

Technical and Sociological Infiltration of the Underground Economy

Possibilities & Issues

Christian Kreibich

International Computer Science Institute



The Underground Economy

- » Financially motivated Internet-driven abuse
 - » Fraud, identity theft, extortion, money laundering...
- » Complex real-world market
 - » Vendors, merchants, spammers, malware authors, botmasters, affiliate programs, ...
- » Prevention extremely difficult
 - » Technical and sociological problem
- » What can we do?

Botnet infiltration

- » Botnets: a central ***technical*** component
 - » A ***weakness*** we can attack
- » 2007 brought a perfect opportunity: ***Storm***
 - » New research experience
 - » Even a little scary
 - » Many seized the opportunity
- » We infiltrated Storm for 10+ months
 - » ***Very fruitful*** effort
 - » But fraught with ***legal & ethical issues***

Insights

Issues

Technical

?

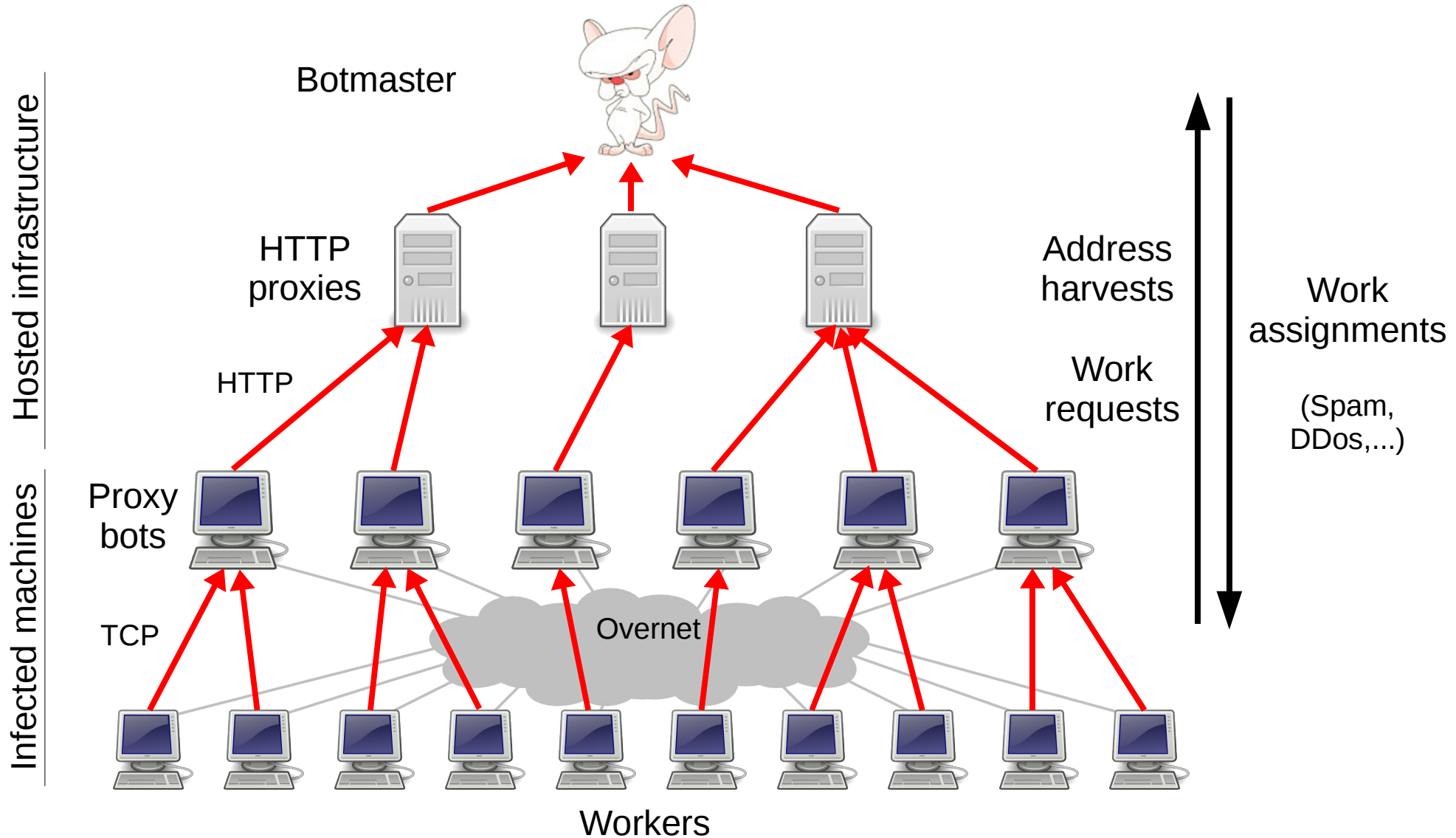
?

