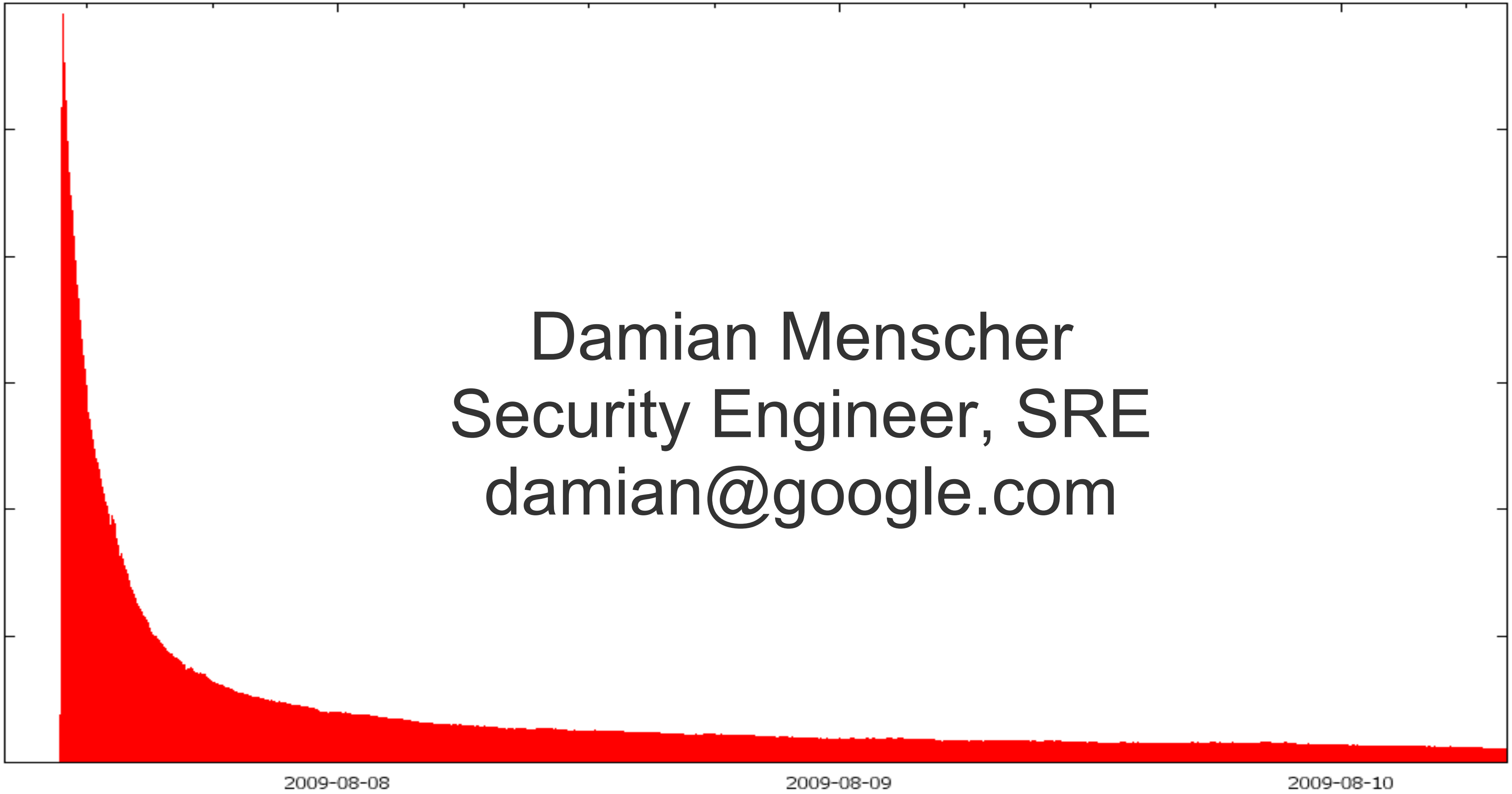
Botnet Attacks: Defense and Offense



Damian Menscher
Security Engineer, SRE
damian@google.com

Non-DDoS Bot Activities

Goal is to get user credentials: bank; credit card; corporate

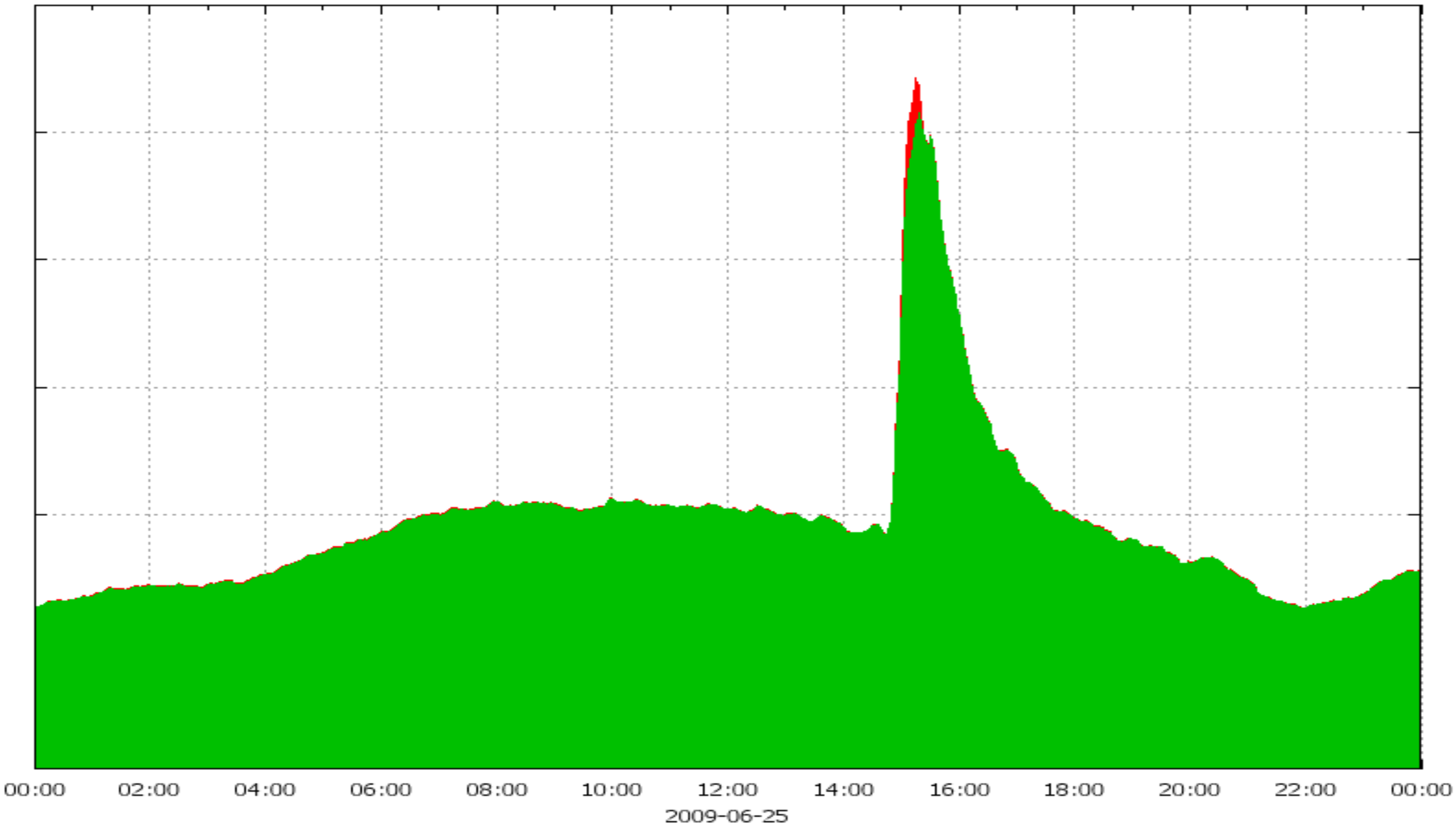
- harvest directly off of compromised machines
- compromised servers can host DNS and pharma sites, or promote fake AV
    - find them using search worms
- create email accounts to send spam lures
    - hijack email accounts you can't create (using shared passwords with compromised sites), use botnet to log in and send the spam

