

Reflections on Unwanted Traffic After the IAB Workshop

Abuja, May 2007

**Loa Andersson
Internet Architecture Board
MPLS WG co-chair**



“I don’t live in Abuja”





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 and growing economic losses





Evolution of Threats - I

We had:

- Worms and viruses that simply did wreak havoc on the network

Now we see:

- malware that propagates, compromises hosts and enables command and control infrastructure and services platforms for malicious activity
 - Code Red (DDoS against IP)
 - Blaster (DDoS against hostname)
 - Deloder (Arbitrary DDoS toolkit)





Evolution of Threats - II

Initial major threat from botnets

- (D)DoS attacks

Today it forms an array of employment functions for

- (mostly) threats with economic motivations
- (to a lesser degree) threats have religious, political, etc, motivation 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-03.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!



The Underground Shopping Mall

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 goods, belongings and assets are bought and sold
- The shopping mall and its members are managed by criminals
- They use the tools and techniques they have developed to run their business
- Inventories include credit cards, bank accounts, domain names, internet routers, business licenses, physical servers, bots, botnets, etc.

**They work hard
for our money!**



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 (spooof 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

Vulnerabilities

Source address spoofing

BGP route hijacking

“Everything over HTTP”

Everyone comes from

Everywhere

**Complex network
authentication**

Security tools - unused

Solutions

Internet

Access control lists (ACL)

BGP null routing

BCP38

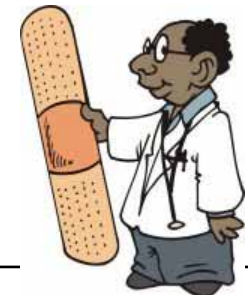
uRPF/BCP 84

Enterprise

Firewalls

ALGs

Anti-Spam SW





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



Bad - going on worse

But we see things that can be done!
There is a light in the end of the tunnel!
Situation will stay “gloomy” only as long
as we don’t act!
The hydra!







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 kids 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**





End of presentation

Questions?