FTC High-Tech Enforcement Case Study
ICANN DNS Abuse Forum
Nairobi, Kenya
March 11, 2010

The views expressed do not necessarily reflect those of the Commission.

What is the FTC?

- The only general jurisdiction consumer protection agency in the United States
- Independent federal agency headquartered in Washington, DC with 8 regional offices
- Enforcement through federal district court and administrative litigation.

Legal Framework

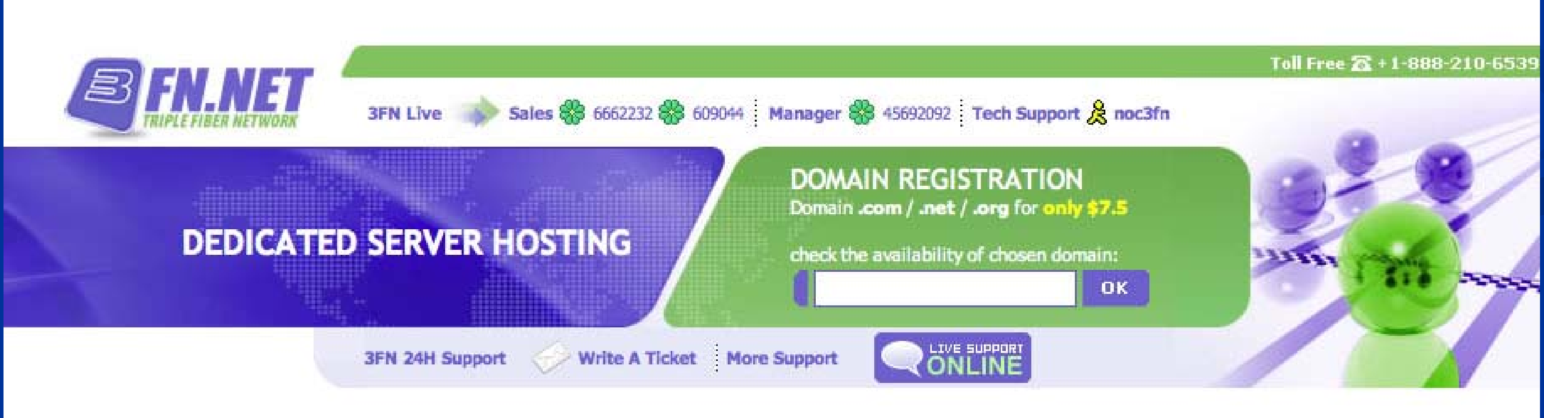
- Section 5 of the FTC Act: unfair or deceptive acts or practices
- Other statutes:
  - Children's Online Privacy Protection Act
  - CAN-SPAM Act
  - Gramm-Leach-Bliley Act
  - Fair Credit Reporting Act
  - Telemarketing and Consumer Fraud and Abuse Prevention Act

High Tech Enforcement Activities

- Internet fraud
- Spyware
- P2P file sharing
- Digital rights management
- Social networking
- Spam

FTC v. Pricewert LLC ("3FN")

- Rogue Internet Service Provider with hundreds of servers in the United States
- Child pornography, online pharmacies, botnet C&Cs, pirated music and software, spam tools, rogue anti-virus, etc…

