Spam, Malware and Cybercrime

John R. Levine

CAUCE North America

CANTO August 2014

John.levine@cauce.org

Spam

- Fake drugs
- Porn
- One Million Dollars
- ...

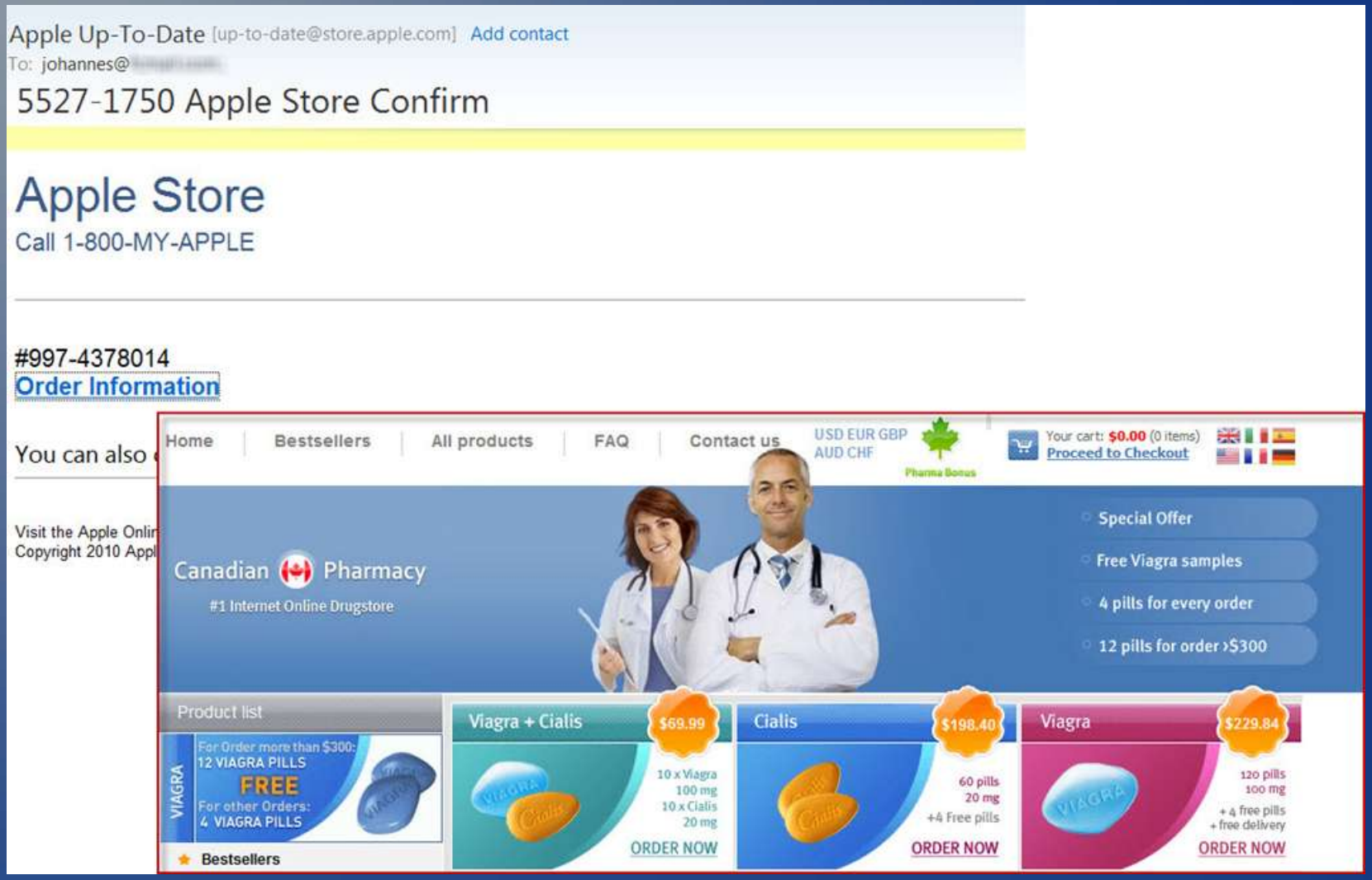
Spam ➔ Web

- Click on this link for ...
- Fake drugs
- Phishing
- Porn
- ...

