BotNets- Cyber Torrirism

Battling the threats of internet

Assoc. Prof. Dr. Sureswaran Ramadass

National Advanced IPv6 Center - Director

Why Talk About Botnets?

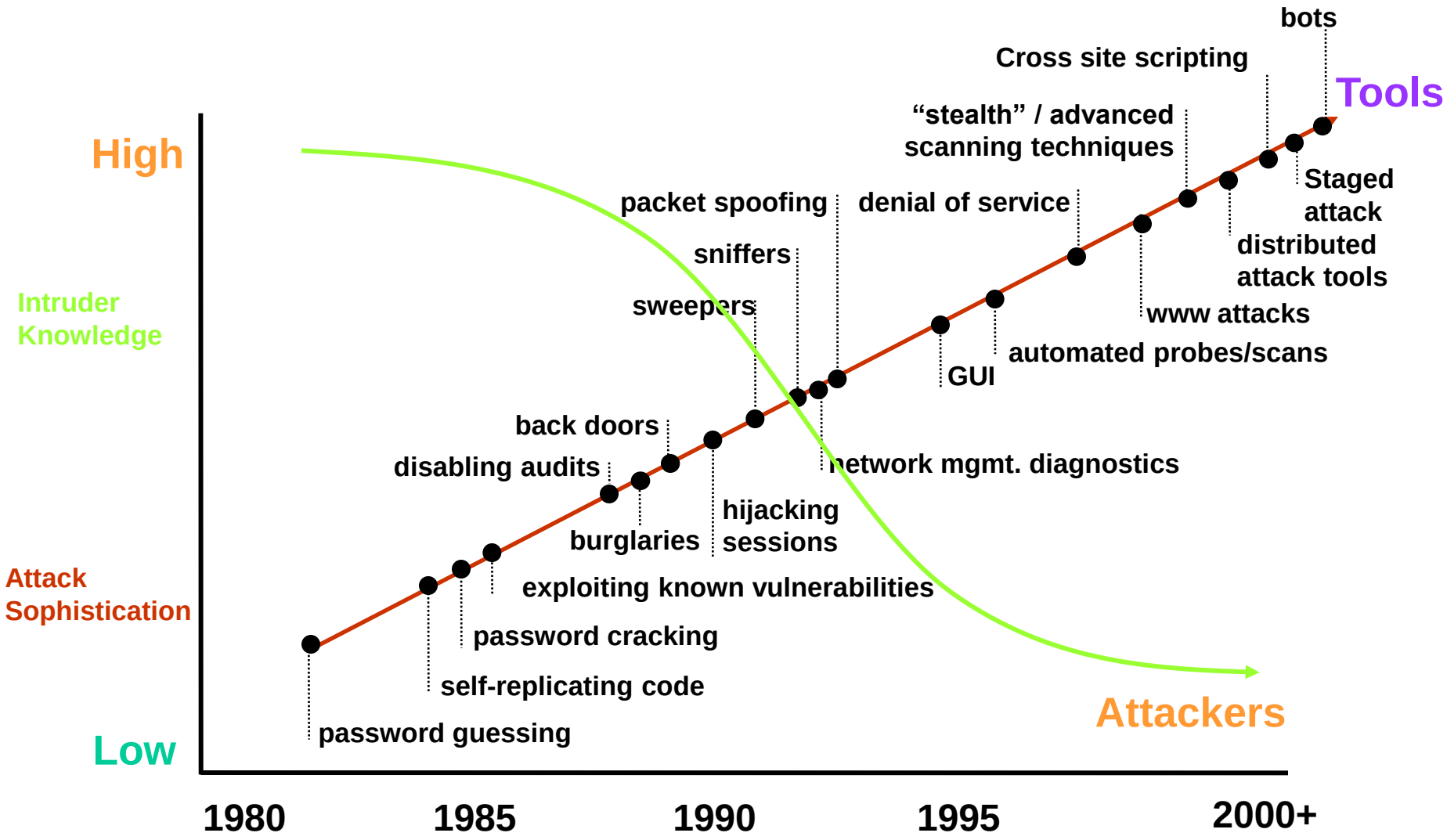
Because Bot Statistics Suggest Assimilation

- In 2006, *Microsoft's Malicious Software Removal Tool (MSRT)* found backdoor trojans on 62% of the 5.7 million computers it scanned. The majority of these were bots.
- *Commtouch* found, 87% of all email sent over the Internet during 2006 was spam. Botnets generated 85% of that spam.
- *Commtouch's GlobalView™* Reputation Service identifies between 300,000 and 500,000 newly active zombies per day, on average.
- *ISPs* rank zombies as the single largest threat facing network services and operational security*.

* Worldwide Infrastructure Security Report, Arbor Networks, September 2007.

Why Talk About Botnets?

Cyber Attack Sophistication Continues To Evolve



Source: CERT

Botnet Powered Attacks

Targeting the World

With full control of a massive army of machines, the only limit to

a botherder's attack potential is his imagination.

- **Distributed Denial of Service (DDoS) Attacks**
  - BlueSecurity
  - Estonia
  - Extortion of small businesses
- **Spamming**
  - Email spam
  - SPIM
  - Forum spam

What is Botnets?

Zombie Army

- A Botnet is a network of compromised computers under the control of a remote attacker. Botnets consist of:
  - **Bot herder**

    The attacker controlling the malicious network (also called a Botmaster).
  - **Bot**

    A compromised computers under the Bot herders control (also called zombies, or drones).
  - **Bot Client**

    The malicious trojan installed on a compromised machine that connects it to the Botnet.
  - **Command and Control Channel (C&C)**

    The communication channel the Bot herder uses to remotely control the bots.

What is Bot herder?

Bot master

- Botnet originator (*bot herder, bot master) starts the process*
  - *Bot herder sends viruses, worms, etc. to unprotected PCs*
    - » *Direct attacks on home PC without patches or firewall*
    - » *Indirect attacks via malicious HTML files that exploit vulnerabilities (especially in MS Internet Explorer)*
    - » *Malware attacks on peer-to-peer networks*
  - *Infected PC receives, executes Trojan application ⇒ bot*
  - *Bot logs onto C&C IRC server, waits for commands*
  - *Bot herder sends commands to bots via IRC server*
    - » *Send spam*
    - » *Steal serial numbers, financial information, intellectual property, etc.*
    - » *Scan servers and infect other unprotected PCs, thereby adding more "zombie" computers to botnet*

What is Bot?
The Zombie/drone

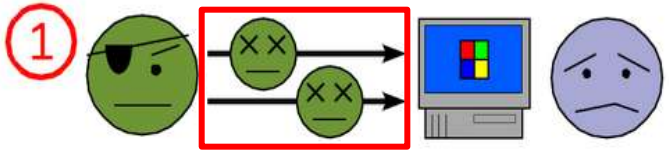
- Bot = autonomous programs capable of acting on instructions
  - Typically a large (up to several hundred thousand) group of remotely controlled “zombie” systems
    - » Machine owners are not aware they have been compromised
    - » Controlled and upgraded via IRC or P2P
- Used as the platform for various attacks
  - Distributed denial of service
  - Spam and click fraud
  - Launching pad for new exploits/worms

What is Bot Client?