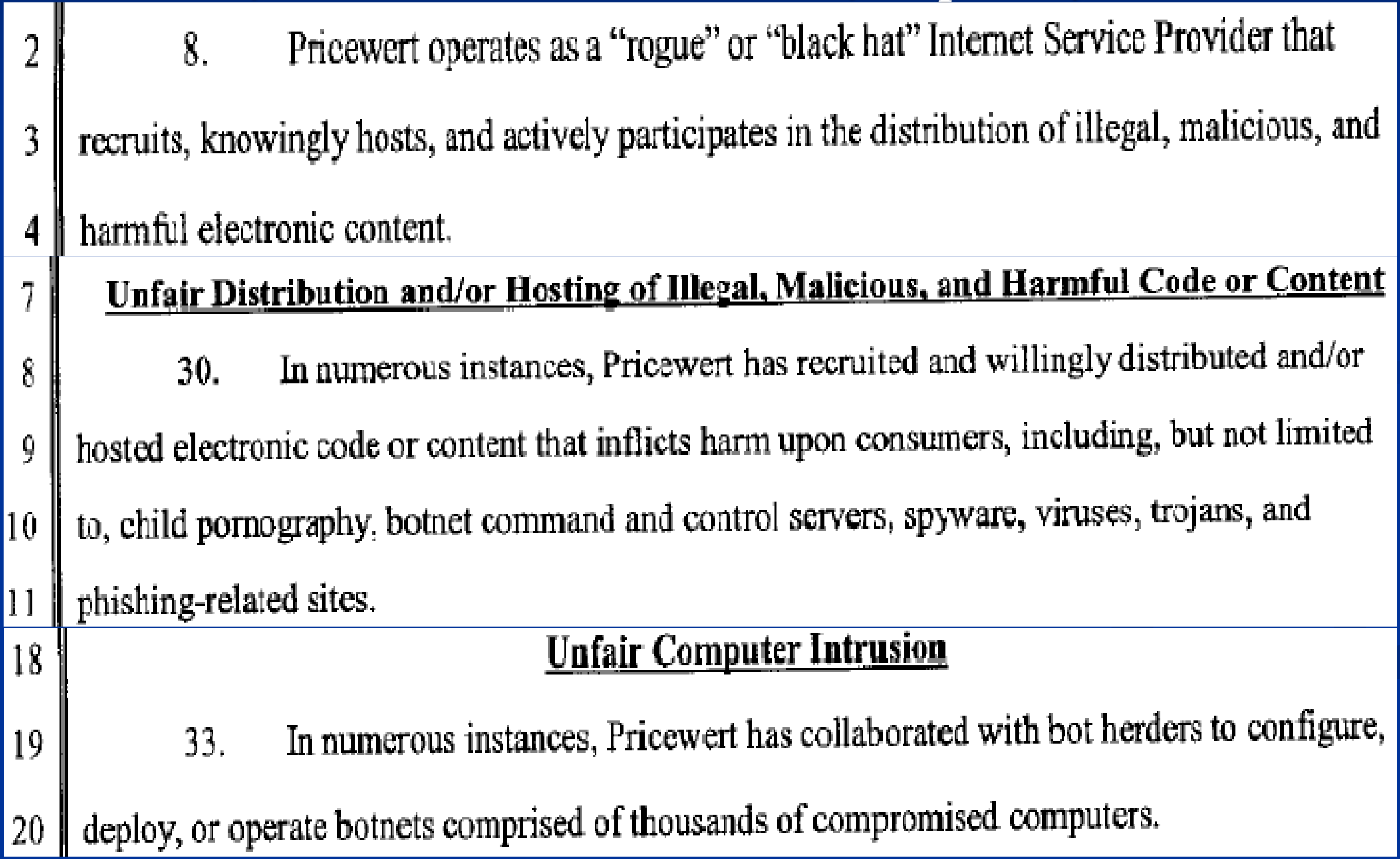


Domain .com / .net / .org for only $7.5

check the availability of chosen domain:

FTC Complaint vs. 3FN

- June 1, 2009 in N.D. California, *ex parte*, under seal



8. Pricewert operates as a "rogue" or "black hat" Internet Service Provider that recruits, knowingly hosts, and actively participates in the distribution of illegal, malicious, and harmful electronic content.

Unfair Distribution and/or Hosting of Illegal, Malicious, and Harmful Code or Content

30. In numerous instances, Pricewert has recruited and willingly distributed and/or hosted electronic code or content that inflicts harm upon consumers, including, but not limited to, child pornography, botnet command and control servers, spyware, viruses, trojans, and phishing-related sites.