Sociological

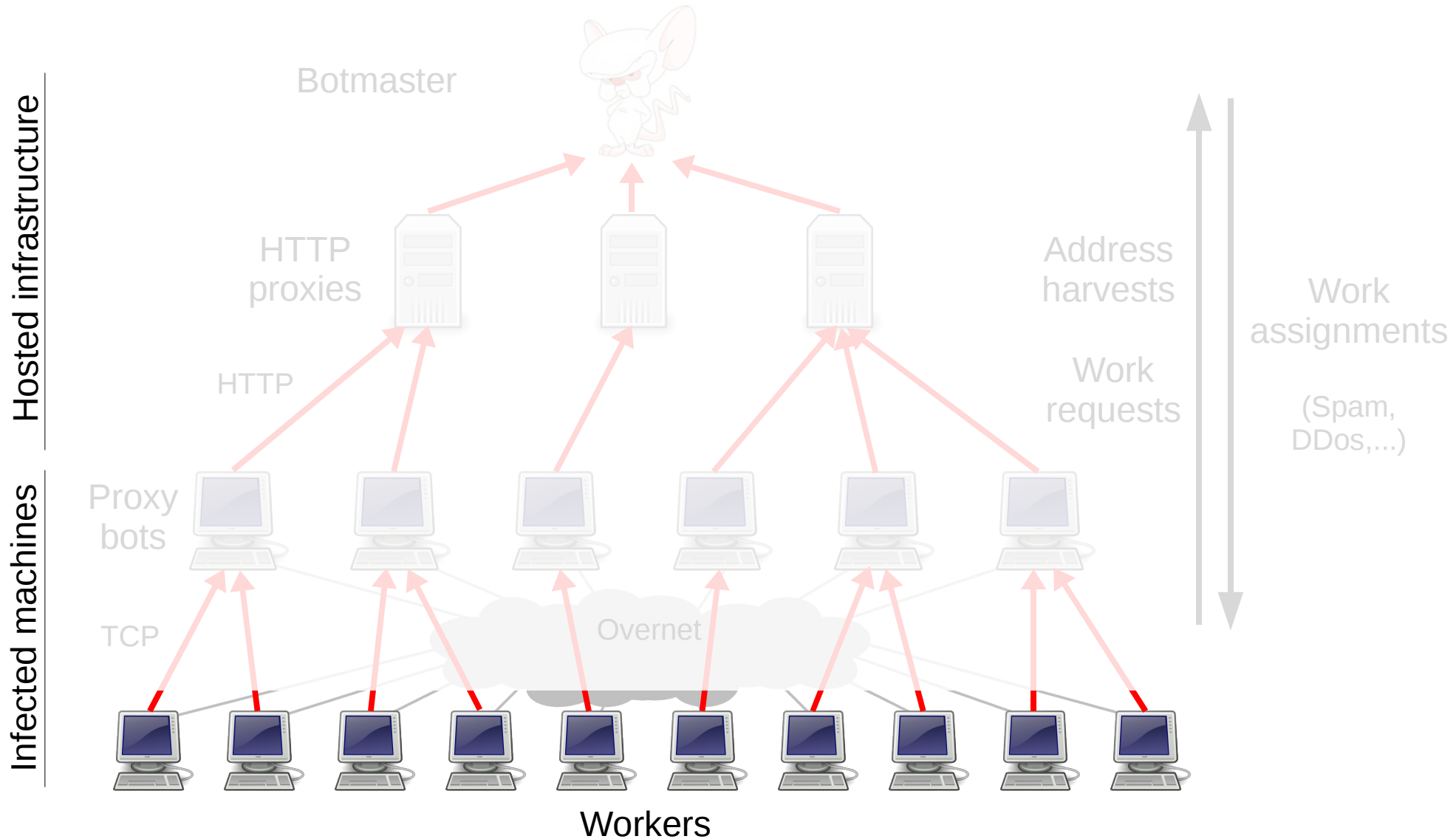
?

?