Compromising a machine-worms

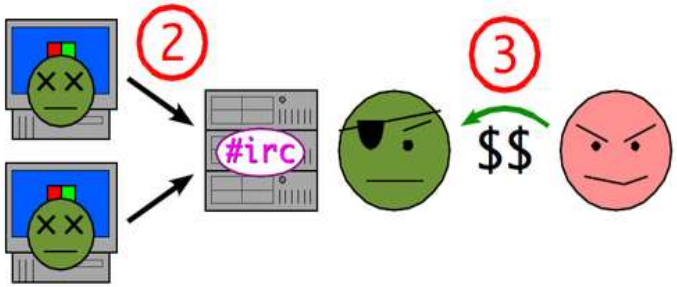
1. Botnet operator sends out viruses or worms (bot client)

→infect ordinary users [trojan application is the *bot]*



2. The *bot* on the infected PC logs into an IRC serve

→Server is known as the command-and-control server

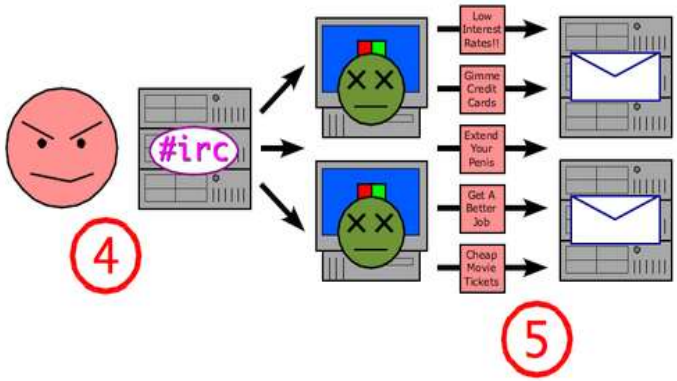


3. Attackers gets access to botnet from operator

- Spammers

4. Attackers sends instructions to the infected PCs

- To send out spam



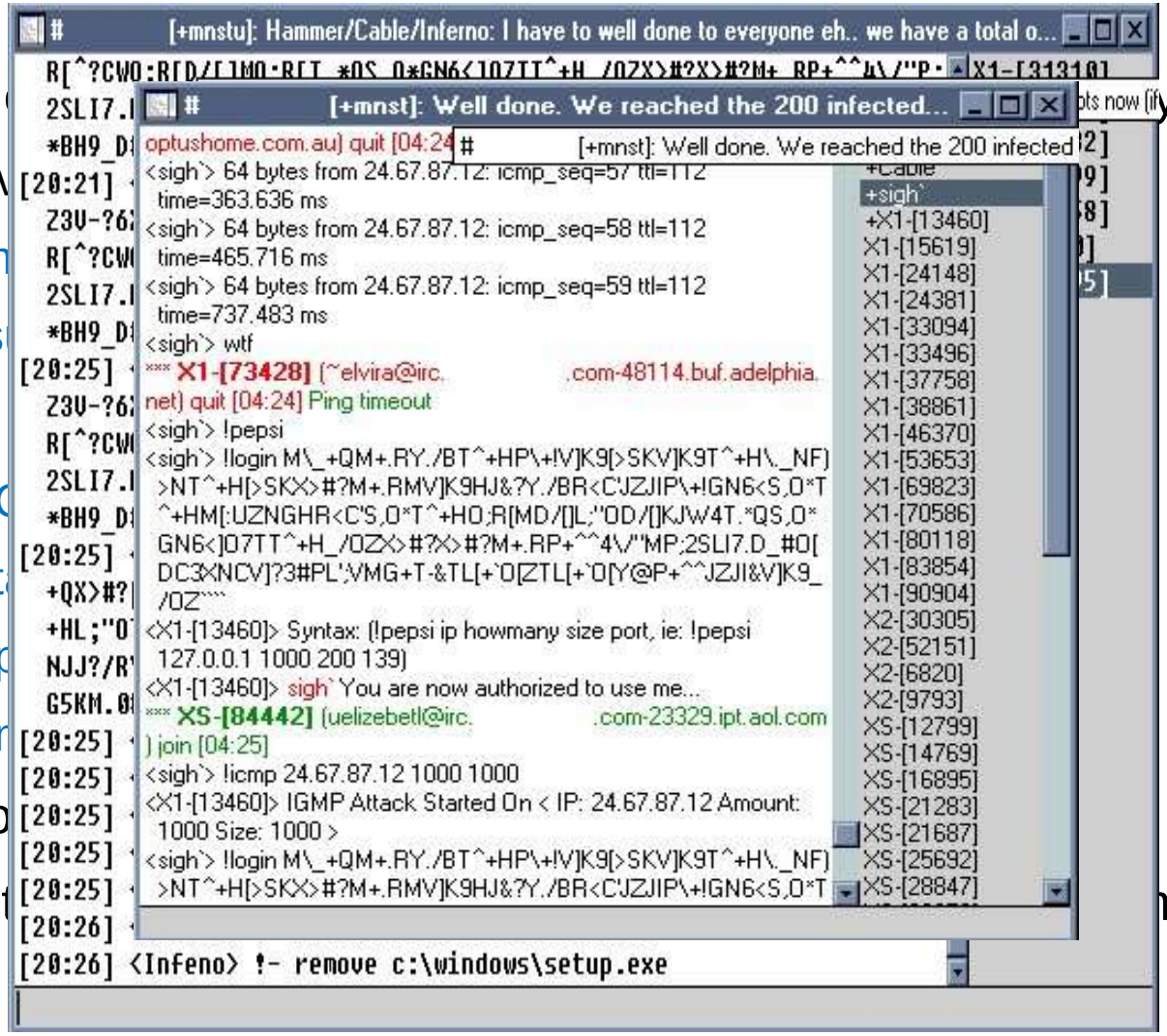
5. Infected PCs will

- Send out spam messages

What is Bot C&C?

Command and Control Server (C2)

- Without bot
  - IRC serv
    - » Sin
    - » Us
- **However,**
    - » IRC
    - » Att
      exp
      con
- Bots log into
- Bots are writ
  (sometimes



What is Bot C&C?

Command and Control Server (C2)

- Today, bot herders primarily rely on these three protocols for their C&C:
  - » Internet Relay Chat (IRC) Protocol
  - » Hyper-Text Transfer Protocol (HTTP)
  - » Peer-to-Peer (P2P) networking protocols.

Botnet Life Cycle?

