Network Security: Botnet

Seungwon Shin
GSIS, KAIST

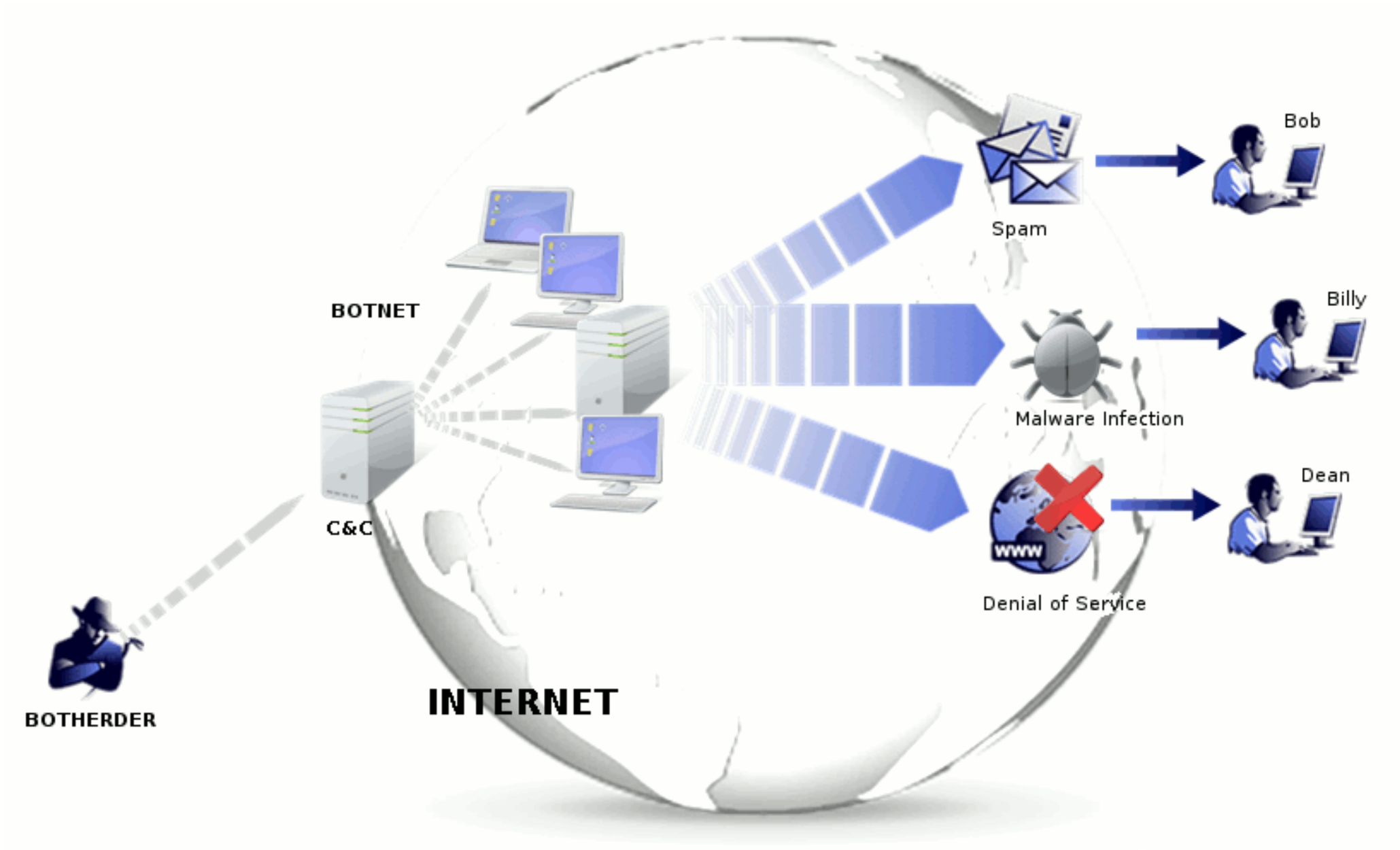
many slides from Dr. Yan Chen

Definition

- Bot
  - a software application that runs automated tasks over the Internet
- Botnet
  - a collection of Internet-connected programs communicating with other similar programs in order to perform tasks

