The Evolution of Computer Security Attacks and Defenses

Angelos D. Keromytis
Columbia University
angelos@cs.columbia.edu

This talk

- A look at the evolution of:
  - nature of attackers and their goals
  - cyber attacks and defenses (techniques)
- Hard research problems
  - balance of technology, economics and usability
- Embedded systems are constrained yet powerful
  - already targets of attack

Important caveats

- No such thing as a “secure” system
- No broad definition of attack
    - attacks will follow path of least resistance
        - sometimes, non-technical means can be used
- No good, broad metrics for system security

Traditional security considerations

- Confidentiality, Integrity, Availability
  - systems vs. information
  - military/intelligence vs. commercial world
- Initial focus on isolated systems (e.g., mainframes)
  - “data at rest”
  - threat model focusing on data exfiltration and corruption/modification

Network Security

- Focus on protection of data in transit
    - e.g., cryptographic protocols
- Use of distributed systemsto improve AIC
    - secret sharing
    - Byzantine Fault Tolerance
    - redundant data storage

The Internet

- Physical security measures become inadequate
- Attacks come from anywhere, anytime
  - Attribution becomes difficult
- High degree of attack automation
  - Manual reaction becomes impossible
- Complexity and scale
  - Difficult to distinguish legitimate vs. attack traffic

Source: New Yorker

"On the Internet, nobody knows you're a dog."

Phase 1: Hacking for fun (1969-1995)

- Attacker goal: gain access to remote system(s)
- Motivation: mostly curiosity
  - some cases of espionage (read “Cuckoo’s Egg”)
  - large-scale “accidents” (1988 Internet Worm)
- Methods: password guessing, bad configuration, viruses, trojan horses
  - buffer overflow attacks make guest appearances (more in the next lecture!)

Problems exposed

- User-friendly password hardening
  - users set/remember weak passwords
  - two-factor authentication is cumbersome
- Configuration management
- Virus detection
  - esp. in the face of polymorphism/metamorphism
  - NP-hard problem

Phase 2: Casual hacking (1995-2001)

- Attacker goal: gain access to remote systems
- Motivation: “showing off”, publicity
- Methods: buffer overflows, email viruses/ attachments

Additional problems exposed

- Software hardening is an active research area
  - better tools/languages for development and QC
  - post-development hardening (runtimes)
  - compromise detection (intrusion detection)
- Performance is a big issue
- Adoptability by developers an issue in some cases

Phase 3: Amateur hacking (2001-2005)

- Attacker goal: attract attention through large-scale activities
- Motivation: publicity and money
- Methods: denial of service attacks, worms
- Botnets start appearing, rootkits in wide use

Worms

- Self-propagating code operating over a network
  - related to computer viruses
- High-profile worms: Slammer, Blaster, Welchia, Code Red, Melissa,
- Three components
  - target selection
  - infection vector
  - payload

Worms (cont.)

- Target selection
  - random scanning vs. hitlist (pre-scanning)
  - global vs. local preferences
- Infection vector can vary significantly
  - buffer overflows
  - auto-execute attachments
  - email attachments that users click on

Worms (cont.)

- Payload (other than further target acquisition)
  - for many years, none
  - occasionally, destructive payload (e.g., erase HDD)
  - today, bot agents, rootkits and other malware

Speed of worms

- CodeRed (2001) infected at least 250K hosts over a few days
- Slammer (2003) infected ~100K hosts in <10 minutes
  - infected embedded systems (ATMs, nuclear power plant, etc.)
- Academic worms designed to infect 1MM hosts in .5s