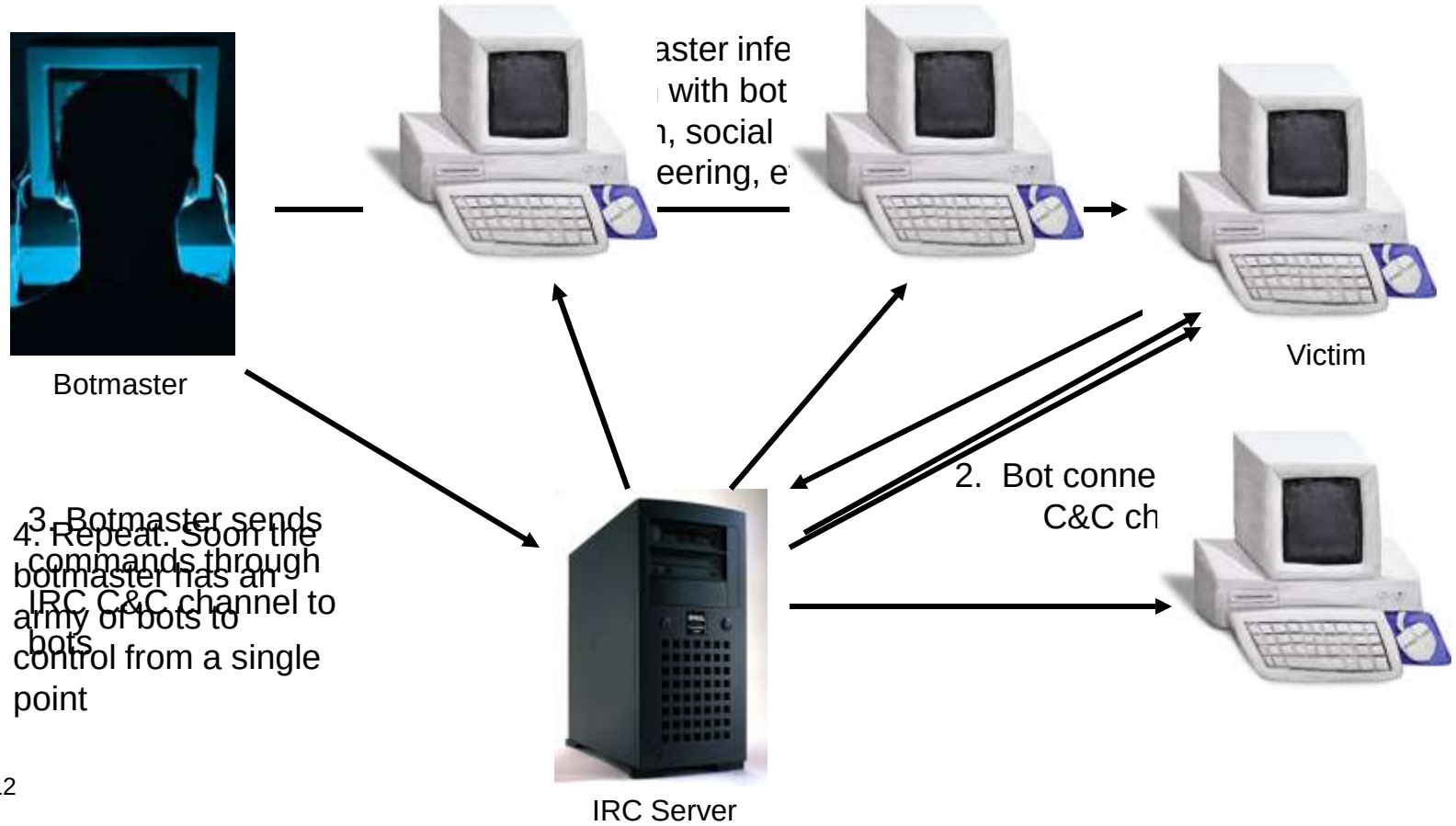
Botnet and bot Life Cycle

- **Botnet Life Cycle**
  - Bot herder configures initial parameters: infection vectors, payload, stealth, C&C details
  - Bot herder registers dynamic DNS server
  - Bot herder launches, seeds new bots
  - Bots spread, grow
  - Other botnets steal bots
  - Botnet reaches stasis, stops growing
  - Bot herder abandons botnet, severs traces thereto
  - Bot herder unregisters dynamic DNS server

- **Bot Life Cycle**
  - Bot establishes C&C on compromised computer
  - Bot scans for vulnerable targets to “spread” itself
  - User, others take bot down
  - Bot recovers from takedown
  - Bot upgrades itself with new code
  - Bot sits idle, awaiting instructions

Botnet in Action?

Putting all together



Botnets used for?

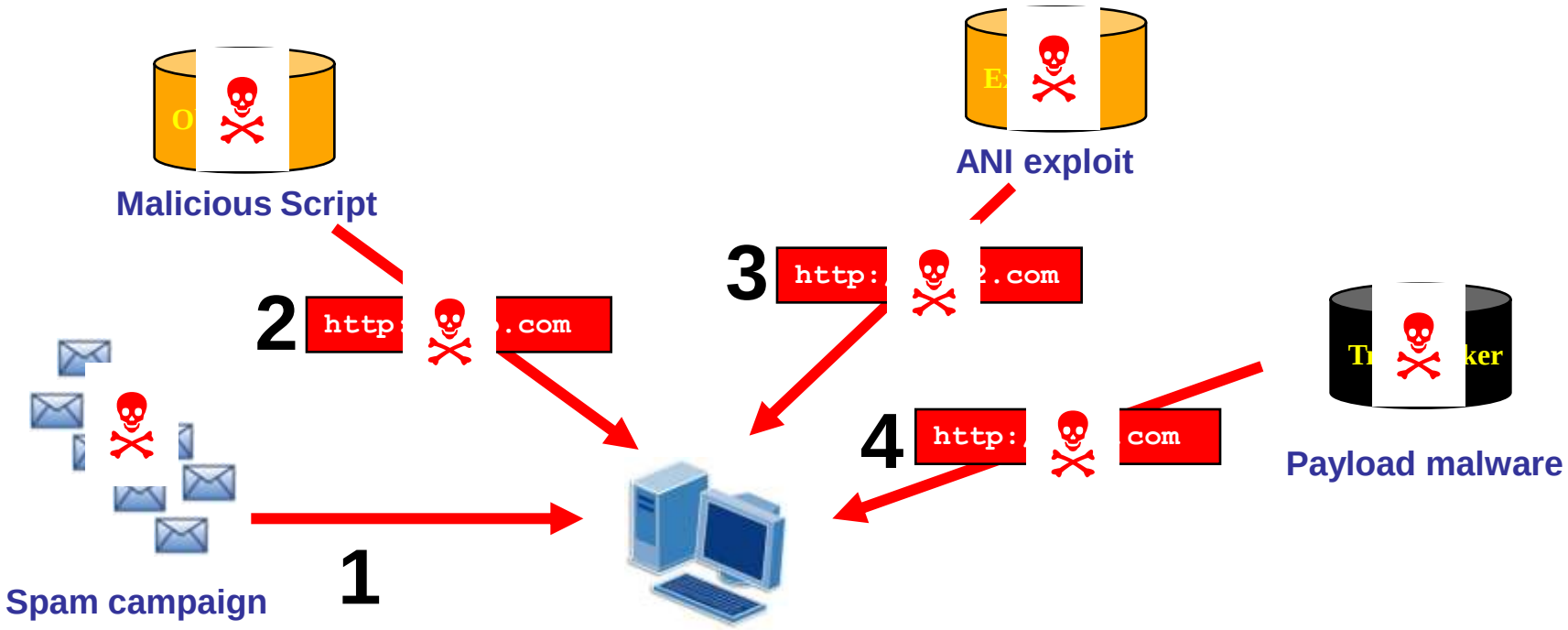
Hiring the Botnets

- Phishing
- Spam
- Distributed Denial of Service
- Click Fraud
- Adware/Spyware Installation
- Identity Theft
- Making Additional Income!!!
- Keystroke logging
- Stealing registration keys or files

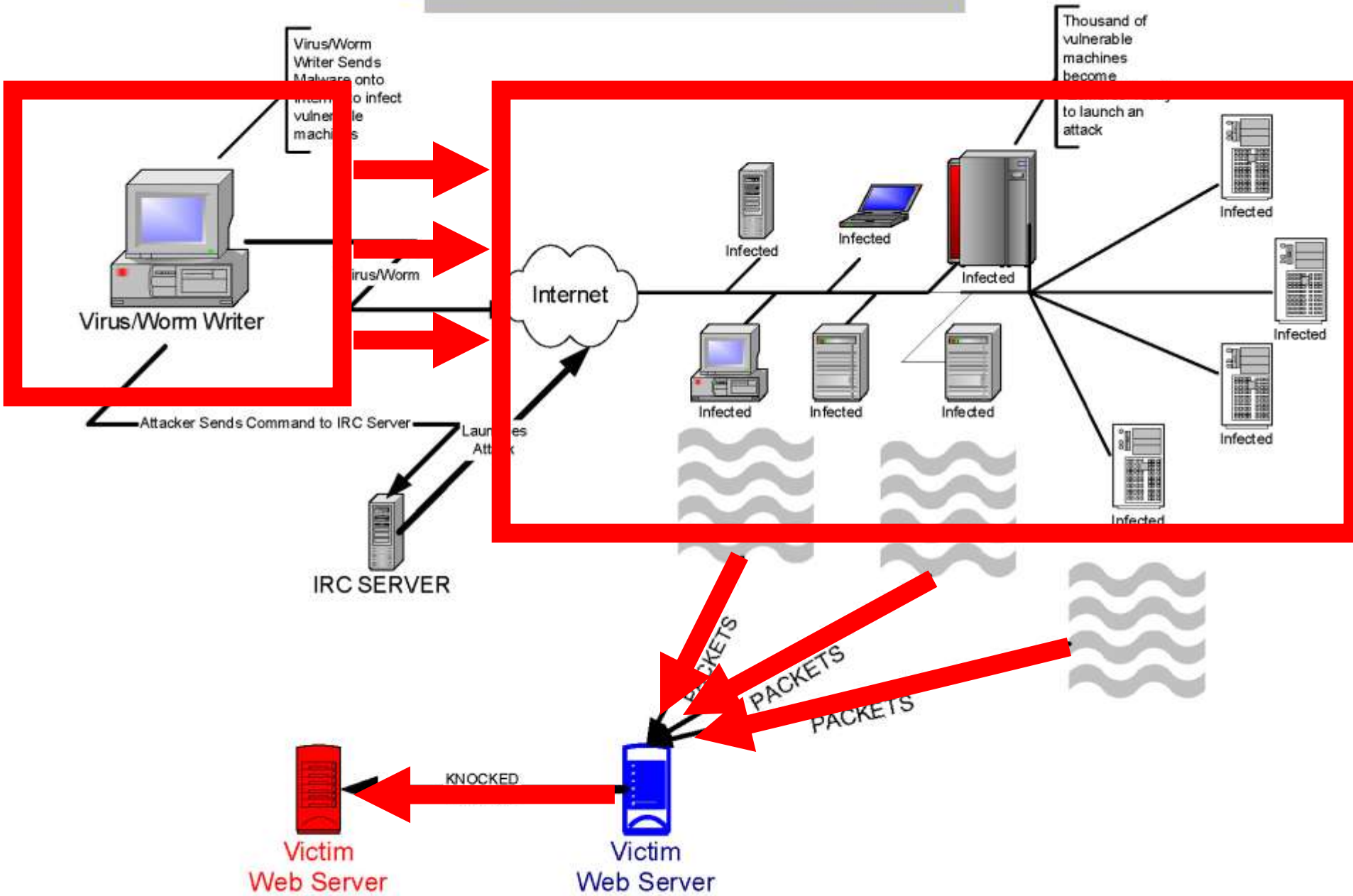
Whatever you pay for them to do! Or whatever makes money or is fun for the operator.

