

Internet Security 2

(aka Advanced InetSec)

Malware 2: Botnets

Christian Platzer

Gilbert Wondracek

Markus Kammerstetter

Edgar Weippl

inetsec@seclab.tuwien.ac.at

News from the Lab

Int. Secure Systems Lab
Vienna University of Technology

- Challenge 3 (BHO) is over
 - 37 people finished it
- ...and the winner is: Jakob "Radical Buster" Korherr
- Challenge 4 begins today
 - Worm

Overview

Int. Secure Systems Lab
Vienna University of Technology

- Introduction
- Botnets
- Command & Control
- Some example bots

Introduction

Introduction

Int. Secure Systems Lab
Vienna University of Technology

- Viruses and worms demonstrate the feasibility of self-spreading code
 - can compromise millions of computers, and bring down entire networks

- But what do the attackers gain?
 - not easy to turn that into money

The Need for C&C

Int. Secure Systems Lab
Vienna University of Technology

- To maximize profit from compromised machines, attackers need to be able to control them
- Do whatever is most profitable at any point in time
 - Propagate
 - DDoS
 - SPAM
 - Identity theft
 - pay-per-install
 - ...
- All of these actions need to adapt over time
 - SPAM campaigns, target websites for identity theft, propagation vectors,...

The Need for C&C

Int. Secure Systems Lab
Vienna University of Technology

- Attackers need a Command and Control (C&C) infrastructure
- C&C requirements
 - flexible (updates,..)
 - scalable (millions of hosts,..)
 - resilient to shut down attempts (law enforcement, CERTs,..)
 - hard to trace the person sending the commands
- A simple backdoor is not enough (and NAT makes backdoors useless)
 - enter Botnets!

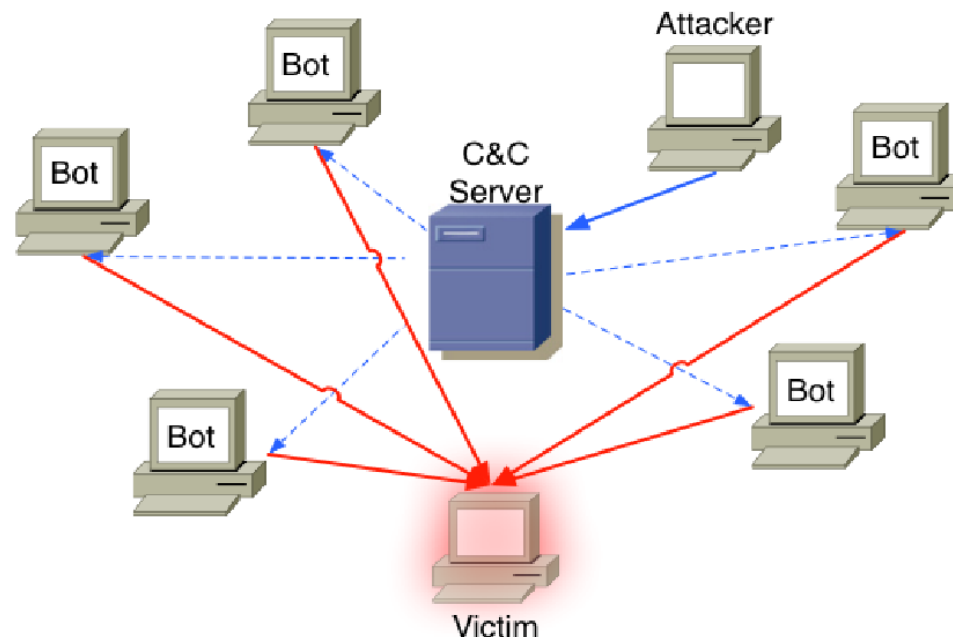
Botnets

Bots

- A bot, a.k.a zombie or drone, is a compromised machine that can be controlled by an attacker remotely.
- Bots have three distinguishing features;
 - Remote control facility
 - Implementation of different commands
 - Spreading mechanism for propagation purposes

Botnets

- A botnet is a network that consists of several malicious bots that are controlled by a commander, commonly known as bot master or bot herder.



Historical Evolution of Botnets

*Int. Secure Systems Lab
Vienna University of Technology*

- First bots were invented for benign use, worked in the IRC network;

The Jargon File, version 4.4.7:

```
bot: n [common on IRC, MUD and among gamers; from  
"robot"]
```

```
1. An IRC or MUD user who is actually a program. On IRC,  
typically the robot provides some useful service. Examples  
are NickServ, which tries to prevent random users from  
adopting nicks already claimed by others, and MsgServ,  
which allows one to send asynchronous messages to be  
delivered when the recipient signs on.
```

```
[...]
```

Historical Evolution of Botnets

Int. Secure Systems Lab
Vienna University of Technology

- After a while, the attackers abused the usage of IRC bots and waged IRCwars;
 - _ IRCwars were one of the first documented distributed denial of service attacks
- 1999: trinoo "distributed denial of service attack tool"
 - _ originally ran on solaris (later ported to windows)
 - _ setup of the botnet was mostly manual
 - _ August 1999: DDoS attack against a server at University of Minnesota using at least 227 bots
 - _ <http://staff.washington.edu/dittrich/misc/trinoo.analysis>
- 2000: DDoS attacks against high profile websites (amazon, CNN, ebay,..) got huge media coverage
- While DDoS was the first application, botnets are now used for many types of internet crime
 - _ \$\$\$!