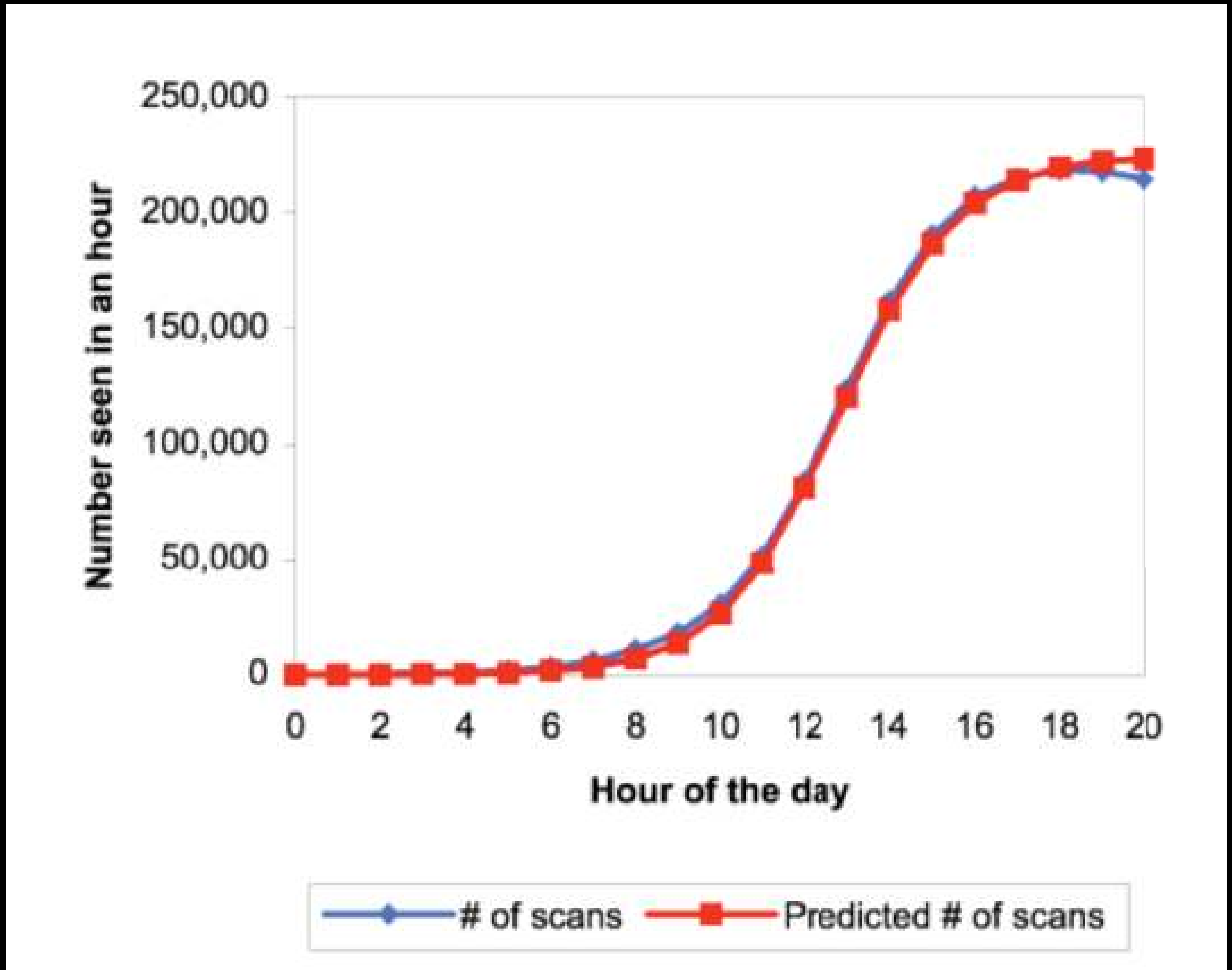
Worm propagation model

- Worms follow model for epidemic diseases

$$\frac{di}{dt} = \beta i(1-i)$$

b is contact rate