Botnet in Action

Attack Summary

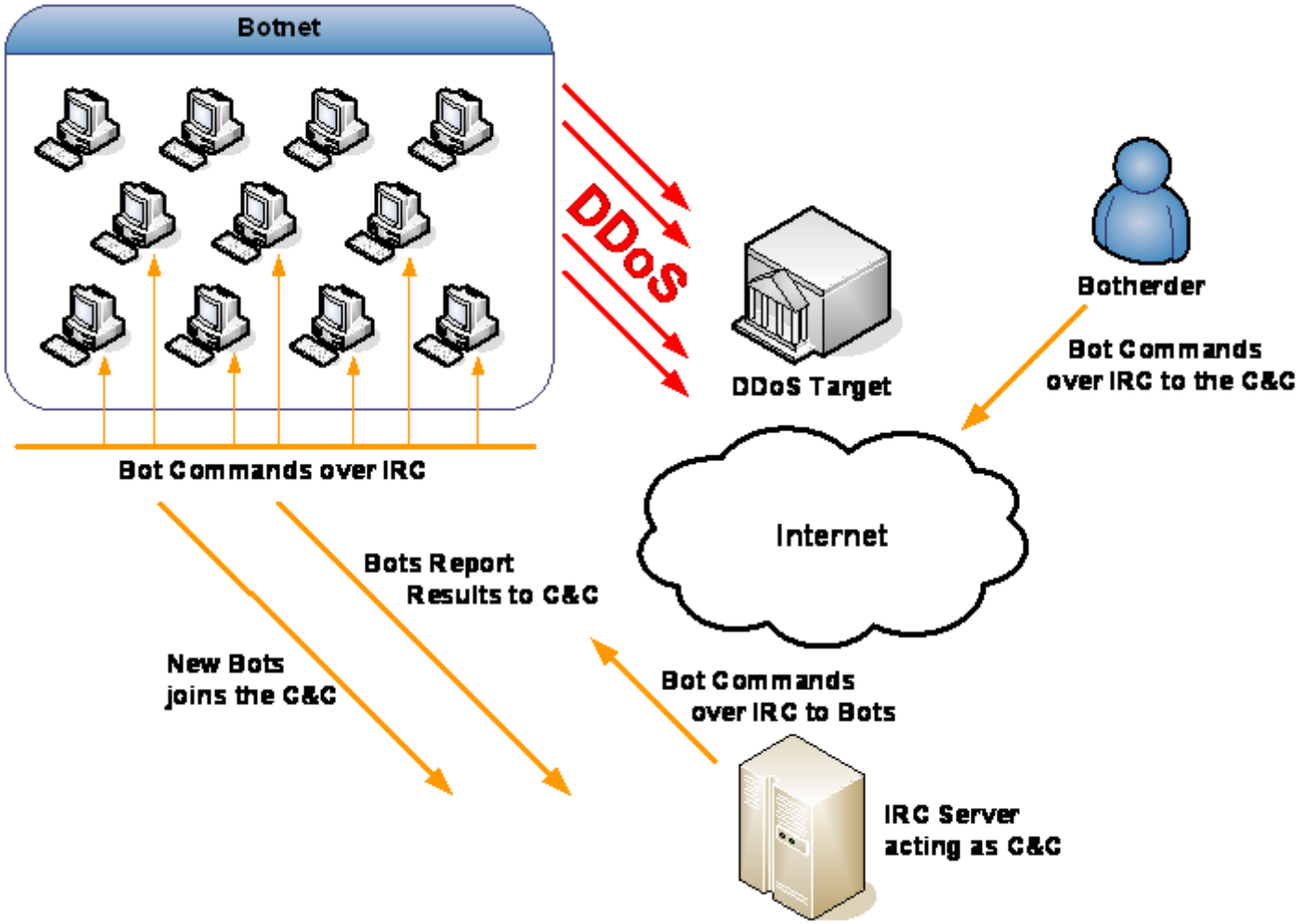


Distributed Denial of Service Attack



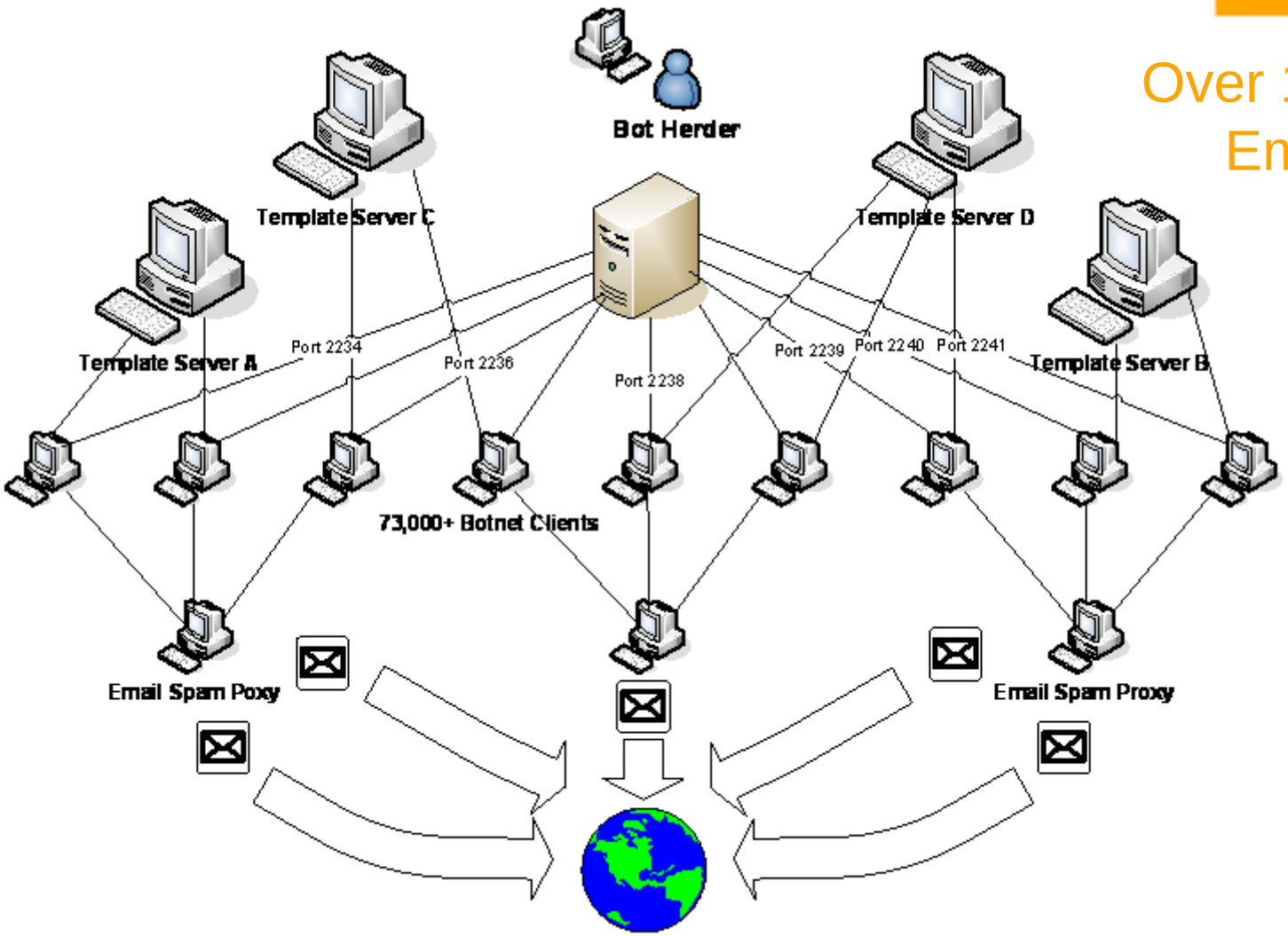
The Botnet: contined

The Lifecycle of a Botnet



The Current Threats

The SpamThru Trojan



Over 1 Billion Emails

Break

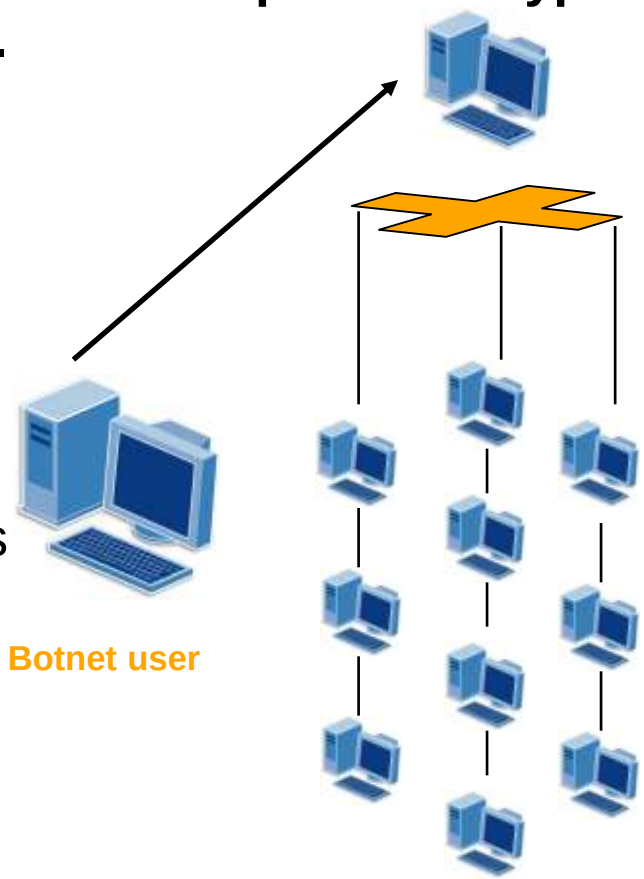
Visualizing a Botnet

Relax, and Enjoy the Video

Types Botnets
IRC botnets

Until recently, IRC-based botnets were by far the most prevalent type exploited in the wild.

- Benefits of IRC to botherder:
  - ✓Well established and understood protocol
  - ✓Freely available IRC server software
  - ✓Interactive, two-way communication
  - ✓Offers redundancy with linked IRC servers
  - ✓Most blackhats grow up using IRC.

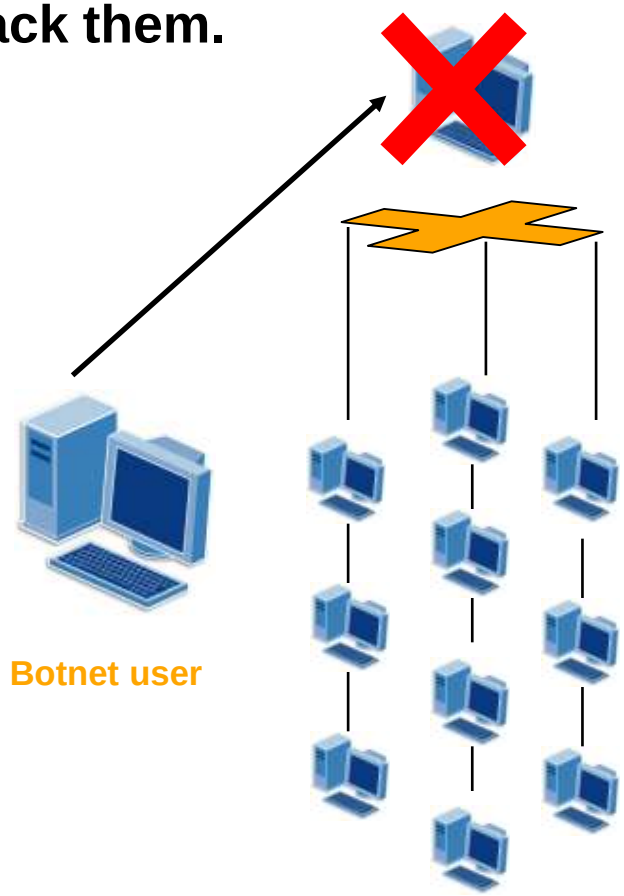


Types Botnets
IRC botnets

Botherders are migrating away from IRC botnets because researchers know how to track them.

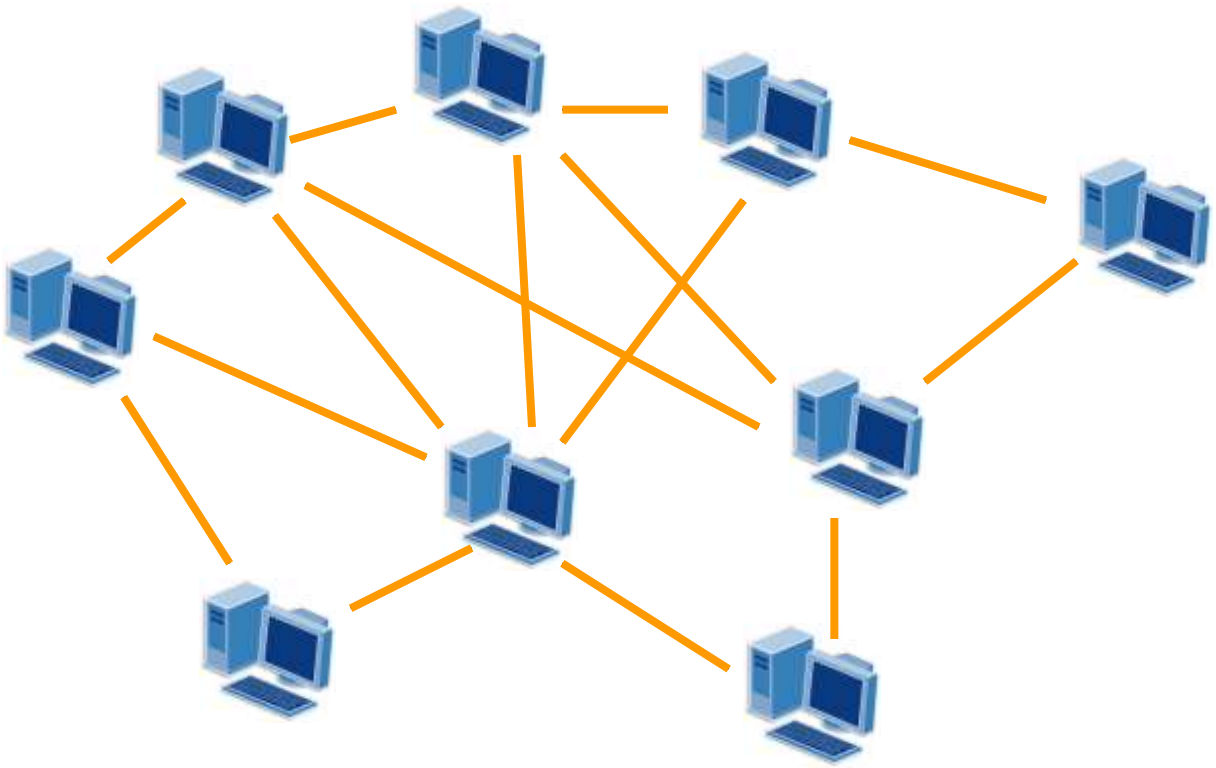
- Drawbacks:
  - ✓Centralized server
  - ✓IRC is not that secure by default
  - ✓Security researchers understand IRC too.