The Storm Botnet



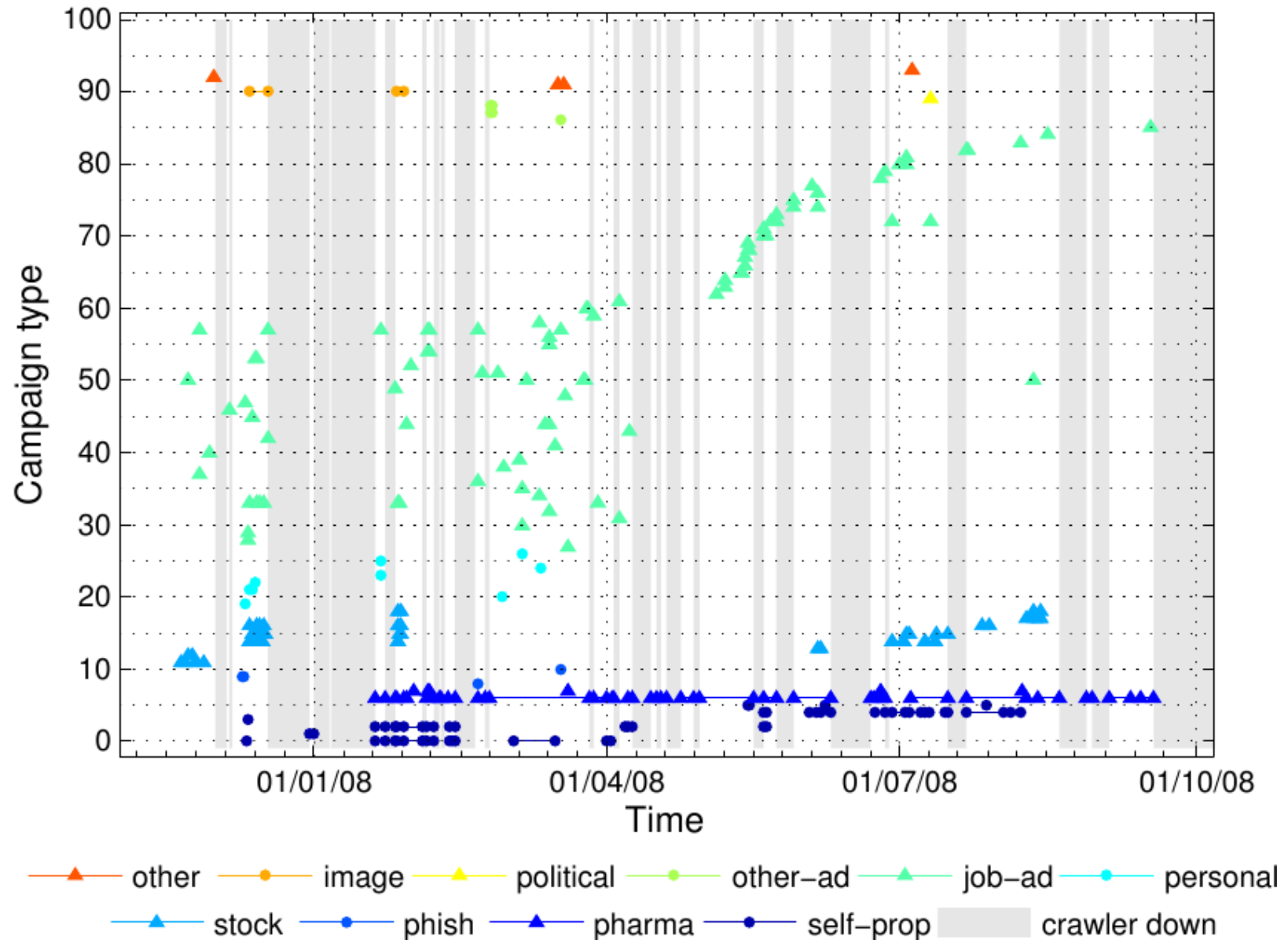
The Storm Botnet



Issue: Malware Containment

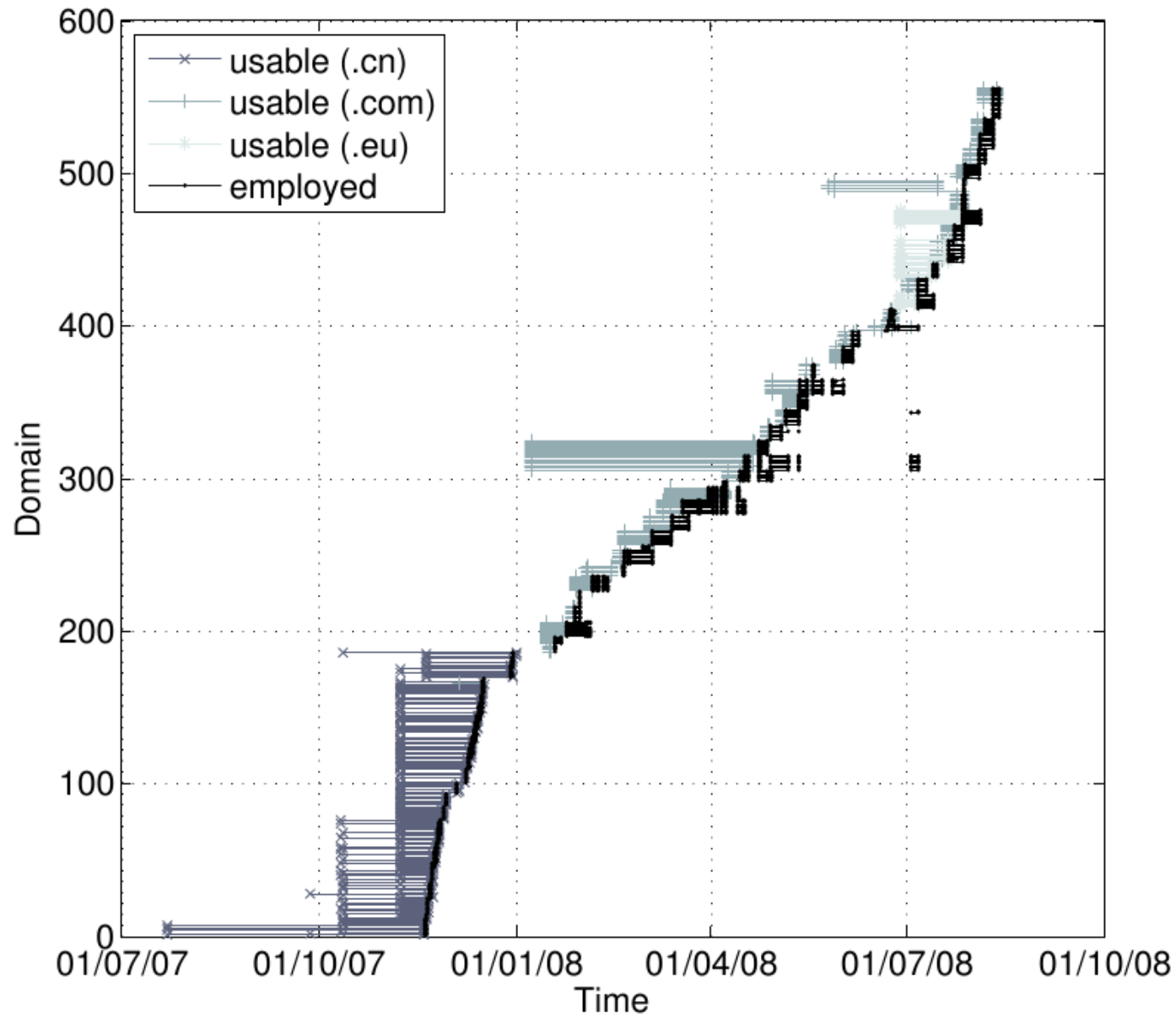
- » Must operate malware ***safely***
 - » Spamming, DDoS, iframe & SQL injections, ...
- » Tight containment is ***time-consuming***
 - » Each botnet unique