i is # of infected hosts

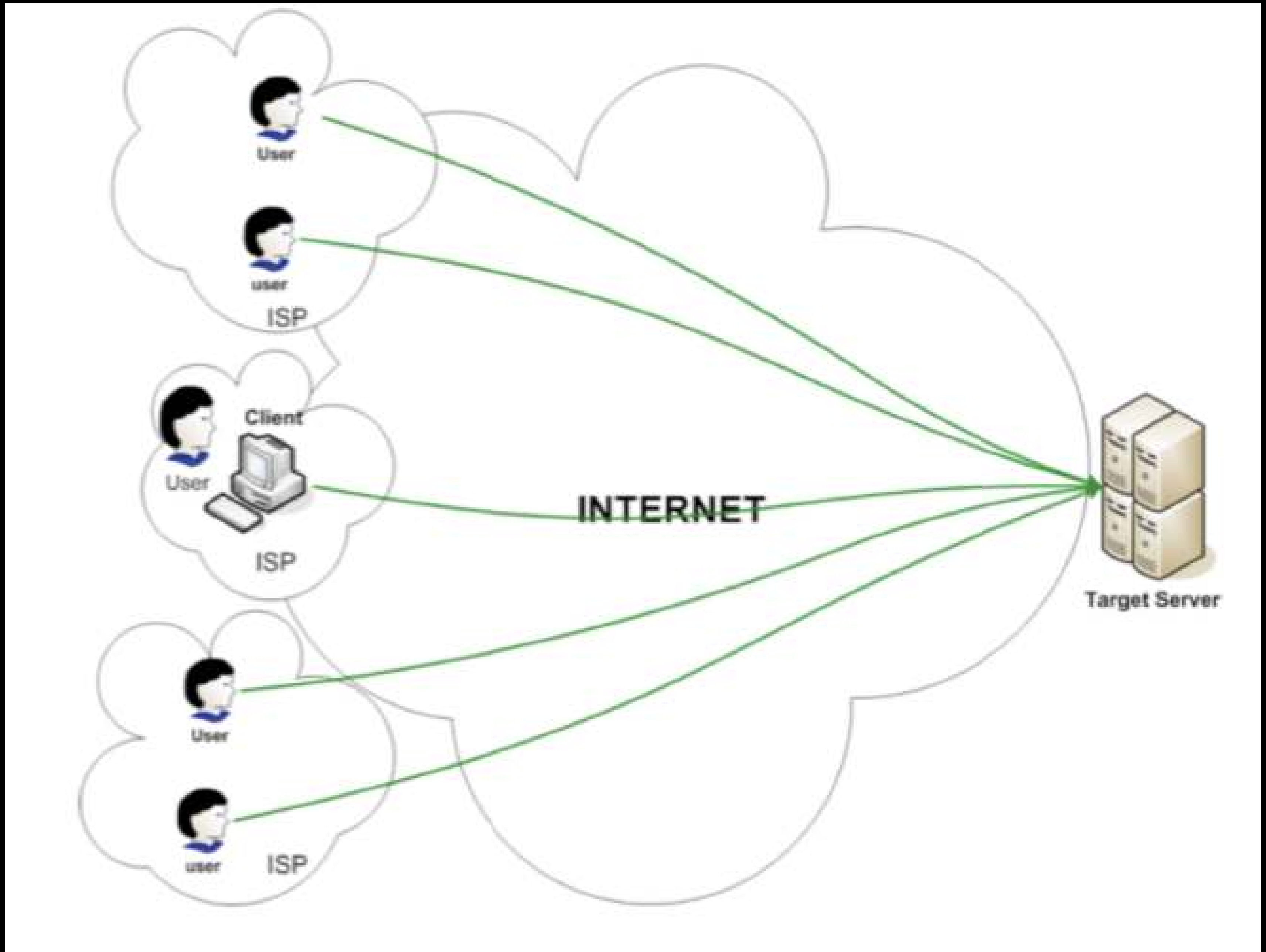


“How to 0wn the Internet in Your Spare Time”, Staniford, Paxson, Weaver
USENIX Security 2002

