The Zombie Roundup:

Understanding Detecting, and Disrupting Botnets

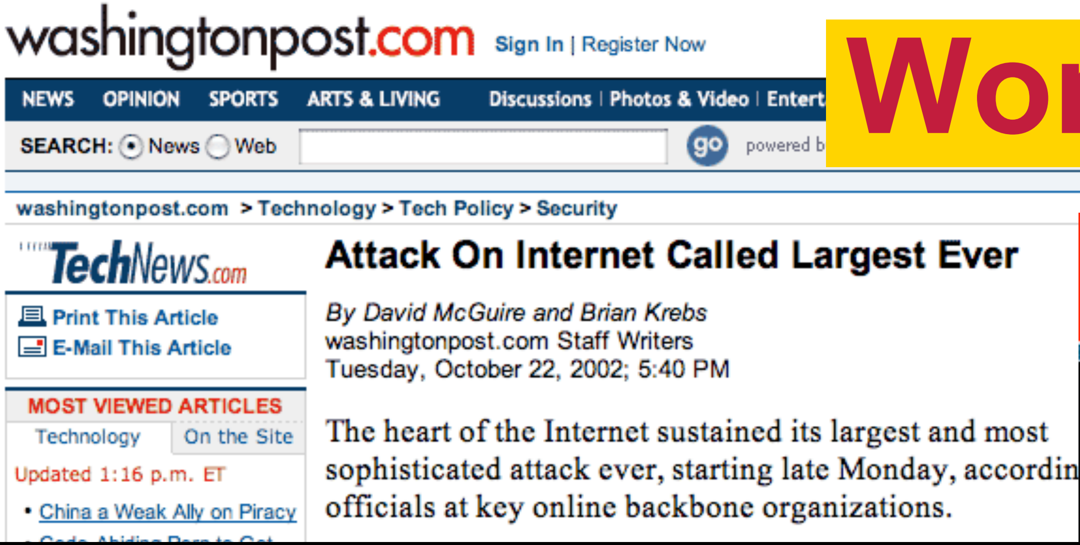
Evan Cooke[*], Farnam Jahanian[*†], Danny McPherson[†]

[*]Department of EECS - University of Michigan

[†]Arbor Networks

SRUTI Workshop 2005
July 7, 2005

The Old Days…



washingtonpost.com Sign In | Register Now

NEWS OPINION SPORTS ARTS & LIVING Discussions | Photos & Video | Entert

SEARCH: ● News ○ Web go powered b

washingtonpost.com > Technology > Tech Policy > Security

TechNews.com

Print This Article
E-Mail This Article

MOST VIEWED ARTICLES
Technology | On the Site
Updated 1:16 p.m. ET
- China a Weak Ally on Piracy
- Federal Agents St File-Sharing Web

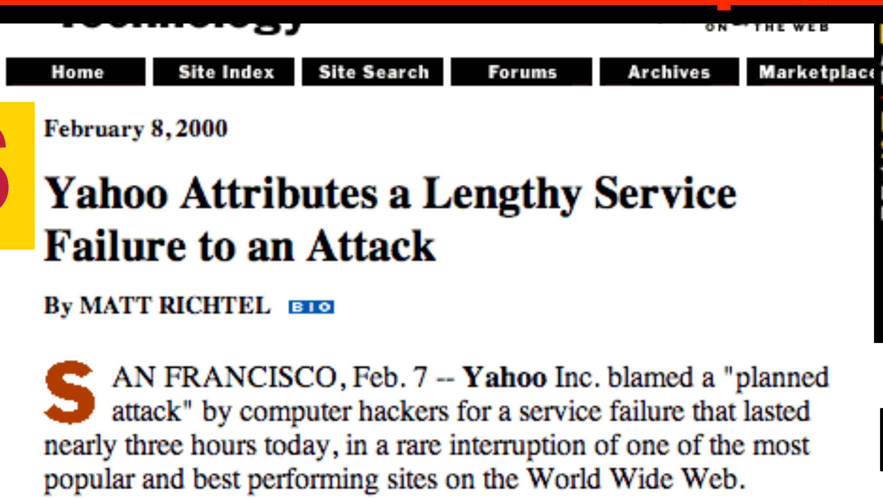
Attack On Internet Called Largest Ever

By David McGuire and Brian Krebs
washingtonpost.com Staff Writers
Tuesday, October 22, 2002; 5:40 PM

The heart of the Internet sustained its largest and most sophisticated attack ever, starting late Monday, accordin officials at key online backbone organizations.