wikipedia.com

Botnet

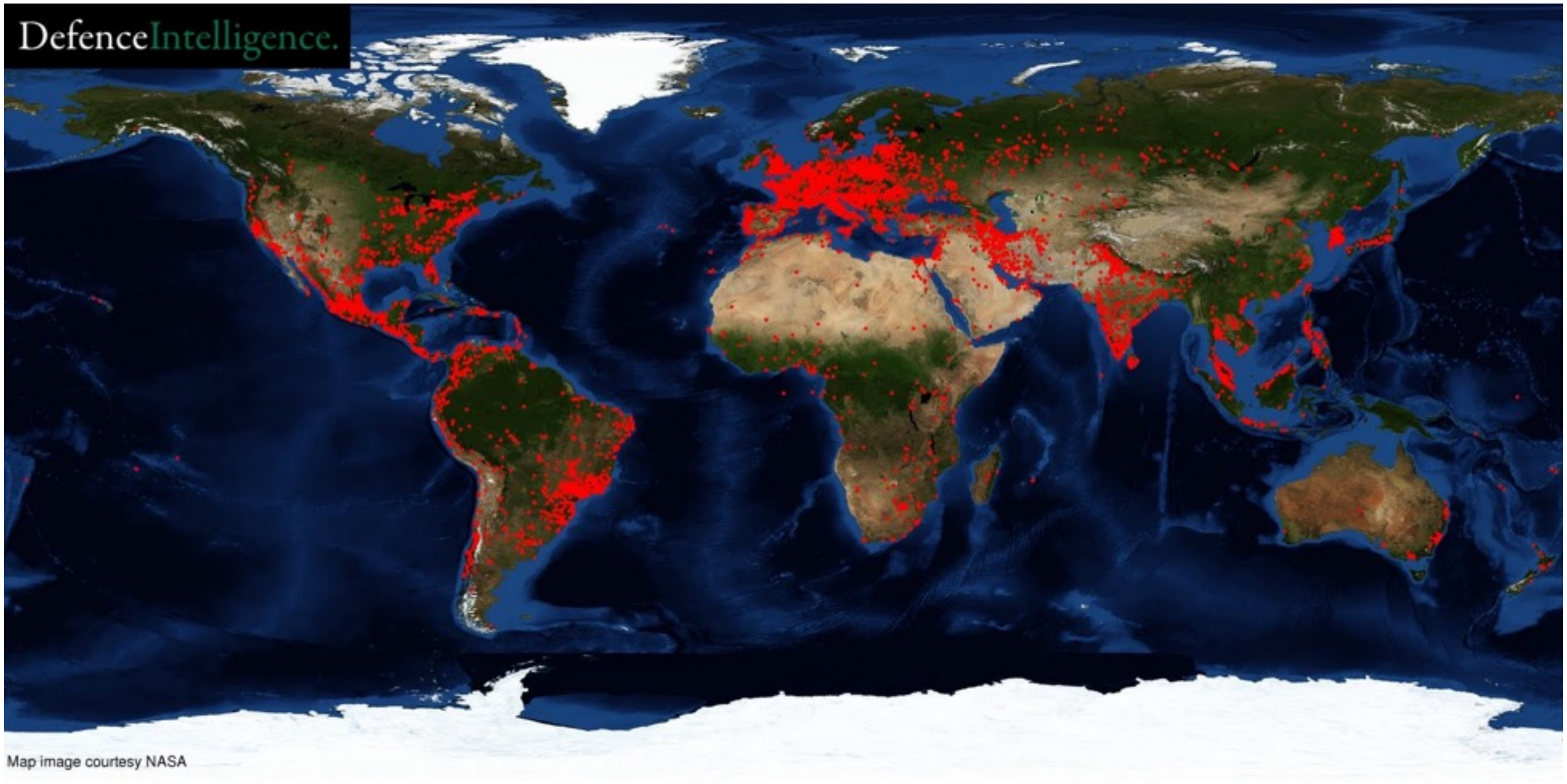


f-secure.com

Botnet Threat

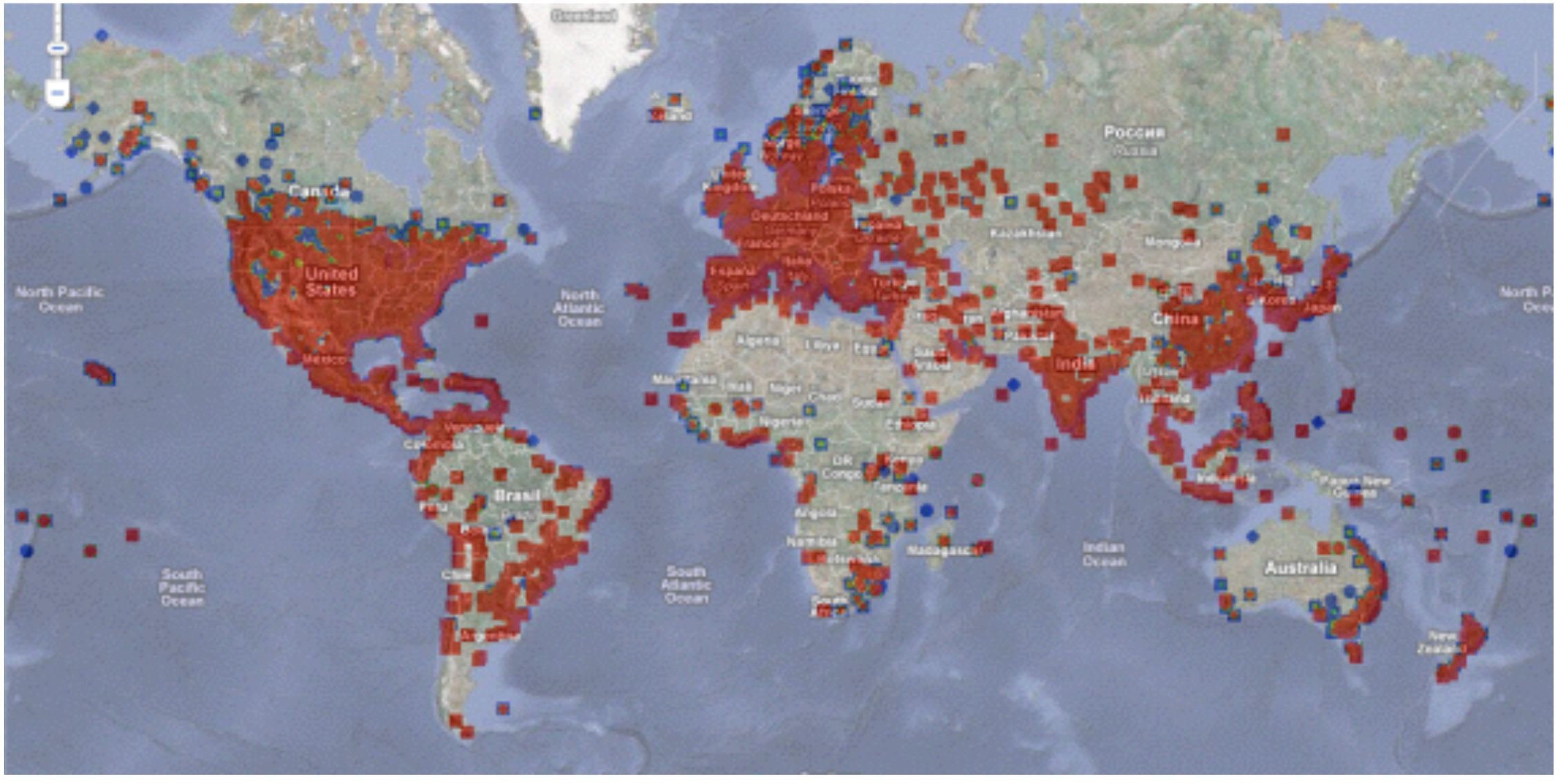
- Botnets are a major threat to the Internet because:
  - Consist of a large pool of compromised computers that are organized by a master.
    - a.k.a., Zombie Armies
  - Carry out sophisticated attacks to disrupt, gather sensitive data, or increase armies
  - Armies are in the 1000's to aggregate computing power
  - Communication network allows bots to evolve on a compromised host

Bot Infection - Mariposa



Map image courtesy NASA

Bot Infection - Conficker



Botnet example - AgoBot

- Most sophisticated
  - 20,000 lines C/C++ code
- IRC based command/control
- Large collection of target exploits
- Capable of many DoS attack types
- Shell encoding/polymorphic obfuscation
- Traffic sniffers/key logging
- Defend/fortify compromised system
- Ability to frustrate dissassembly

Botnet example - SDBot

- Simpler than Agobot, 2,000 lines C code
- Non-malicious at base
- Utilize IRC-based command/control
- Easily extended for malicious purposes
  - Scanning
  - DoS Attacks
  - Sniffers
  - Information harvesting

Botnet Taxonomy

- Attacking Behavior
- C&C Models
- Rally Mechanisms
- Communication Protocols
- Observable botnet activities
- Evasion Techniques

Attacking Behavior

Attack Behaviors

- Infecting new hosts
  - Social engineering and distribution of malicious emails or other electronic communications (i.e. Instant Messaging)
    - Example - Email sent with botnet diguised as a harmless attachment.
- Stealing personal information
  - Keylogger and Network sniffer technology used on compromised systems to spy on users and compile personal information
- Phishing and spam proxy
  - Aggregated computing power and proxy capability make allow spammers to impact larger groups without being traced.
- Distributed Denial of Service (DDoS)
  - Impair or eliminate availability of a network to extort or disrupt business

C&C Model

Command and Control

- Essential for operation and support of botnet
  - 3 Styles
    - Centralized
    - P2P
    - Randomized
- Weakest link of the botnet because:
  - Elimination of botmaster takes out the botnet
  - High level of activity by botmaster makes them easier to detect than their bots