How does the bot know it's got an internet connection?

Try fetching the google.com homepage!

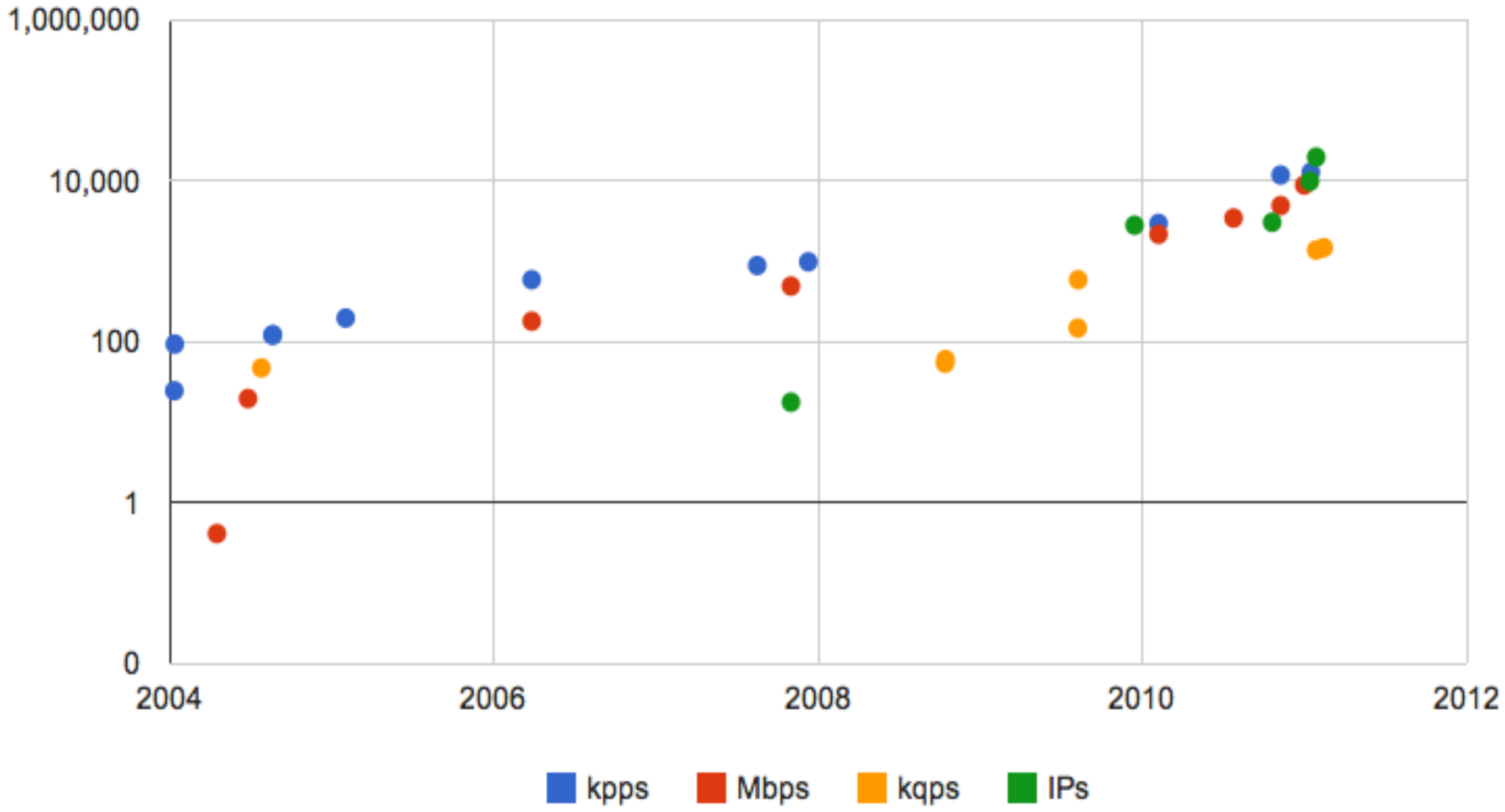
Google™

Defender's View

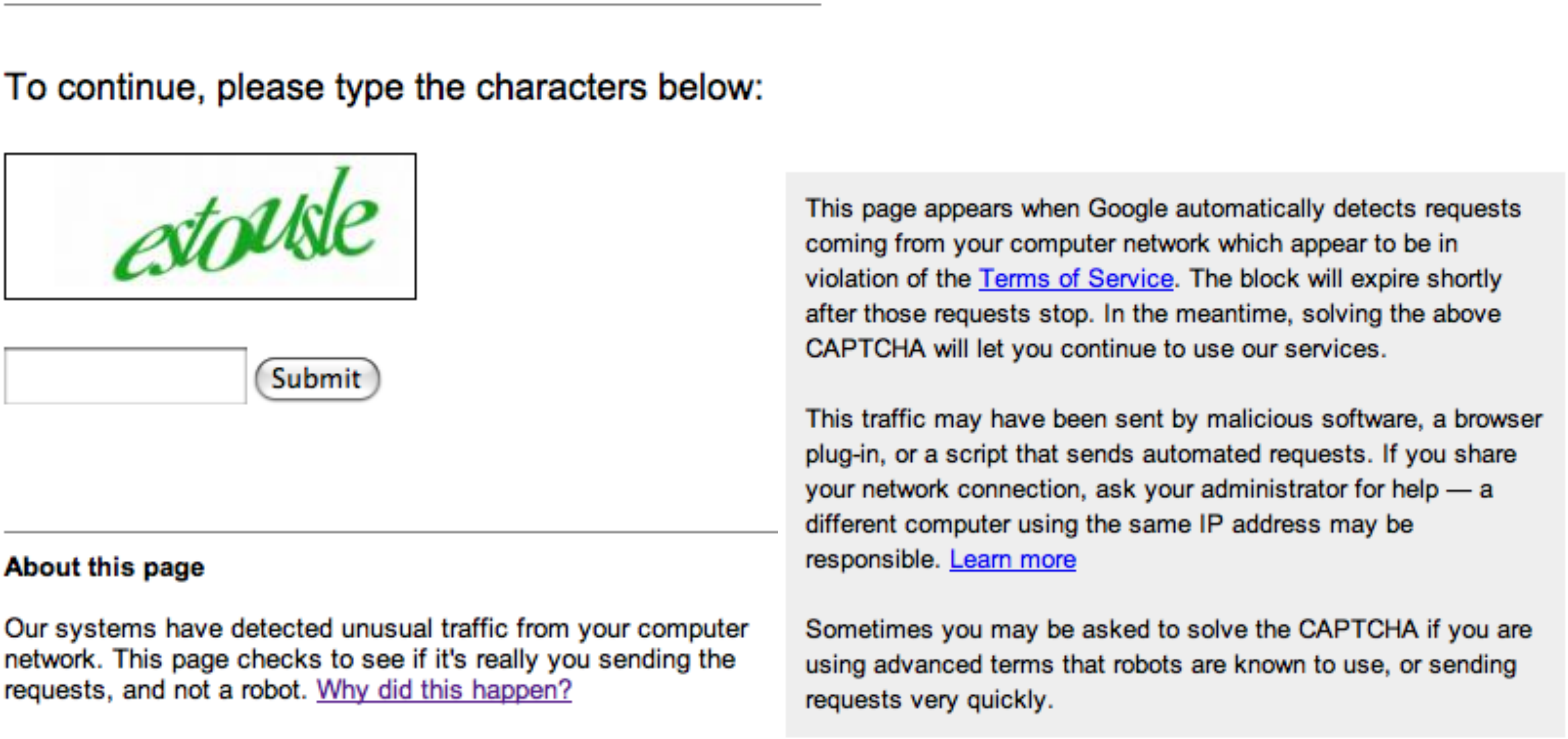


Attack, or real users? (hint: Google News)

DDoS Attack Trends



What about False Positives?



To continue, please type the characters below:

About this page

Our systems have detected unusual traffic from your computer network. This page checks to see if it's really you sending the requests, and not a robot. Why did this happen?

This page appears when Google automatically detects requests coming from your computer network which appear to be in violation of the Terms of Service. The block will expire shortly after those requests stop. In the meantime, solving the above CAPTCHA will let you continue to use our services.