Worms

These attacks disrupt infrastructure



Technology ON THE WEB

Home | Site Index | Site Search | Forums | Archives | Marketplace

February 8, 2000

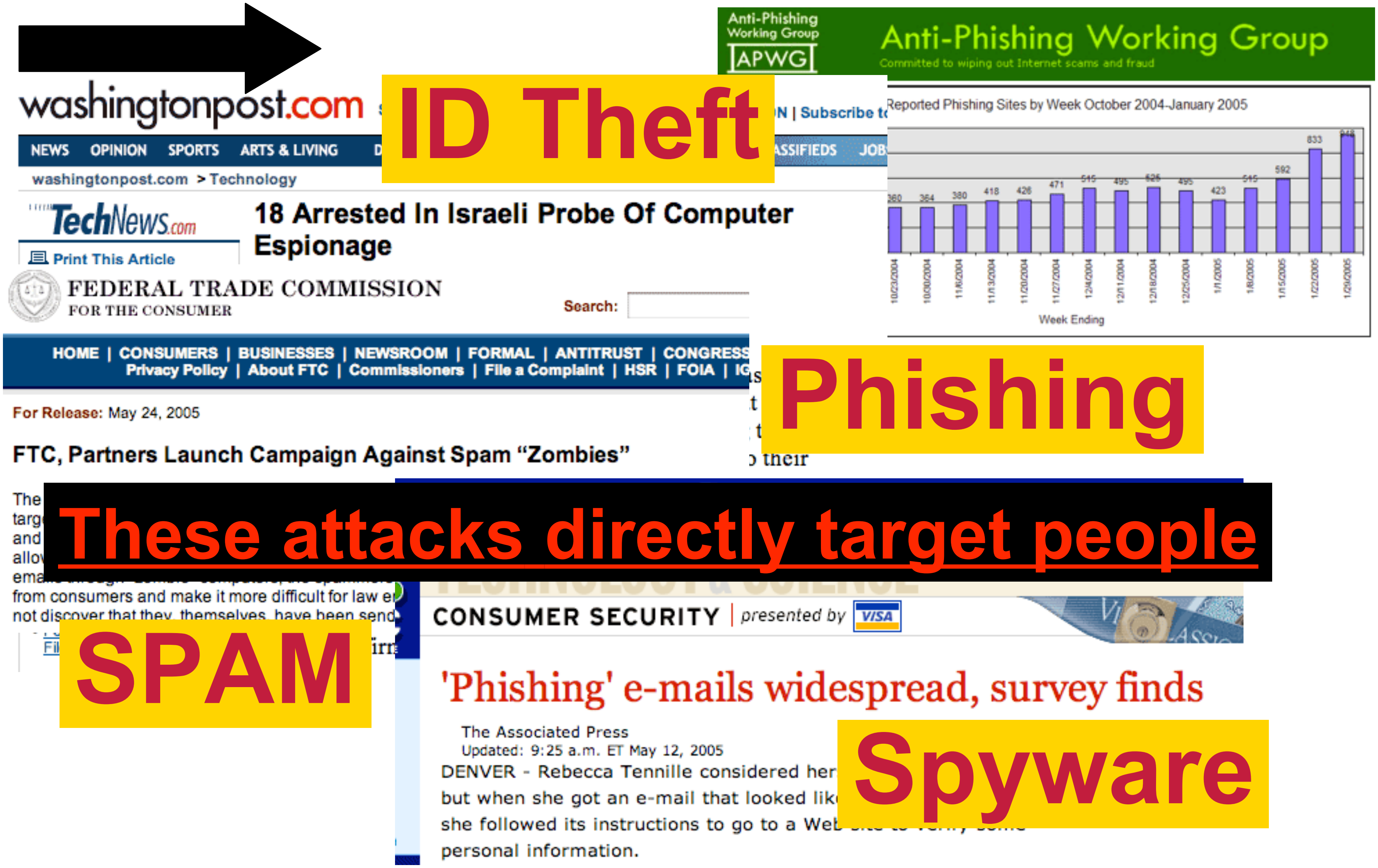
Yahoo Attributes a Lengthy Service Failure to an Attack

