GOV<>CERT.NL

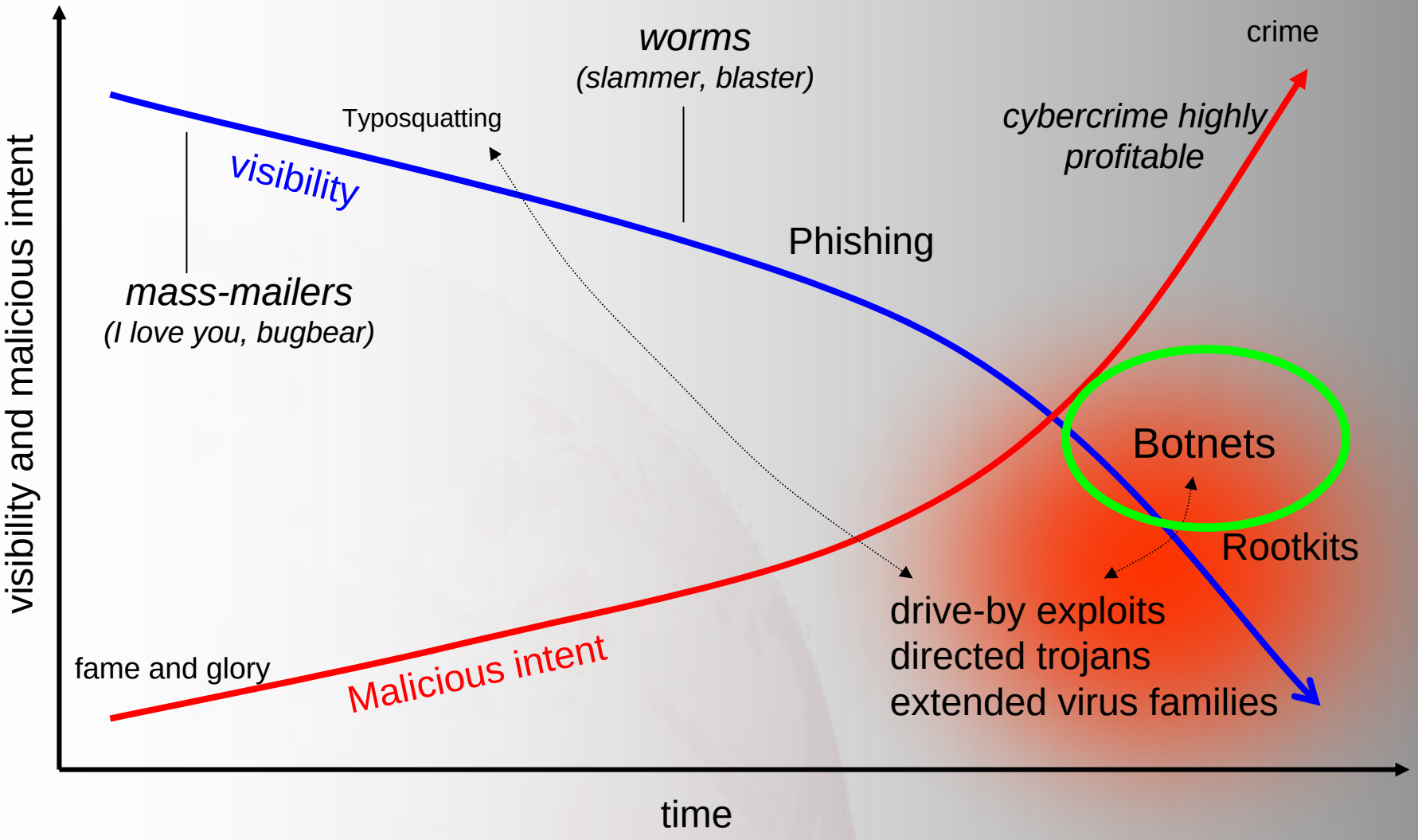
BOTNETS

Douwe Leguit, Manager Knowledge Center GOVCERT.NL

Agenda

- Bots: what is it
- What is its habitat
- How does it spread
- What are its habits
- Dutch cases
- Ongoing developments

Visibility of malware vs malicious intent



Bots – *What is it*

- autonomous program (ro*bot)*
- performs actions without user intervention
- good or bad?
  - in the security world: bot = mostly bad

- used for malicious / criminal purposes
- modular
  - keyloggers, backdoors, packet sniffers
  - update functionality
- large # of bots under one control = botnet

Bots - *habitat*

- bots prefer broadband
- bots are not picky, but prefer more recent OS
- unprotected / under protected machines