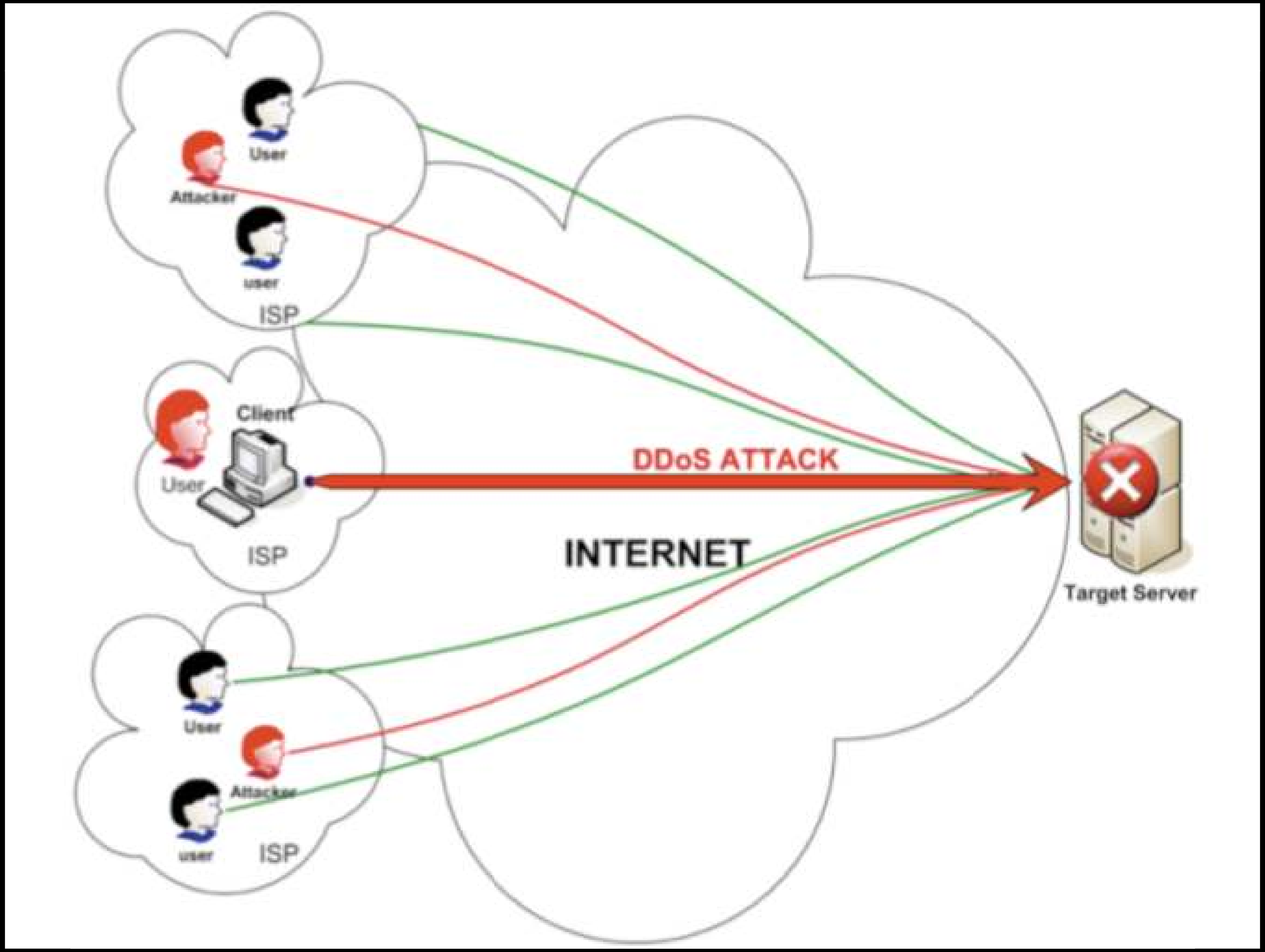
Additional problems exposed

- How do we detect the early stages of an epidemic?
  - sensor types, deployment hurdles, accuracy
- How do we stop/contain an epidemic?
  - quarantine
  - aggressive filtering
  - anti-bodies
- How do we disinfect a compromised system?