By MATT RICHTEL BIO

SAN FRANCISCO, Feb. 7 -- **Yahoo** Inc. blamed a "planned attack" by computer hackers for a service failure that lasted nearly three hours today, in a rare interruption of one of the most popular and best performing sites on the World Wide Web.

DoS

A Dramatic Escalation/Transformation



washingtonpost.com

NEWS OPINION SPORTS ARTS & LIVING D … N | Subscribe to … ASSIFIEDS JOBS

washingtonpost.com > Technology

TechNews.com

Print This Article

18 Arrested In Israeli Probe Of Computer Espionage

ID Theft

Anti-Phishing Working Group APWG

Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud

Reported Phishing Sites by Week October 2004-January 2005

FEDERAL TRADE COMMISSION
FOR THE CONSUMER

Search:

HOME | CONSUMERS | BUSINESSES | NEWSROOM | FORMAL | ANTITRUST | CONGRESS
Privacy Policy | About FTC | Commissioners | File a Complaint | HSR | FOIA | IG

Phishing

For Release: May 24, 2005

FTC, Partners Launch Campaign Against Spam "Zombies"

The … targ… and … allo… ema… from consumers and make it more difficult for law e… not discover that they, themselves, have been send…

These attacks directly target people

SPAM

CONSUMER SECURITY | presented by VISA

'Phishing' e-mails widespread, survey finds

The Associated Press
Updated: 9:25 a.m. ET May 12, 2005

DENVER - Rebecca Tennille considered her … but when she got an e-mail that looked lik… she followed its instructions to go to a Web … personal information.