Unfair Computer Intrusion

33. In numerous instances, Pricewert has collaborated with bot herders to configure, deploy, or operate botnets comprised of thousands of compromised computers.

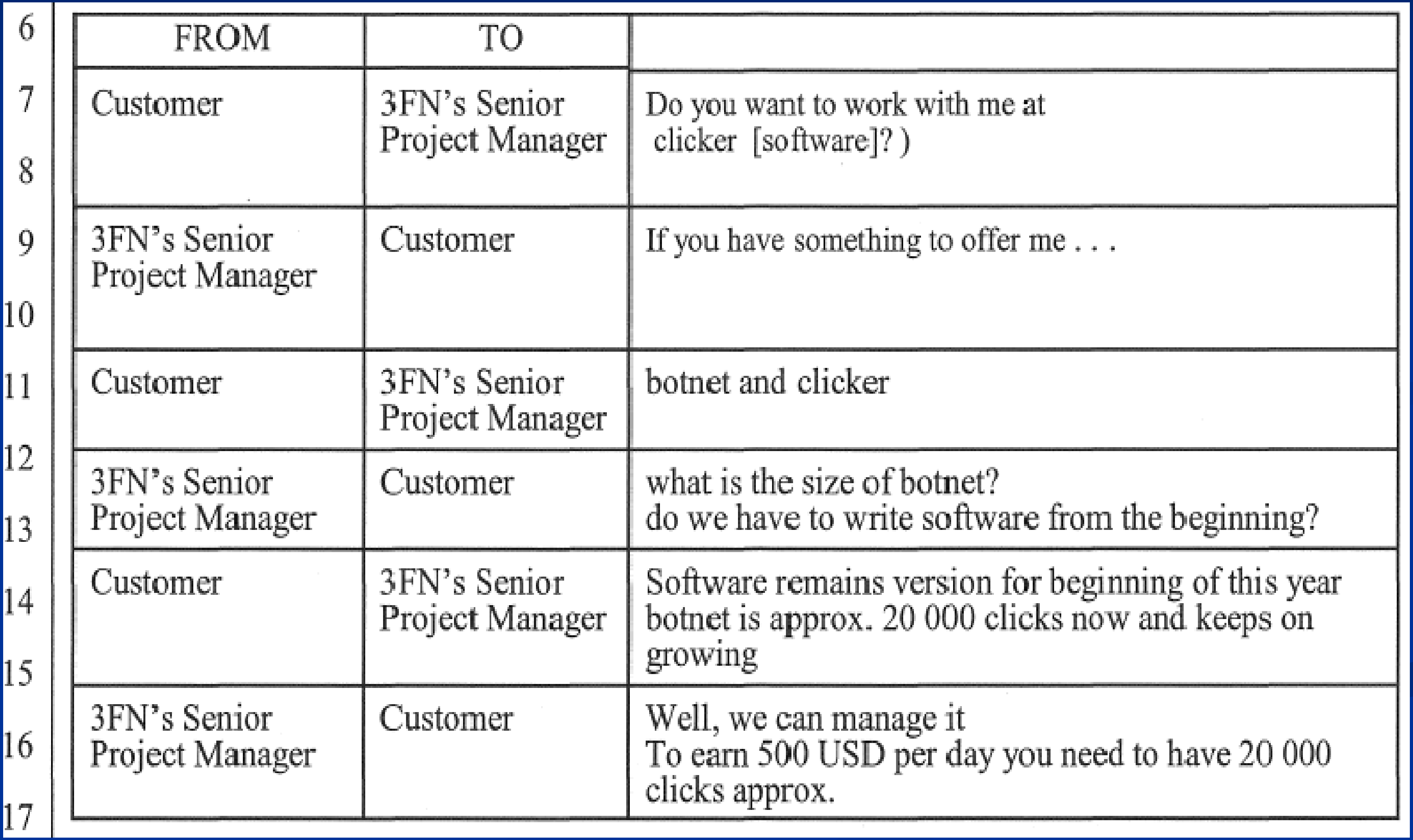
FTC v. 3FN - Evidence

- Declarations
  - NASA Office of Inspector General
  - University of Alabama
  - Nat’l Center for Missing and Exploited Children
  - The SpamHaus Project, Ltd
  - The Shadowserver Foundation
  - Symantec
  - FTC’s In-House Investigator

