

# Botnet Infiltration

## Possibilities & Challenges

Christian Kreibich

International Computer Science Institute

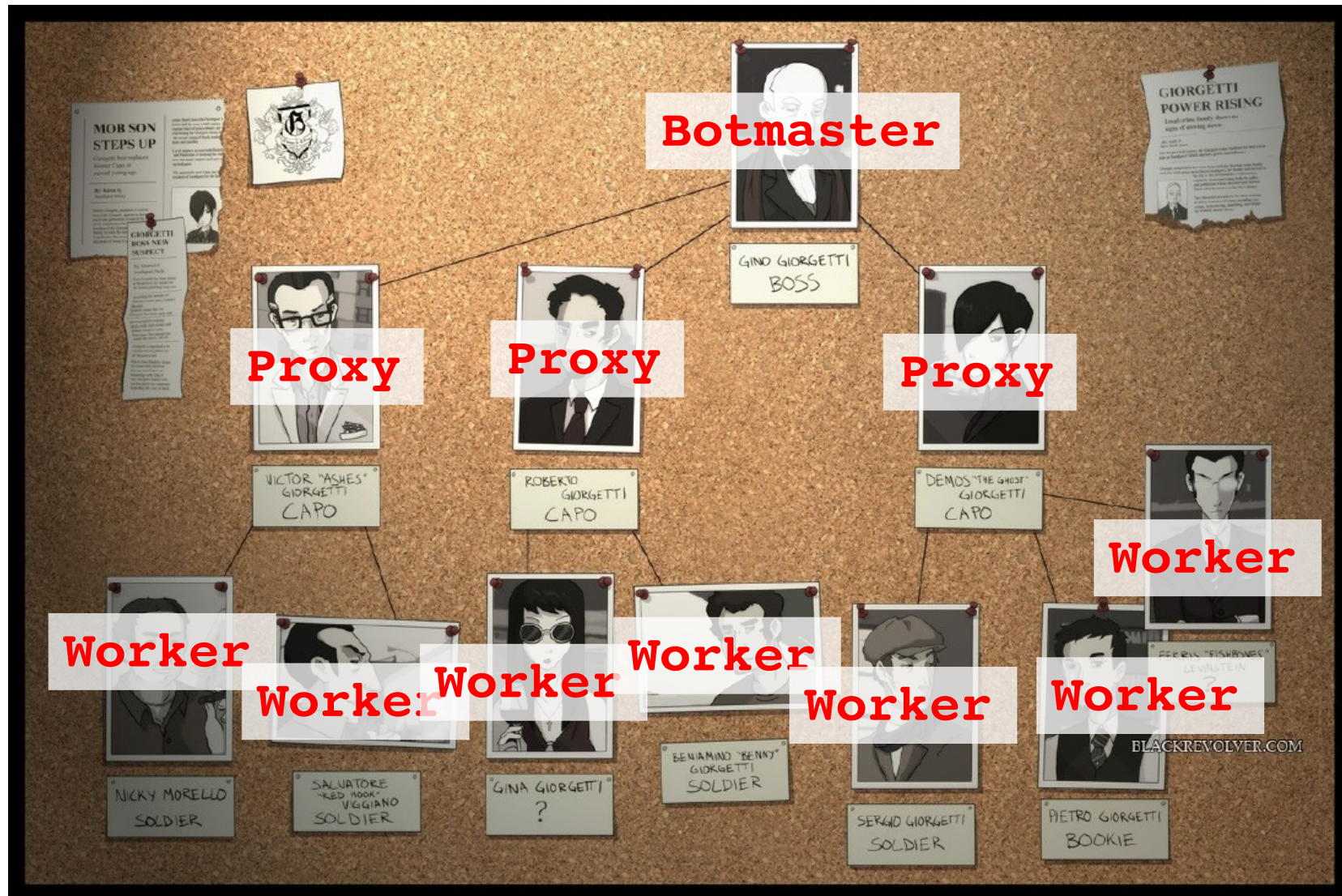


# The “Underground” Economy

---

- » 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?