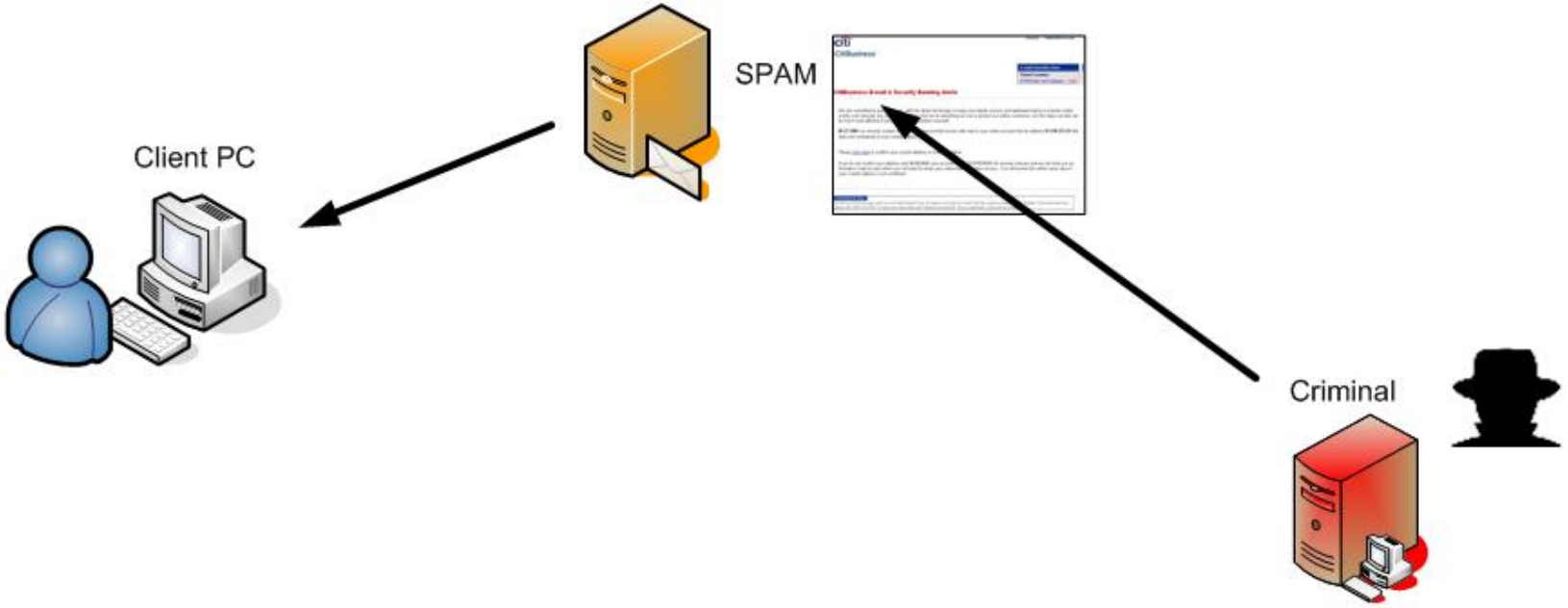
Targets:

- home computers
- corporate networks
- government agencies
- universities
- .....

Bots - *spreading*

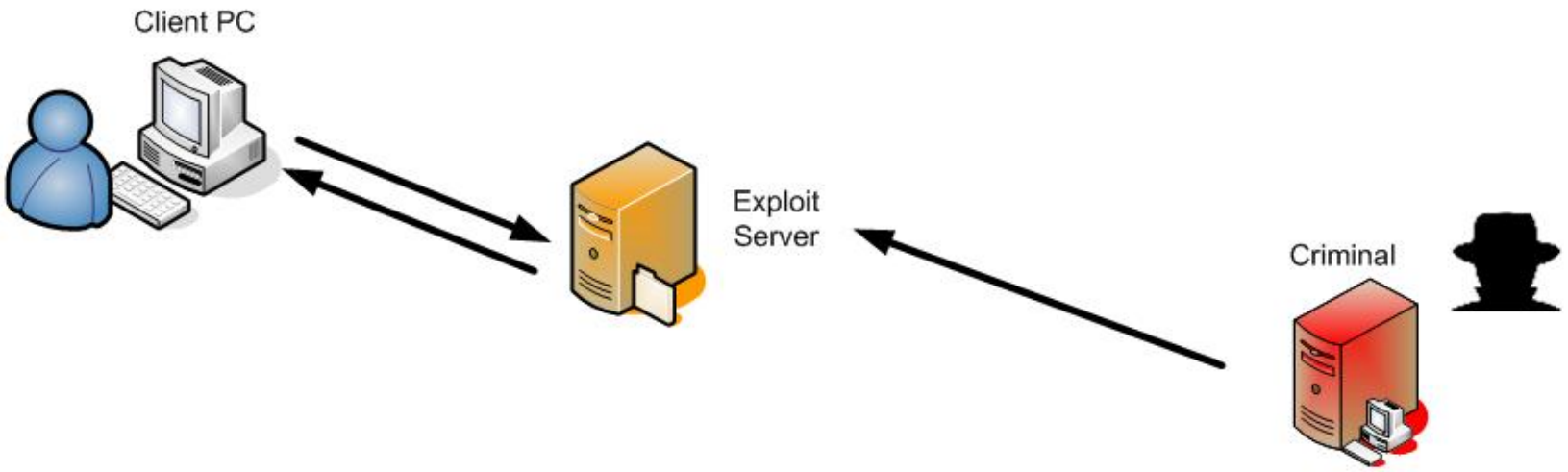
- two tier approach
  - [1] get a foothold
  - [2] scan for more victims
- bots use a variety of vectors
  - drive-by infection (exploiting vulnerabilities in browsers)
  - network infection, scansploit (lsass, dcom, asn.1 etc...)
  - IM, P2P (mostly useful for home computers)
  - e-mail