NASA

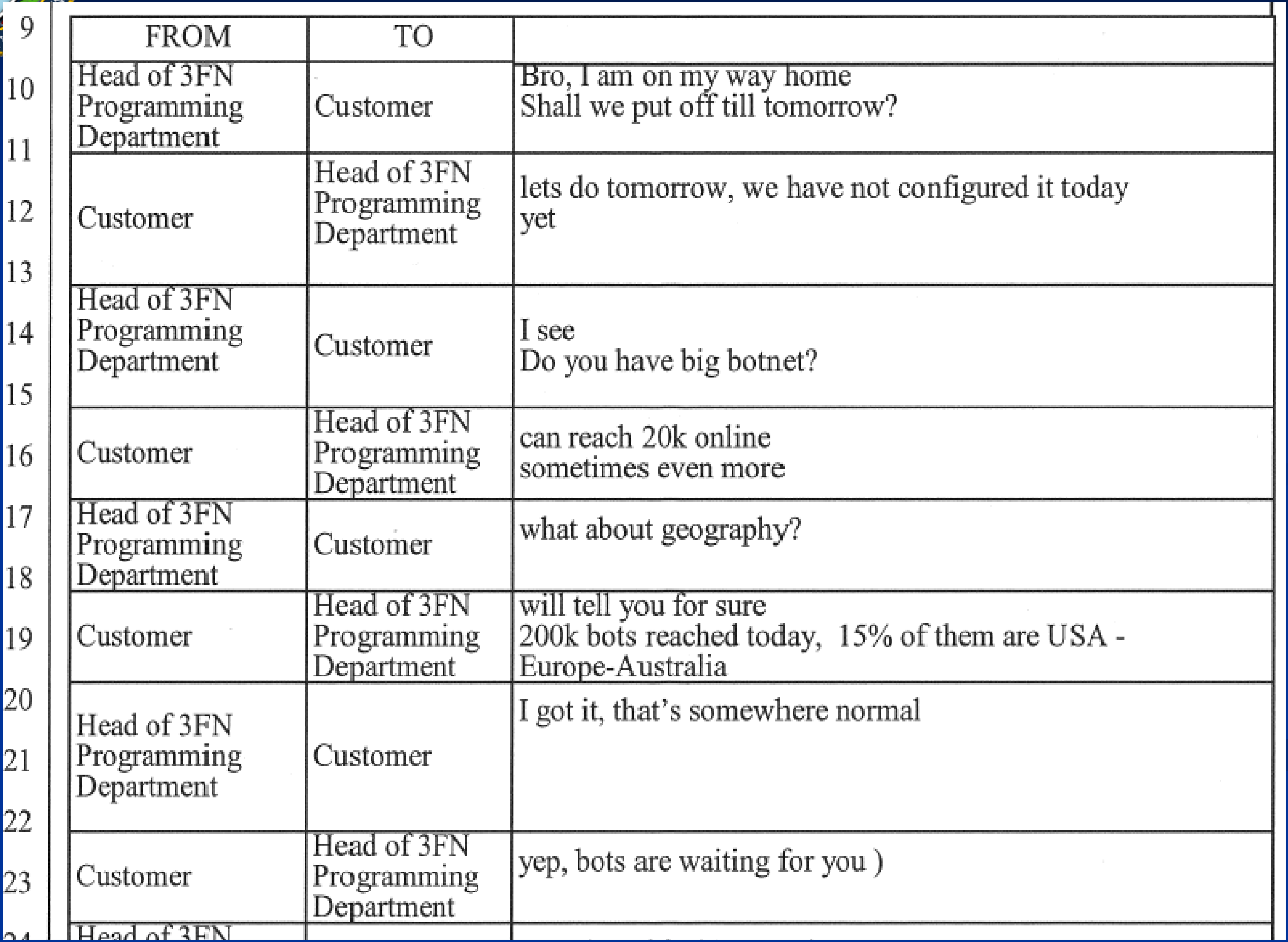
- “Discovery” of 3FN
  - Computer intrusion at NASA traced to McColo and 3FN
  - Location of 3FN datacenters
  - 3FN ICQ logs
    - arguably the most important evidence in the case