Timeline of Botnets

*Int. Secure Systems Lab
Vienna University of Technology*

Date	Name	Description
12/1993	EggDrop	Non-malicious IRC bot
04/1998	Gtbot	Malicious IRC bot based on MIRC
04/2002	Sdbot	Provided own IRC client
10/2002	Agobot	Robust, flexible, modular design
04/2003	Spybot	Extensive feature set based on Agobot
03/2004	Phatbot	P2P bot based on WASTE
03/2006	SpamThru	P2P bot
04/2006	Nugache	P2P bot
01/2007	Peacomm	P2P bot based on Kademlia
10/2007	Storm	Uses its own P2P network

Timeline of Botnets

Int. Secure Systems Lab
Vienna University of Technology

Date	Name	Description
2008	Waledac	Taken down 2010 by MS
2009	Cimbot	

Bot Activity

Int. Secure Systems Lab
Vienna University of Technology

- For the infected host: information harvesting
 - Identity data
 - Financial data
 - Private data
 - E-mail address books
 - Any other type of data that may be present on the host of the victim.

- For the rest of the Internet
 - E-mail Spamming
 - Denial of Service Attacks
 - Propagation (network worm/email worm,..)
 - Support infrastructure for illegal internet activity (the botnet itself, but also to host phishing sites, drive-by-download sites,..)

Botnet Characteristics

- Remote Control Facility
 - allows the attacker to have full control over the infected machines.
- A wide range of commands
 - Allows the attacker to command bots for specific purposes
- Spreading mechanism for further propagation
 - e.g. exploiting vulnerabilities,
- While remote control mechanism and commands differentiate bots from worms, they have similar spreading mechanisms as worms have.

Spreading Mechanisms

Int. Secure Systems Lab
Vienna University of Technology

- The more compromised machines it has, the most effective the botnet is...
- Propagation Mechanisms, finding vulnerable victims...
 - Random Scanning
 - Permutation Scanning
 - Hit-List Scanning
 - Combining Techniques, e.g. Warhol worm
- Generate new polymorphic variant of bot for each installation
 - to evade signature-based detection

Some commands available in Agobot/Phatbot family

*Int. Secure Systems Lab
Vienna University of Technology*

- harvest email addresses from host
- log all keypresses
- sniff network traffic
- take screenshots
- start an http server that allows to browse C:
- kill a hard-coded list of processes
 - AV programs
 - rival malware
- steal windows CD keys
 - also keys to popular games
- Socks proxy
 - sets up a proxy to be used as a "stepping stone" for SPAM
- download file at an url
- run a shell command
- Update
 - allows to change the available commands!

C&C Strategies

Command and Control Mechanisms (C&C)

Int. Secure Systems Lab
Vienna University of Technology

- The most distinguishing and powerful feature of Botnets...
- As long as there is an update command defined for the bots, the botmaster can change the command set by updating her bots.
 - in other words, commands can be delivered in the form of executable code
- Thus, C&C brings a great flexibility to the activities that can be performed by bots
- However, C&C is also the weakest link of the system
 - shutdown C&C, and all bots become "mostly harmless"

The C&C Arms Race

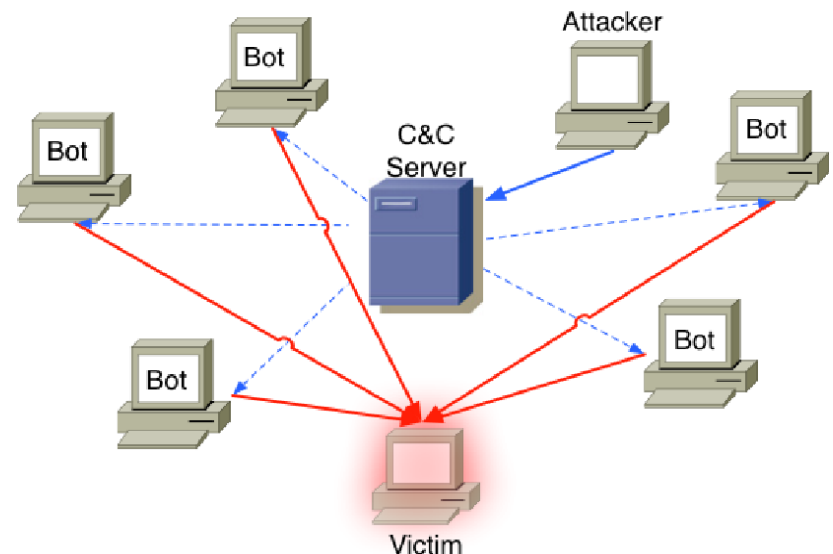
Int. Secure Systems Lab
Vienna University of Technology

- Botnet operators try to achieve reliable C&C
 - centralized or p2p C&C
 - fast flux
 - domain generation algorithms (DGA)
 - analysis resistance (as discussed in previous lecture)
- White hats try to shut them down
 - coordinated take-downs
 - de-peering of malicious ISPs

Single Point of Failure

*Int. Secure Systems Lab
Vienna University of Technology*

- If there is a single C&C server it is trivial to shutdown
- Real botnets don't work this way
 - even Trinoo (1999) allowed multiple masters!