Spam ➔ Web ➔ Malware

- **Malicious or hacked site**
- **Installs malware**

Phishing


Apple Up-To-Date [up-to-date@store.apple.com] Add contact
To: johannes@
5527-1750 Apple Store Confirm
Apple Store
Call 1-800-MY-APPLE
#997-4378014
Order Information
You can also
Visit the Apple Onlir
Copyright 2010 Appl
Home
Bestsellers
All products
FAQ
Contact us
USD EUR GBP
AUD CHF
Pharma Bonus
Your cart: $0.00 (0 items)
Proceed to Checkout
Canadian Pharmacy
#1 Internet Online Drugstore
Special Offer
Free Viagra samples
4 pills for every order
12 pills for order >$300
Product list
For Order more than $300:
12 VIAGRA PILLS
FREE
For other Orders:
4 VIAGRA PILLS
VIAGRA
Bestsellers
Viagra + Cialis
$69.99
10 x Viagra 100 mg
10 x Cialis 20 mg
ORDER NOW
Cialis
$198.40
60 pills 20 mg
+4 Free pills
ORDER NOW
Viagra
$229.84
120 pills 100 mg
+ 4 free pills
+ free delivery
ORDER NOW

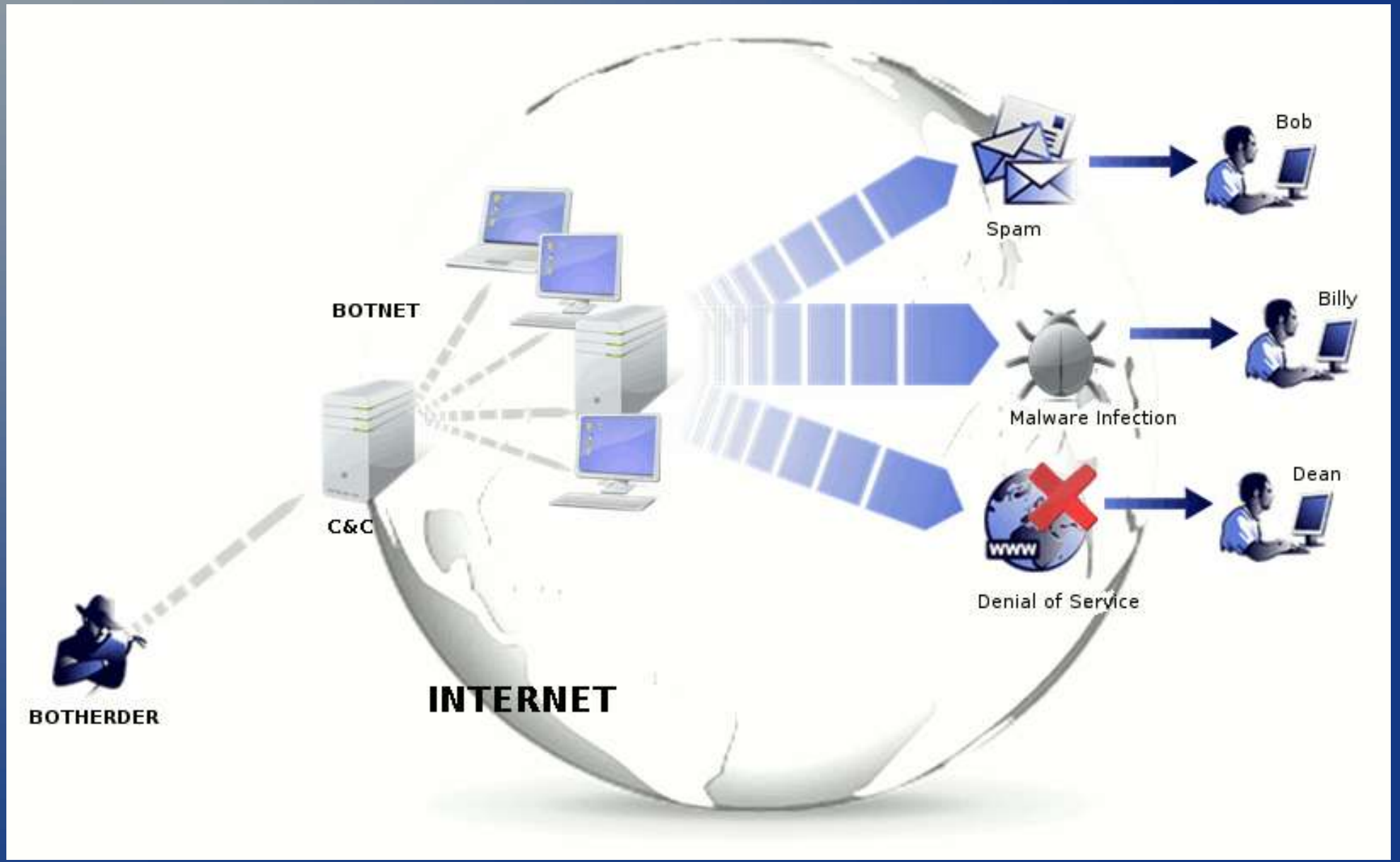
Attacking your users

- **Adware: shows annoying ads**
  - May replace legit ads
- **Clickware: fake clicks**
  - “Man in Browser” clicks on ads
- **Credential theft: online accounts**
  - Steal mail and web logins
  - Send spam as your user

Attacking your users

- **Credential theft: financial accounts**
  - Steal banking credentials
  - Insert fake transactions with real ones

Botnets


Bob
Spam
BOTNET
Billy
Malware Infection
C&C
Dean
www
Denial of Service
INTERNET
BOTHERDER

Botnets

- Hijack computer to send spam
  - Provokes complains
  - Wastes your bandwidth
  - Gets your network blocked