# n Bot-net



# Botnet infiltration

---

- » Botnets: a central *technical* phenomenon
  - » Distributed systems: a *weakness* we can attack
- » Since around 2007, a **constant presence**
  - » Storm, MegaD, Waledac, ...
  - » New research experience, lots of interest
  - » Even a little scary — DDoS threat? Kneecaps?
- » We have infiltrated several botnets longitudinally
  - » Storm: 1 year, MegaD: 3 months, others passively
  - » *Very fruitful* efforts
  - » But fraught with *legal & ethical challenges*

# Insights

---

# Challenges

---

Technical

?

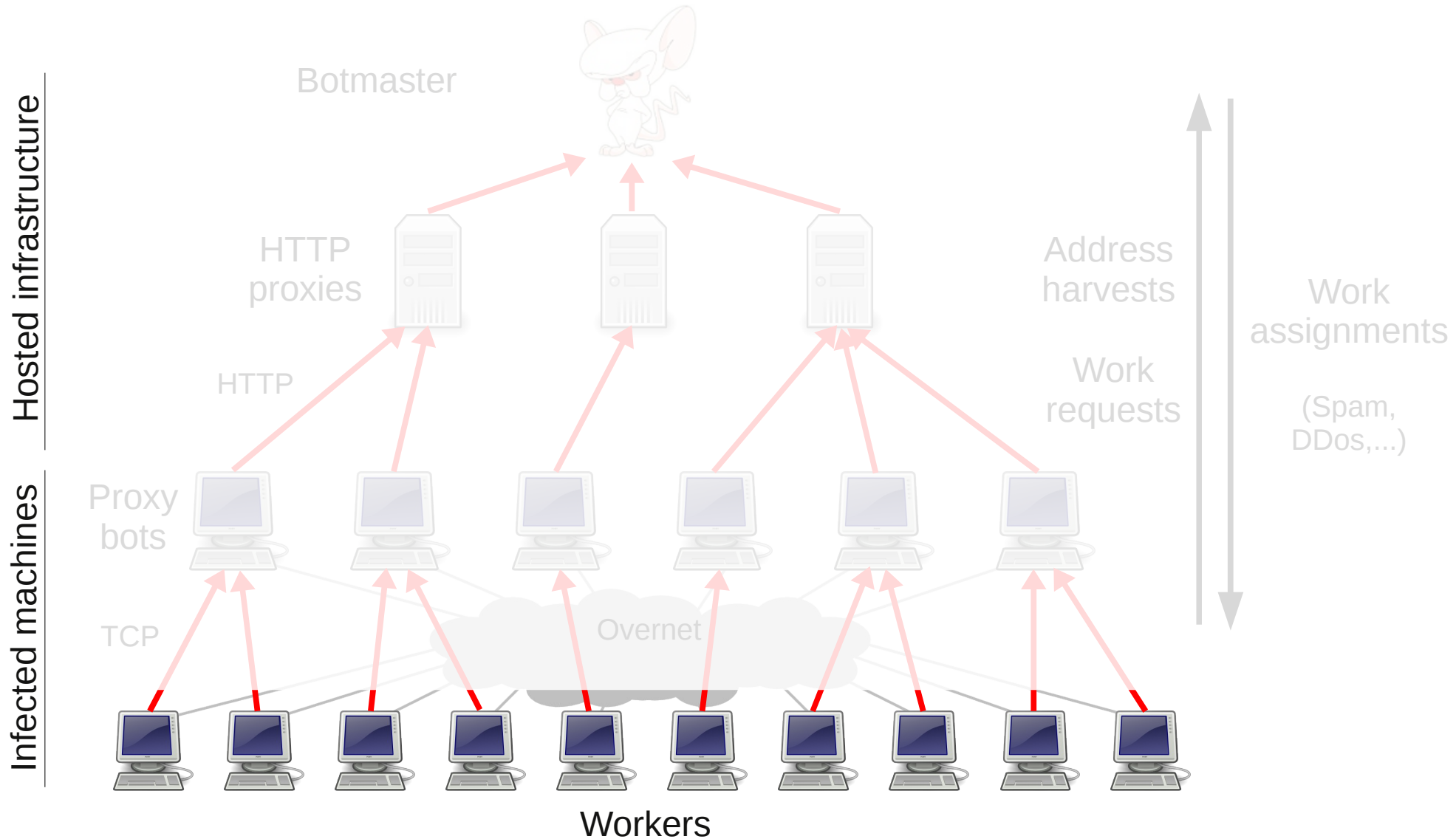
?