Spyware

Rise of the Zombies

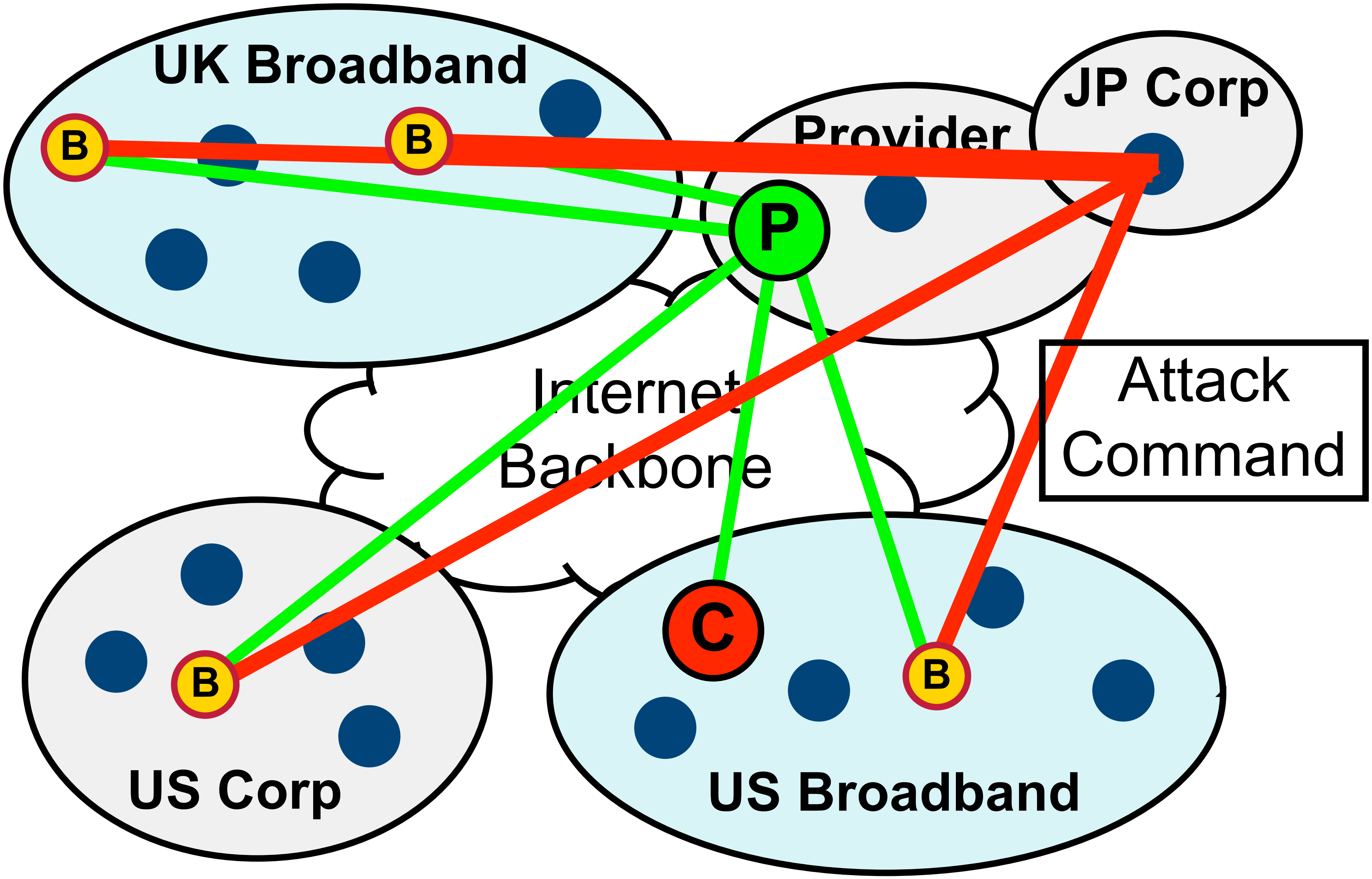
- New ***personal*** attacks often rely on an another resource (e.g. phishing site, SPAM relay)
- Anonymous use of resource highly desirable

  => attackers use another compromised system as a proxy!

  Attackers have learned a compromised system is more useful alive than dead!

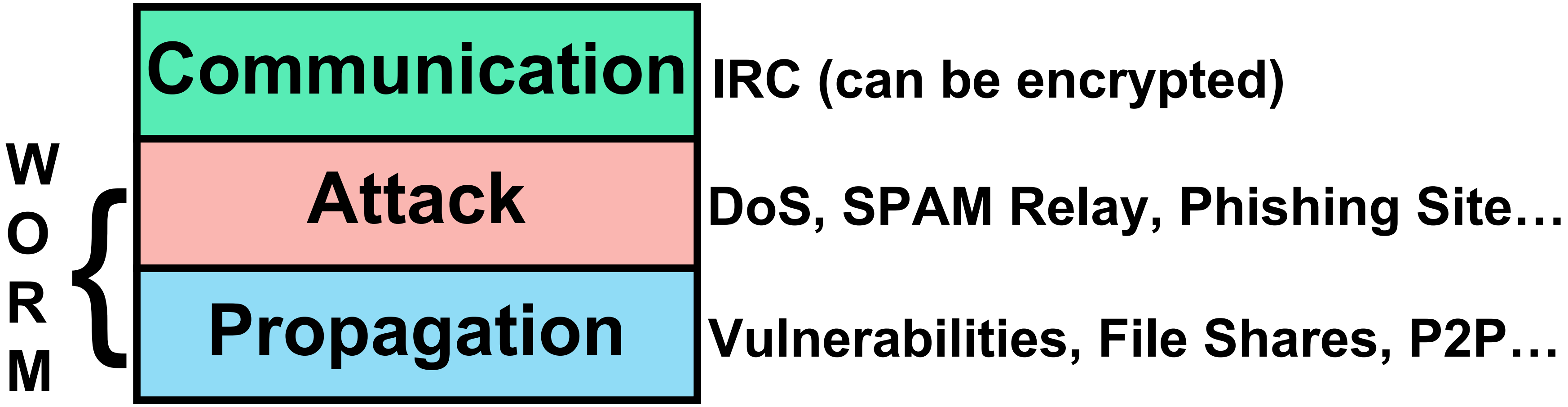
This talk is about detecting and disrupting access to the anonymous infrastructure used in these attacks