- Common IRC Bots:
  - ✓SDBot
  - ✓Rbot (Rxbot)
  - ✓Gaobot



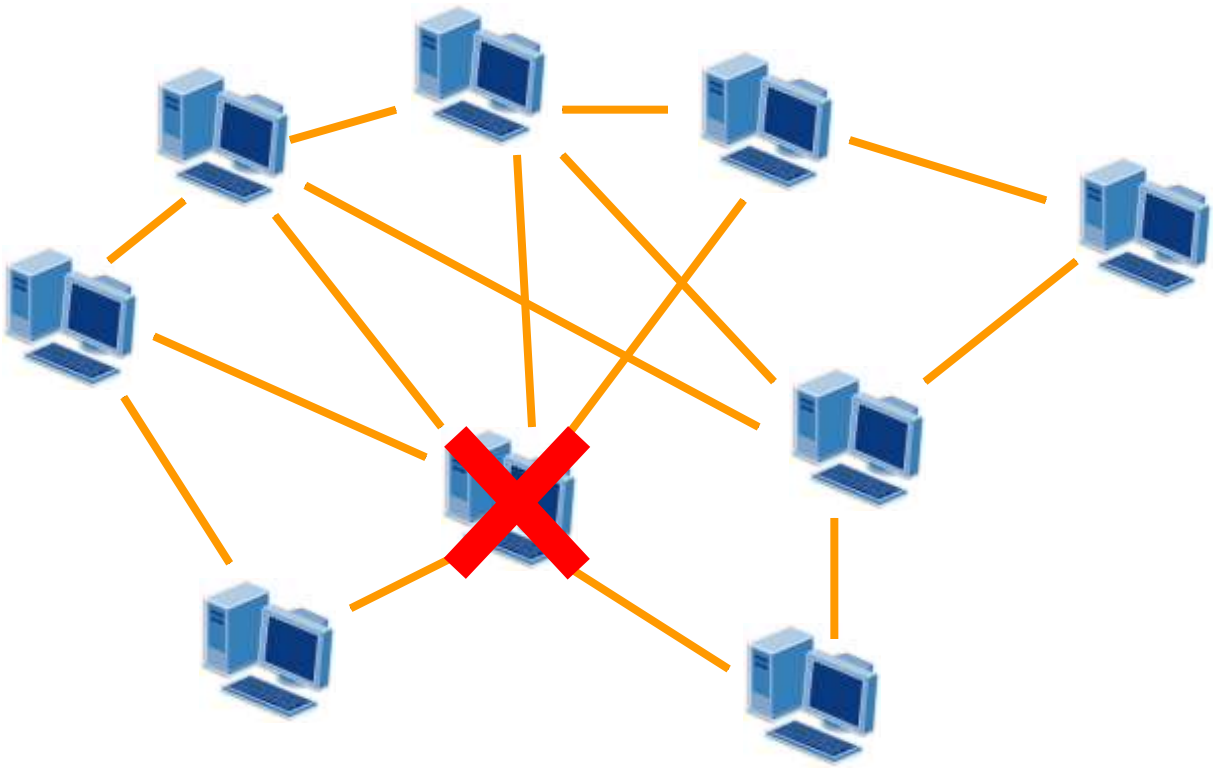
Types Botnets
P2P botnets

- Distributed control



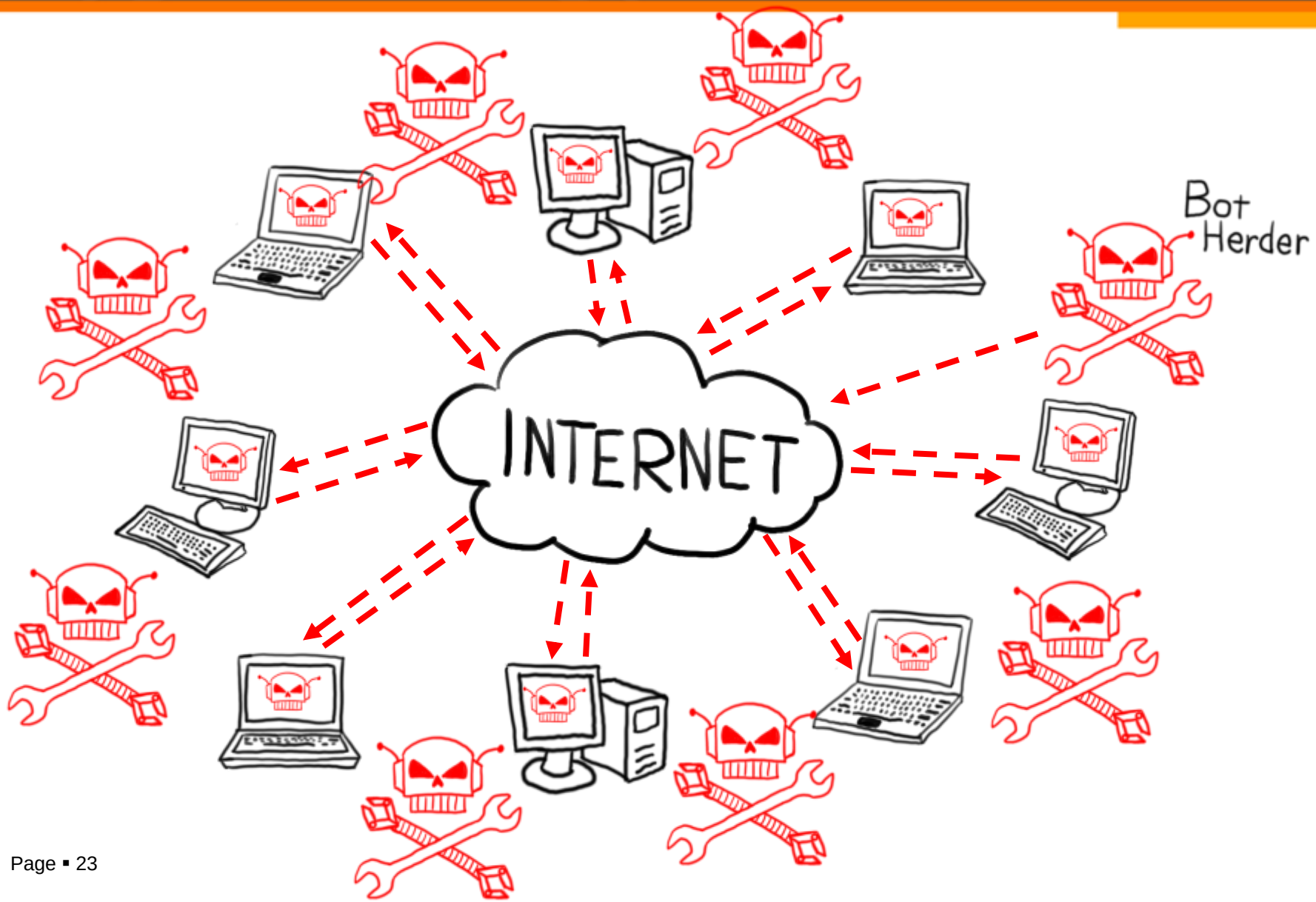
Types Botnets
P2P botnets

- Hard to disable



What is a Botnet?