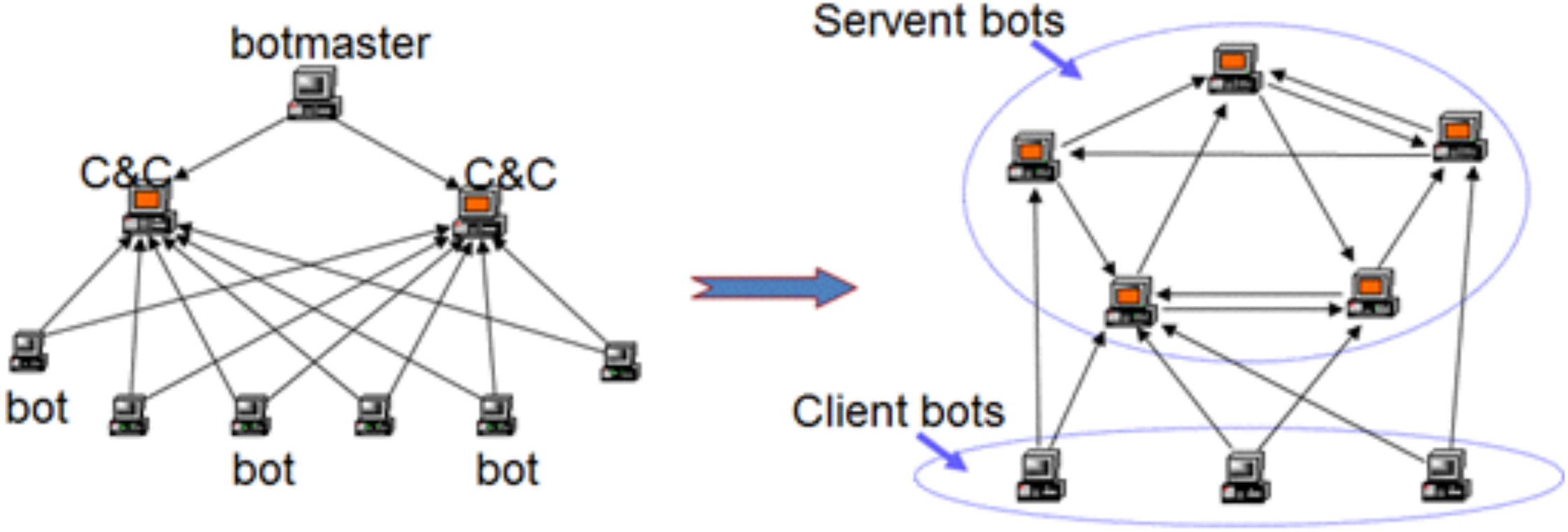
Centralized C&C

- Simple to deploy, cheap, short latency for large scale attacks
- Easiest to eliminate