The Botnet


UK Broadband
B
B
Provider
JP Corp
P
Internet
Backbone
Attack
Command
C
B
B
US Corp
US Broadband

Bot History and Structure

- Not New: An original use, help Internet Relay Chat (IRC) Operators (*Eggdrop/1993*)
- Nefarious attack bots soon emerged (*DDoS*)
- Developed Sophisticated Hiding and Attack Capabilities (*SubSeven, Bot/Bionet Bot*)
- Modern Bots: (***AgoBot****[PhatBot],****GTBot****[rBot]*)



Communication — **IRC (can be encrypted)**

Attack — **DoS, SPAM Relay, Phishing Site…**

Propagation — **Vulnerabilities, File Shares, P2P…**

Big Bad Bots

- Total infected bot hosts **800,000 - 900,000** [CERT CA-2003-08]

  > **100,000 nodes/botnet**
- **1000's of new bots** each day [Symantec 2005]
- Many articles/press citing thousands of infected hosts [IEEE S&P, Register]
- Difficult to measure:

  => Population likely *much much* larger!

Bot/Botnet Measurements - Operators

- Very little hard data on botnets!
- We asked operators (five Tier-1 & Tier-2 ops):
  - They are actively fighting the problem
  - # of Botnets - *increasing*
  - Bots per Botnet - *decreasing*

    Used to be 80k-140k, now 1000s (evasion/economics?)
  - More firepower:

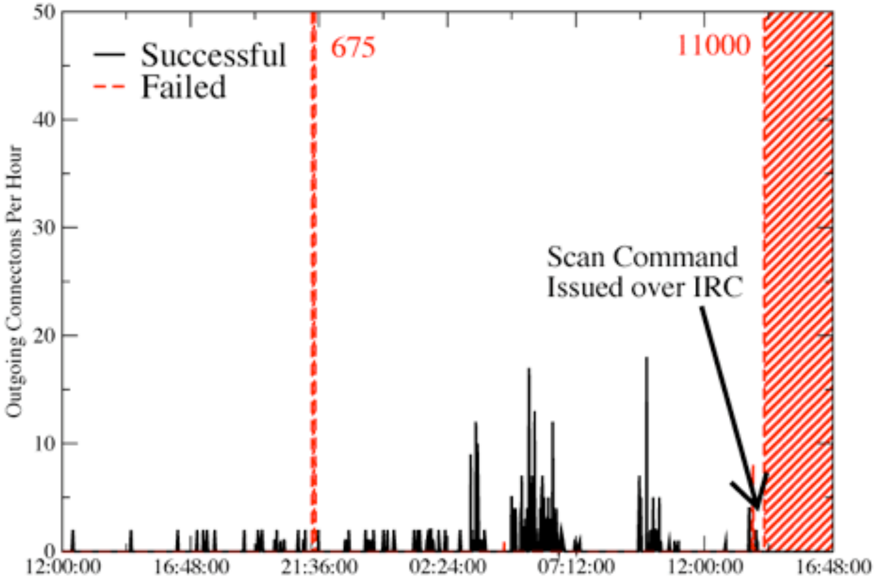
    Broadband (1Mbps Up) x 100s == OC3!!!
  - Custom botnets (all .edu, .gov/.mil) - economics?