Denial of service attacks



Denial of service attacks



DDoS

- TCP traffic will back off
- Other protocols will content with attack traffic
  - we have seen attacks as large as 10Gbps or more
    - attack on Estonia (May 2007)
  - Used for extortion or revenge/spire
    - Cloud9 ISP (2002)

Defenses

- Most ISPs use blackholing
  - more advanced ISPs may use redirection+cleaning
- End customers may use multi-homing or a CDN
  - not helpful/possible in many scenarios
- Several research proposals
  - traceback, capabilities, overlays, migration

Additional problems exposed

- Detect and filter DDoS traffic
  - accuracy problem: flash crowds vs. DDoS
  - protocol-specific attacks can be very low rate
  - who bears the deployment and operational cost?
- Counter/mitigate DDoS attacks
  - replication- and overlay-based techniques
  - network capability models

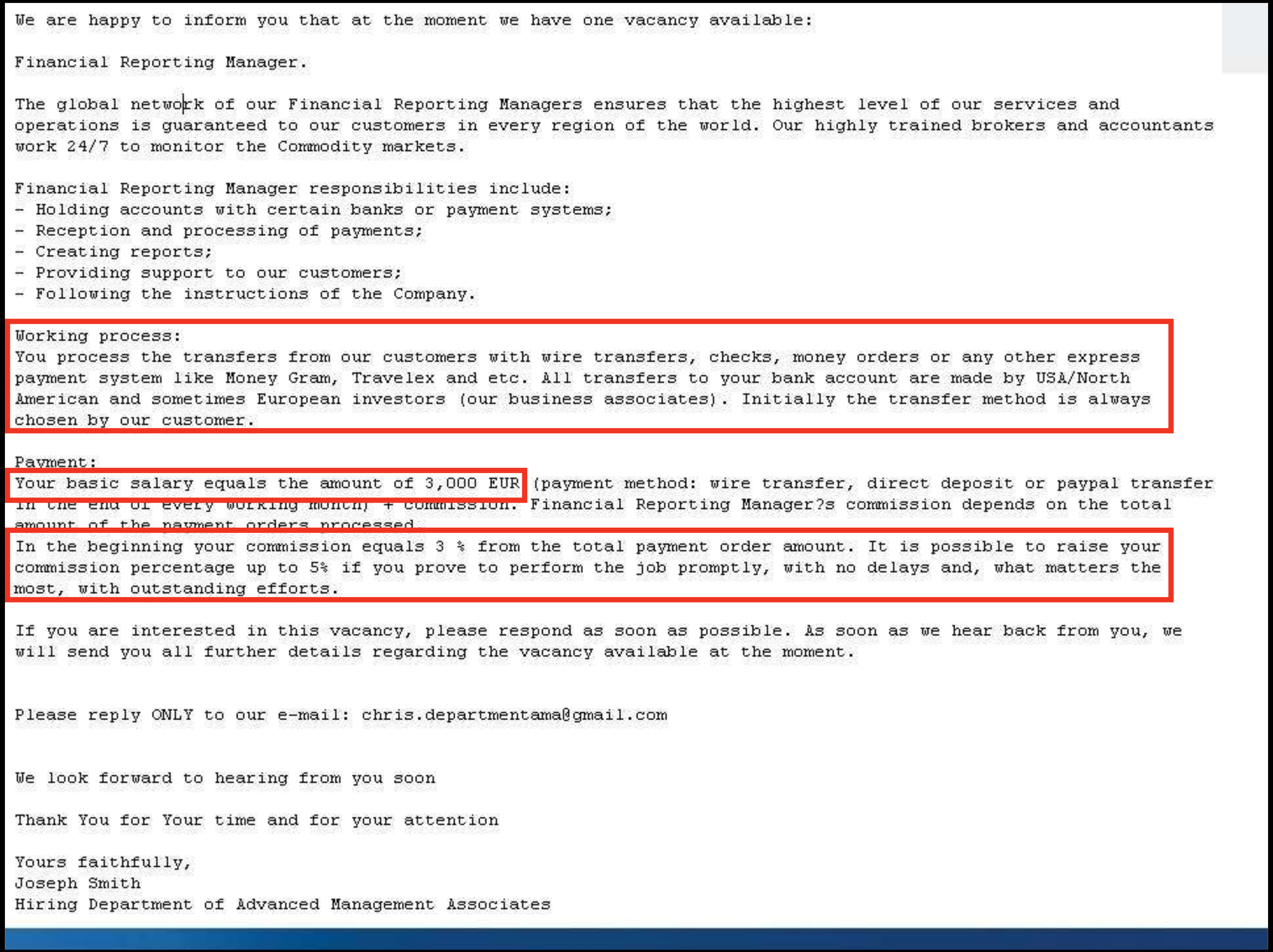
Phase 4: Professional hacking (2005-...)