This traffic may have been sent by malicious software, a browser plug-in, or a script that sends automated requests. If you share your network connection, ask your administrator for help — a different computer using the same IP address may be responsible. Learn more

Sometimes you may be asked to solve the CAPTCHA if you are using advanced terms that robots are known to use, or sending requests very quickly.

Captcha Solvers

nopho
pices
reehos
72316
minas
ruest
persess
rotter
cheot
gewin
backy
58519
18275
supse
Google

"Seize, retain, and exploit the initiative"

Attacker

- untraceable
- laws irrelevant
- multiple tries
- millions of machines
- reuse botnet to attack other targets

Defender

- fixed name in DNS
- can't violate laws
- single outage is bad
- limited budget
- each defender must construct their own defenses

2008: Russia-Georgia conflict

- Attacks on Georgia sites by "patriots"

2009: Attempt to silence a prominent blogger

- Aug 6: attacked multiple companies
- Aug 7: attack returns, more focused

Shut Down Command and Control?

- Bulletproof hosting
  - How long did it take to shut down McColo?
- Jurisdiction issues
  - Is the activity illegal in the source jurisdiction?
  - Is dealing with it a priority?
  - Sometimes government will "look the other way"
    - Russian attacks on Georgia were by "patriots"
- P2P control
- Leaves infected machines behind
  - What about user education?

