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

Alerts

Customers

AT&T GNOC

Rapid Response

AT&T
Internet
Protect (SM)
Flow Record Analysis
AT&T processing designed to identify suspicious traffic patterns

<table>
<thead>
<tr>
<th>Source Addr</th>
<th>Dest Addr</th>
<th>Port</th>
<th>Flags</th>
<th>Pkts</th>
<th>Bytes</th>
<th>Date</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>200.121.13.98</td>
<td>192.31.106.4</td>
<td>25</td>
<td>-APRSF</td>
<td>6</td>
<td>315</td>
<td>10/1/2005</td>
<td>1:48:02</td>
</tr>
<tr>
<td>200.121.13.98</td>
<td>63.240.122.252</td>
<td>25</td>
<td>-----S-</td>
<td>1</td>
<td>64</td>
<td>10/1/2005</td>
<td>1:48:08</td>
</tr>
<tr>
<td>200.121.13.98</td>
<td>192.35.35.3</td>
<td>25</td>
<td>-APRSF</td>
<td>6</td>
<td>315</td>
<td>10/1/2005</td>
<td>1:48:24</td>
</tr>
<tr>
<td>80.140.222.170</td>
<td>166.102.165.21</td>
<td>25</td>
<td>--SF</td>
<td>5</td>
<td>208</td>
<td>10/4/2005</td>
<td>12:16:36</td>
</tr>
</tbody>
</table>

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