Bots - *spreading*



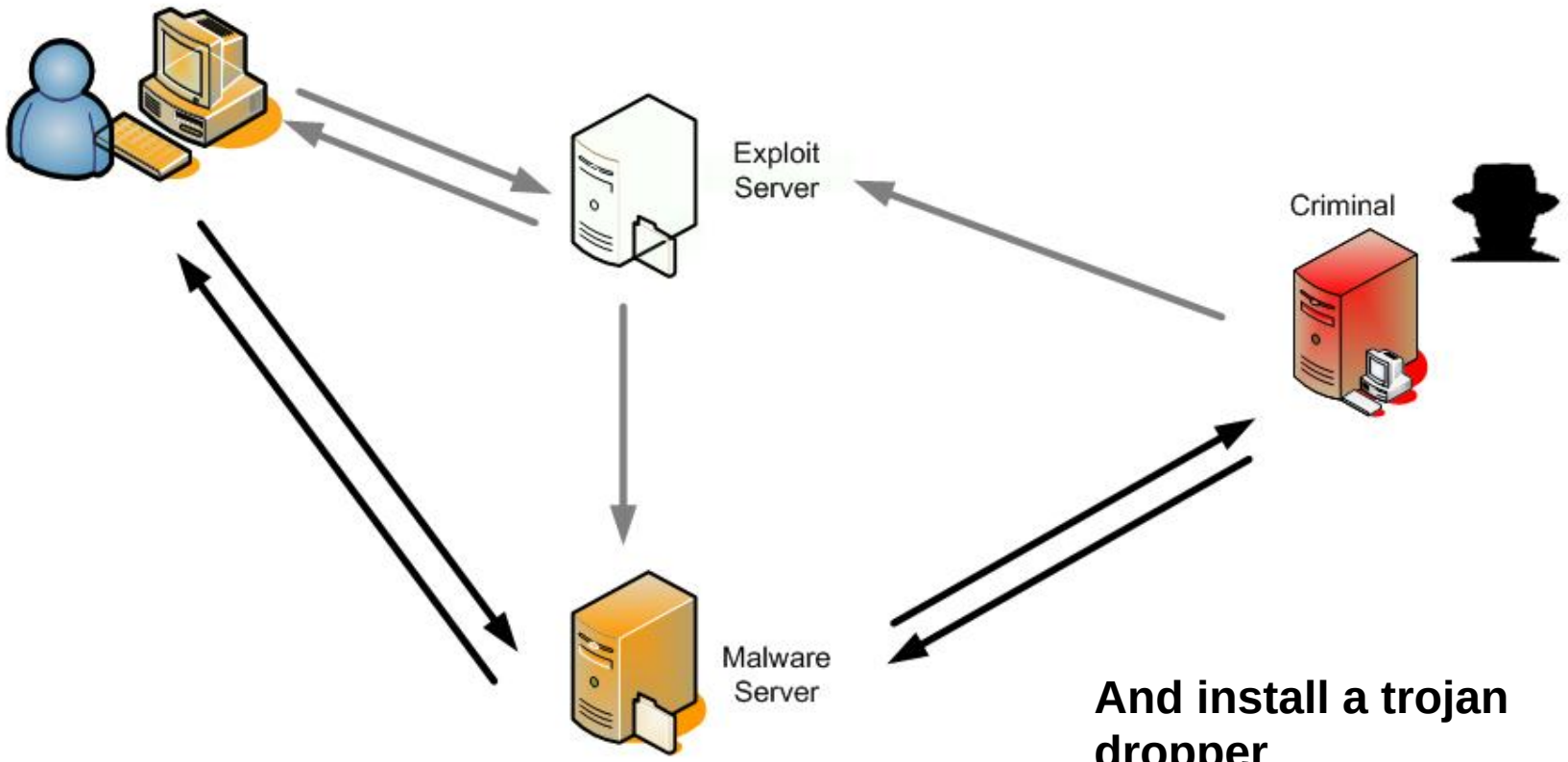
Lure end users into the trap using e.g. Spam

Bots - *spreading*



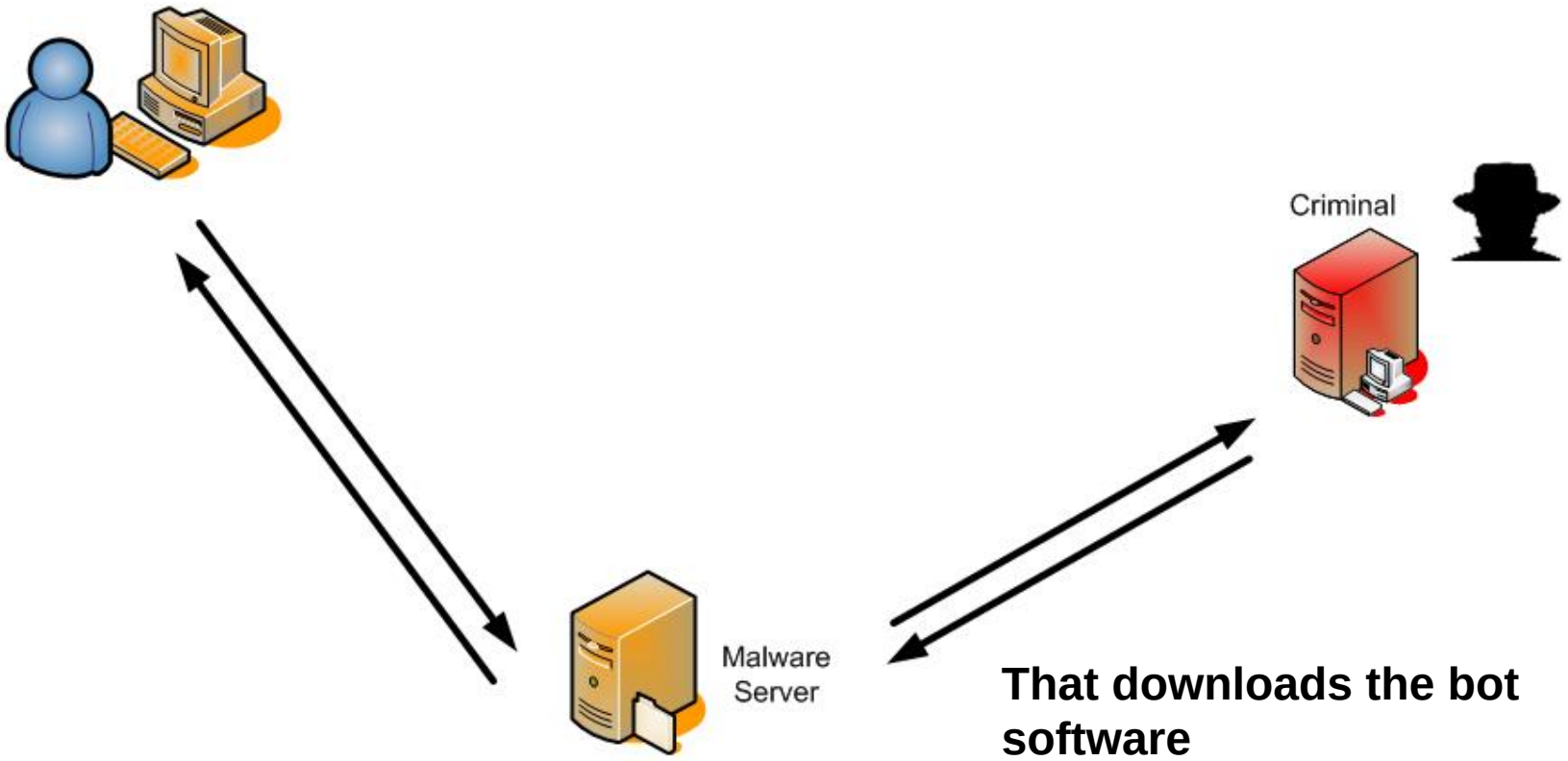
Scanning for vulnerabilities and exploiting them