 - » C&C nature not known ahead of time
- » Transparent app-layer ***containment proxy***
 - » Default-deny, filtering, redirection
 - » Iteratively expand understanding of the C&C

Insight: Campaign Awareness



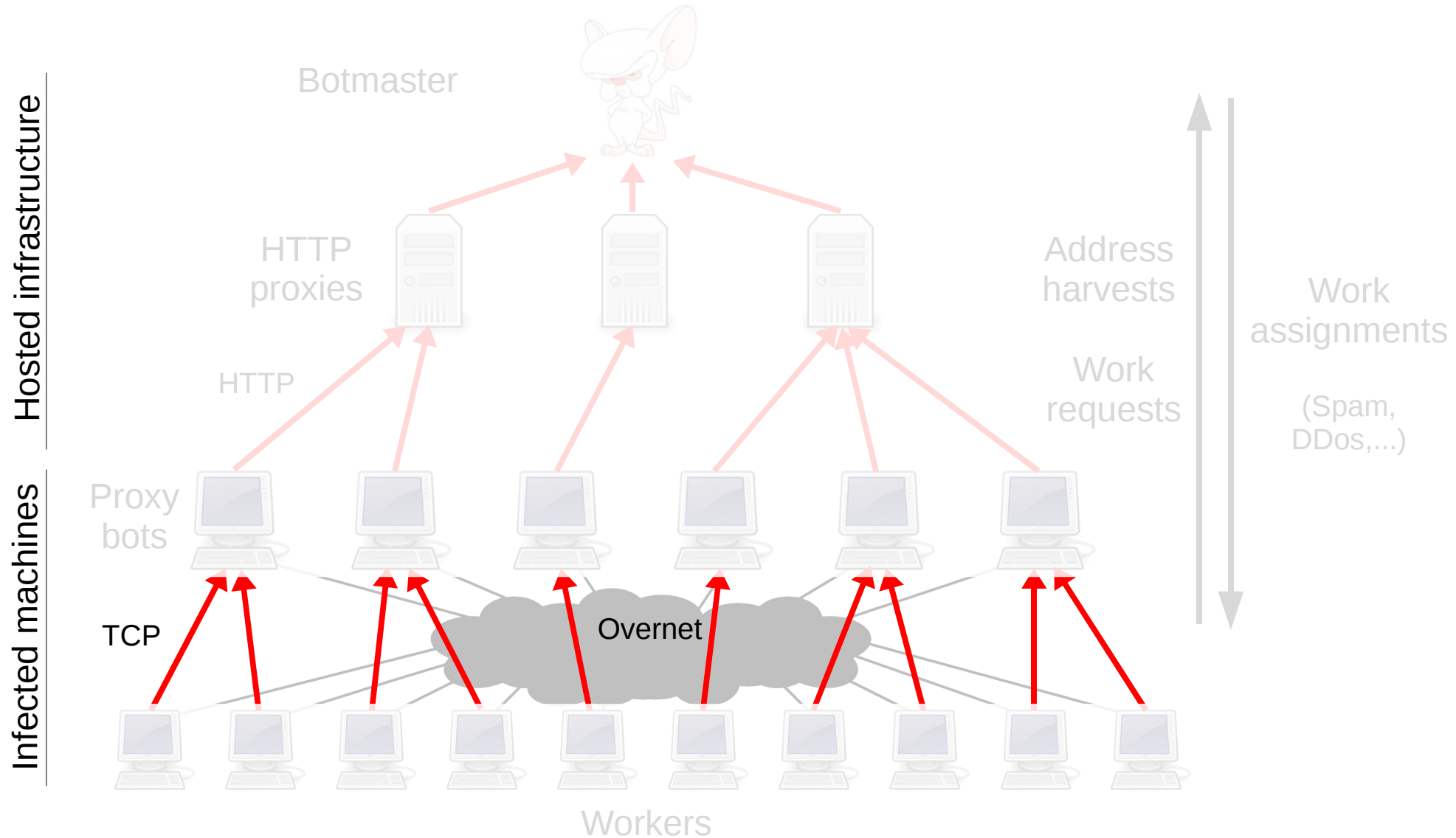
» From: Spamcraft: An Inside Look At Spam Campaign Orchestration, LEET'09