P2P Botnet Diagram



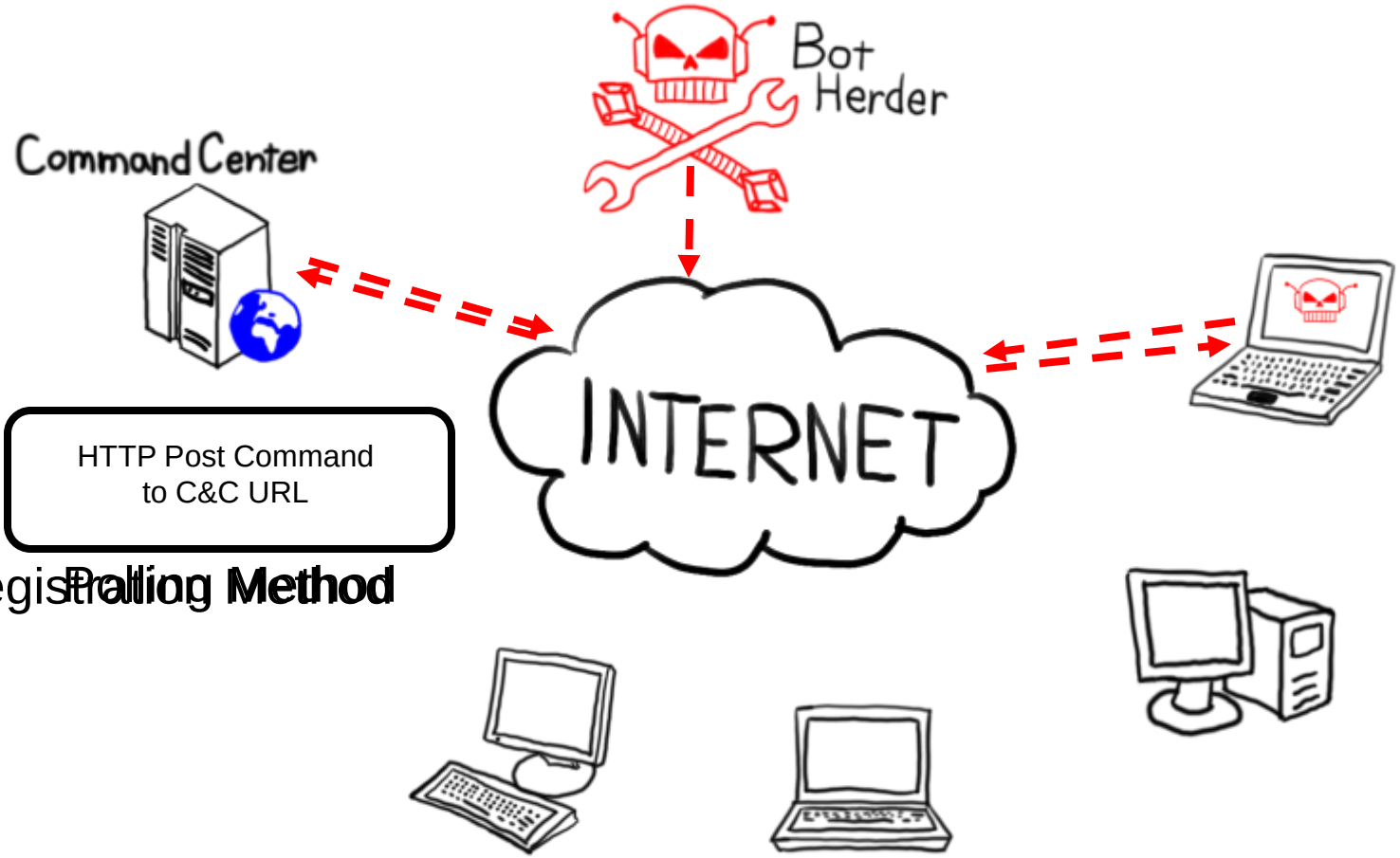
Types Botnets
P2P botnets

P2P communication channels offer anonymity to botherders a and resiliency to botnets.

- Benefits of P2P to botherder:
  - » Decentralized; No single point of failure
  - » Botherder can send commands from any peer
  - » Security by Obscurity; There is no P2P RFC
- Drawbacks:
  - » Other peers can potentially take over the botnet
- P2P Bots:
  - » Phatbot: AOL's WASTE protocol
  - » Storm: Overnet/eDonkey P2P protocol

Types Botnets

HTTP botnet



HTTP Post Command
to C&C URL

Registration Method

Polling Method

What is a Botnet?
HTTP Botnets

Botherders are shifting to HTTP-based botnets that serve a single purpose.

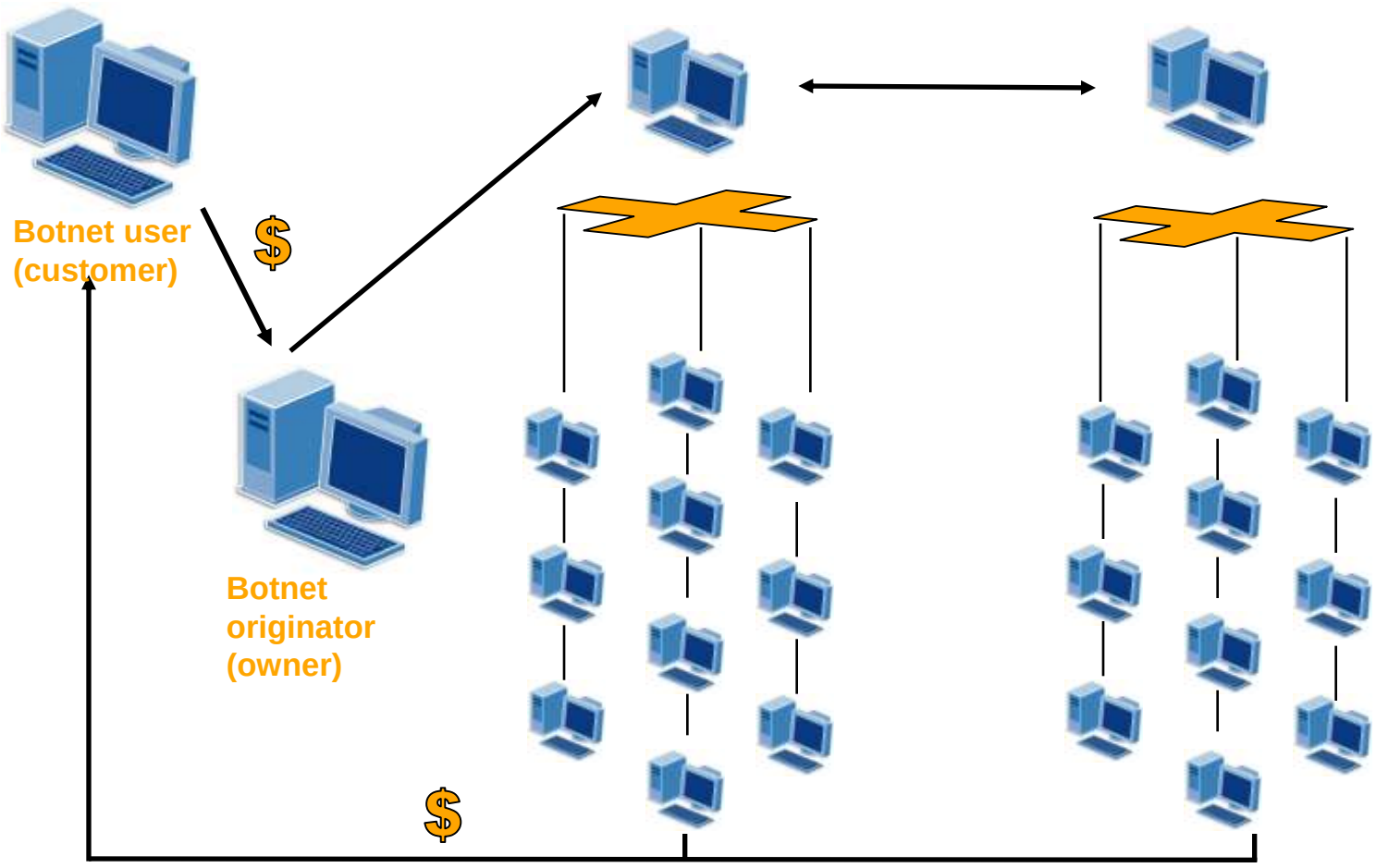
- Benefits of HTTP to botherder:
  - » Also very robust with freely available server software
  - » HTTP acts as a “covert channel” for a botherder’s traffic
  - » Web application technologies help botherders get organized.
- Drawbacks:
  - » Still a Centralized server
  - » Easy for researchers to analyze.
- Recent HTTP Bots:
  - » Zunker (Zupacha): Spam bot
  - » BlackEnergy: DDoS bot

