Report: The IAB Workshop on Unwanted Traffic

Loa Andersson
Danny McPherson
IAB Unwanted Traffic Workshop
USC/ISI - Marina del Rey,
March 2006
Why an “Unwanted Traffic” workshop

• Lots of Unwanted Traffic on the Internet today
  – (D)DoS, Spam, viruses, worms, etc.

• The trend
  – The ratio of Unwanted Traffic is increasing, not decreasing
  – Persistence of infected hosts considerable

• The impact
  – Significant economic losses and growing
Evolution of Threats

• From worms/viruses that simply wreak havoc on the network to malware that propagates, compromises hosts and enables command and control infrastructure and services platforms for malicious activity. E.g.:
  – Code Red (DDoS against IP)
  – Blaster (DDoS against hostname)
  – Deloder (Arbitrary DDoS toolkit)
  – Fully extensible today

• (D)DoS was initial botnet threat, array of employment functions today; mostly with economic motivators, though religious, political, etc.. as well
The Workshop

• IAB called the workshop to
  – Assess the state of affairs
  – Examine existing counter measures
  – Collect input for action planning

• Participants

• The major findings are report in:
  – draft-iab-iwout-report-00.txt
The Workshop Findings

• An Underground Economy exists
  – It drives majority of unwanted traffic

• An arms race with the evolving underground economy
  – Currently the situation is getting worse
  – Increasing virulence of malware
  – Persistence of existing compromised systems

• An action plan is needed!
5th Floor
Servers:
Military
Government
Business

4th Floor
Retail:
Credit cards
Social Security No's
Bank Accounts

3rd Floor
Internet:
Hosts
Core Routers
Spoofed Addresses

2nd Floor
Equipment:
Bots & Botnets
The Root of All Evils: An Underground Economy

- The Underground Economy is a virtual shopping mall where your belongings and assets are bought and sold.
- The shopping mall and stores are managed by criminals.
- They use the tools we have developed to run the warehouse.
- Inventory list: credit cards, bank accounts, core Internet routers, business critical servers, bots, botnets, etc.
Why an Underground Economy?

• The monetary incentives are HUGE!
• Lack of meaningful deterrence
  – Vulnerable host platforms
  – Lack of education to add protection or prompt repair
  – Prosecution of miscreants - extremely difficult
• No proactive actions from service providers
  – Lack of resources
  – Lack of adequate tools
  – Efforts go into reactive patches (damage control, miscreants move around)
  – Rare for mitigation to involve sanitizing hosts
  – ROI
The botnet example

• Vectors
  – Vulnerability -> Exploit
  – Compromise/Infection
  – Propagation
  – C & C

• Employment
  – DDoS (spoof and non)
  – Spam
  – Spam w/phishing, host phishing sites
  – Open proxies
  – ID theft
  – Key loggers
  – Lift CD keys
  – Click Fraud
  – Stream video?
  – Marketing!
## Current Vulnerabilities and Existing Solutions

<table>
<thead>
<tr>
<th>Vulnerabilities</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Source address spoofing</td>
<td><strong>Internet</strong></td>
</tr>
<tr>
<td>• BGP route hijacking</td>
<td>• Access control lists (ACL)</td>
</tr>
<tr>
<td>• “Everything over HTTP”</td>
<td>• BGP null routing</td>
</tr>
<tr>
<td>• Everyone comes from Everywhere</td>
<td>• BCP38</td>
</tr>
<tr>
<td>• Complex network authentication</td>
<td>• uRPF/BCP 84</td>
</tr>
<tr>
<td>• Security tools - unused</td>
<td><strong>Enterprise</strong></td>
</tr>
<tr>
<td></td>
<td>• Firewalls</td>
</tr>
<tr>
<td></td>
<td>• ALGs</td>
</tr>
<tr>
<td></td>
<td>• Anti-Spam SW</td>
</tr>
</tbody>
</table>
Why Existing Solutions Fail

• Tools are inadequate …
  …or improperly deployed

• Competence is low …
  … and education is inadequate

• Network operators must demonstrate ROI for CAPEX and BCP investment, not immediately obvious
Hard Questions

- Internet Architecture and stopping Unwanted Traffic
  - Cryptographic mechanisms
  - Curtailing the openness
  - Increasing the system complexity
  - Architectural principles we need to preserve
  - Separate control plane
  - The adversary is very adaptive …
    … and will take counter actions for any move we make to defend ourselves - e.g., BlueSecurity example
Medium and Long Term

• Tightening security of the routing infrastructure
• Cleaning up the Internet Routing Registry Repository [IRR], and securing both the database and the access, so that it can be used for routing verifications
• Take down bots and botnets
• Even without a magic wand we are able to take measures to reduce the unwanted traffic
• Community education (e.g., TCP MD5, use the filtering BCP’s, etc..)
• Layer security, raise the bar
Actionable

- Update the host requirements
- Update the router requirements.
- Update ingress filtering (BCP38 [RFC2827] and BCP 84 [RFC3704]).
- The IAB
  - inform the community about the existence of the underground economy.
- The IRTF
  - steps toward understanding the Underground Economy
  - encourage research on effective countermeasures.
A Concluding Note

• The Underground Economy is different from what we have seen before
  – It’s no longer kiddies with nothing better to do
  – It is a financially motivated illegal activity
  – The technology and global connectedness of the Internet is just the enabler

• The situation is getting worse

• However, there is growing awareness of the issues of the Underground Economy and that is the first step towards effective solutions