Takedown strategies

- Take down master:
 - ask ISP to block IP address
 - ask .com administrators to change entry for evil.com
- Take over the master:
 - take control of the IP/DNS name running the master
 - issue commands to the botnet
 - uninstall the bot
 - warn user he is infected
 - risky from a legal point of view
 - what if you inadvertently cause harm?
 - only works if C&C is not well-protected using cryptography
 - digital signatures on bot commands
 - botmaster has the private key

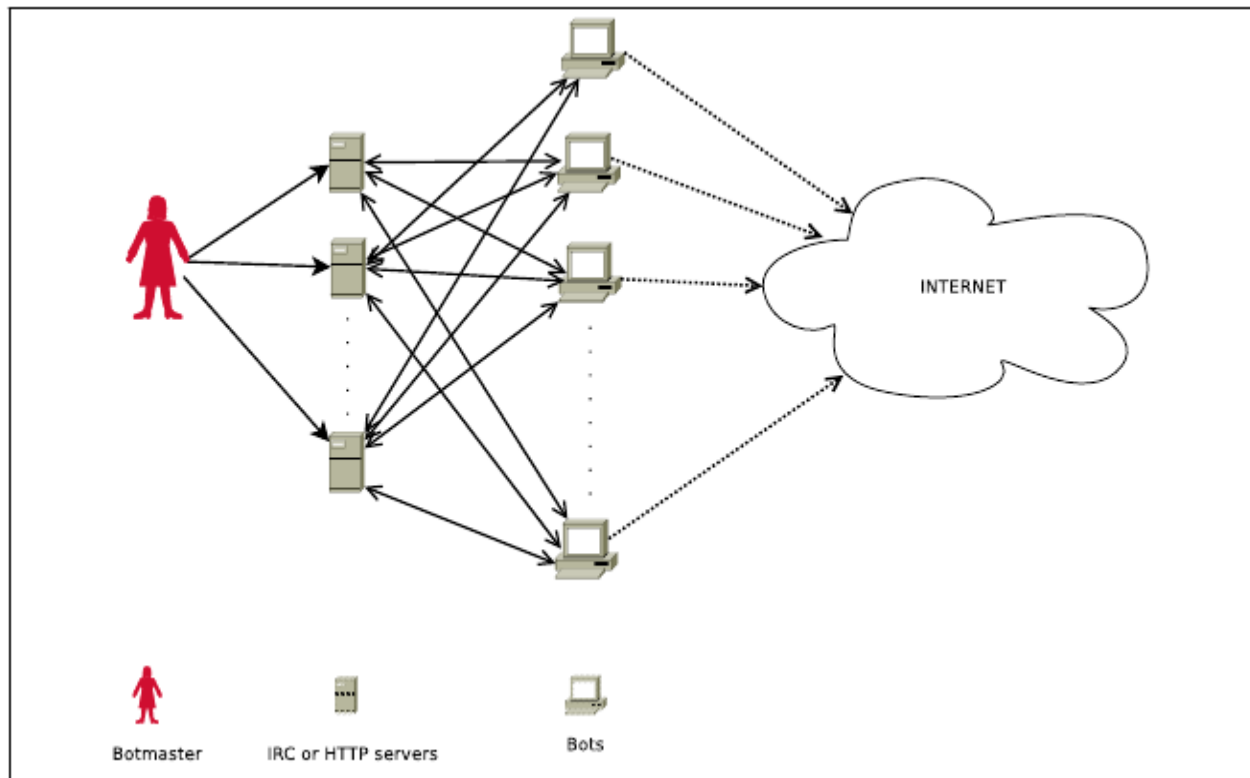
Command and Control Mechanisms (C&C)

Int. Secure Systems Lab
Vienna University of Technology

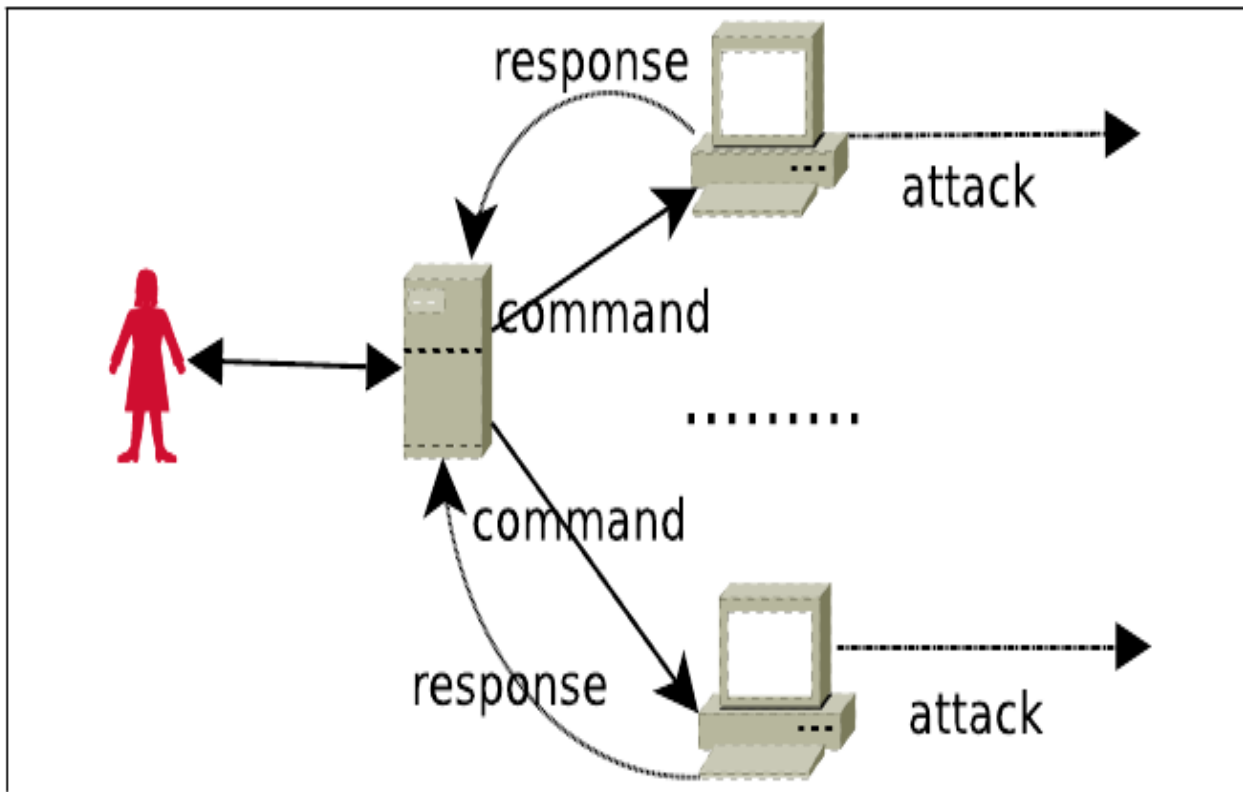
- Centralized Command and Control Mechanisms
 - Push style C&C, e.g. IRC
 - Pull style C&C, e.g. HTTP