Evidence – ICQ Chat Log



FROM	TO	
Customer	3FN's Senior Project Manager	Do you want to work with me at clicker [software]?)
3FN's Senior Project Manager	Customer	If you have something to offer me . . .
Customer	3FN's Senior Project Manager	botnet and clicker
3FN's Senior Project Manager	Customer	what is the size of botnet? do we have to write software from the beginning?
Customer	3FN's Senior Project Manager	Software remains version for beginning of this year botnet is approx. 20 000 clicks now and keeps on growing
3FN's Senior Project Manager	Customer	Well, we can manage it To earn 500 USD per day you need to have 20 000 clicks approx.

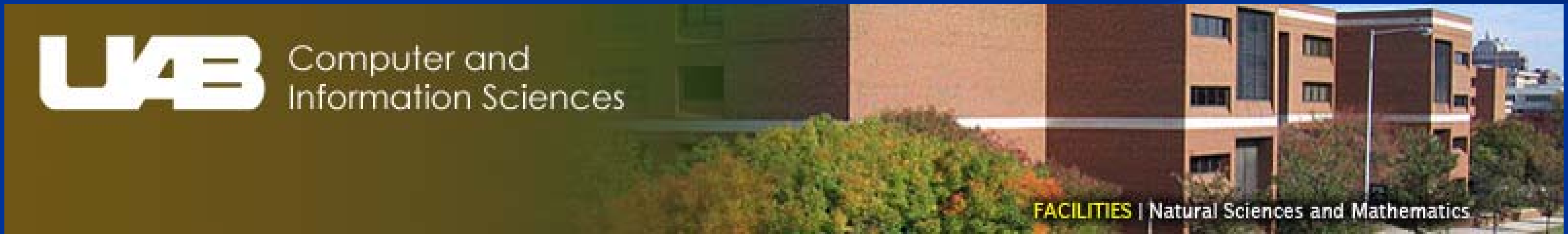
Evidence – ICQ Chat Log



FROM	TO	
Head of 3FN Programming Department	Customer	Bro, I am on my way home Shall we put off till tomorrow?
Customer	Head of 3FN Programming Department	lets do tomorrow, we have not configured it today yet
Head of 3FN Programming Department	Customer	I see Do you have big botnet?
Customer	Head of 3FN Programming Department	can reach 20k online sometimes even more
Head of 3FN Programming Department	Customer	what about geography?
Customer	Head of 3FN Programming Department	will tell you for sure 200k bots reached today, 15% of them are USA - Europe-Australia
Head of 3FN Programming Department	Customer	I got it, that's somewhere normal
Customer	Head of 3FN Programming Department	yep, bots are waiting for you)
Head of 3FN		

University of Alabama

- Examples of malicious content hosted at 3FN
  - child pornography
  - spam generation software
  - pirated music / software
  - online pharmacies
- Crutop.nu
  - Forum for spammers
  - Examples of 3FN advertising to criminals


UAB
Computer and Information Sciences
FACILITIES | Natural Sciences and Mathematics