pcworld.com

P2P C&C

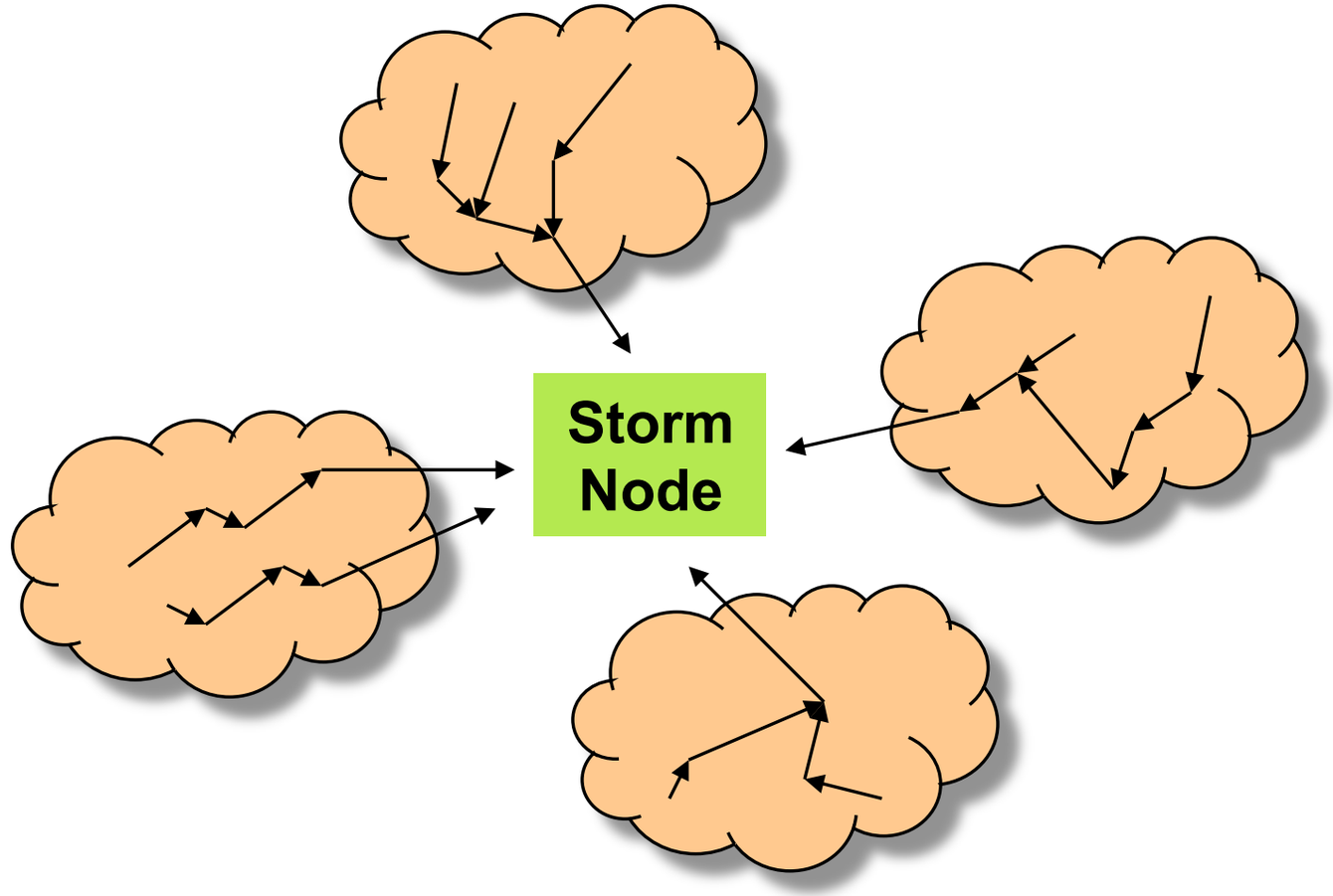
- Resilient to failures, hard to discover, hard to defend.
- Hard to launch large scale attacks because P2P technologies are currently only capable of supporting very small groups (< 50 peers)



From centralized botnet to hybrid peer-to-peer botnet

P2P C&C: Storm Bot

- The Overnet network that Storm uses is extremely dynamic.
- Peers come and go and can change OIDs frequently.
- In order to stay “well connected” peers must periodically search for themselves to find nearby peers:



P2P C&C: Storm Bot

Strom Bot message passing

Connect:

A peer uses connect messages to report their OID to other peers and to receive a list of peers somewhat close to the peer.

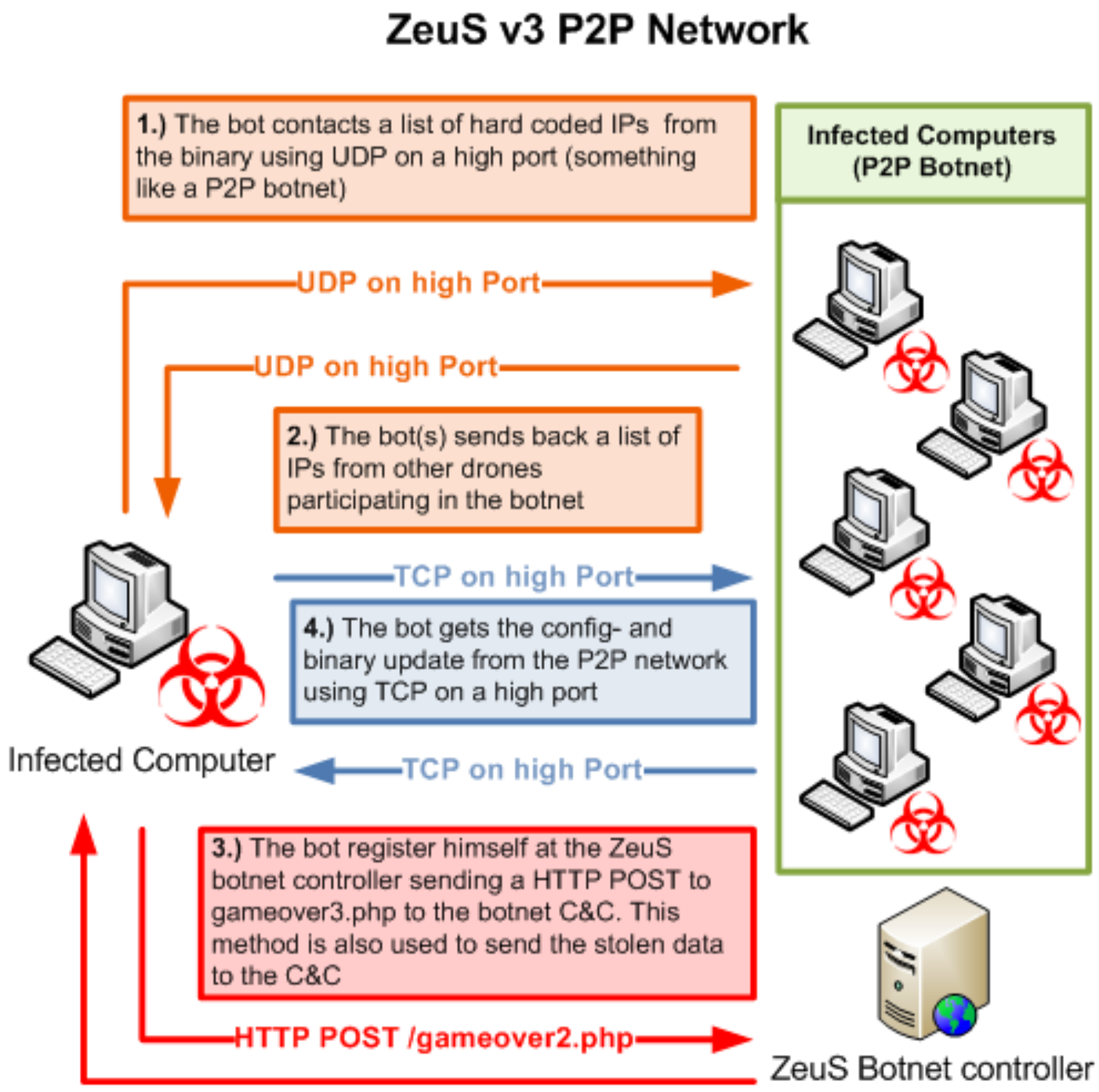
Search:

A peer uses search messages to find resources and other nodes based on OID.

Publicize:

A peer uses publicize messages to report ownership of network resources (OIDs) so that other peers can find the resource later.

P2P C&C: Zeus Bot



abuse.ch

Randomized C&C

- Theoretical architecture
  - Evan Cooke, et al describe the model
- Easy implementation and resilient to discovery and destruction
- Scalability limitations make it impractical for large scale attacks.
- Bots sleep and are not activated until Bot Master is ready to attack

Rally Mechanism

Rally Mechanism

- Hard-coded IP address
  - The bot communicates using C&C IP addresses that are hard-coded in it’s binary files.
  - Easy to defend against, as IP addresses are easily detectable and blocked, which makes the bot useless.

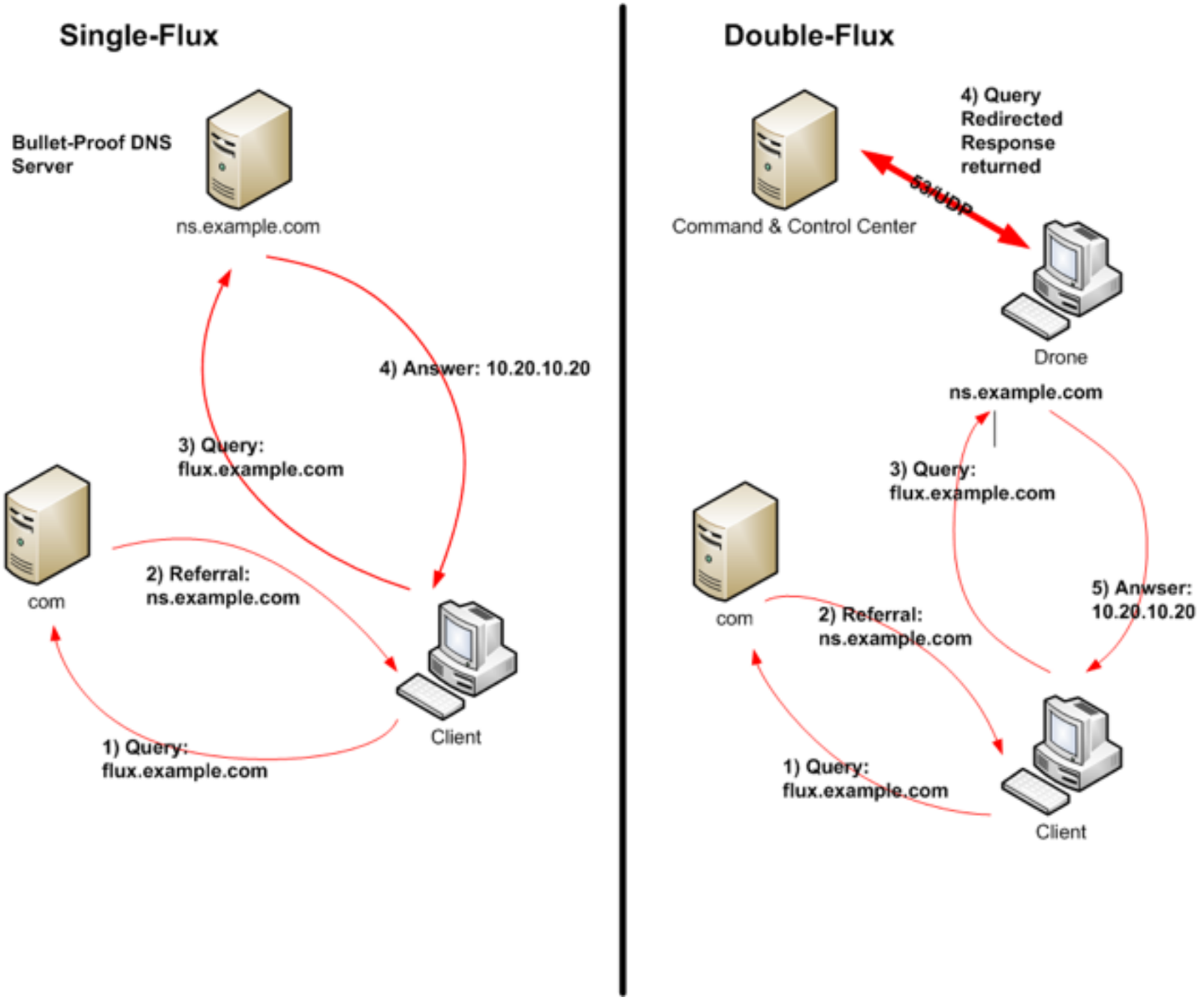
Rallying Mechanism

- Dynamic DNS Domain Name
  - Hard-coded C&C domains assigned by dynamical DNS providers.
  - Detection harder when botmaster randomly changes the location
  - Easier to resume attack with new, unblocked Domain Name
  - If connection fails the bot performs DNS queries to obtain the new C&C address for redirection.

Rallying Mechanism

