Denial of Service

QUICK QUESTION

- What happened on November 2nd 1988?

FIRST INTERNET WORM WAS LAUNCHED

- Moved relentlessly across network connections from computer-to-computer
- Within 12 hours, first Berkeley Uni then Purdue Uni distributed patches to stop spread.
- Computers affected 2,000-3,000 (maybe more)
- Even those computers not affected had to be tested !
- Cost? Estimated between $1M and $100M. A great deal of time and resources expended.

- **Robert T Morris Jr.**(Student at **Cornell Univ.**)
- Claimed it was an experimental program that had a bug
- **2yrs later -> 3yr** probation, **$10K** fine, **400** hours community service.

WHAT'S THE PROBLEM?

KEY PROBLEMS

- Confidentiality
- Authentication
- Integrity
- Non-repudiation
- Availability
- Access Control

CONFIDENTIALITY(SECRECY)

- Protect transmitted data
- Protect against traffic analysis

AUTHENTICATION

- Assurance that message is from proper source
- Protect from third party masquerade

INTEGRITY

- Message is received as sent
- Modification
- Also interested in replay, re-ordering, deletion, delay

AVAILABILITY

- Complete loss of availability
- Reduction/Degradation in availability

NON-REPUDIATION

- Prevents parties from denying they sent or received a message; ie. concerned with protecting against legitimate protocol participants, not with protection from external source
- Receiver can verify **and prove** who sent a message
- Sender can verify **and prove** who received a message