Bot/Botnet Measurements - Honeypot

- Windows 2000/XP Honeypot
- Placed behind proxy:
  1. Rate limit traffic 12KB/s
  2. Disallow local network
  3. Log all traffic
- 12 experimental runs over a month:
  - 12-72 hour traces > 100MBs
  - Recruited into least **15 unique botnets**
  - Bots used DCOM/RPC, LSASS

=> Bots are extremely prevalent

Successful and failed outgoing connections from bot infected honeypot



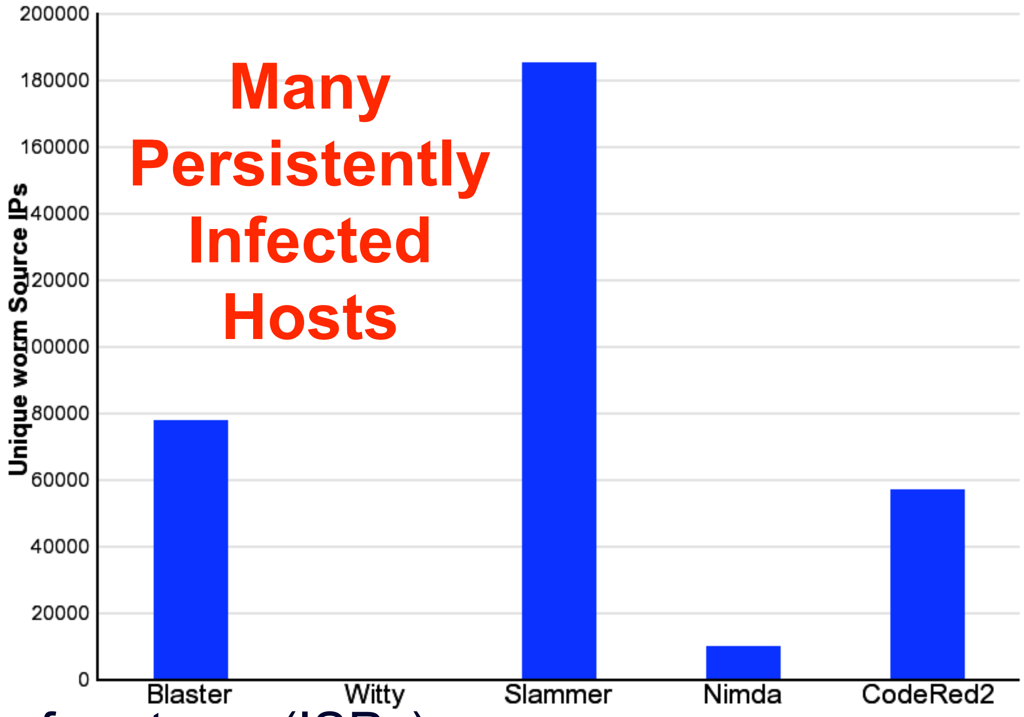
Just 2 worm infections during the experiment!

Detecting and Stopping Bots

1. Prevent systems from getting infected
2. Directly detect *bot* communications between *bots* and between *bots* and *bot controllers*
3. Detect the secondary features of a *bot* infection like propagation or attacks