- Decentralized Command and Control Mechanisms
 - P2P C&C, e.g. Storm

Centralized C&C

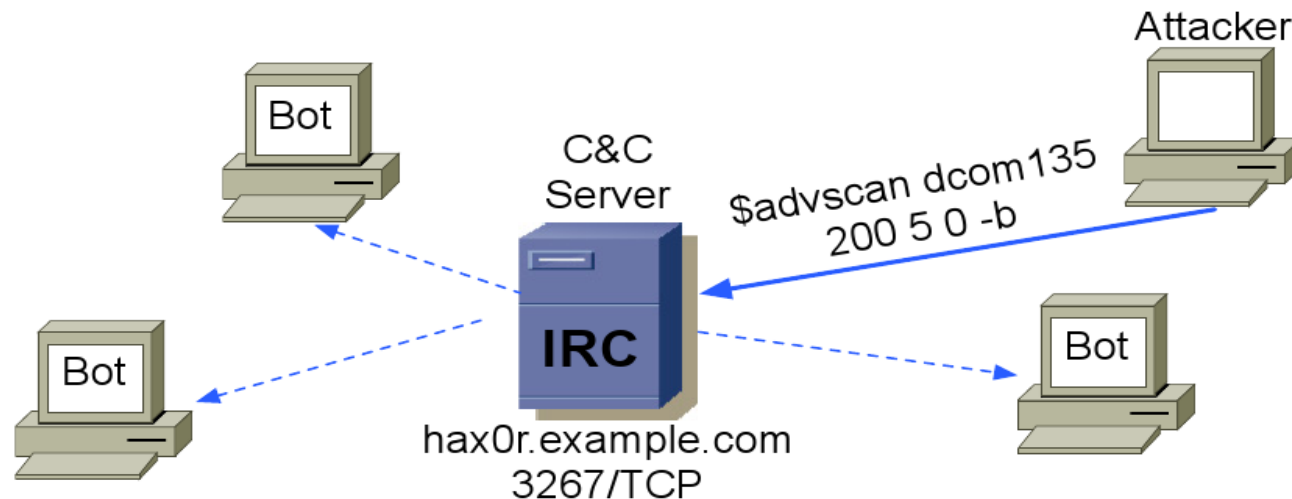


Push Style C&C



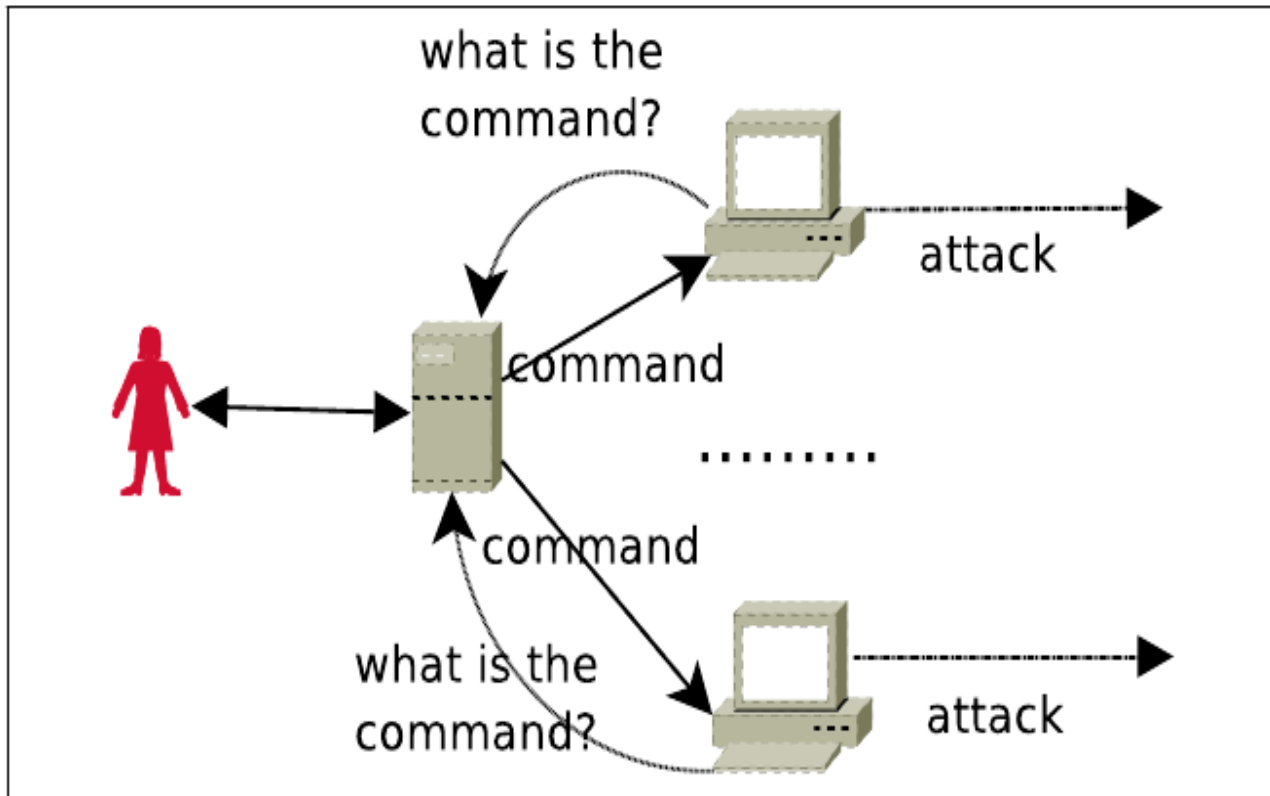
Push Style C&C using IRC

- Typical communication flow using central IRC



- *advscan lsass 200 5 0 -b*
- *ddos.syn XXX.XXX.XXX.XXX 80 600*

Pull Style C&C



Pull Style C&C using HTTP

Int. Secure Systems Lab
Vienna University of Technology

File Edit View Go Bookmarks Tools Window Help

http://www.kimart.biz/uy1euyhw/socks/bot/cmd.htm

Remark: in "SHELL COMMAND" do not use symbol " "
Remark: bots checks the next command each 5 seconds. Send next command after this time is left

Show stats Clear cmd.txt

DOWNLOAD AND EXEC FILE	URL: http://	LOCAL FILENAME: c:\	PERSONAL COMMAND:	Submit	
SHELL COMMAND			PERSONAL COMMAND:	Submit	
STORE SCREENSHOT IN LOCAL FILE	FILE		PERSONAL COMMAND:	Submit	
CHANGE URL FOR LOGS			PERSONAL COMMAND:	Submit	
URL THAT SHOULD BE BLOCKED	http://		PERSONAL COMMAND:	Submit	
CLEAR HOSTS FILE			PERSONAL COMMAND:	Submit	
UPLOAD FILE	FTP:	LOCAL FILENAME: c:\	FTP LOGIN:	FTP PASSWORD:	PERSONAL COMMAND:

UPLOAD HOSTS FILE:

Submit ID:

STATS: - Mozilla

Last command sent to botnet: SHELL
cmdstring:copy_nul_%SYSTEMROOT%\SYSTEM32\DRIVER:
cmdid:1112293461
Total count of bots, which receives command: 49
Total infection count (counted from logger.txt): 255

Close

HTTP and IRC

- IRC

- used because it is directly suitable to the purpose of sending commands to bots
 - legitimate IRC server can be used, acts as stepping stone
- also for historic reasons
 - sdbot/agobot/phatbot source-code is available
- quite unusual on modern networks! suspicious/blocked...

- HTTP

- outgoing HTTP allowed everywhere (sometimes through proxy)
- a lot of complex applications are delivered on top of HTTP
- hard to model "normal" HTTP traffic
 - hard to detect "unusual" botnet traffic

Centralized C&C

- Multiple C&C servers (typically http/IRC)
 - _ multiple layers of hosts between bot and botmaster (hard to trace back)