Sociological

?

?

# The Storm Botnet

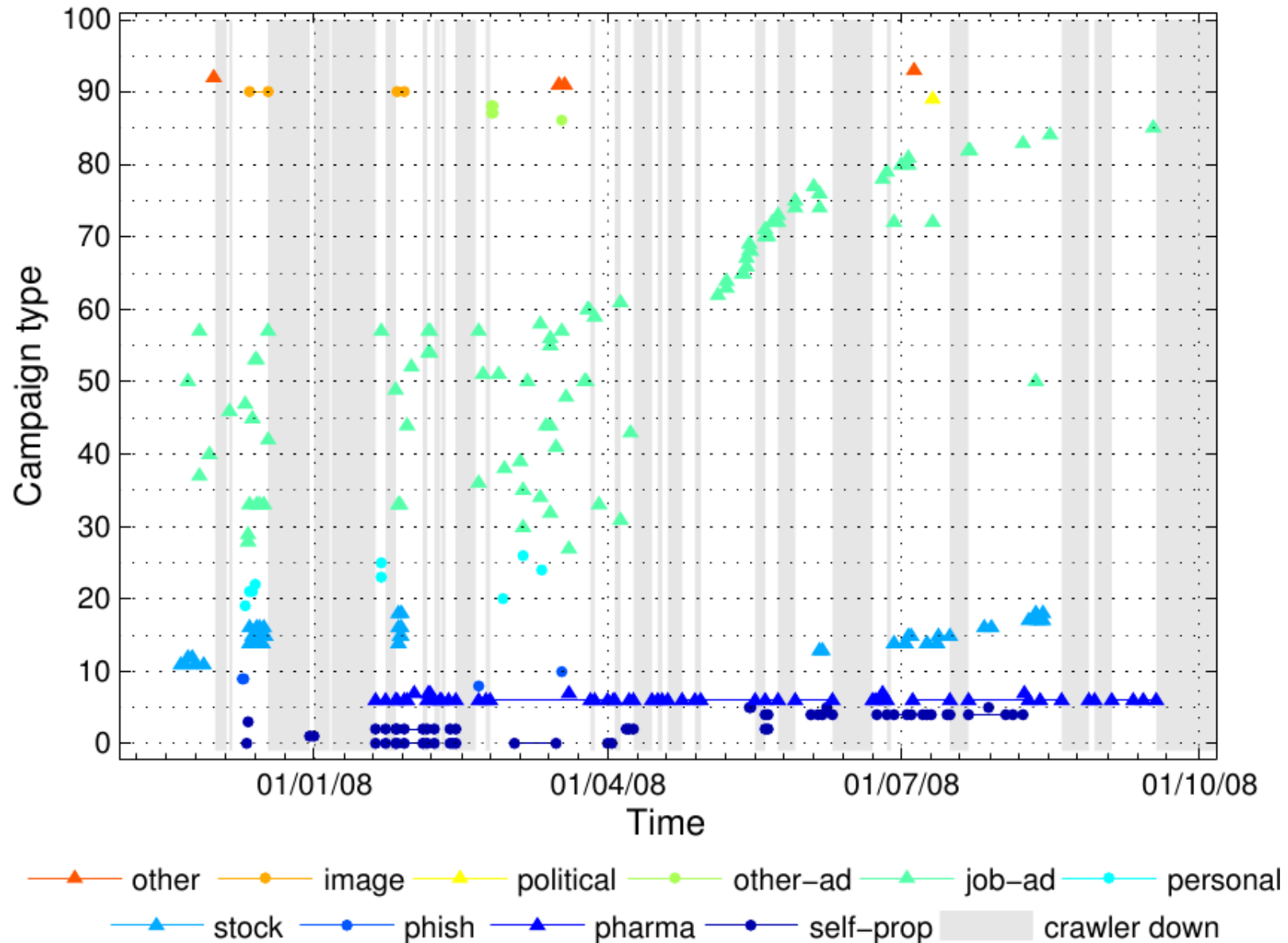


# Challenge: Malware Containment

---

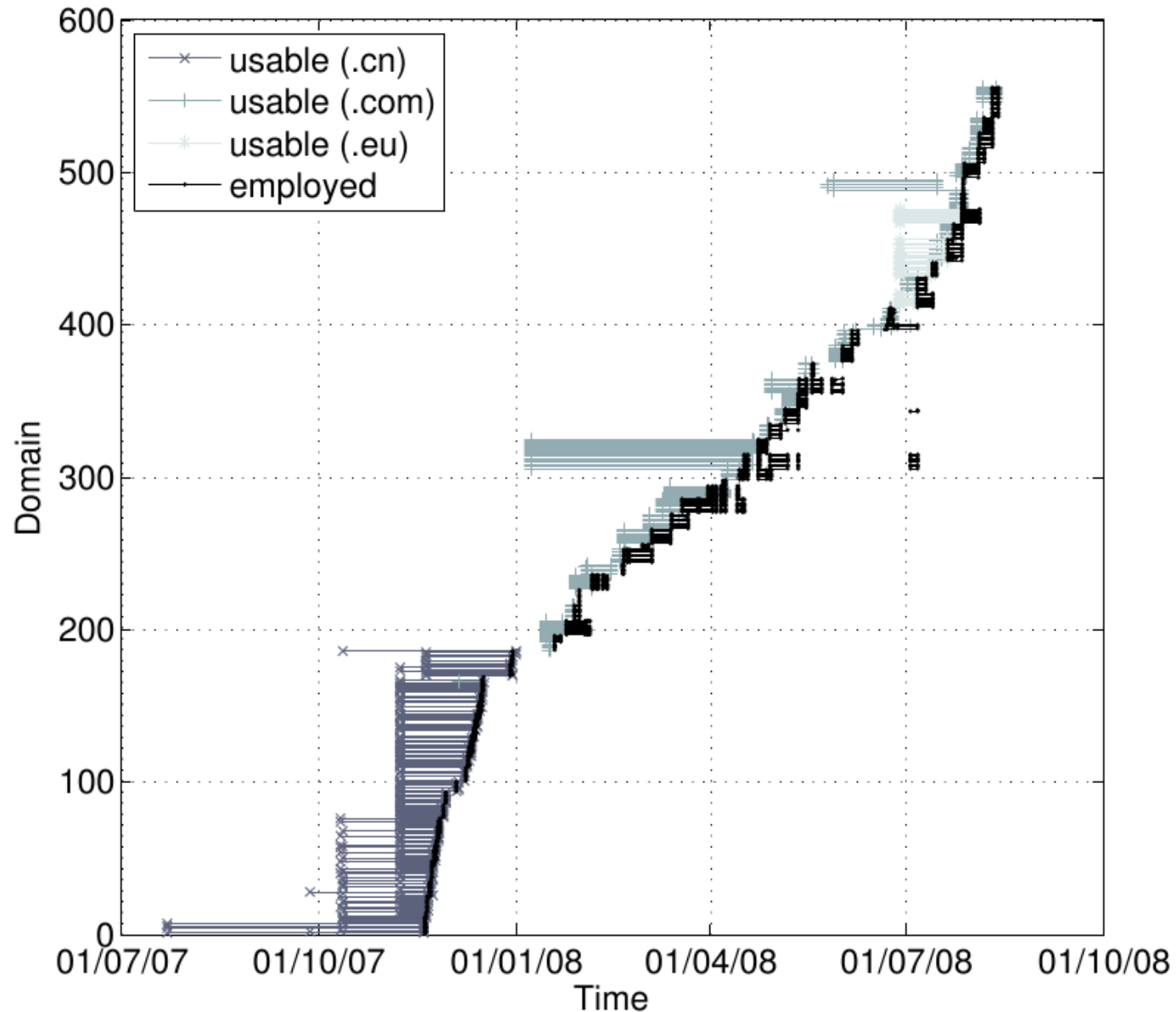
- » Must operate malware *safely*
  - » Spamming, DDoS, iframe & SQL injections, ...
- » Undercover bots are **sensitive** and **scarce**
- » Tight containment is *time-consuming*
  - » Each botnet unique
  - » C&C nature not known ahead of time
- » Transparent app-layer *containment proxy*
  - » Default-deny,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