Prevent Infection

- Well developed methods:
  - Anti-virus
  - Firewalls
  - Patching

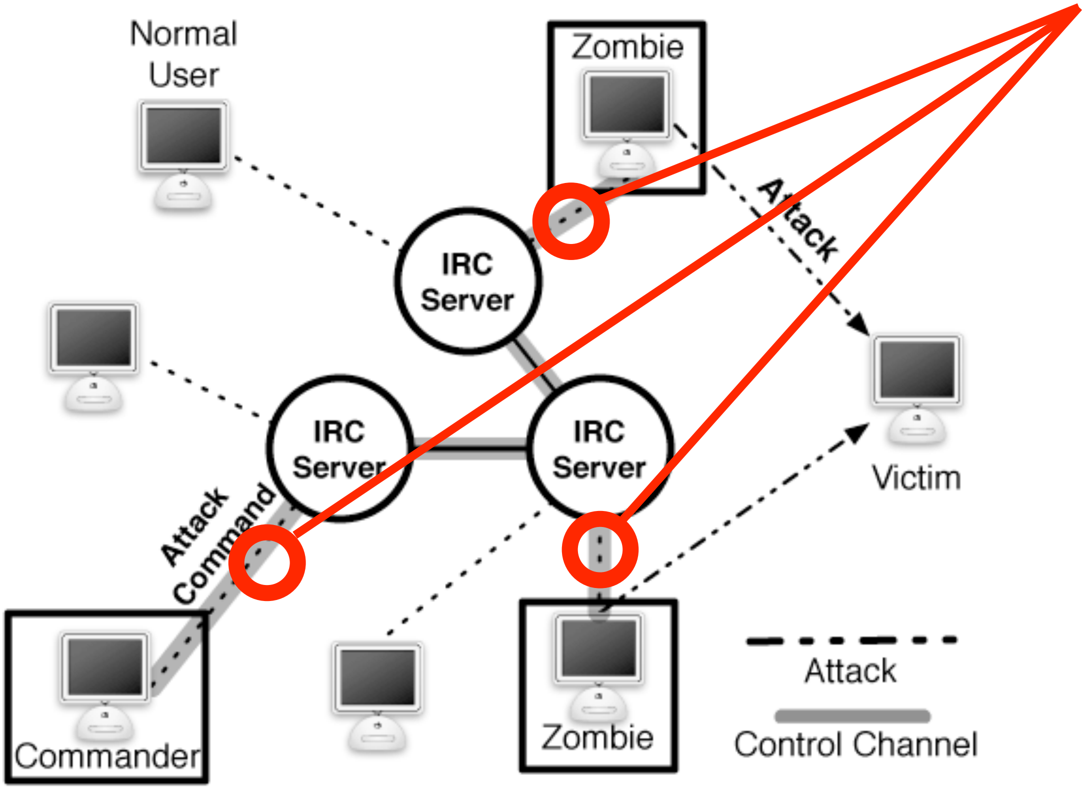


Many Persistently Infected Hosts

- But:
  - Might not directly control of systems (ISPs)
  - Can’t upgrade certain systems (Win98 DAQ)
  - Complex infection vectors: App-level (javascript, AIM)
  - Custom threat (Israeli trojan)
- Naïve to assume 100% protected

Detect Bot Communication

- Many bots use IRC for Command and Control



Detect IRC Bot Commands

- Offramp TCP port 6667
- Inspect Payloads (*advscan*…) [honeynet05]
- IRC Behavior [Racine04]