- Attacker goal: account and system compromise, identity theft, information exfiltration
- Motivation: $$$
- Methods: web attacks, phishing/pharming, spear-phishing, and anything that works
    - the term "malware" comes into wide use
- Large-scale botnets, hacking as professional service

Profit sources

- Email spam using compromised hosts
- Extortion (DDoS, data as hostage, ...)
- Identity theft & fraud
  - credit cards, loans, bank accounts, etc.
- Software piracy
- Re-selling access to botnets
- Large support economy

Support economy



We are happy to inform you that at the moment we have one vacancy available:

Financial Reporting Manager.

The global network of our Financial Reporting Managers ensures that the highest level of our services and operations is guaranteed to our customers in every region of the world. Our highly trained brokers and accountants work 24/7 to monitor the Commodity markets.

Financial Reporting Manager responsibilities include:
- Holding accounts with certain banks or payment systems;
- Reception and processing of payments;
- Creating reports;
- Providing support to our customers;
- Following the instructions of the Company.

Working process:
You process the transfers from our customers with wire transfers, checks, money orders or any other express payment system like Money Gram, Travelex and etc. All transfers to your bank account are made by USA/North American and sometimes European investors (our business associates). Initially the transfer method is always chosen by our customer.

Payment:
Your basic salary equals the amount of 3,000 EUR (payment method: wire transfer, direct deposit or paypal transfer in the end of every working month) + commission. Financial Reporting Manager?s commission depends on the total amount of the payment orders processed.
In the beginning your commission equals 3 % from the total payment order amount. It is possible to raise your commission percentage up to 5% if you prove to perform the job promptly, with no delays and, what matters the most, with outstanding efforts.

If you are interested in this vacancy, please respond as soon as possible. As soon as we hear back from you, we will send you all further details regarding the vacancy available at the moment.