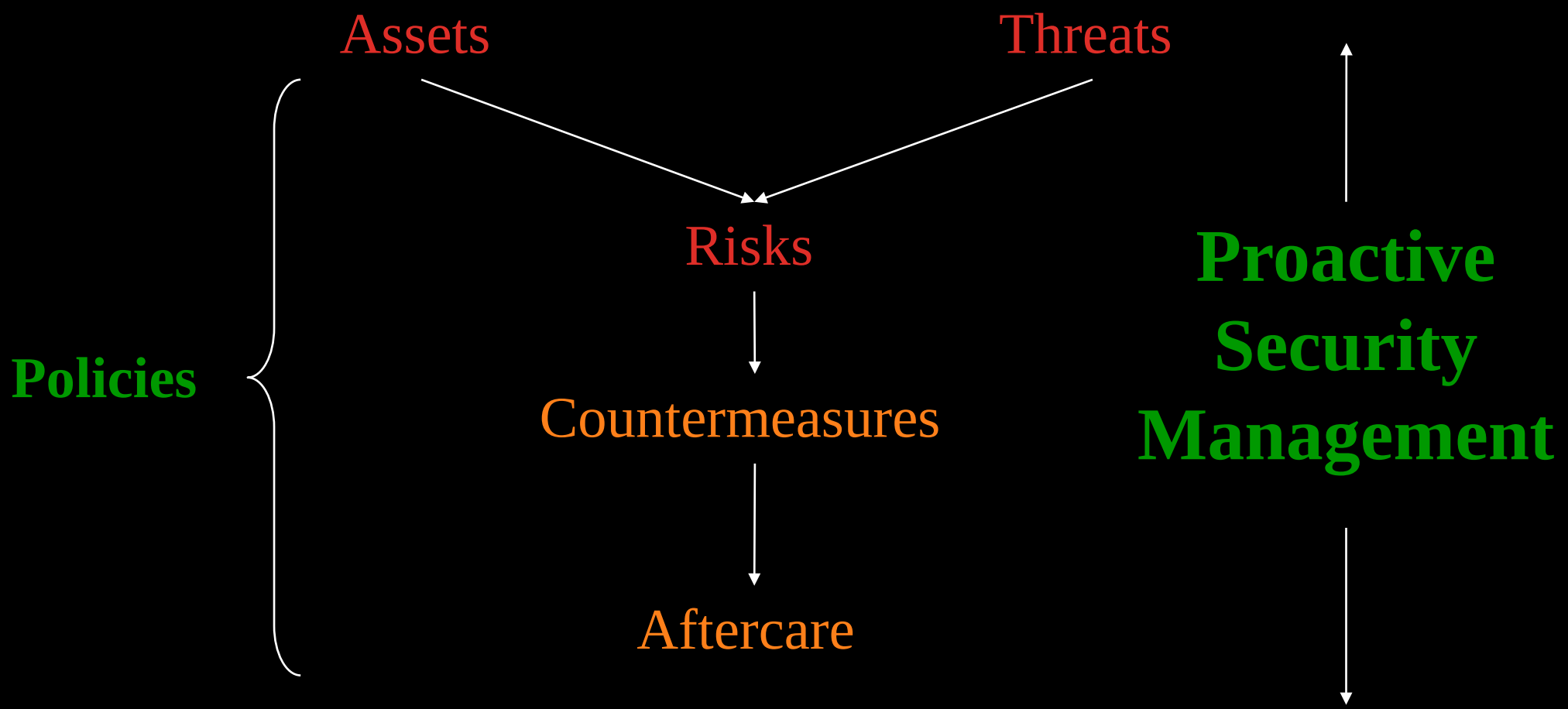
ACCESS CONTROL

- Limit & control access to host system/services
- Limit & control access to networks
- Authenticate each party so that access rights can be assigned
- More fine-grained solutions, e.g. Digital Rights Management

THREATS

- Hardware errors
- Terrorists
- Theft, Malicious, Microsoft
- Industrial espionage, Government
- Malicious software
- Pirating
- Password cracking
- Denial of Service
- Masquerade
- Misuse of resources
- Social engineering
- Reverse engineering

THREAT ANALYSIS



COUNTERMEASURES - SYSTEMS

- Anti-virus software
- Backups
- Firewalls
- CERT
- Security Policies
- Physical security
- Disaster recovery
- Intrusion detection Systems
- Hardware dongles
- Patches
- Cryptography
- Access control
- Increasing bandwidth

COUNTER MEASURES - PEOPLE

- Good pay, food, computers, gym
- Train users
- Patents, copyrights, lawyers
- Contracts
- Background people
- Insurance

DISTRIBUTED DENIAL OF SERVICE

- DDOS - Why bother?
  - It’s not about the fame
  - Sometimes it’s about Money

HOW IT WORKS

- Targets
  - Gambling Sites
  - Pornographic Sites
  - Religious Sites
  - Pro-life Sites
  - Or anyone with money!! – Corporations, Big Business, Banks

BOTNETS

- Botnets are sets of machines, all controlled by a ‘master node’
- Often machines are infected when visiting a website
  - Largest botnet found so far had > 1,000,000 machines in it

BOTNETS: HOW TO **PREVENT** YOUR COMPUTER FROM BECOMING A ZOMBIE

AFTER CONNECTION TO A COMMAND AND CONTROL SERVER, THE INFECTED COMPUTER OR SMARTPHONE:

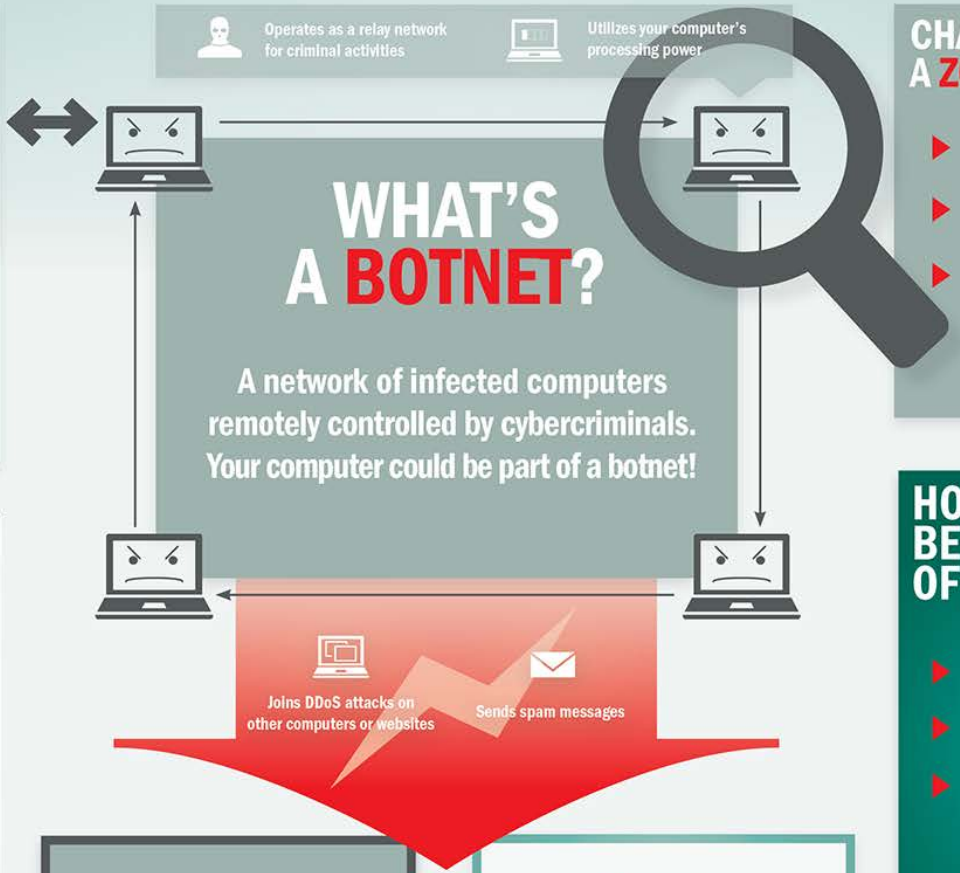
- Checks for updated malicious code
- Carries out commands
- Steals and uploads personal information