# Insight: Campaign Awareness



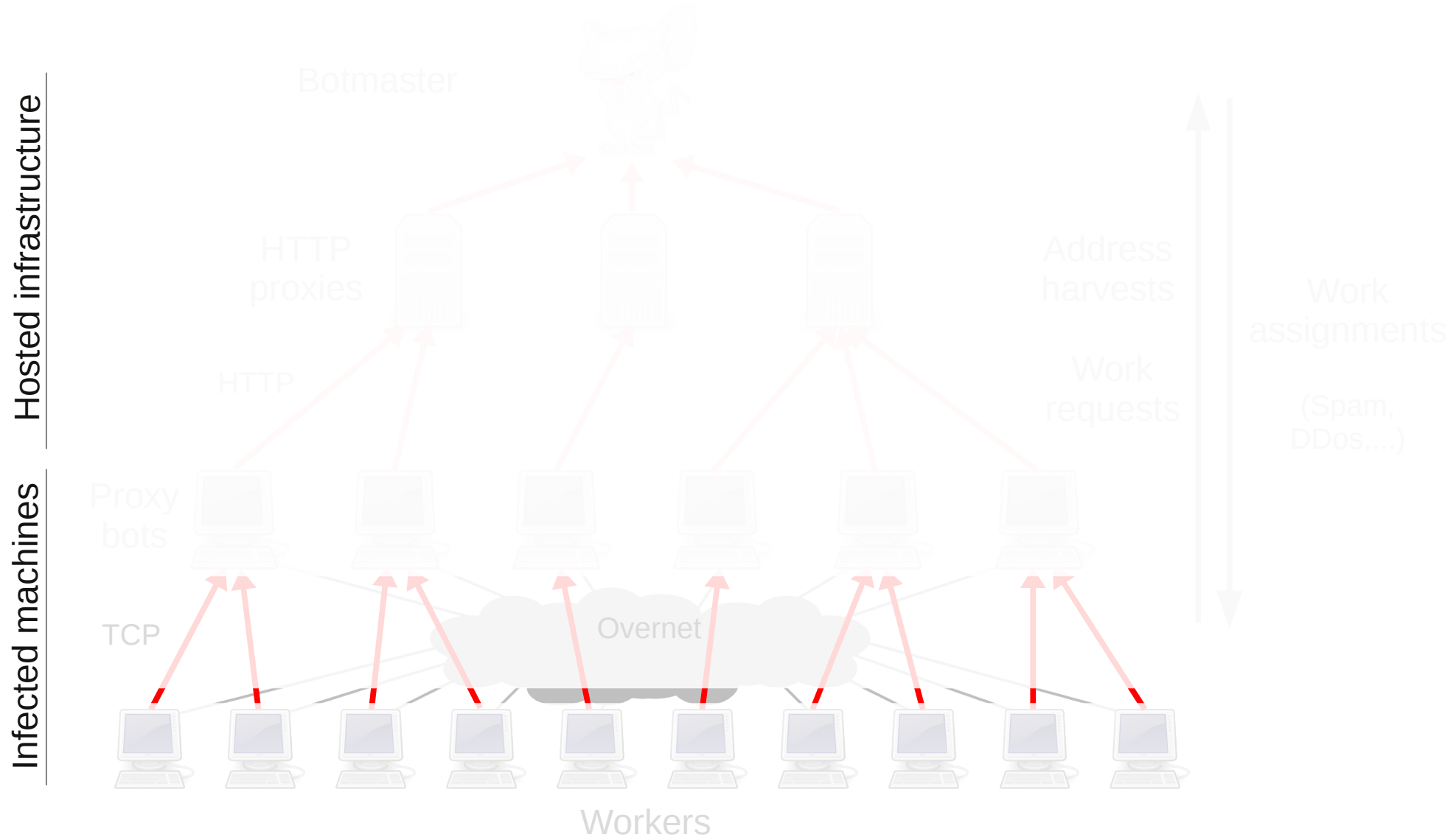
» From: Spamcraft: An Inside Look At Spam Campaign Orchestration, LEET'09