Bots - *spreading*



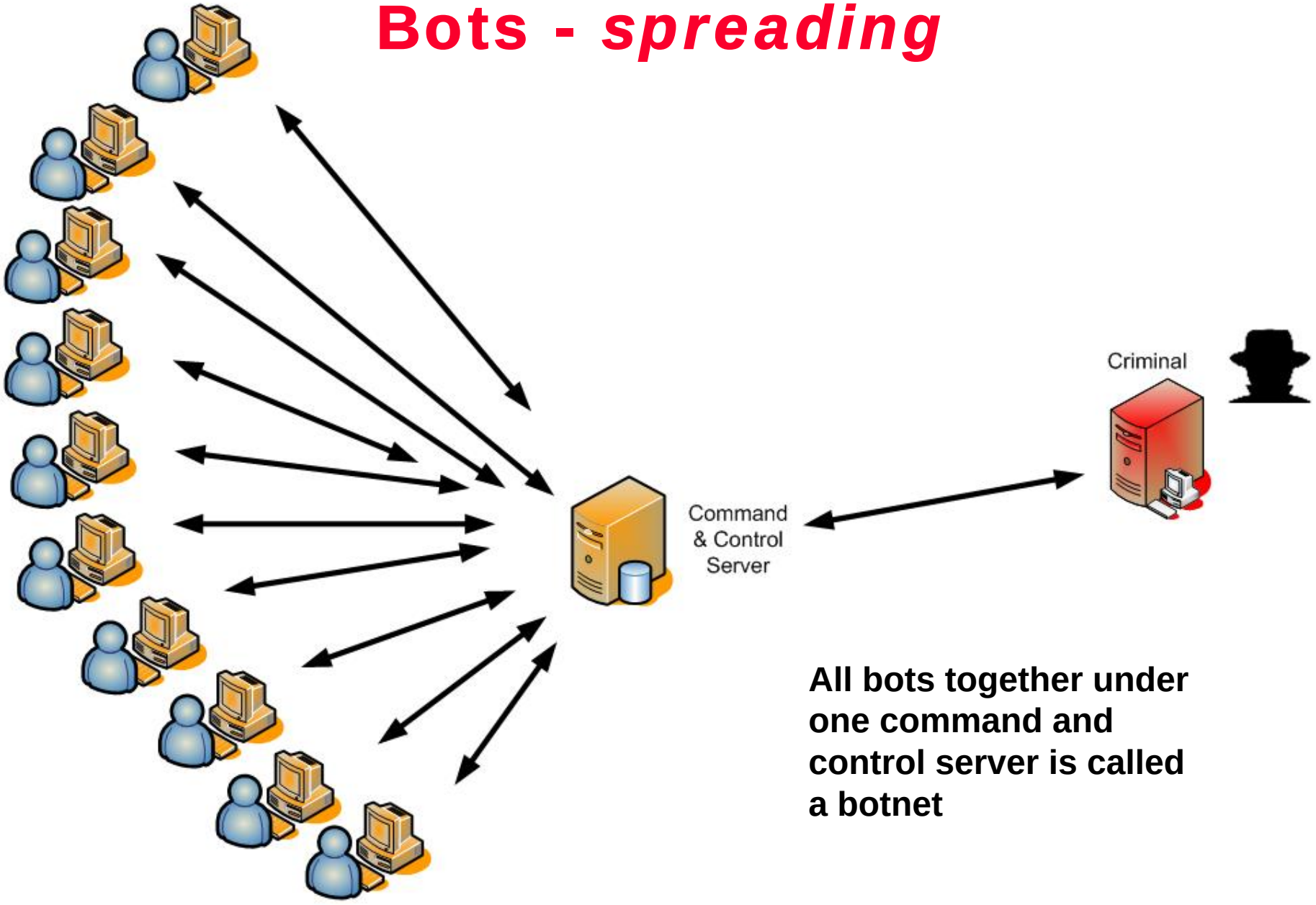
And install a trojan dropper

Bots - *spreading*



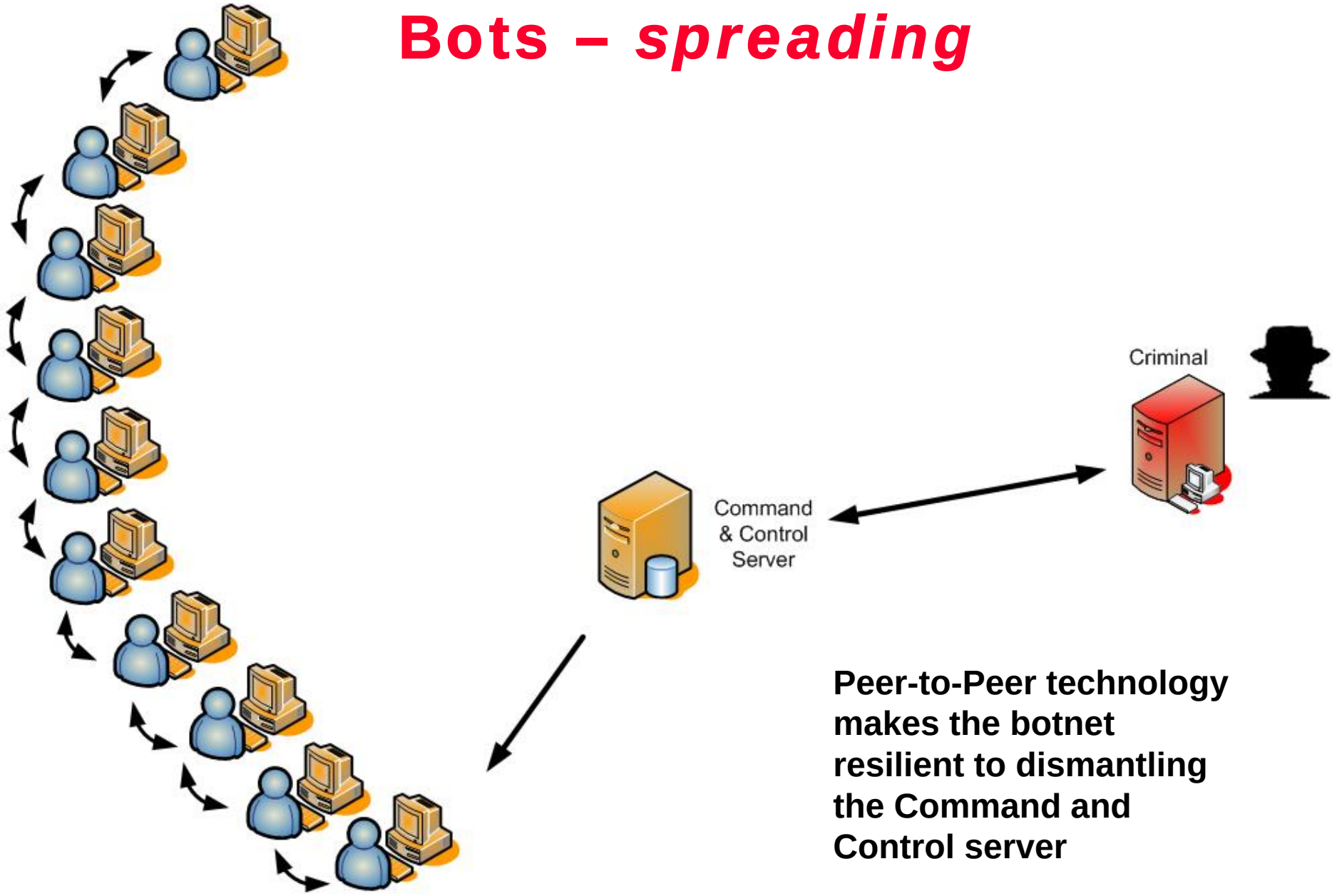