Insight: Domain Use & Usability



» From: Spamcraft: An Inside Look At Spam Campaign Orchestration, LEET'09

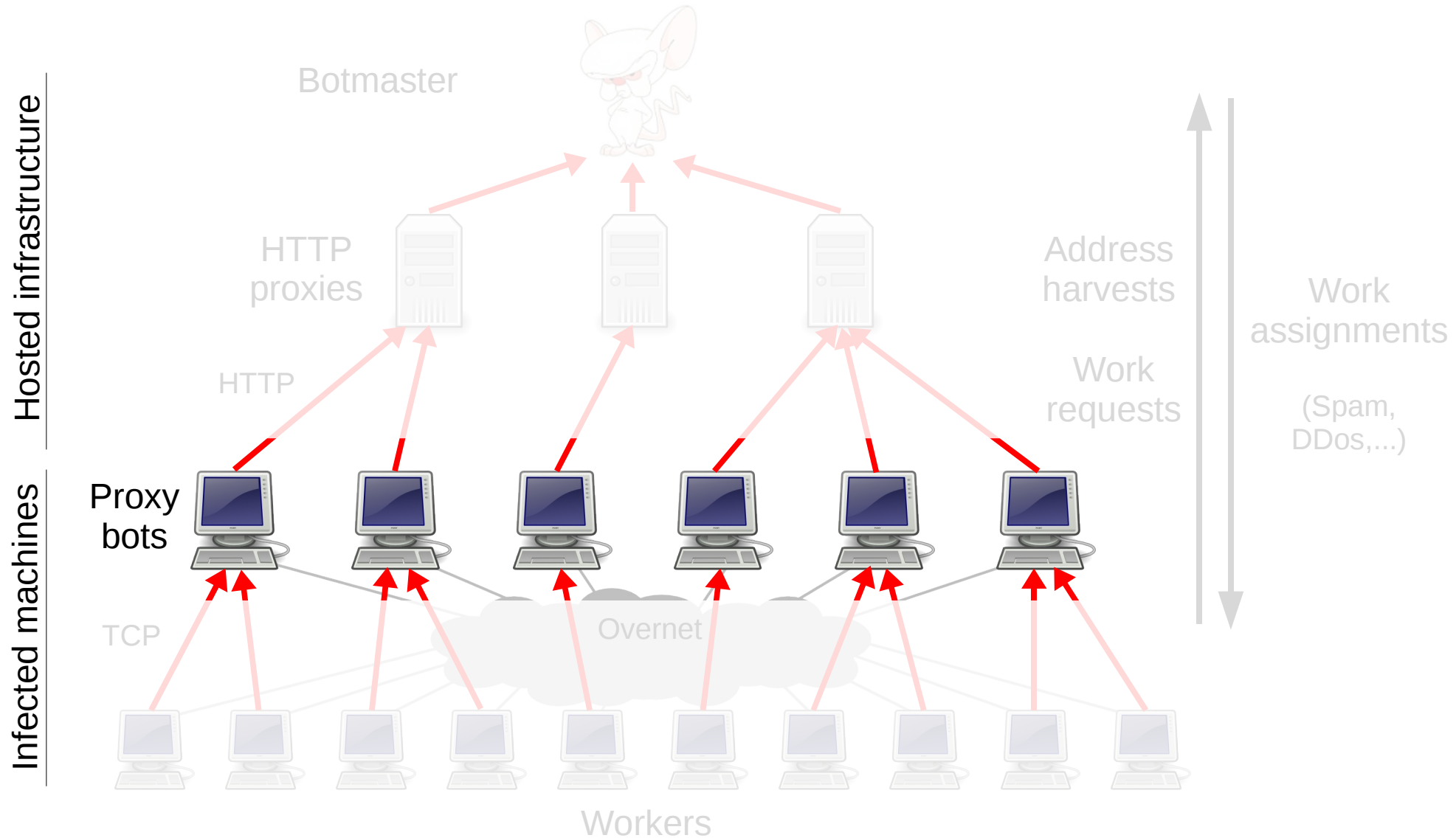
The Storm Botnet



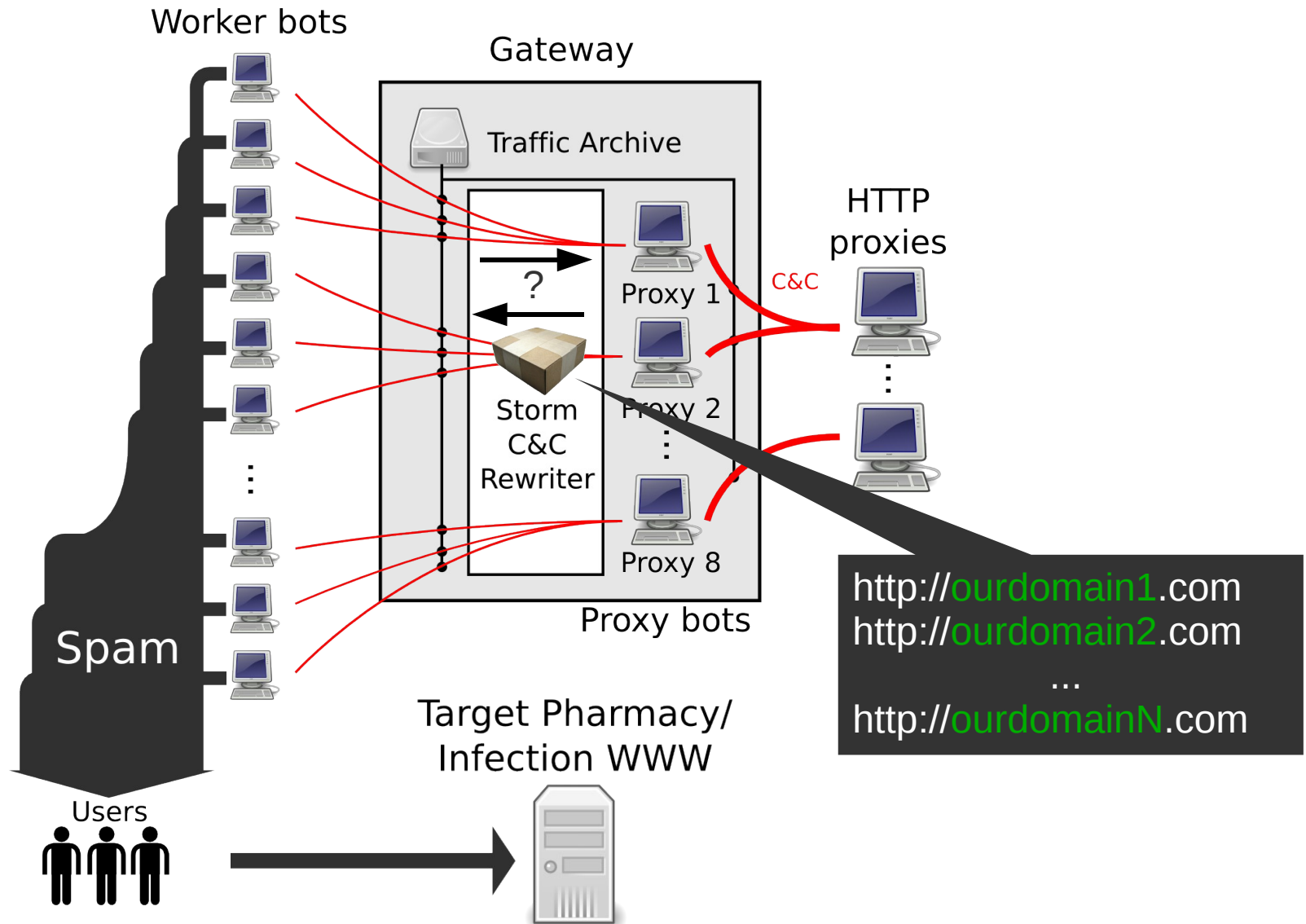
Insight: Rendezvous Infiltration

- » Accurate ***size measurement*** — carefully!
 - » Responding nodes?
 - » NATed?
 - » IDs vs IPs?
- » Colliding experiments!

The Storm Botnet



C&C inspection and rewriting





Your download will start in 5 seconds.
If your download does not start, [click here](#)

©2000-2008 AwesomePostCard.com - All rights reserved.

