Glasnost or Tyranny?
You Can Have Secure and Open Networks!

Steven Hurst CISSP
Director - AT&T Security Services and Technology
AT&T Chief Security Office
Everything is Moving to IP

- **130** Web sites
- **48 million** Internet users
- **253 million** email addresses
- **200 million** Web sites
- **135 million** Web sites
- **1.3 billion** Internet users
- **More than 1.6 billion** email addresses
- **More than 2 billion** email addresses
- **2 billion** Internet users

Wireless data traffic **quadruples** every year
(Web, video, image sharing, messaging)
IP-enabled Devices on the Global IP Network

More than 1 billion devices connected
AT&T Global IP Network

An Incredible Vantage Point!
Network Security Threats

- Botnets
- Distributed Denial of Service
- Phishing, Sniffing, Keylogging, etc.
- "Data Leakage" • Lost/Stolen Laptops, Unsecured Servers
- Spam for Hire
- Social Engineering
- Insider Threats
### Example - Internet Anomalies Tracked by AT&T

Significant increase in sources scanning port 23/tcp

<table>
<thead>
<tr>
<th>DATE</th>
<th>HOUR</th>
<th>CODE_LINK</th>
<th>CHANGE</th>
<th>UNITS</th>
<th>HIGHSIG</th>
<th>PERIODS</th>
<th>BREADTH</th>
<th>PRIORITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>20090305</td>
<td>01</td>
<td>tcp_dpport.1024</td>
<td>Probes incr</td>
<td>Sources</td>
<td>2</td>
<td>4</td>
<td>5</td>
<td>40</td>
</tr>
<tr>
<td>20090305</td>
<td>01</td>
<td>tcp_dpport.3072</td>
<td>Probes incr</td>
<td>Sources</td>
<td>2</td>
<td>4</td>
<td>5</td>
<td>40</td>
</tr>
<tr>
<td>20090305</td>
<td>01</td>
<td>tcp_dpport.5900</td>
<td>Probes incr</td>
<td>Sources</td>
<td>1</td>
<td>6</td>
<td>5</td>
<td>30</td>
</tr>
<tr>
<td>20090304</td>
<td>23</td>
<td>tcp_dpport.23</td>
<td>Probes incr</td>
<td>Sources</td>
<td>2</td>
<td>11</td>
<td>7</td>
<td>154</td>
</tr>
<tr>
<td>20090304</td>
<td>23</td>
<td>ip_proto.6</td>
<td>Volume incr</td>
<td>Flows</td>
<td>1</td>
<td>3</td>
<td>10</td>
<td>30</td>
</tr>
<tr>
<td>20090304</td>
<td>23</td>
<td>udp_dpport.34740</td>
<td>Volume incr</td>
<td>Bytes</td>
<td>1</td>
<td>2</td>
<td>10</td>
<td>20</td>
</tr>
<tr>
<td>20090304</td>
<td>23</td>
<td>udp_dpport.53</td>
<td>Volume incr</td>
<td>Flows</td>
<td>1</td>
<td>1</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>20090304</td>
<td>23</td>
<td>udp_dpport.35052</td>
<td>Volume incr</td>
<td>Bytes</td>
<td>1</td>
<td>1</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>20090304</td>
<td>23</td>
<td>ip_proto.50</td>
<td>Volume incr</td>
<td>Flows</td>
<td>1</td>
<td>1</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>20090304</td>
<td>22</td>
<td>tcp_dpport.445</td>
<td>Probes incr</td>
<td>Sources</td>
<td>1</td>
<td>8</td>
<td>4</td>
<td>32</td>
</tr>
<tr>
<td>20090304</td>
<td>22</td>
<td>tcp_dpport.3306</td>
<td>Volume incr</td>
<td>Bytes</td>
<td>1</td>
<td>1</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>20090304</td>
<td>20</td>
<td>udp_dpport.5004</td>
<td>Volume incr</td>
<td>Bytes</td>
<td>1</td>
<td>3</td>
<td>10</td>
<td>30</td>
</tr>
</tbody>
</table>
Scan Activity Targeting Telnet
The characteristics that highlight the activity

Unique source IP addresses scanning

Number of probes
Early Indications of Worm Activity
Evolution and status of worm variants

- Variant A: Nov 21
- Variant B: Dec 29
- Early Indicator SMB scanning: Nov 4
- Increased scanning from Downadup.A and other malware
- Downadup.B and other malware spreading: Feb 06
- Variant C: Mar 05
- Variant D: Mar 17
- New Variant E: April 07
- Variant C/D Activation
- New Variant E Self delete: May 03

Out of Cycle RPC Patch, MS08-067 (Advisory on Oct 23)
In Cycle SMB Patch, MS08-068

© 2009 AT&T Intellectual Property. All rights reserved.
AT&T and the AT&T logo are trademarks of AT&T Intellectual Property. AT&T Proprietary
Indicators of the StormWorm (W32/Nuwar, Trojan.Peacomm) active on changing udp ports