Please reply ONLY to our e-mail: chris.departmentama@gmail.com

We look forward to hearing from you soon

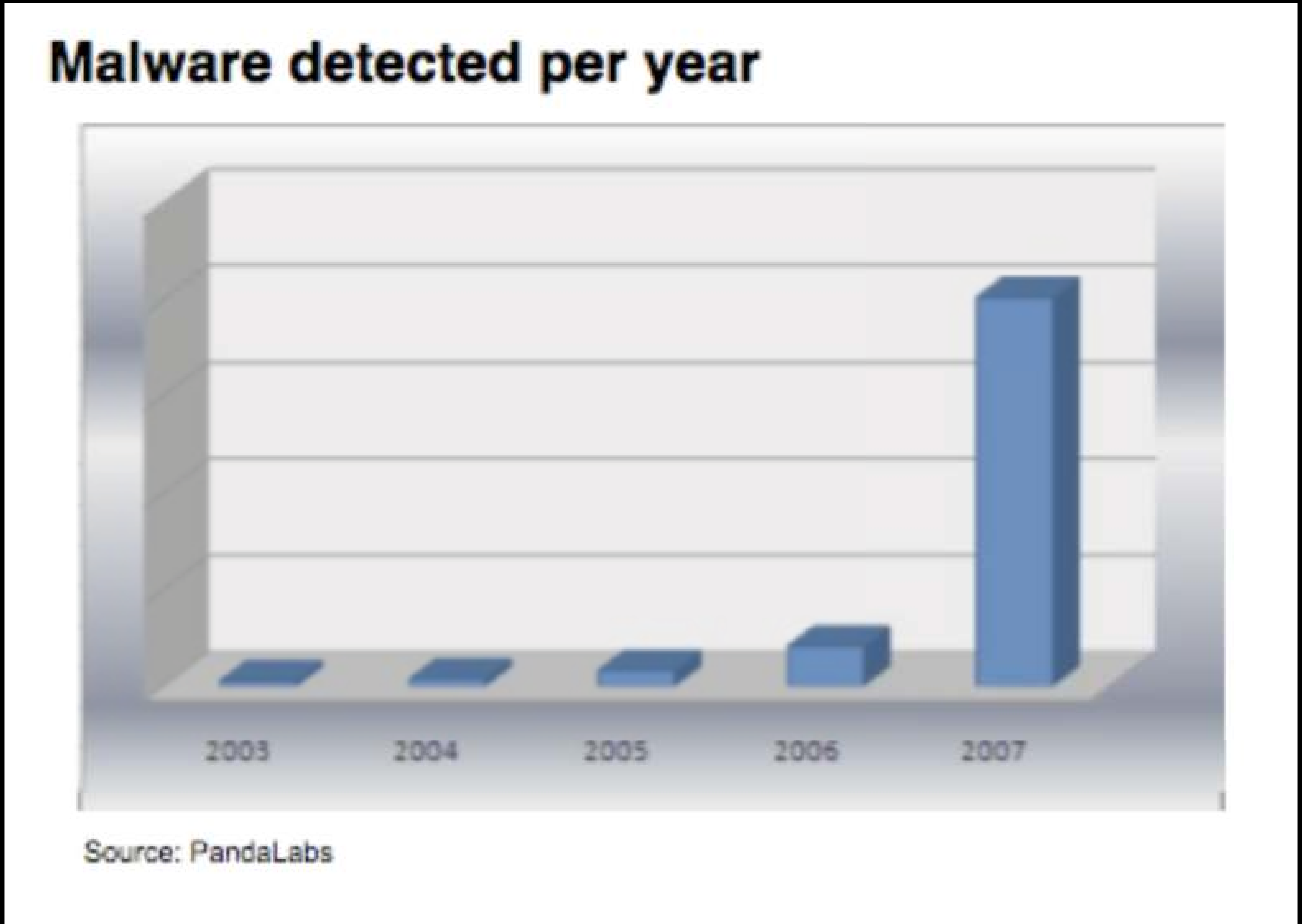
Thank You for Your time and for your attention

Yours faithfully,
Joseph Smith
Hiring Department of Advanced Management Associates