- address of C&C server(s) must be available to each bot
 - _ in binary, config file, etc
 - _ frequently updated
- large botnets often partitioned into several smaller ones
 - _ each bot knows only a few C&C servers
 - _ you do not know everything about a botnet just by looking at 1 sample!

Bullet-Proof Hosting

Int. Secure Systems Lab
Vienna University of Technology

- Sometimes C&C is hosted by ISPs that are completely unresponsive to abuse complaints
- In these cases, a solution can be to take down the entire ISP
- De-peering: other ISPs rescind their peering agreements with the malicious ISPs
 - evidence is required that abuse breached clauses of peering contracts
 - may involve law enforcement, FTC, etc
- Examples:
 - Russian Business Network (2007), Atrivio (2008), McColo (2008), 3FN (2009)

Botnet Take-Downs

- Taking down a centralized botnet looks easy
 - just shut down all the C&C servers!
- Not so easy in practice
- C&C servers can be hosted by tens of different providers all over the world
 - some ISPs will respond to abuse complaints more promptly than others
- For a take-down to "stick", all C&C servers need to be taken down at the same time
 - if a single server is still up, it can update the bots to use new C&C servers

Botnet Take-Downs

- Some history:
 - "Takedowns: The Shuns and Stuns That Take the Fight to the Enemy" by Brian Krebs
- A few take-downs have been fully successful
 - Mega-D, waledec, ...
- More often, only some of the C&C servers can be shut down, and most of the bots eventually reconnect to the botmaster
 - pushdo/cutwail takedown of ~20/30 C&C servers in August 2010

Fast-Flux Hosting

- Technique used by botmasters to provide reliable hosting of services on unreliable bots
 - network has high churn (bots frequently come and go)
 - user switches his infected computer off/on
 - infected host is cleaned
 - new victims are infected
- Can be used to host master servers for botnets
 - choose infected hosts that are not behind NAT/firewall
- Can host many other things
 - phishing pages, drive-by-download attacks,...