- Distributed DNS Service
  - Hardest to detect & destroy.
  - Newest mechanism.
  - Sophisticated.
  - Botnets run own DNS service out of reach of authorities
  - Bots use the DNS addresses to resolve the C&C servers
  - Use high port numbers to avoid detection by security devices and gateways

FastFlux


Single-Flux
Bullet-Proof DNS Server
ns.example.com
4) Answer: 10.20.10.20
3) Query: flux.example.com
com
2) Referral: ns.example.com
Client
1) Query: flux.example.com
Double-Flux
4) Query Redirected Response returned
53/UDP
Command & Control Center
Drone
ns.example.com
3) Query: flux.example.com
com
2) Referral: ns.example.com
5) Anwser: 10.20.10.20
Client
1) Query: flux.example.com

Communication Protocol

Communication Protocol

- In most cases botnets use well defined and accepted Communication Protocols.
- Understanding the communication protocols used helps to:
  - Determine the origins of a botnet attack and the software being used
  - Allow researchers to decode conversations happening between the bots and the masters

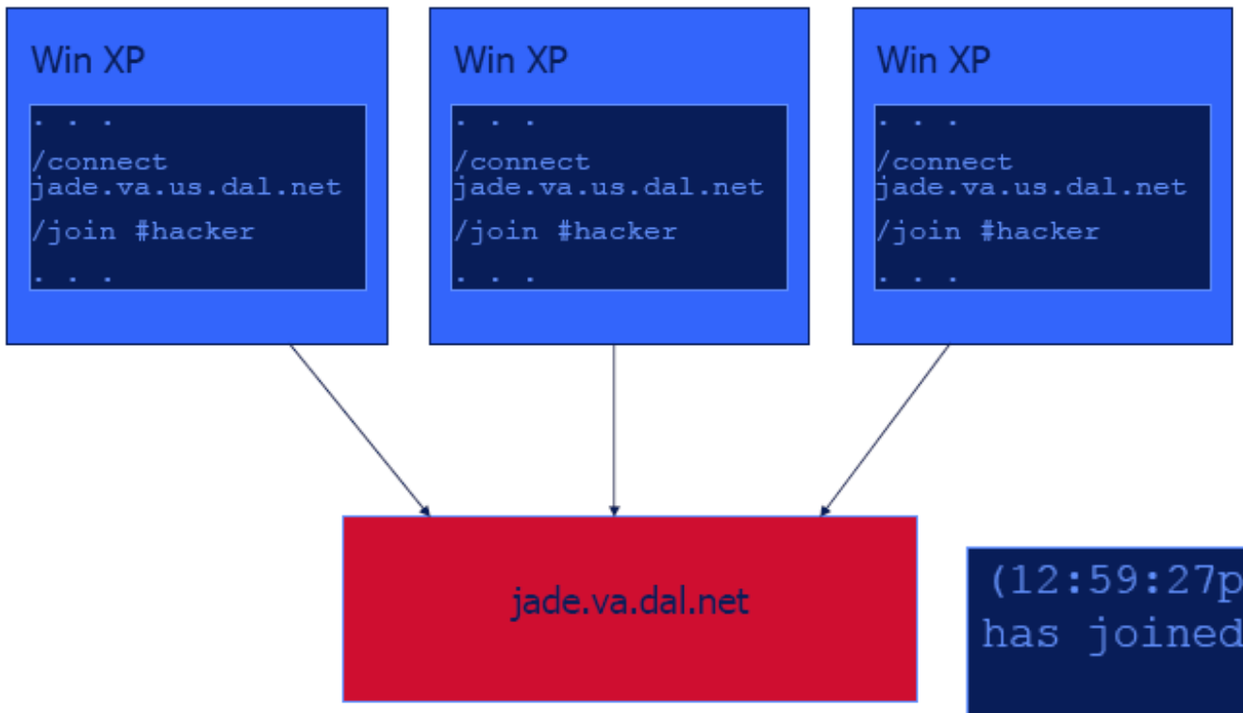
- There are two main Communication Protocols used for bot attacks:
  - IRC
  - HTTP
  - P2P
  - Custom protocol