Information is money

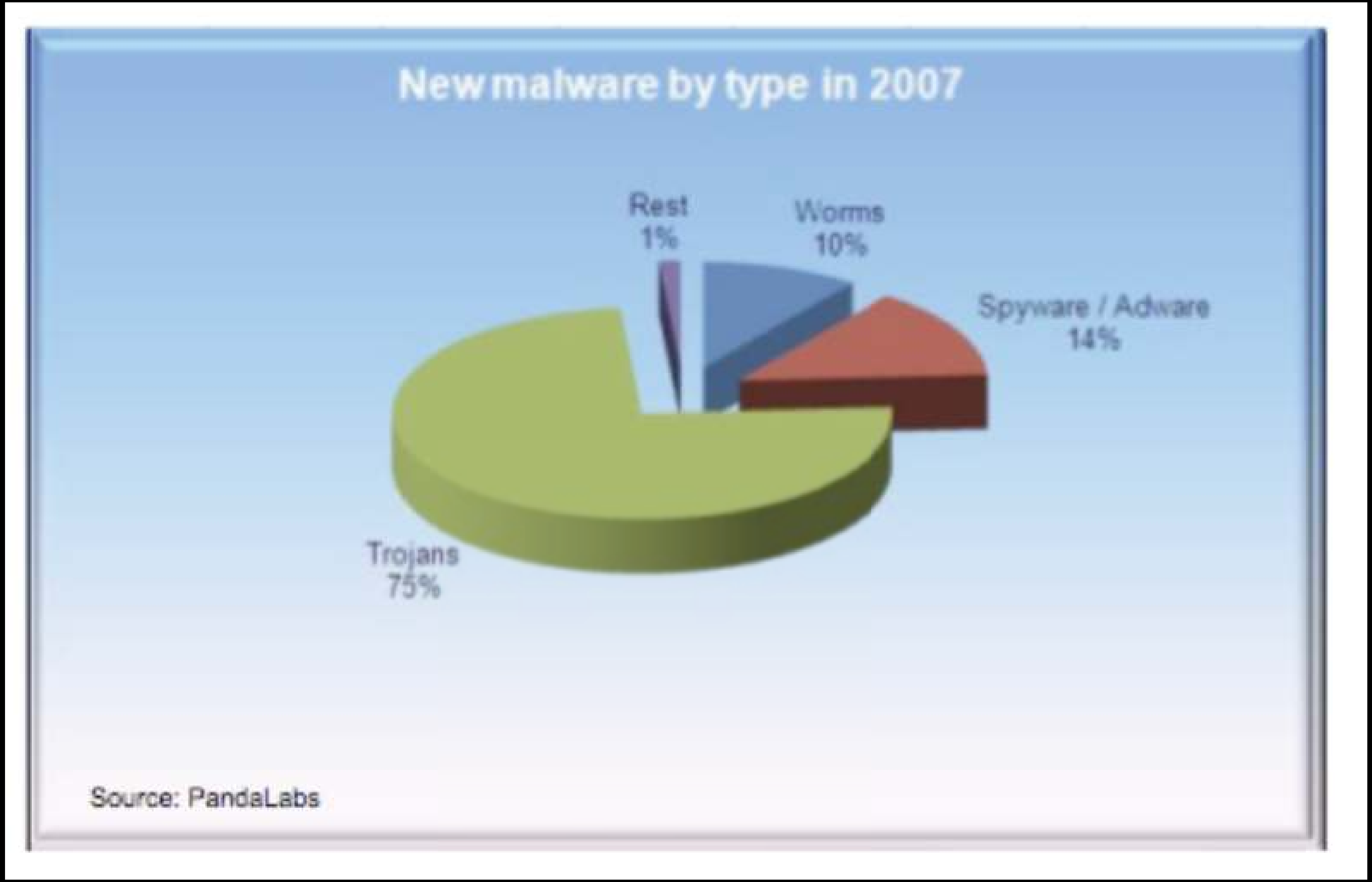
- Stolen accounts
  - account for FTP access: US$1
  - ICQ account: $1 - $10
- Credit cards
  - VISA/MC: $2/card for 1-10 cards; $1.5 for 10-100
  - AmEx: $2.5/card for 1-10 cards; $2 for 10-100
- Passports: $5

Scale of the problem



Source: PandaLabs

Malware



Source: PandaLabs

Additional problems exposed

- Attackers expose user-interface issues or "features"
  - "security must be invisible" doesn't work!
  - security and usability emerges as research area
- Passwords are huge liability
  - what other technology is cost-effective and accessible to users?
- How do we detect and eliminate rootkits?
- Attacker focus increasingly on data, not systems

Currently...

- Organized crime has taken over online fraud
- Cyber-warfare actively pursued by >130 countries
  - mostly oriented toward espionage (information exfiltration)
  - also building up capabilities (tools, botnets, access) in case of conflict
- SCADA systems are being actively targeted
  - (often severe) impact on real world

Current/traditional defenses

- Perimeter access control (e.g., firewall)
    - but, everything is being routed over HTTP...
- Signature-based intrusion detection (e.g., anti-virus)
- Traffic encryption protocols (IPsec, SSL)
- Password-cracking/checking tools

Defenses

- Access control
  - integrated access control across enterprise
- Authentication
  - two-factor authentication
  - credential management
  - secure password protocols

Defenses (cont.)

- Intrusion & anomaly detection
  - host vs. network dichotomy
  - behavior modeling
    - training on “dirty” data
    - allergy attacks
    - false positives vs. false negatives

Defenses

- Cryptography
  - lifecycle protection of data
  - zero-knowledge proofs
  - operation on encrypted data
- Software hardening
  - better languages and tools
  - adaptive, “self-healing” systems

Why is it so difficult?

- We operate a fundamentally open environment
  - contrast the Internet with POTS
- Code (or "code-like" data) may be found everywhere
  - see next lecture!
- Halting problem makes malware detection intractable
- Security almost always added as afterthought

The good news

- Security is a very hard problem
    - there will always be need for it
- Exciting, “target rich” research area
- Many opportunities for real-world impact