**Storm Worm Tracker**

- Storm worm transitions to new port
- Storm worm continuing to utilize ports 11275/udp and 16275/udp
Illustrative Power of Botnets
Just a few bots can disrupt business operations

Number of Bots (600Kbps upload)

- T1 1.5 Mbps: 3 bots
- OC3 155 Mbps: 259 bots
- OC12 622 Mbps: 1,037 bots
- OC48 2.4 Gbps: 4,147 bots
- OC192 10 Gbps: 16,667 bots

Power Required to Disrupt a Business

Power Required to Disrupt Typical ISP or Hosting Provider

© 2009 AT&T Intellectual Property. All rights reserved.
Cyber Attack Strategy
Adversary Performs Reconnaissance to Exploit Vulnerabilities

Web-Based Information Collection
- Social Engineering

Broad Network Mapping
- Targeted Scan

Service Vulnerability Exploitation
- Password Guessing

DDOS Zombie Code Installation
- System File Delete

Use of Stolen Accounts for Attack
- Log File Changes

Reconnaissance
- Preventive Phase (Defense)

Scanning
- Reactive Phase (Defense)

System Access
- Indications and Warning Threshold (Defense)

Damage

Track Coverage

- Execute security policies
- Contain and remediate
- Perform forensics to diagnose event
- Update security stance

- Observe & recognize anomalies as messengers of impending security event
- Develop situational awareness
- Identify vulnerabilities
- Implement layers of security to update stance
Top 10 Potential Bots
Potential threats identified, yet still active and waiting

<table>
<thead>
<tr>
<th>Name</th>
<th>Members</th>
<th>Servers</th>
<th>Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>Darkwarez070323</td>
<td>3427</td>
<td>1</td>
<td>4139</td>
</tr>
<tr>
<td>0Day060531</td>
<td>59073</td>
<td>9</td>
<td>32</td>
</tr>
<tr>
<td>Evilpacket060823</td>
<td>30803</td>
<td>6</td>
<td>238</td>
</tr>
<tr>
<td>unnamed</td>
<td>7182</td>
<td>67</td>
<td>380</td>
</tr>
<tr>
<td>Letmein060206</td>
<td>16686</td>
<td>21</td>
<td>151</td>
</tr>
<tr>
<td>Nadersamar061220</td>
<td>16271</td>
<td>9</td>
<td>42</td>
</tr>
<tr>
<td>Fucuzzy060731</td>
<td>6035</td>
<td>26</td>
<td>237</td>
</tr>
<tr>
<td>Foolishfoe070227</td>
<td>7202</td>
<td>17</td>
<td>173</td>
</tr>
<tr>
<td>Frf1Dns2go060613</td>
<td>9546</td>
<td>6</td>
<td>76</td>
</tr>
<tr>
<td>Debelizombi060928</td>
<td>847</td>
<td>3</td>
<td>503</td>
</tr>
<tr>
<td>Others</td>
<td>17108</td>
<td>133</td>
<td>1342</td>
</tr>
</tbody>
</table>

NOTES:
- One day of activity
- Actual size could be at least 10-20x larger
- This report only covers top 10 active IRC-based botnets.
Network-Based Security Services
Protection in the Provider Core

- Internet Protect
- Distributed Denial of Service (DDoS) Defense

AT&T Security Node

Enterprise DMZ

Network Based Security Data Center (NB-SDC)

IDS/IPS Secure Email, Web...

Attacker

AT&T IP Backbone

Internet

Enterprise Intranet

Reduced Enterprise Investment (People, Capital, Software)
AT&T Approach For Cyber Security
Observe, Protect, and Prevent

- **Observe**
  - Collection
  - Analyze
  - Report
  - Act
  - Situational Awareness
  - Perimeter protection of the network with self protecting network.
  - Observe, track, and report enterprise security anomalies in real-time.

- **Protect**
  - Authentication
  - Firewall
  - Intrusion detection and prevention
  - Antivirus
  - AntiSPAM
  - Perimeter protection of the network with self protecting network.

- **Prevent**
  - Certification and accreditation (C&A)
  - Testing
  - Training
  - Proactive engineering and operations.
Providing Real-Time Security Management

24/7 Situational Cyber Security Awareness

Management Servers, Consoles, and Database

Customized Event Parsers and Consolidators

AT&T Global Network Operations Center

AT&T Custom Database Technology

Daytona Data Mining System

AT&T Enterprise and Internet Feeds

- IDS Alarms
- Firewall Logs
- DLP Alarms
- Netflow
- Proxy Logs

- Server Alarms
- Internet Alarms
- DDOS Detection
- VPN Logs
- Honey Pots

~600 Million Events/Day

~40 Cases/Day

~170 Alerts/Day
Security Operations Center (SOC)

24x7 Discovery
- via GNOC hotline
- via Incident Response Mailbox
- via Threat Management System

100+ years of Security Focus
Back-Up to Redundant SOC
Network Security
Layered ‘Threat Protection’

- Security Event & Threat Analysis
- Internet Embedded Defenses
- WAN Traffic Analysis
- Network Embedded Gateways
- Premises Security Devices
Secure Node Architecture