That downloads the bot software

Bots - *spreading*



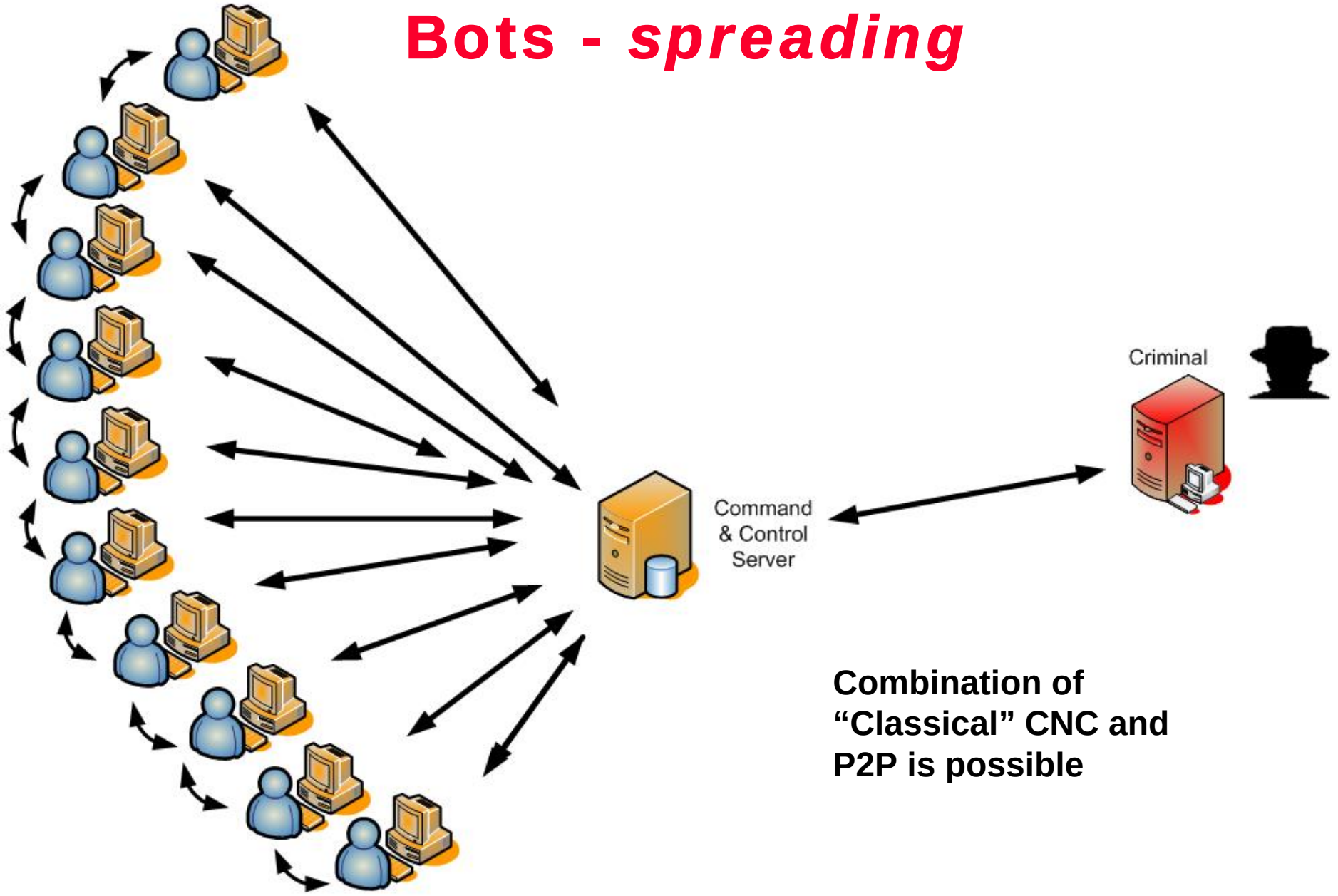
All bots together under one command and control server is called a botnet