# Insight: Domain Use & Usability



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

# The Storm Botnet

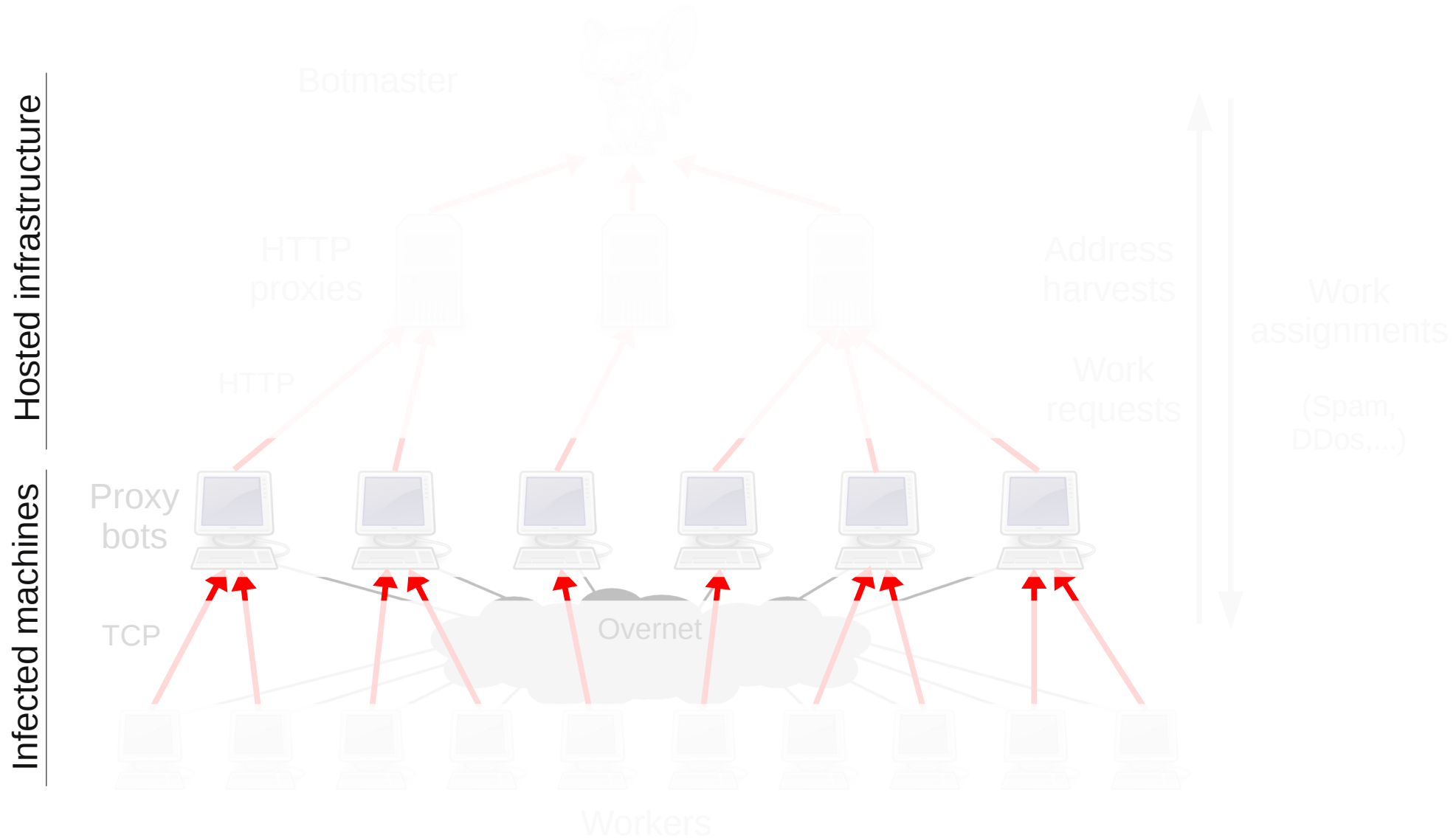


# Insight: Rendezvous Infiltration

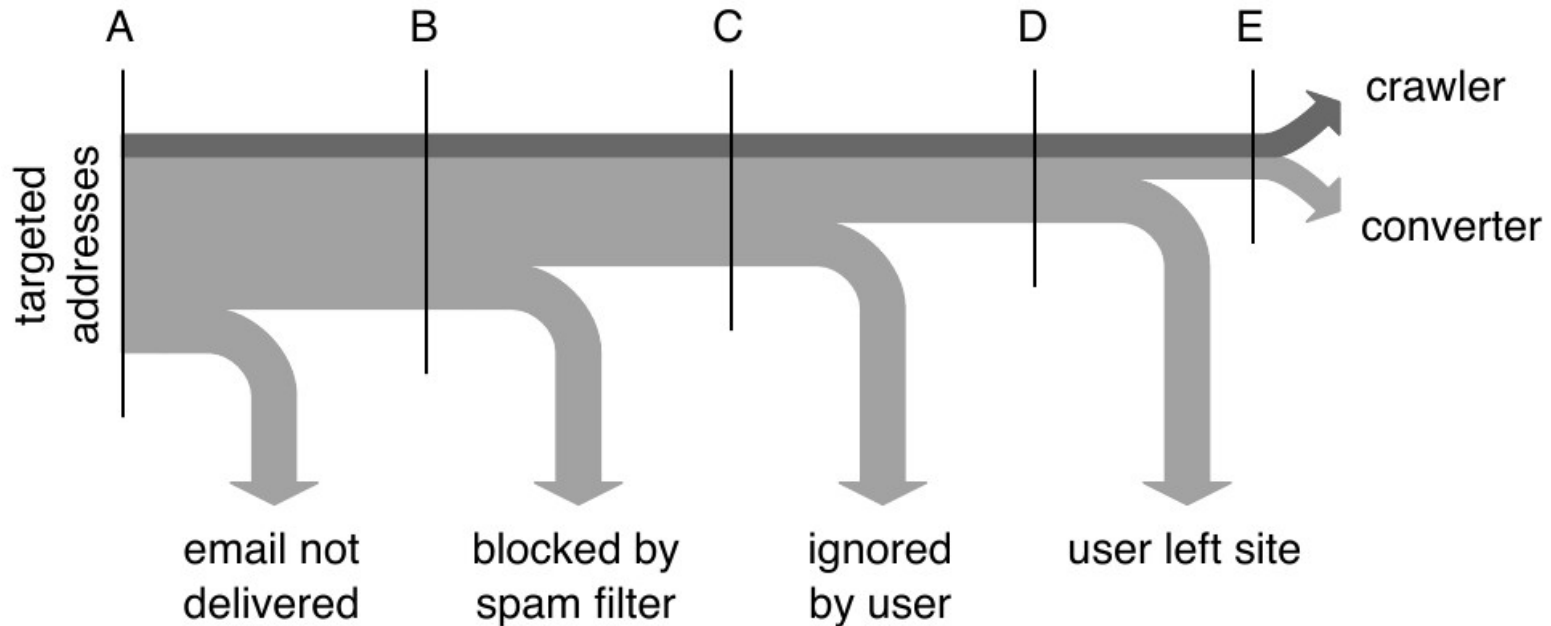
---

- » Accurate **size measurement** — carefully!
  - » Real bots or former bots' addresses?
  - » Machines behind NATs?
  - » Bot IDs vs IP addresses?
- » More recently: **domain generation algorithms**
- » **Colliding experiments!**