Operates as a relay network for criminal activities

Utilizes your computer's processing power

WHAT'S A BOTNET?

A network of infected computers remotely controlled by cybercriminals. Your computer could be part of a botnet!



CHARACTERISTICS OF A ZOMBIE COMPUTER

- Can be a PC, Mac or even a smartphone
- Often appears to be operating normally
- Usually has no security software or it is outdated/ineffective

WHAT ARE THE CONSEQUENCES?

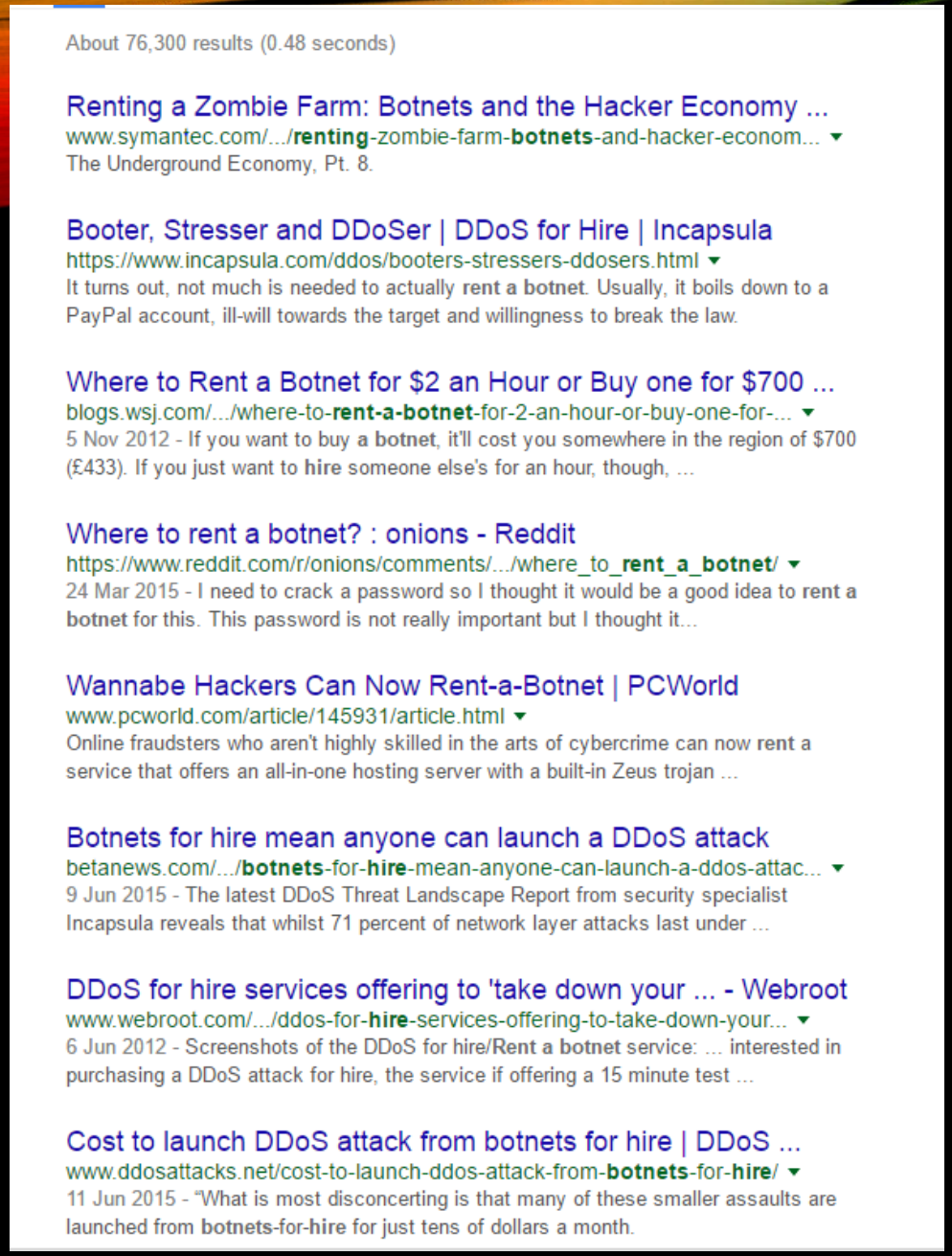
- Huge Internet bills
- Slow and unstable computer performance
- Potential legal implications if your computer is compromised
- Stolen personal data