IRC Protocol

- IRC Botnets were the predominant version
  - IRC mainly designed for one to many conversations but can also handle one to one
  - IRC servers are:
    - freely available
    - easy to manage
    - Attackers have experience with IRC
  - IRC bots usually have a way to remotely upgrade victims with new payloads to stay ahead of security efforts

- Most corporate networks does not allow any IRC traffic so any IRC requests can determine and external or internal bot
  - Outbound IRC requests means an already infected computer on the network
  - Inbound IRC requests mean that a network computer is being recruited

IRC Botnet




```
(12:59:27pm) -- A9-pcgbdv (A9-pcgbdv@140.134.36.124)
has joined (#owned) Users : 1646

(12:59:27pm) (@PhaTTy) .ddos.synflood 216.209.82.62

(12:59:27pm) -- A6-bpxufrd (A6-bpxufrd@wp95-
81.introweb.nl) has joined (#owned) Users : 1647

(12:59:27pm) -- A9-nzmpah (A9-nzmpah@140.122.200.221)
has left IRC (Connection reset by peer)

(12:59:28pm) (@PhaTTy) .scan.enable DCOM

(12:59:28pm) -- A9-tzrkeasv (A9-tzrkeas@220.89.66.93)
has joined (#owned) Users : 1650
```

HTTP Protocol

- Due to prevalence of HTTP usage it is harder to track a botnet that uses HTTP Protocols
- Using HTTP can allow a botnet to skirt the firewall restrictions that hamper IRC botnets
- Detecting HTTP botnets is harder but not impossible since the header fields and the payload do not match usual transmissions
- Some new options emerging are IM and P2P protocols and expect growth here in the future

Botnet Activities

Botnet Activities

- Three categories of observable Botnet behaviors:
  - Network-based
  - Host-based
  - Global Correlated

Network Activities

- Network patterns can be used to detect Botnets
  - IRC & HTTP are the most common forms of Botnet communications
  - Detectable by identifying abnormal traffic patterns.
    - IRC communications in unwanted areas
    - IRC conversations that human's can not understand
- DNS domain names
  - DNS queries to locate C&C server
  - Hosts query improper domain names
  - IP address associated with a domain name keeps changing periodically
- Traffic
  - Bursty at times, and idle the rest of the time
  - Abnormally fast responses compared to a human
  - Attacks
    - E.g., (Denial of Service) Large amounts of invalid TCP SYN Packets with invalid source IP addresses

Host Activities

- Botnet behavior can be observed on the host machine.
  - Exhibit virus like activities
  - When executed, Botnets run a sequence of routines.
    - Modifying registries
    - Modifying system files
    - Creating unknown network connections
    - Disabling Antivirus programs

Global Activities

- Global characteristics are tied to the fundamentals Botnets
  - Not likely to change unless Botnets are completely redesigned and re-implemented
  - Most valuable way to detect Botnets
- Behavior the same regardless if the Botnets are communicating via IRC or HTTP
  - Global DNS queries increase due to assignment of new C&C servers
  - Network Flow disruptions

Evasion Technique

Evasion Ways

- Sophistication of Botnets allow them to evade
  - AV Engines
  - Signature base intrusion detection systems (IDS)
  - Anomaly-based detection systems

- Techniques
  - Executable packers
  - Rootkits
  - Protocols

Evasion Ways

- Moving away from IRC

- Taking control of
  - HTTP
  - VoIP
  - IPV6
  - ICMP
  - Skype protocols

Collect Bot Samples

BotLab - Collect Storm Bot