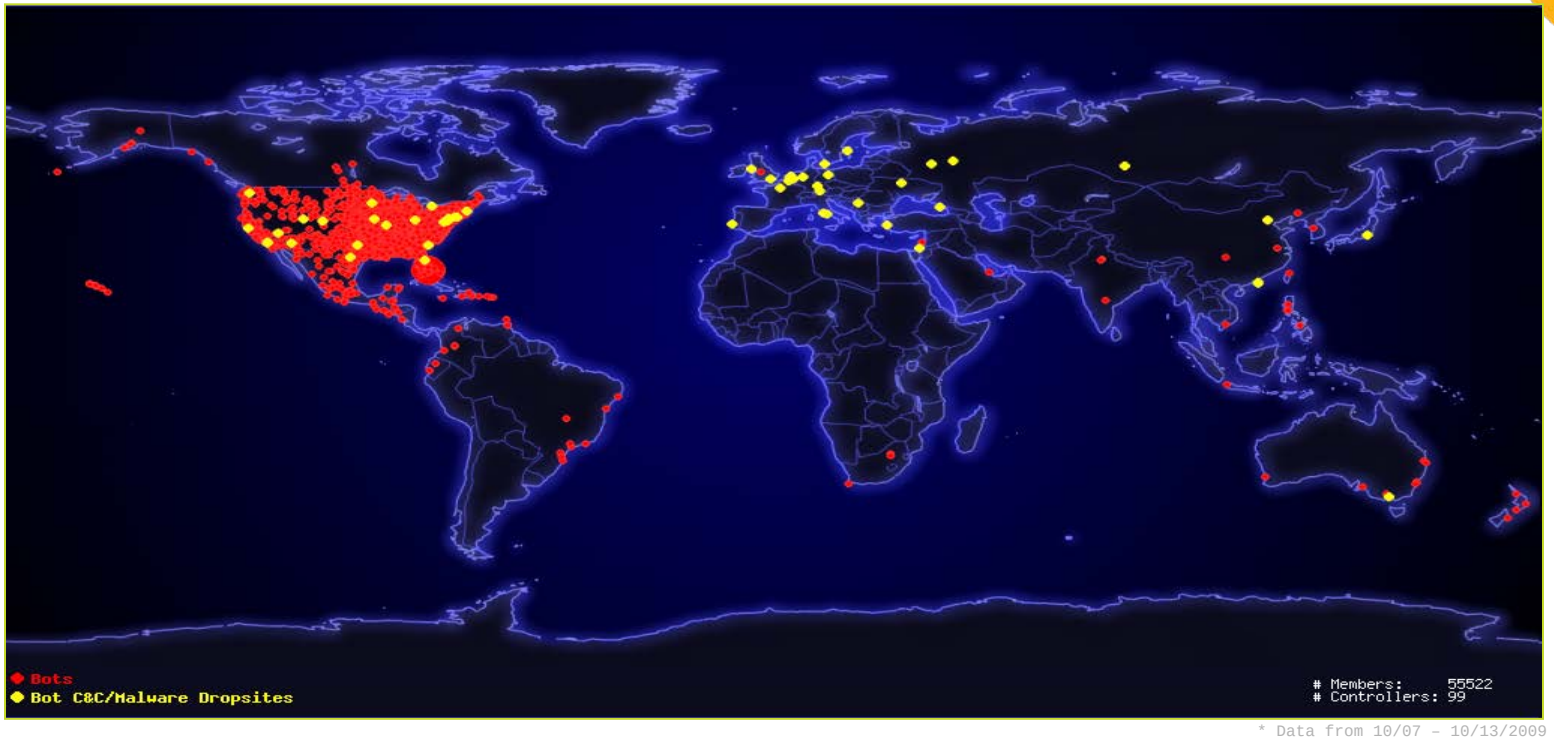
AT&T processing designed to identify suspicious traffic patterns

Source Addr	Dest Addr	Port	Flags	Pkts	Bytes	Date	Time
200.121.13.98	192.31.106.4	25	-APRSF	6	315	10/1/2005	1:48:02
200.121.13.98	63.240.122.252	25	----S-	1	64	10/1/2005	1:48:08
200.121.13.98	192.35.35.3	25	-APRSF	6	315	10/1/2005	1:48:24
80.140.212.26	66.246.215.72	25	-AP-SF	4	1719	10/3/2005	13:58:27
80.140.222.170	66.235.221.51	25	-AP-SF	8	417	10/4/2005	12:16:00
80.140.222.170	166.102.165.21	25	-A--SF	5	208	10/4/2005	12:16:36

- Analog of “Call detail records” for Internet traffic
- Process approx 3 Billion records per hour



Botnet Koobface



* Data from 10/07 – 10/13/2009

- First discovered in Dec 2008, Koobface initially spread by delivering Facebook messages to “friends” of the infected victim. It has since extended to propagate over additional social networking sites including MySpace, Twitter, Friendster, Bebo, hi5, Tagged, Netlog, fubar and myYearbook.
- Once a PC is infected, it is instructed to download additional components for: Browser Search Hijacking, Software Key Stealing, CAPTCHA breaking, Pushing Rogue Anti-malware software, Acting as a malicious host to serve the malware to new victims.

The AT&T GNOC at Bedminster, NJ

Integrated Cyber Security & Network Operations

- Manages the largest and most sophisticated IP/MPLS Core Infrastructure
- Comprehensive cyber situation awareness of our global infrastructure
- Most powerful analytic tools
- Active Defense embedded in our core network
- Complete array of network-based security services

Prevent Cyber Attacks or Network Failures before they happen