Bots – *spreading*



Peer-to-Peer technology makes the botnet resilient to dismantling the Command and Control server

Bots - *spreading*



Combination of "Classical" CNC and P2P is possible

Bots – *habits (2)*

Multi-functional:

- **http – useful for phishing**
- **smtp – useful for spam and phishing**
- **webserver**
- **repository - piracy / data drop off**
- **dDoS agent – extortion**
- **packet sniffing / key logging / screen capturing**
- **information harvesting (serials, CD keys, banking info)**

Bots- botconomics

spam

phishing and scams

fake websites

dDoS-attacks

proxies

Botnet-PC's

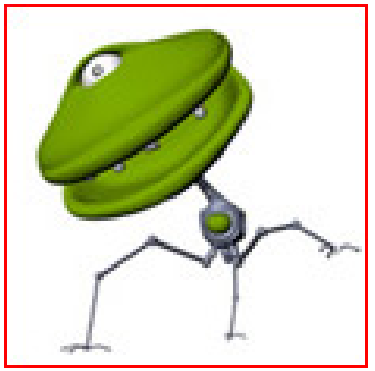
virusses,
worms,
backdoors,

Information
Harvesting

22 April 2007

CASE 1: Toxbot - botnet

- Large botnet, “made in Holland”
- Conviction early 2007
- Public Prosecutor:
  - ‘… ten thousands of compromised computers, but probably millions …’
  - ‘… extortion …’
  - ‘… creditcard and transaction data stolen …’
  - ‘… confidence in internet affected …’



Press release: 1.5 Million unique IP addresses

22 April 2007

Toxbot – *botnet information*

Bots reside in:

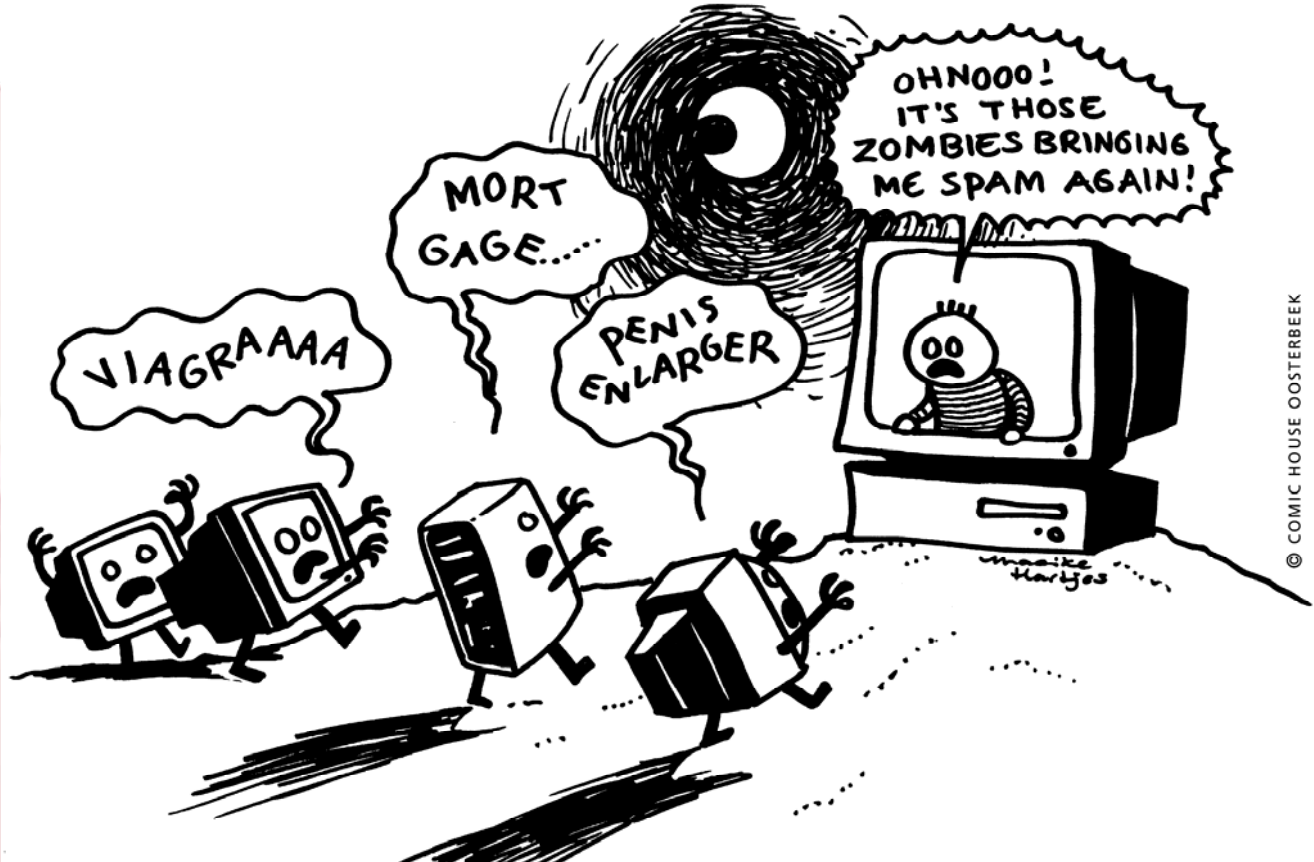
- **Italy**
- **Netherlands**
- **France**
- **USA**
- **Belgium**
- **UK**
- **Eastern Europe**
- **Middle East**