Fast-Flux Hosting

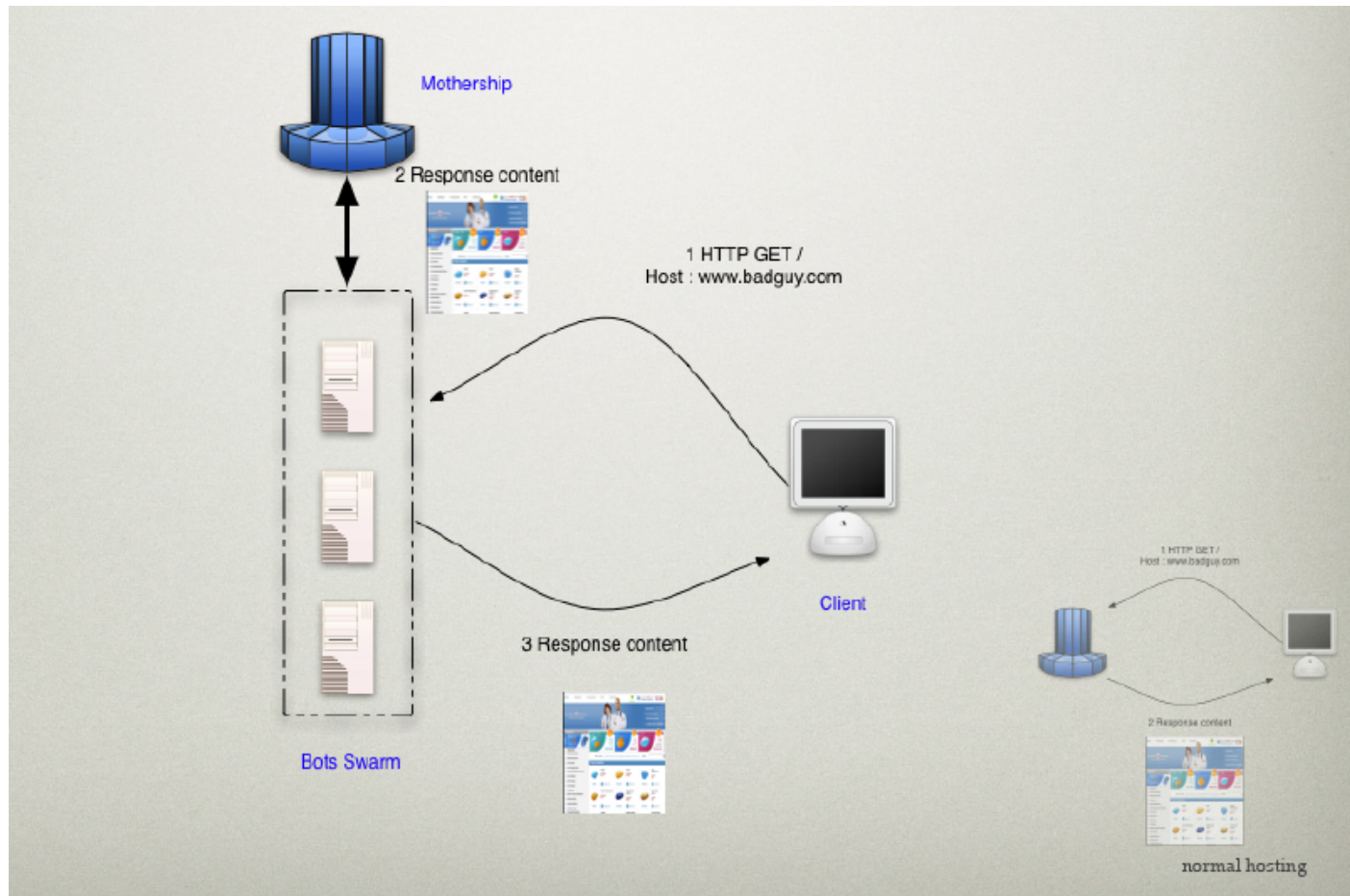
- Round Robin DNS
 - A DNS answer consists of several DNS A records.
 - Each time the order of the answer list is different
 - The idea behind this is to balance the workload on different servers
- TTL value
 - Normally, the DNS records include a TTL value between 1 and 5 days for taking benefit from the DNS caching system
 - Recently, content delivery networks set the TTL value to very low values, i.e. between 0 and 900 seconds
- Fast-Flux
 - Several IP addresses in the DNS record
 - Low TTL value
 - Usage of round robin DNS