Done



Your cart: \$0.00 (0 items) [Proceed to Checkout >](#)

Canadian Pharmacy
#1 Internet Online Drugstore



Products list

VIAGRA

For Order more than \$300:
12 VIAGRA PILLS

FREE

For other Orders:
4 VIAGRA PILLS

★ Bestsellers

- Male Enhancement
- Men's Health
- SALES - 20% OFF
- Female Enhancement
- Weight Loss
- Gums **New!**
- Body-Building
- Hypnotherapy

Viagra + Cialis **69⁹⁹\$**

10 x Viagra
100 mg
10 x Cialis
20 mg

[ORDER NOW](#)

Penis Growth Pack **179⁹⁵\$**

Penis Growth Pills
1 bottle x 60caps
Penis Growth Oil
1 tube x 2oz

[ORDER NOW](#)

Viagra **225⁶¹\$**

120 pills
100 mg
+4 Free pills

[ORDER NOW](#)

Search by name: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 5

Search:

Today's Bestsellers

Viagra

Our price **\$1.21**

[More info](#) [Add to cart](#)

Cialis

Our price **\$2.18**

[More info](#) [Add to cart](#)

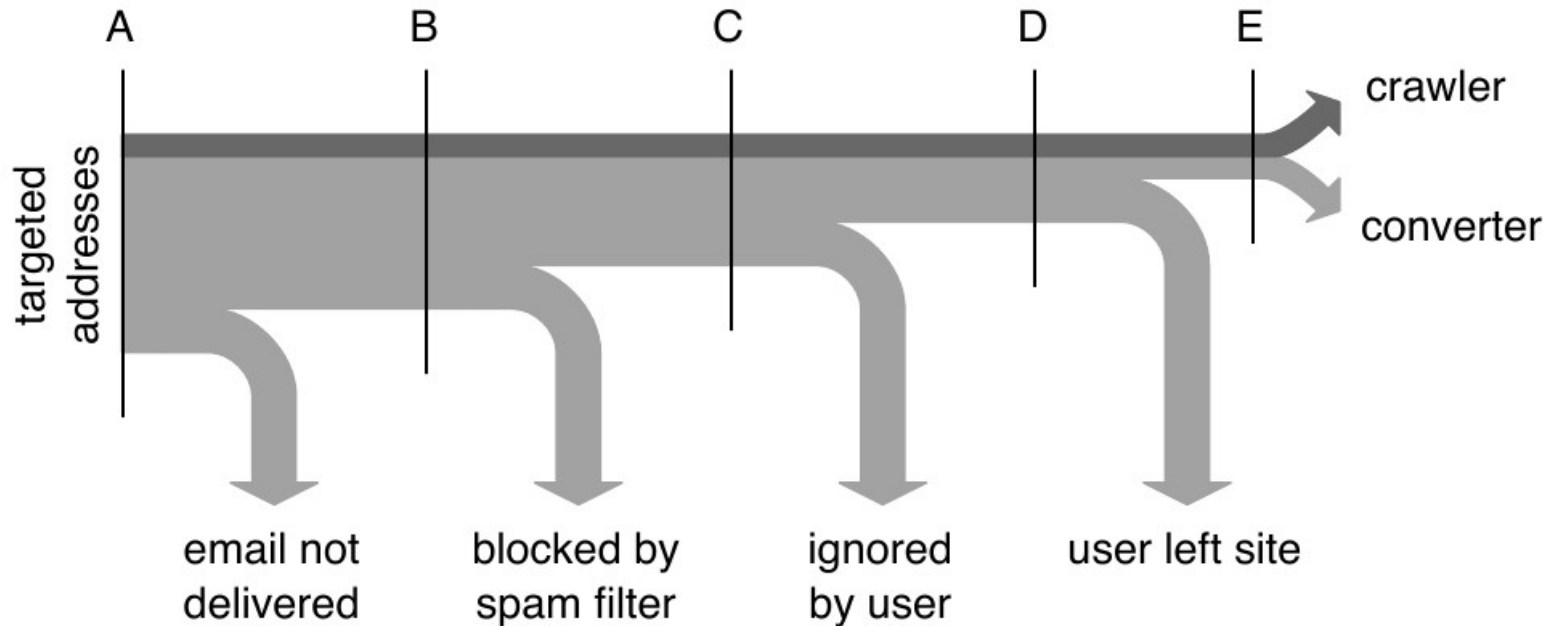
Viagra Professional

Our price **\$3.73**

[More info](#) [Add to cart](#)

Done

Insight: Spam Conversion



- » 1 in 12.5m pharma targets yields sale
- » 1 in 265k greeting card targets yields infection
- » 1 in 10 visitors of infection site ran offered program
- » Revenue: ~3.5M US\$ / year