What it sniffed

- Banks
- eBay
- PayPal
- Hotmail / MSN Messenger
- Airlines / Various travel agencies
- Several Universities
- Yahoo! / Google Mail / Webmail in general
  - Including .gov.cn, .gov.ae, .gov.in, etc
- Medical Transcription Services / Online pharmacies / Hospitals
- Online games / Poker / Betting
- Online dating / sex sites
- ... & much more.

Bots - *Scam and Spam*

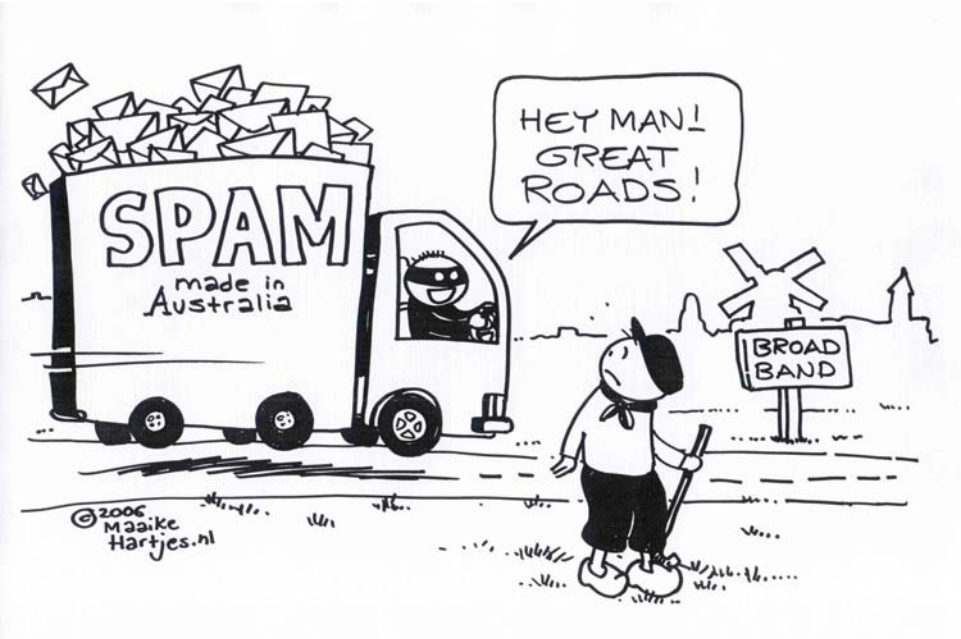
- Still very profitable
- Increase in targeted spam and scam



CASE 2: SPAM via botnet

- Conviction of a Dutch spammer febr. 2007
- 9 billion spam emails
- In 14 months

He used a botnet of only 700 zombie pc's!