NCMEC

- NCMEC's Child Pornography CyberTipline
- Analysis of Tipline reports for 3FN IP ranges
  - 700 reports of child pornography
  - More than 500 confirmed cases

NATIONAL
CENTER FOR
MISSING &
EXPLOITED
CHILDREN®
www.missingkids.com

SpamHaus

- Direct contact with 3FN Representative
  - Proof that 3FN collaborates with and protect clients
  - Evidence of foreign control of 3FN
- “Massive” number of Botnet C&Cs
- Comparison to McColo and Intercage

THE SPAMHAUS PROJECT

ShadowServer

- Another catalog of 3FN-hosted malicious content
- Review of 3FN IP Ranges
  - 311 3FN IP addresses participated in or facilitated malicious activity
  - 4,576 unique malware / virus specimens used 3FN servers for C&C
  - “wide spectrum of malicious activity”

Symantec

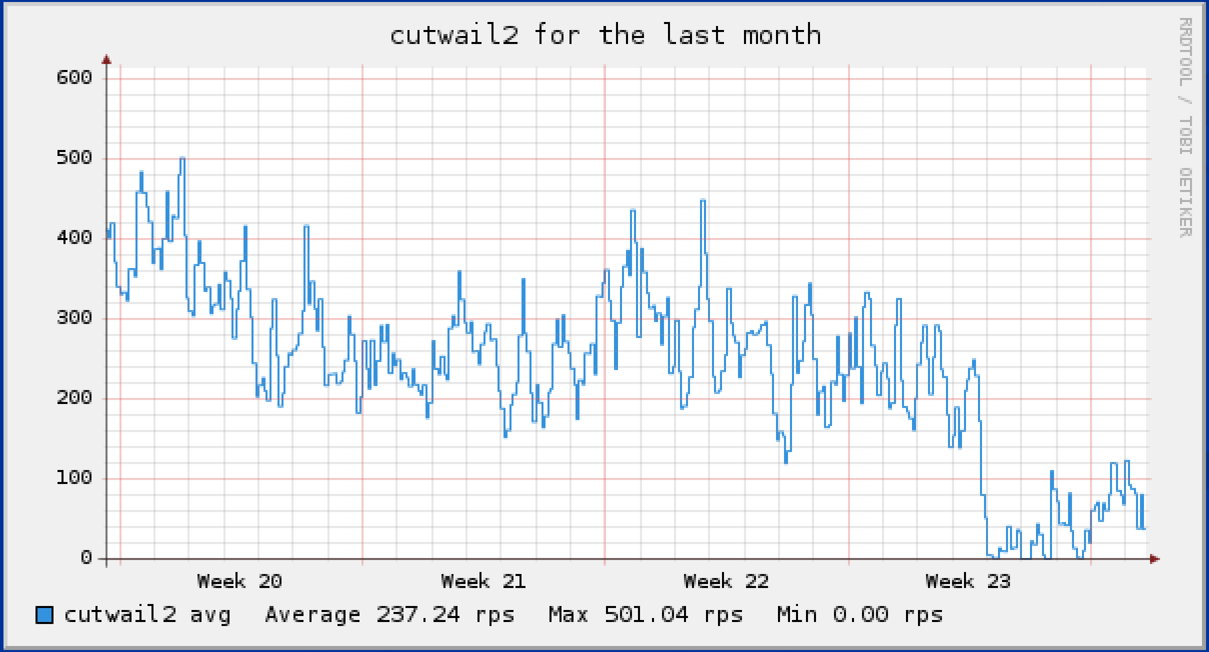
- Review of 3FN IP Ranges
- Analysis of Significant Attacks (spreadsheets)
- Analysis of Specific Attack Types
  - Bot Attacks
  - Bot C&C Activity
  - SPAM Attacks
  - Phishing Attacks

FTC Investigator

- 3FN WHOIS info
  - Connecting aliases to Pricewert corporate shell
- 3FN Run From Outside the United States
- ICQ translation
- Online Complaint Review