Detecting Bot Communication…

Less knowledge of peers per Bot

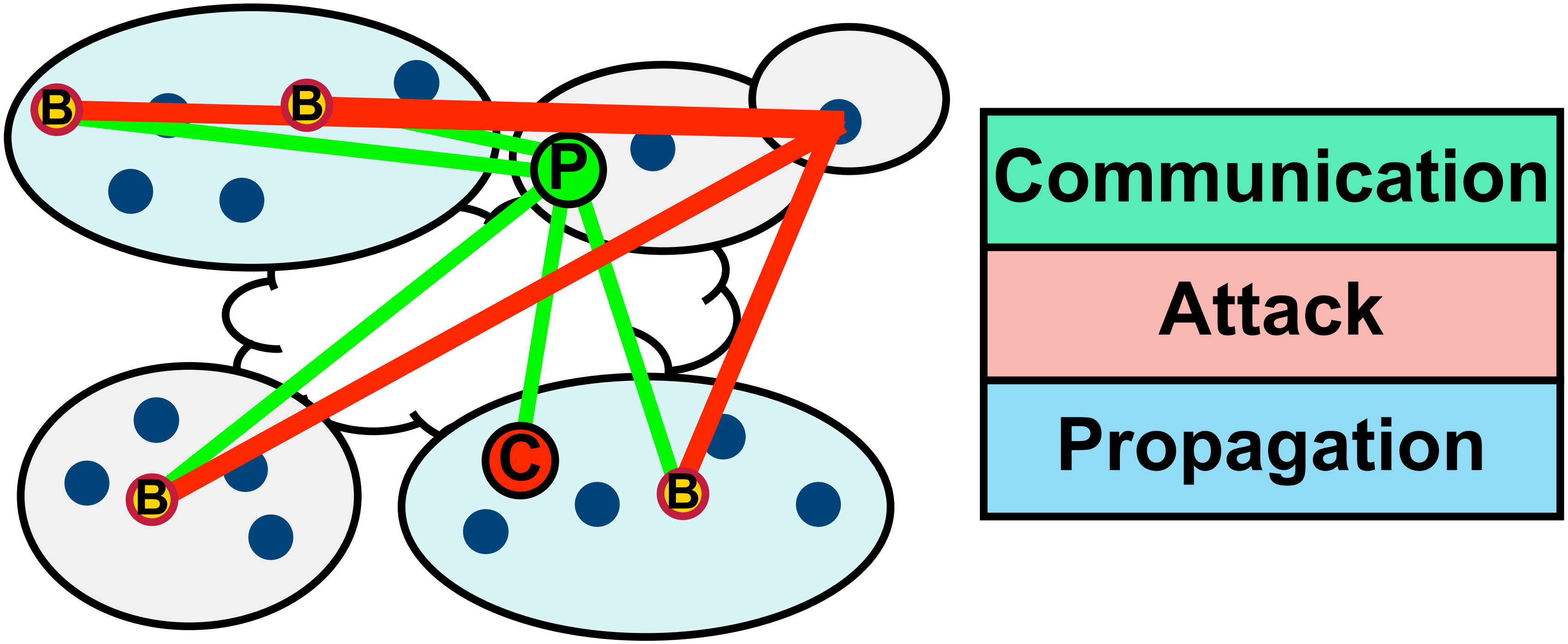
Topology	**Design Complexity**	**Detectablity**	**Message Latency**	**Survivability**
Centralized	*Low*	*Medium*	*Low*	*Low*
Peer-to-Peer	*Medium*	*Low*	*Medium*	*Medium*
Random	*Low*	*High*	*High*	*High*

Taxonomy of Bot Communication Topologies

- Reliance on detecting *Bot Communication* degenerates into **arms race** between bot authors and defenders
- Communication is very flexible
    - Easy to Encrypt/Obfuscate

Advanced Botnet Detection

- Relying on detecting bot communication is *not* viable in the long term
- Leverage *all* available bot characteristics
- Build detectors for each bot behavior



🟩 Communication

🟥 Attack

🟦 Propagation

Behavioral Bot Detection

- Preliminary evidence very promising:
- Strong correlation between bot ***communication*** and bot ***propagation***

Correlating data sources from a large live network (payloads & IMS dark IP sensors):

Bot Command Detected	Δ IMS Detection Time	Scan Type
ipscan r.r.r.r dcom2	*11 secs*	*Global Random*
ipscan s.s.s.s dcom2	*0 secs*	*Global Seq.*
ipscan 24.s.s.s dcom2	-	*Local 24/8 Seq.*
ipscan 69.27.s.s dcom2	-	*Local 69.27/16 Seq.*
ipscan s.s.s lsass	*0 secs*	*Local /8 Seq.*
ipscan s.s webdav3	*0 secs*	*Local /16 Seq.*

Conclusions

- Bots provide support infrastructure for a large range of devastating Internet attacks
- IRC-based botnet detection may be effective tool today
- Tomorrow must focus on holistic view of bot behavior
- Interesting questions:
  - How do we measure bots?
  - Who is responsible for cleanup? (Organizations/ISPs/Law Enforcement)
  - Global enforcement => bots in US attack China?

Questions

- Questions?

Many thanks to Michael Bailey, Jose Nazario, Chris Morrow, Tim Battles, Nicolas Fischbach, and Rob Thomas for helpful comments and feedback.

http://ims.eecs.umich.edu ims@umich.edu

Botnet Disruption

- Once you detect a bot how to shut it down?
- Two goals

  1. Take down the bot
  2. Take down the botnet

- Problem is similar to infiltrating a gang: monitoring the bot => provide info on botnet (i.e. a “narc”)
- Problem is complicated because many botnets span many countries