Security Functions:
- Firewall
- IDS/IPS
- URL/ Web filtering
- Logging/Reporting
- Anti-virus
- User Authentication
- Email scanning
- DDoS
- DLP

Clean Pipe
Alert Summary

Alert Details

Port Watch

Alert Summary

Alert Summary Page

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
<th>Risk</th>
<th>Alert ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>20140920/21 00:00</td>
<td>Increased Traffic on port 22644</td>
<td>Medium</td>
<td>A0000110</td>
</tr>
<tr>
<td>20140920/21 00:10:47</td>
<td>Increased Traffic on port 21824</td>
<td>Medium</td>
<td>A0000112</td>
</tr>
<tr>
<td>20140920/21 00:45:45</td>
<td>Malicious login activity on port 31222 (Updated 20140515)</td>
<td>Medium</td>
<td>A0000117</td>
</tr>
<tr>
<td>20140921/20:42:51</td>
<td>Increased Traffic on Port 443 (186.96)</td>
<td>Medium</td>
<td>A0000119</td>
</tr>
<tr>
<td>20140922/01:47:27</td>
<td>Increased Activity on port 50013</td>
<td>Medium</td>
<td>A0000120</td>
</tr>
<tr>
<td>20140923/01:38:29</td>
<td>Increased Traffic on port 14408 (156)</td>
<td>Medium</td>
<td>A0000125</td>
</tr>
<tr>
<td>20140925/02:47:57</td>
<td>Increased Traffic on port 10003 (156)</td>
<td>Medium</td>
<td>A000015</td>
</tr>
<tr>
<td>20140926/01:12:40</td>
<td>Increased Traffic on port 50615 (156)</td>
<td>Medium</td>
<td>A000014</td>
</tr>
</tbody>
</table>

Port Watch

Count of Flows across All Ports

Top Change in Share for Ports with Significant Values

Legend:
- Protocol: TCP, UDP, TCP & UDP
- Class: Byte (B), Packet (P), Total (T)
- Color: Green (Increased), Red (Decreased)
- Bar: Current share (top) vs. previous share (bottom)
AT&T Private Intranet Protect Service

Including:

- Top Talkers Sending Traffic into Your Network
- TCP or UDP Protocol Distribution of Traffic Coming into Your Network
AT&T Distributed Denial of Service (DDoS) Defense

Multiple Points of Vulnerability

Features

- Accurately identify attacks in seconds
- Immediately mitigate a broad range of DoS and DDoS attacks
- Dedicated, Shared, or Subscription options

Benefits

- Defense against attacks designed specifically to disable infrastructure resources, applications and businesses
- Secures availability and ensures business continuity
AT&T Distributed Denial of Service (DDoS) Defense

Multiple Points of Vulnerability

**Features**
- Accurately identify attacks in seconds
- Immediately mitigate a broad range of DoS and DDoS attacks
- Dedicated, Shared, or Subscription options

**Benefits**
- Defense against attacks designed specifically to disable infrastructure resources, applications and businesses
- Secures availability and ensures business continuity
AT&T Distributed Denial of Service (DDoS) Defense

Multiple Points of Vulnerability

Features
- Accurately identify attacks in seconds
- Immediately mitigate a broad range of DoS and DDoS attacks
- Dedicated, Shared, or Subscription options

Benefits
- Defense against attacks designed specifically to disable infrastructure resources, applications and businesses
- Secures availability and ensures business continuity
AT&T’s Security Capabilities
How we protect your network infrastructure

- Employ the network as the first line of defense
- Utilize AT&T’s predictive security capabilities
- Implement a defense-in-depth strategy
- Use a Risk-Based approach
- Apply reactive to proactive to predictive to adaptive
- Provide a broad portfolio of security services

Quick Facts about AT&T Managed Security
- End to end Security Capabilities - from end point to the cloud
- Security integrated with AT&T services as appropriate
- “In the Cloud” security industry recognition
- More than 1,500 world-class security experts and support professionals
- SAS70 and PCI Compliant services
- Customer access to reports and tools via AT&T BusinessDirect® Portal
Thank You!
AT&T Managed Security Services

**Threat Management**

**Attack & Traffic Information**
- General Internet
- Customer’s VPN
- Broader customer network

**Mitigation**
- Internet attack
- General network attack
- Threat, Intelligence, Operations

**On-Going Protection**

**Firewalls**
- Take advantage of AT&T’s network
- Protect the perimeter
- Protect the edge

**Content**
- Email
- Web Activity
- Content Protection
- User Authentication

**Custom or Other Specific Needs**

**AT&T Managed Services**

- AT&T Internet Protect®
- Private Intranet Protect
- Intrusion Detection Services
- DDoS Defense & My Internet Protect
- Intrusion Prevention Services
- Fully Managed 24X7 Security Operations
- Network-Based Firewall
- Premises-Based Firewall
- End-Point Security
- Secure Email Gateway
- Web Security
- Data Leakage Protection
- Token Authentication
- Security Professional Services