Cybercrime

TEAM CYMRU
WWW.CYMRU.COM

John Kristoff jtk@cymru.com

Agenda

- Who am I?
- Who is Team Cymru?
- What does cyber crime look?
- How does DNS play a role?
- What can you do?
- Q&A

whoami

- Network engineering and security practitioner
- Many formative years in U.S. .edu environment
- DNS-related work led me to UltraDNS (Neustar)
- Now almost 5 years with Team Cymru
- Managing director for Dragon Research Group
- “I don't know Perl, I know **combat** Perl”

The One-time Face of Cyber Crime

```
<a> i need 50 roots k?
<b> k ill send them after u put $50
    in my paypal
<a> $50? u can get a lot more shells
    or ccs instead
<b> ya but i can go to the movies
    with $50
```

Welcome to the UE 2013!

Goldinstalls PayPerInstalls (PPI)

http://goldinstalls.org

Мы платим хорошую цену за установку. Мы принимаем в каждой стране.

Всегда предоставлять FUD EXE. Мгновенный статистики. Быстрые выплаты.

Цены:

What We've Seen in 2013-01

- Over 1,400 DDoS targets, or ~2 per hour
- 928,588 distinct IRC, IRC?!?! bots
- Over 1.3 million web-based bots
- Over 20, yes two-zero, million spam sources
- A new piece of malware every 1.7 seconds

Recent UE Price List

```
+ US: (vis,mas) = 3$/1cvv
+ Germany:
    Master,visa = 19$/1cvv
    Amex,discover = 23$/1cvv
+ Switzerland:27$/1cvv
[...]
Hacked bank accounts ...
  Balance 7000$ = 300$
  Balance 14000$ = 500$
  Balance 18000$ = 800$
[...]
  Paypal with balance 3000 = 200$
  Paypal with balance 5000 = 350$
  Paypal with balance 7000 = 500$
```

Motivation

- Money
- Politics
- Retribution
- Thrill
- Opportunity

The Subsystem Known as DNS

- The Internet, a huge, complex, man-made system
- The DNS is arguably one of two of key subsystems
  - the other being routing (BGP)
- Technically we don't need DNS, practically we do
- If you can control or influence the DNS
  - you can direct users wherever they ask to go
  - or not
  - i.e. scams, denial of service, extortion

Common DNS Threats

- Fraudulent domain name registrations
- Domain name registration hijack
- Domain name hijack
- Denial of Service, packet floods

Fraudulent Domain Name Registrations

- Hmmm...

```
Registrant Name: Jon Christoff
Registrant Company: DBag Research, Inc.
Registrant Email Address: dwha...
Registrant Address: 1 Washington Blvd.
Registrant City: Chicago
Registrant State/Region/Province:
Registrant Postal Code: 60604
Registrant Country: US
Registrant Tel No: +1.7734042827
Registrant Fax No:
```

Domain Name Registration Hijack

```
Technical Contact:

 OWNED NETWORK OPERATIONS
   ROOT
   US
   DESTROYED, MA 02139-4307
   UNITED STATES
   (617) 253-1337
   owned@mit.edu

Name Servers:
   FRED.NS.CLOUDFLARE.COM
   KATE.NS.CLOUDFLARE.COM

Domain record activated:    23-May-1985
Domain record last updated: 22-Jan-2013
```

Domain Name Hijack (poison)

- dns-operations list Subjects in 2012-10
  - “Massive DNS poisoning attacks in Brazil”
  - “AT&T DNS Cache Poisoning?”
- Neither were
- Most turn out to just be bad cache behavior
- I've never actually seen it and I've tried finding it
- It is a real threat, but... not commonly exploited
- But, DNSSEC finally saw some deployment! :-/

Domain Name Hijack (theft)

- Walled garden
- Sinkhole
- System compromise
  - e.g. “DNSChanger

Denial of Service, packet floods

The DNS 'IN ANY' Attacks

- Current, ongoing, very annoying activity
- Q: “Tell me all your know about .CH” (~50 bytes)
- A: “SOA, RRSIG, DNSKEY, NS...” (~1800 bytes)
  - greater than 35 to 1 amplification
  - some answers are even bigger

What Can You Do?

- Monitor and log as much as you can
- Know what normal is, so you know when it's broken
- Help enforce anti-spoofing mechanisms
- Help ensure good data gets into the system
- Be helpful and know how to get help

Q&A

- We're here to help

  http://www.team-cymru.org

  info@cymru.com

- As am I:

  http://www.cymru.com/jtk/

  jtk@cymru.com