Fast-Flux Hosting

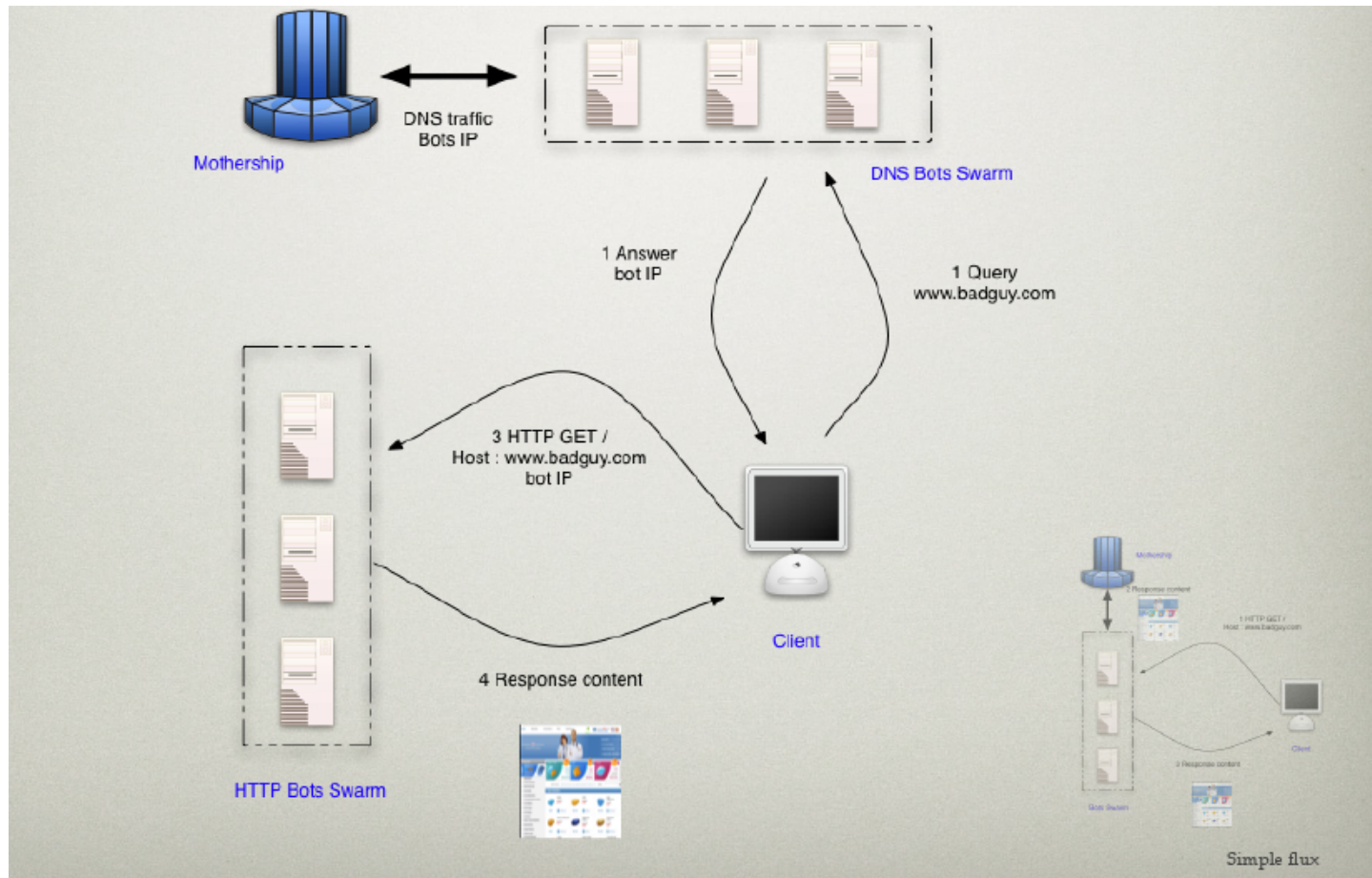
Int. Secure Systems Lab
Vienna University of Technology

- DNS entries need to be frequently updated (churn, takedown)
- some domain registrars allow their customers to change their DNS entries every few minutes
 - some registrars do not allow this
 - ICANN may forbid this in the future
 - but there are legitimate uses for content distribution networks (load balancing)

Single Fast Flux



Double Fast Flux



Fast-Flux hosting

- Single fast-flux:
 - DNS A (address) entries are frequently changed
- Double fast-flux:
 - DNS NS (name server) entries are frequently changed
 - point to bots that act as DNS servers for the botmaster's domain
 - bots can play many different roles in a botnet!
- target bots can directly host content, or only act as a proxy

Domain Generation Algorithms (DGA)

*Int. Secure Systems Lab
Vienna University of Technology*

- Bot master registers new domains for C&C on a regular basis
- Each bot generates the domain that is going to be reached using a custom domain generation algorithm.
 - _ The algorithm takes the date of the day and a salt as a parameter.
- In this way, you can add a new kind of flux layer in order to hide the mothership
 - _ Conficker
 - _ Mebroot a.k.a Torpig
 - _ Murofet
- By reverse engineering the domain name generation algorithm, you can predict the C&C domains for the future
 - _ shut them down before they are even used!
 - _ <http://www.confickerworkinggroup.org/wiki/>

DGA Economics (1/2)

Int. Secure Systems Lab
Vienna University of Technology

- DGA often used as a backup C&C mechanism
 - use regular C&C servers, fall back to DGA if all servers taken down
- The Murofet DGA generates 800 domains each day
 - bots try to contact some of these at random
 - <http://blog.threatexpert.com/2010/10/domain-name-generator-for-murofet.html>
- The botmaster does not need to register all 800 domains!
 - one or a few each day are sufficient
 - bots try again until they successfully contact a server

DGA Economics (2/2)

- If primary C&C servers are shut down, botnet can use DGA to try new servers
 - bot just needs to reach 1 server to get back online
- To take botnet down, white hats need to register all 800 domains each day
 - quickly gets expensive!
- This happened with the srzbi botnet in 2008
 - after McColo went down, srzbi lost all its C&C servers, but had a backup DGA
 - FireEye security reversed the DGA algorithm and registered all the DGA domains to stop srzbi from getting back up
 - After a few weeks FireEye gave up (registering the DGA domains was too expensive) and srzbi got back online