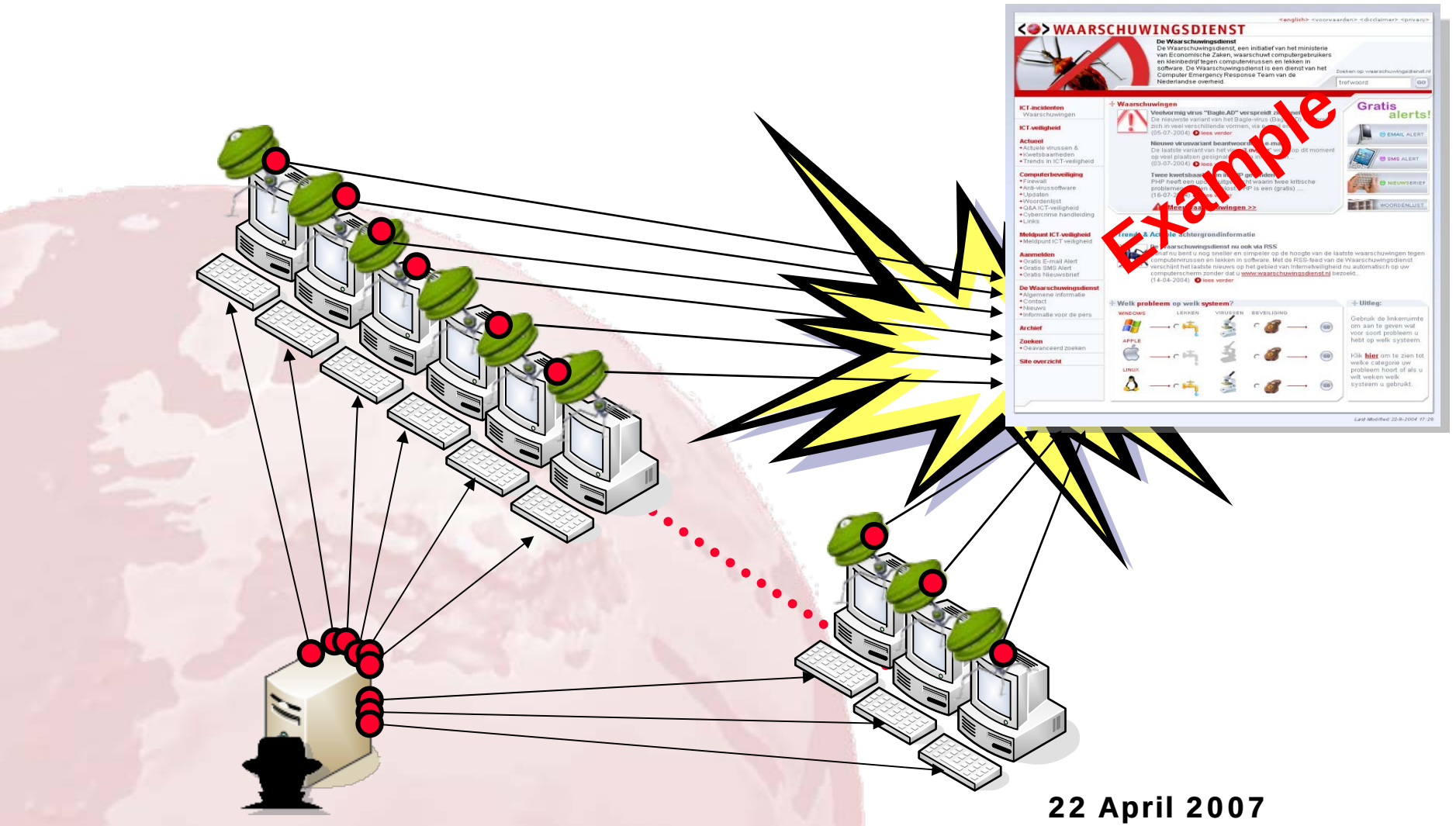
CASE 3: dDoS via botnet

- Early October 2004
- Target: several public government sites
- dDoS attack almost for a week

They used a botnet of 4000 bots!

dDoS: distributed Denial of Service

Overheid.nl – 3 October 2004



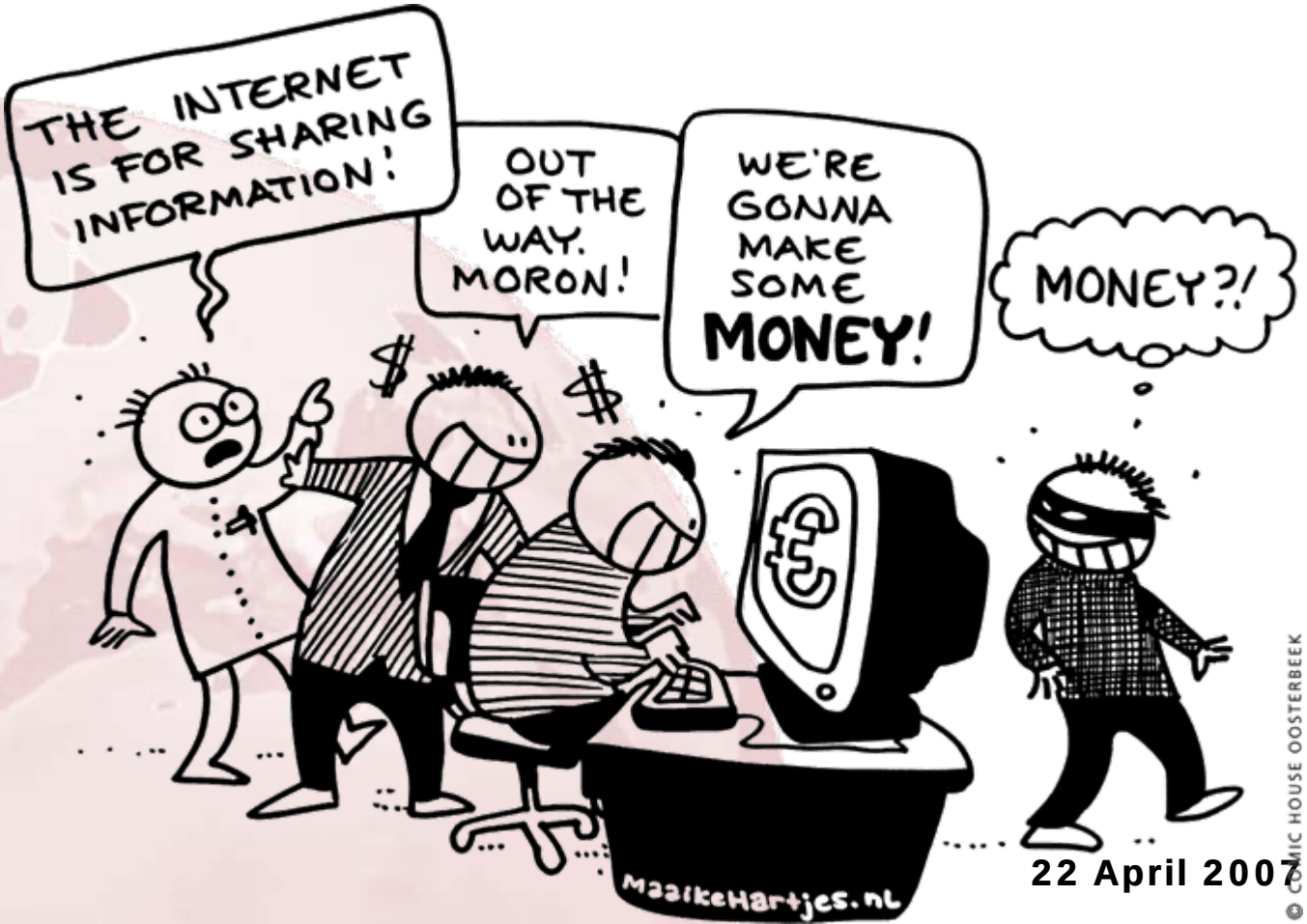
Bots - *developments*

- Botnets are the infrastructure for Cyber Crime
- Criminals will protect their assets

- Recent activity in the P2P space
- Encryption and root kit technology introduced
- Focus on small botnets to prevent detection
- Development is a professional business
- Improvement on functionality

Thank you!

Douwe Leguit
Douwe.Leguit@govcert.nl



22 April 2007