HOW TO AVOID BECOMING PART OF A BOTNET?

- Install a proper, real-time security solution
- Ensure regular updates of installed software
- Pay particular attention to:
  - Windows Updates
  - Adobe Flash
  - Adobe Reader
  - Oracle Java
  - Your Web Browser

KASPERSKY lab

AVAILABILITY OF ACTORS



About 76,300 results (0.48 seconds)

Renting a Zombie Farm: Botnets and the Hacker Economy ...
www.symantec.com/.../**renting**-zombie-farm-**botnets**-and-hacker-econom...
The Underground Economy, Pt. 8.

Booter, Stresser and DDoSer | DDoS for Hire | Incapsula
https://www.incapsula.com/ddos/booters-stressers-ddosers.html
It turns out, not much is needed to actually **rent a botnet**. Usually, it boils down to a PayPal account, ill-will towards the target and willingness to break the law.

Where to Rent a Botnet for $2 an Hour or Buy one for $700 ...
blogs.wsj.com/.../where-to-**rent-a-botnet**-for-2-an-hour-or-buy-one-for-...
5 Nov 2012 - If you want to buy **a botnet**, it'll cost you somewhere in the region of $700 (£433). If you just want to **hire** someone else's for an hour, though, ...

Where to rent a botnet? : onions - Reddit
https://www.reddit.com/r/onions/comments/.../where_to_**rent_a_botnet**/
24 Mar 2015 - I need to crack a password so I thought it would be a good idea to **rent a botnet** for this. This password is not really important but I thought it...

Wannabe Hackers Can Now Rent-a-Botnet | PCWorld
www.pcworld.com/article/145931/article.html
Online fraudsters who aren't highly skilled in the arts of cybercrime can now **rent** a service that offers an all-in-one hosting server with a built-in Zeus trojan ...

Botnets for hire mean anyone can launch a DDoS attack
betanews.com/.../**botnets**-for-**hire**-mean-anyone-can-launch-a-ddos-attac...
9 Jun 2015 - The latest DDoS Threat Landscape Report from security specialist Incapsula reveals that whilst 71 percent of network layer attacks last under ...

DDoS for hire services offering to 'take down your ... - Webroot
www.webroot.com/.../ddos-for-**hire**-services-offering-to-take-down-your...
6 Jun 2012 - Screenshots of the DDoS for hire/**Rent a botnet** service: ... interested in purchasing a DDoS attack for hire, the service if offering a 15 minute test ...

Cost to launch DDoS attack from botnets for hire | DDoS ...
www.ddosattacks.net/cost-to-launch-ddos-attack-from-**botnets**-for-**hire**/
11 Jun 2015 - "What is most disconcerting is that many of these smaller assaults are launched from **botnets**-for-**hire** for just tens of dollars a month.

PHISHING FOR BAIT

- Different types:
  - 400 error scams
  - Bank scams
- Some of these are very realistic
- Banks don’t always help themselves

HOW DOES IT AFFECT YOU?

- Reputational loss
- Potential for damages if you can't show due care
- Copyright violations on your servers
- DDOS attacks against you