Peer-to-peer C&C

Int. Secure Systems Lab
Vienna University of Technology

- Alternative to client-server architecture
 - bot commands propagate in a p2p network
- More robust?
 - more difficult to catch the botmaster
 - even if some of the nodes in the network are shut down, the gaps in the network are closed and the network continues its activities
- In practice there are disadvantages

Custom p2p protocols

Int. Secure Systems Lab
Vienna University of Technology

- Bots can use a custom p2p protocol
 - designed specifically for botnet
 - can be very "noisy"
 - what are all these incoming/outgoing connections?
- Each bot has a list of peers (neighbors)
- A bot needs a way to find new neighbors
 - typically, by traversing the neighborhood graph starting from its neighbors
 - this allows enumeration of peers
 - allows a security researcher to enumerate infected hosts
 - used as part of recent takedown of Waledac botnet

Standard p2p protocols

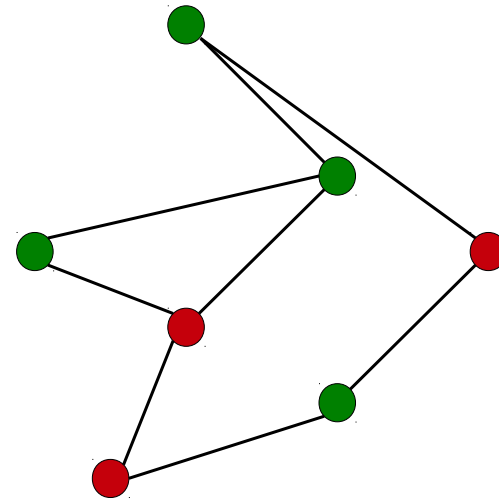
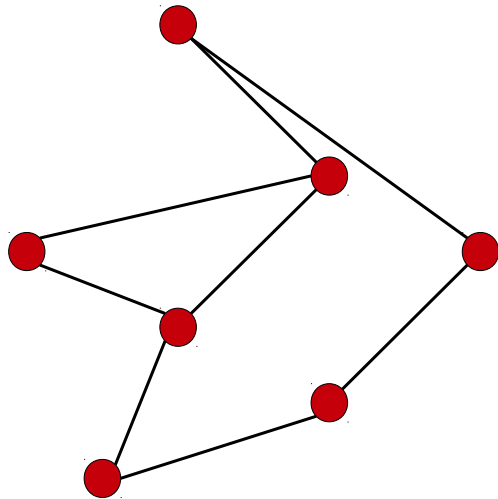
Int. Secure Systems Lab
Vienna University of Technology

- Use standard p2p protocol
 - allows C&C traffic to blend in with legitimate p2p traffic
 - legitimate p2p is still blocked in many locations
- Build C&C on top of legitimate protocol

Peer-to-peer C&C

*Int. Secure Systems Lab
Vienna University of Technology*

- Custom p2p protocol
- standard p2p protocol
 - blend in to p2p network



Bots: a Small Bestiary

Storm Worm

Int. Secure Systems Lab
Vienna University of Technology

- Originally used Overnet network (based on Kademlia)
 - now uses "Stormnet" (similar protocol, but no legitimate peers)
- Bots do not directly send information to each other
- Kademlia protocol implements a distributed hash table (DHT)
- DHT allows to store and retrieve <key,value> pairs
 - stored in the network at a set of peers selected with a specific algorithm

Storm Worm

Int. Secure Systems Lab
Vienna University of Technology

- Bot(master) publishes by storing $\langle k, \text{command} \rangle$ in the DHT
- Bots periodically lookup k in the DHT to retrieve command
 - Storm bots check 32 different keys, which change daily based on a custom algorithm
- Commands are not encrypted / signed
 - it would be possible to take over the Storm botnet
- For analysis / takedown strategy see:
 - Holz et al. "Measurements and Mitigation of Peer-to-Peer-based Botnets: A Case Study on Storm Worm"

Pushdo / Cutwail

- (Mostly) Spam botnet
- Pushdo is a dropper
 - on startup, it downloads and executes code
 - can save the code to file or just inject a thread into an existing process
 - each binary has a hard-coded list of IP addresses from which to download the code
 - most common payload is Cutwail
 - sometimes downloads completely different stuff
 - including pay-per-install executables!

Pushdo / Cutwail Botnet

Int. Secure Systems Lab
Vienna University of Technology

- Cutwail is a template-based spam engine
 - connects to a second C&C (hardcoded) server using proprietary protocol (in our experiments on port 25, SMTP)
 - downloads an (encrypted) configuration file (may include IP of a different C&C server to be used from now on)
 - downloads list of email addresses to spam
 - download spam templates
 - custom markup language
 - checks it is online and not firewalled by connecting to mx.google.com:25, etc.
 - sends SPAM!

Pushdo / Cutwail Botnet

Int. Secure Systems Lab
Vienna University of Technology

- Trend micro report on pushdo/cutwail:
http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/study_of_pushdo.pdf
- "Adding to this confusion is the tendency of the botnet owners to frequently change Pushdo's functionality and code. It is perhaps better to think of Pushdo as a "criminal operation", rather than a single piece of malware"

Conclusion

Int. Secure Systems Lab
Vienna University of Technology

- We talked about bots / botnets
- Botnets / C&C arms race
 - Botnet operators try to achieve reliable C&C
 - White hats try to shut them down
 - Centralized and p2p C&C, Fast Flux, DGA,...
- Next week: Web Security
- Thanks!