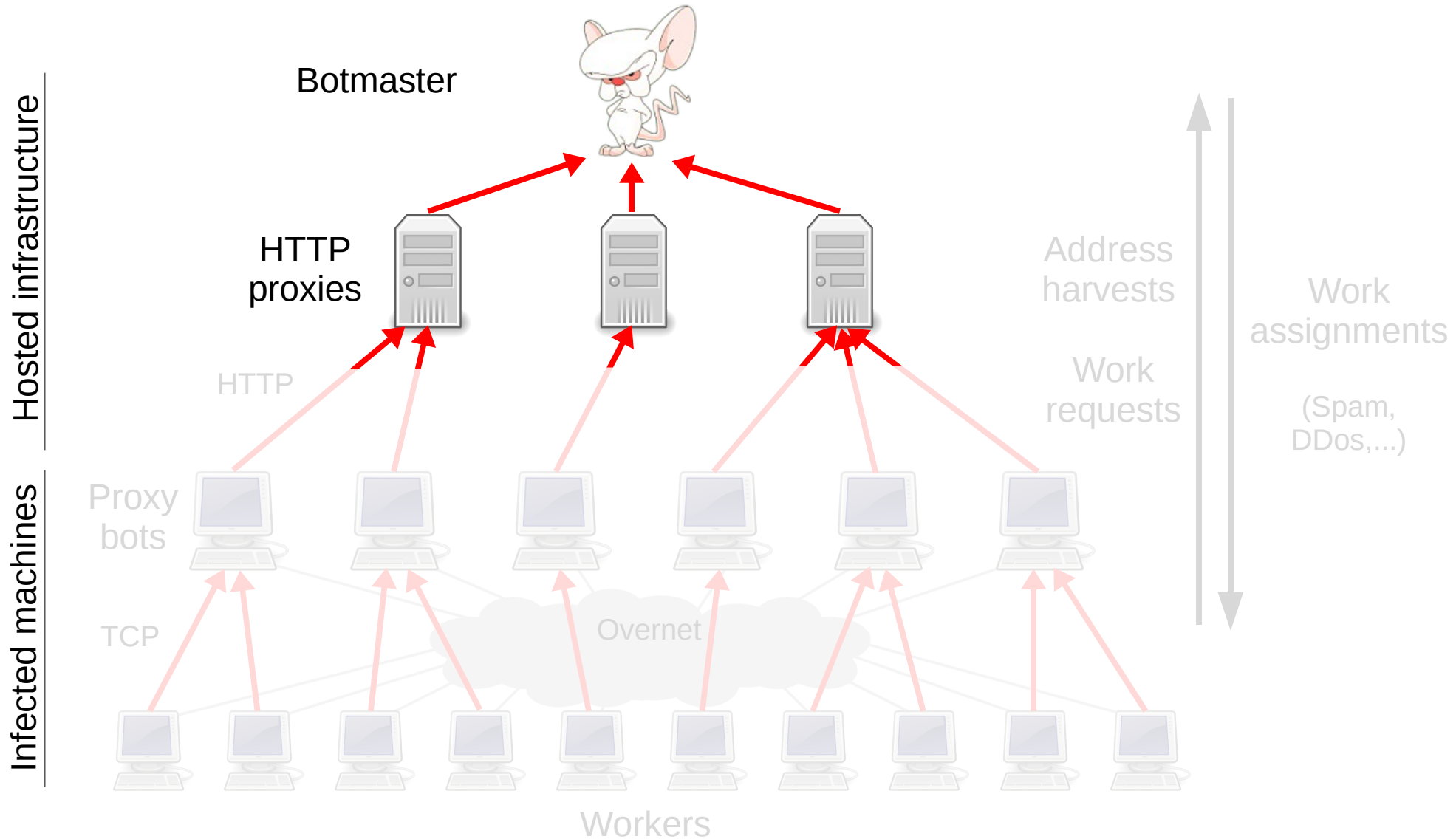
Issue: Law Enforcement

- » FBI takedown order on our servers was in progress
- » Support your local LE unit! :o)

Issue: Human Subjects

- » Privacy concerns
 - » Potentially highly sensitive end-user data
- » In US: Institutional Review Board (IRB) approval
 - » Institutions receiving federal grants must have one
 - » 6-8 weeks processing time for basic cases

The Storm Botnet



Issue: “Offense In Depth” / Rental

- » C&C filtering, signal jamming
- » “White” Botnets: takeover / cleanup
 - » Technically *hard*, ethically *dubious*
- » Do we need a CDC?
- » BBC study on botnet rental

Insights

Issues

Technical

- » Understanding of MO
- » Spam awareness
- » Botnet size estimation
- » C&C rewriting
- » Offense in depth

- » Arms race advancement
 - » Invasion resilience
- » Bot reliability
- » Containment
- » Colliding experiments

Sociological

- » Victim behavior
- » Spammer behavior
- » Bot herder behavior
- » Market analysis
 - » Volumes
 - » profits

- » Victim privacy
- » Human subjects
 - » IRB approval
- » Law enforcement involvement
- » Ethics
 - » Inform of infections
 - » Passive consent