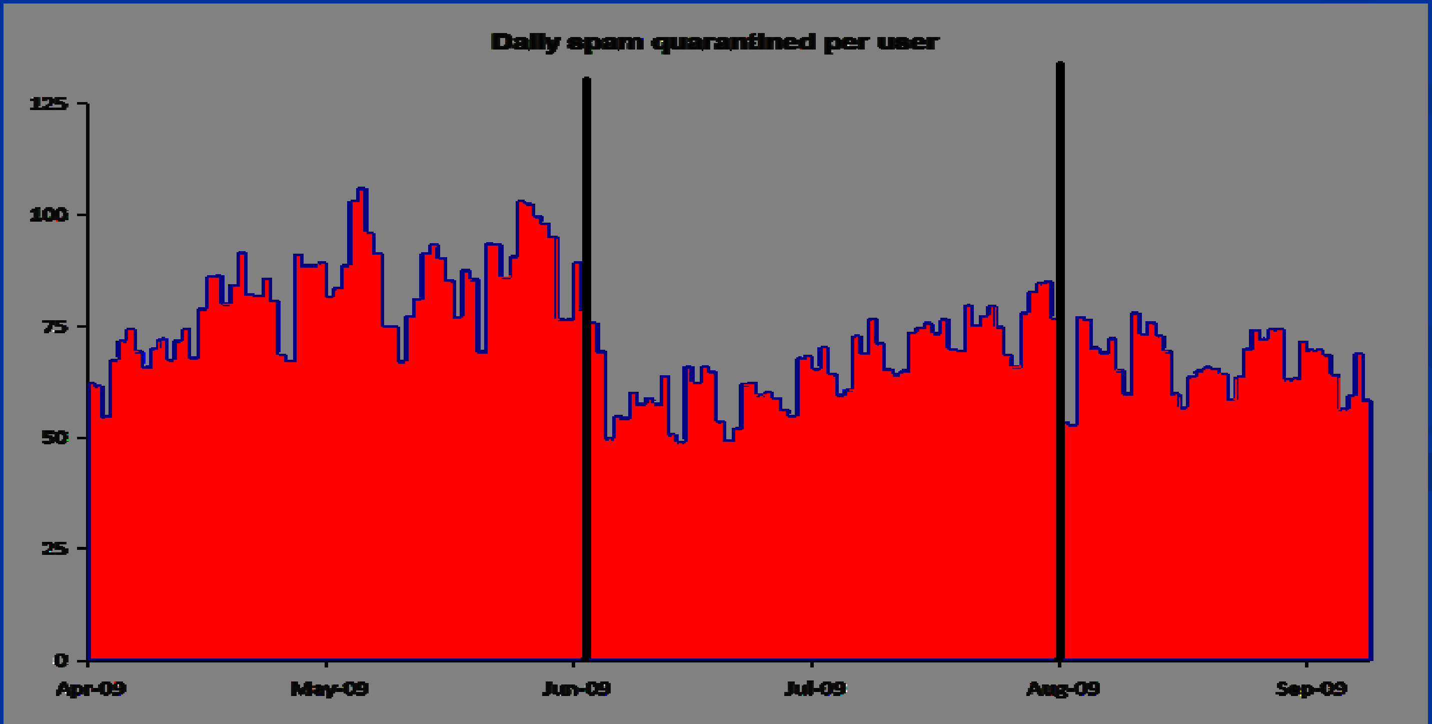
Impact Assessment – The Good News

- What was the impact of the 3FN shutdown?
  - Difficult to measure precisely
  - Significant but temporary drop in spam levels
  - Significant impact on the Cutwail botnet



Impact Assessment – The Bad News

- Criminals are learning and evolving
  - Centralized command servers no longer required
- Botnets and spam continue to grow despite enforcement
- ISP shutdowns have proven to be a temporary fix



Source: Postini

Questions?