What Bots can do?
The Zombie/drone

- Each bot can scan IP space for new victims
  - Automatically
    - » Each bot contains hard-coded list of IRC servers' DNS names
    - » As infection is spreading, IRC servers and channels that the new bots are looking for are often no longer reachable
  - On-command: target specific /8 or /16 prefixes
    - » Botmasters share information about prefixes to avoid
      - ✓ Evidence of botnet-on-botnet warfare
        - DoS server by multiple IRC connections ("cloning")
      - ✓ Active botnet management
        - Detect non-responding bots, identify "superbots"

Botnets used for?

Network for hire



Botnets, the hardest
Challenges

- Determining the source of a botnet-based attack is challenging:
  - » Every zombie host is an attacker
  - » Botnets can exist in a benign state for an arbitrary amount of time before they are used for a specific attack
  - Traditional approach:
    - » identify the C&C server and disable it
  - New trend:
    - » P2P networks,
    - » C&C server anonymized among the other peers (zombies)
- Measuring the size of botnets

Botnets, Research
Methods

- Capture
  - Active (go out and get malware)
    - » Actual (use vulnerable browser/application)
    - » Simulated (use tool that mimics vulnerable app)
    - » FTP (go to malware repository)
  - Passive (let it come to you)
    - » Honeypot/net
    - » Collection from infected end-users

Botnets, Research

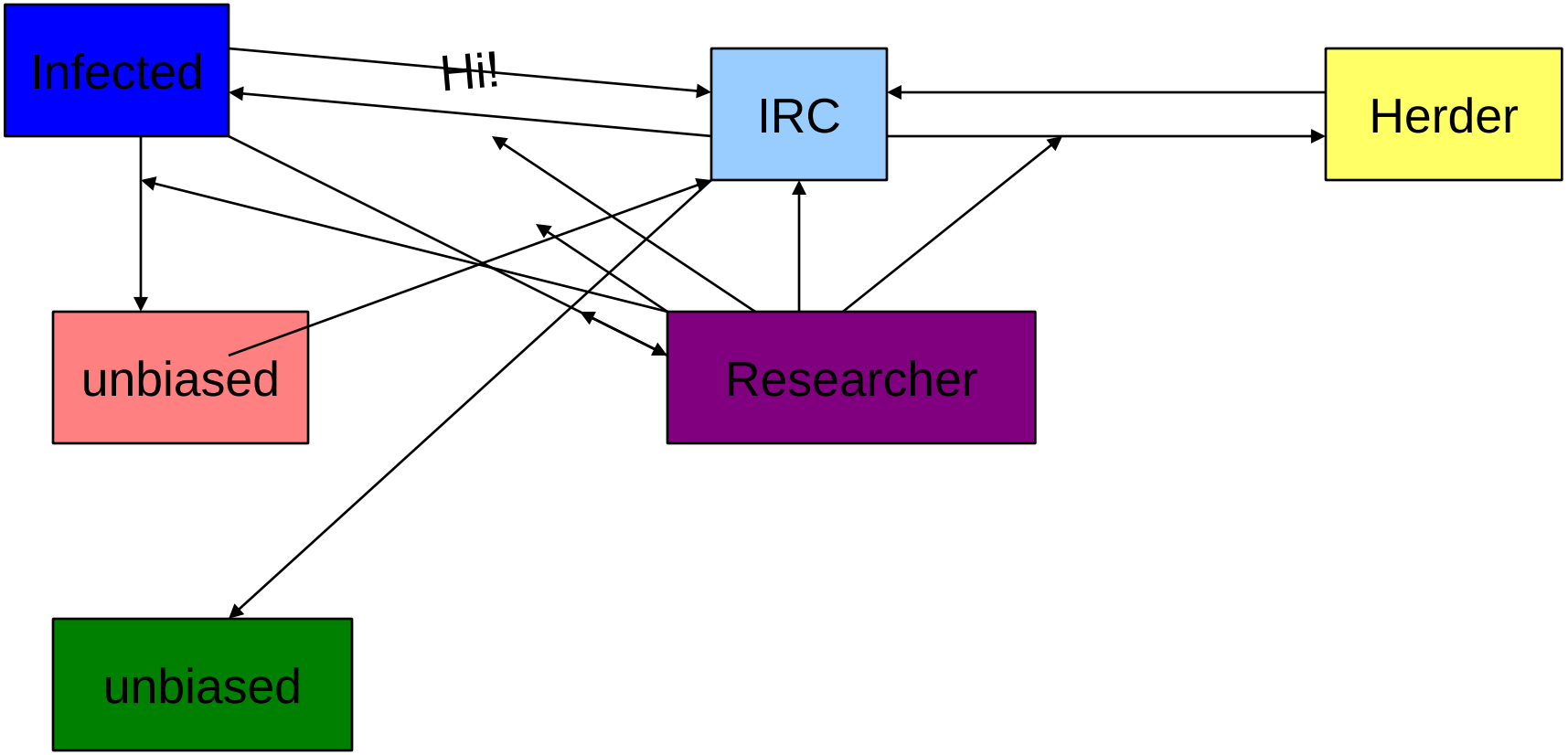
Monitoring of herder - botmatser

- Logging onto herder IRC server to get info
  - Passive monitoring
    - » Either listening between infected machine and herder or spoofing infected PC
  - Active monitoring
    - » Poking around in the IRC server
- Sniffing traffic between bot & control channel

- **What if herder is using 'mixed' server?**
    - » innocent and illegitimate traffic together

Botnets, Research

Monitoring of herder – bot matser



Avoid Assimilation: Botnet Defense

Preventing Bot Infections

- Protecting your network from a botnet's many attack vectors requires "Defense in Depth."
  - Use a Firewall
  - Patch regularly and promptly
  - Use AntiVirus (AV) software
  - Deploy an Intrusion Prevention System (IPS)
  - Implement application-level content filtering
  - Define a Security Policy and share it with your users systematically

USER EDUCATION IS VITAL!

Recommendation Readings

- **Botnets: The Killer Web Application**, Craig Schiller
  ISBN 1-59749-135-7
- **Managing an Information Security and Privacy Awareness and Training Program**, Rebecca Herold
  ISBN 0-8493-2963-9
- **The CISO Handbook: A Practical Guide to Securing Your Company**, Michael Gentile
  ISBN 0-8493-1952-8
- **Google Hacking for Penetration Testers, Volume 1**, Johnny Long
  ISBN 1-93183-636-1

Thank You