# The Storm Botnet



# 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

# Challenge: Law Enforcement

---

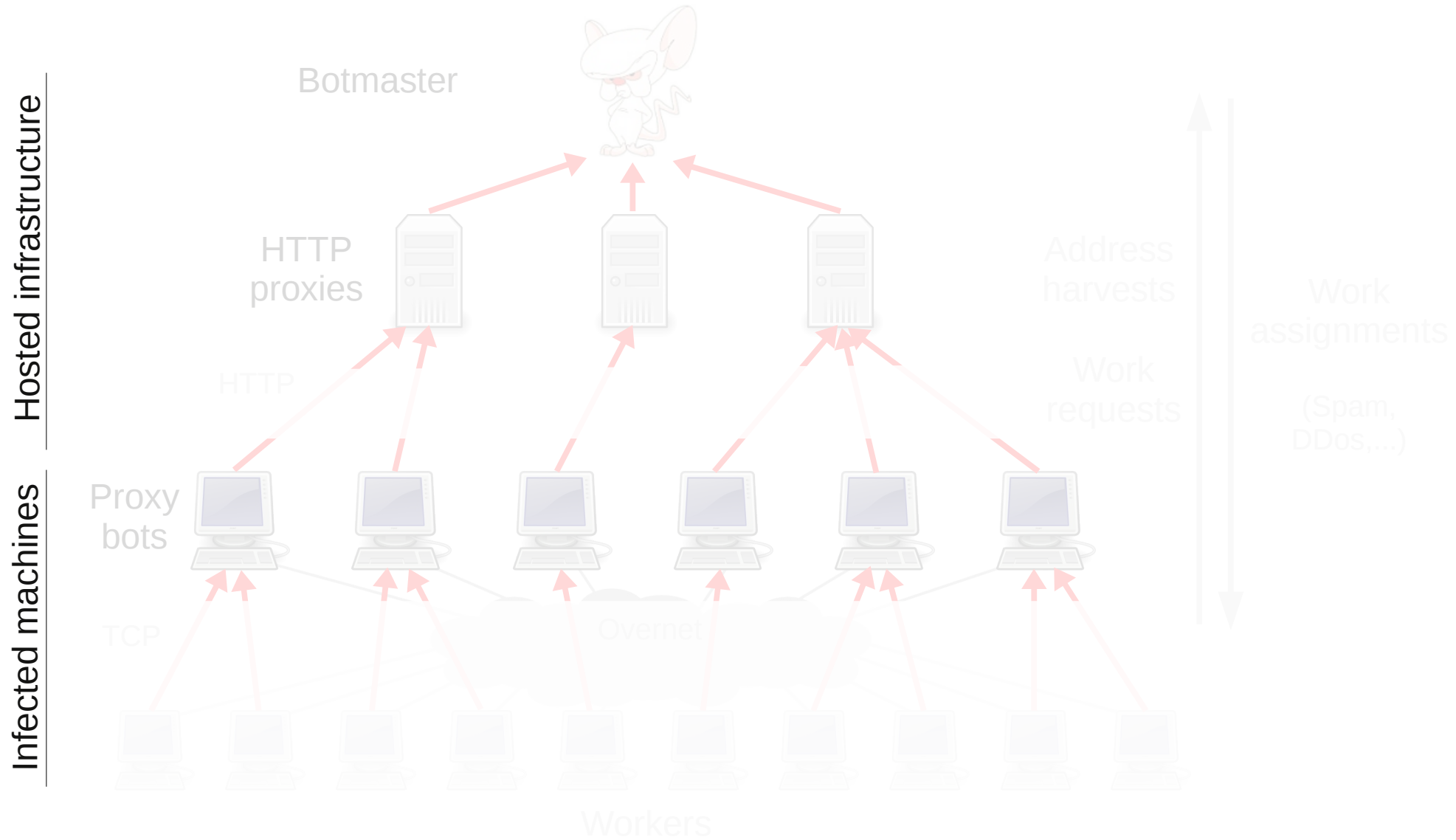
- » FBI takedown order on our servers was in progress
- » Oops!
- » Coordination with LE
  - » May be prudent
  - » May be difficult
  - » May be asymmetric

# Challenge: Human Subjects

---

- » Privacy concerns
  - » We see who is infected
  - » We see who is targeted
  - » We see what people do
  - » **Highly sensitive data!**
- » In US: Institutional Review Board (IRB) approval
  - » Institutions receiving federal grants must have one
  - » 6-8 weeks processing time for basic cases
  - » IRBs lack technical depth

# The Storm Botnet



# Challenge: Ethical Standards

---

- » **“Defense in depth”**: C&C filtering, signal jamming
- » **“White” botnets**: takeover / cleanup
- » Botnet **rental** (BBC study)
- » Product **purchases**
- » Keylogger **data pilfering**
- » Slippery slope — what to do?
  - » Community standards (ethics panels everywhere!)
  - » Do results justify the means?
  - » Some papers rejected (NDSS'10, LEET'10) ...
  - » ... others not (NDSS'10).

# Insights

---

# Challenges

---

Technical

?

?

Sociological

?

?

# Insights

---

# Challenges

---

## Technical

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

- » Arms race advancement
  - » Invasion resilience
- » Bot reliability
- » Malware 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
  - » Do no harm



# C&C inspection and rewriting