- Hijack computer for Denial of Service
  - Wastes a *lot* of bandwidth
  - May get you blocked

Botnets

- Hijack computer as malware host
  - Temporary or proxy web server
  - Wastes your bandwidth
  - Considered antisocial
- Hijack computer for other purposes
  - This month's special:
    Bitcoin mining

Countermeasures

- Stop outgoing spam
- Cooperate to detect and stop abuse
- Share data
- Build capacity

Outgoing spam

- Filtering
- Authentication

DKIM.org

DMARC.org

Cooperation

- Best Current Practices
- Feedback loops
- Data providers
- Ad-hoc groups
- Trade associations

Best current practices (BCP)

- Port management
- Botnet mitigation
- Acceptable User Policies (AUP)

Feedback loops

- Tell senders about their spam
- User reports
- Spam traps

Data providers

- **Spamhaus**
  - Shares with trusted providers
- **Specialists**
  - Team Cymru
  - Return Path
  - Etc.

Ad-hoc groups

- **Fight specific issues**
- **Trust-based Communities**
  - Conficker Working Group
  - Torpig Working Group
  - Mariposa Working Group
  - DNS Changer Working Group

Public/Private initiatives

- Convened by FCC in the United States
- Mostly private members
- Recommendations not binding but persuasive

Intergovernmental groups

- London Action Plan
- ICPEN
- Interpol

CERTs

- Computer Emergency Response Team
- Generally national or regional
- Some public, some private
- Tend to have interesting meetings

Spam, Malware and Cybercrime

John R. Levine

CAUCE North America

CANTO August 2014

John.levine@cauce.org