Doesn't seem to be working

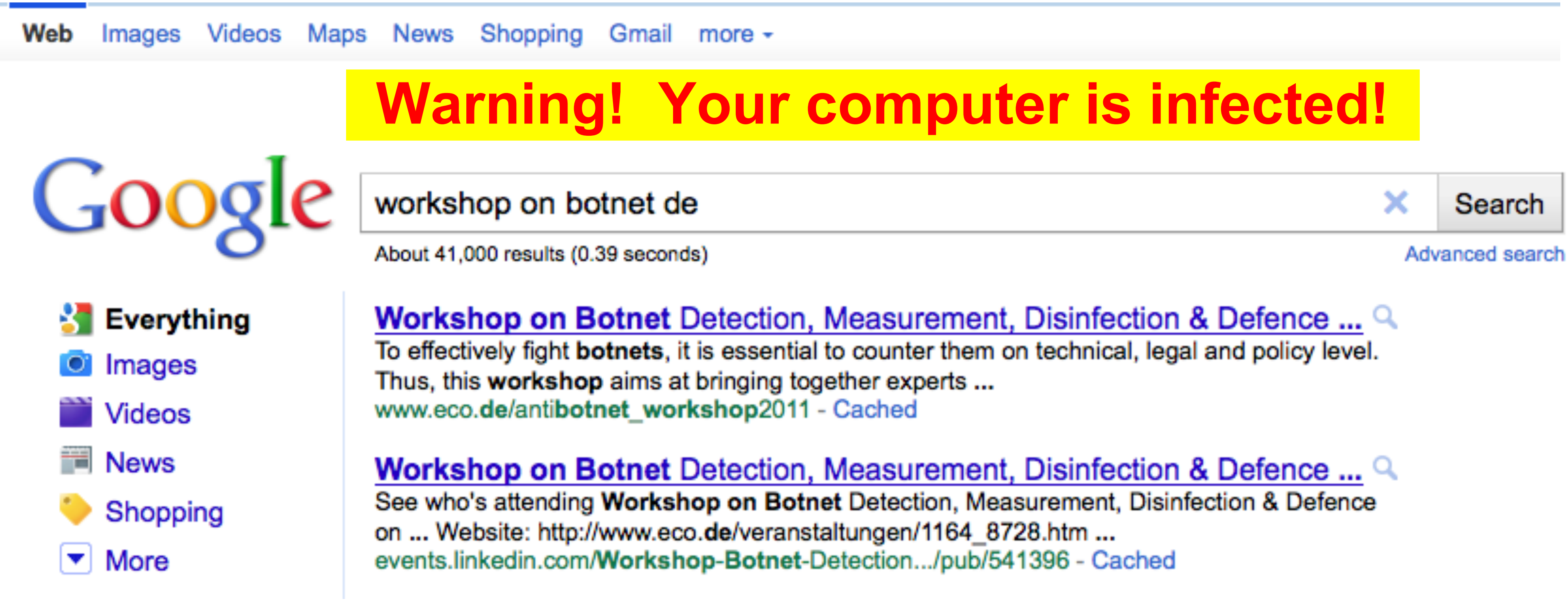
Notify ISPs?

- Who do you tell?
- What do you tell them?
  - Can you share a list of IPs?
- Why should they believe you?
  - Would you believe it if someone claimed you were infected?
- Can the ISP identify the infected user, or just the person who pays the bill?
- What are users expected to do upon receiving notification?
- Can ISPs afford the customer support costs?

Most ISPs do nothing

Notify Users?

What if...



Warning! Your computer is infected!

workshop on botnet de

About 41,000 results (0.39 seconds)

Workshop on Botnet Detection, Measurement, Disinfection & Defence ...
To effectively fight **botnets**, it is essential to counter them on technical, legal and policy level. Thus, this **workshop** aims at bringing together experts ...
www.eco.de/antibotnet_workshop2011 - Cached

Workshop on Botnet Detection, Measurement, Disinfection & Defence ...
See who's attending **Workshop on Botnet** Detection, Measurement, Disinfection & Defence on ... Website: http://www.eco.de/veranstaltungen/1164_8728.htm ...
events.linkedin.com/Workshop-Botnet-Detection.../pub/541396 - Cached

Can users clean their own machines?

Antivirus catch rate: ~30%

User Perspective on being 0wned

Case study:
Users can't log in due to malware that changes their router's DNS to hijack www.google.com to some other IP

> If this is 'not a Google problem' then why does Hotmail work perfectly fine?

> Is Google working on this or are you guys just waiting for the anti-virus/malware companies?

> I've heard rumors of a Google OS. Sure hope they fix the security problems before that hits the market.

Malware Vulnerabilities?

- All software has bugs
  - This includes malware!

- Identify malware vulns and forcibly clean machines
  - What if you make a mistake?
  - Who should do it?
    - Non-profit?
    - Government? Which?
    - Who do you trust?

- Responsible disclosure to the botnet owner? At least then the bot can't be re-compromised....

Practical Offense

Botnets are a growing threat, and the attacker has a distinct advantage.

Q: What should we do?

A: Shut down C&Cs*
B: Notify ISPs*
C: Notify Users
D: Exploit Malware Vulnerabilities*
E: All of the above

* Laws are currently inconsistent

Questions?

damian@google.com

(we're hiring)