Studying the GR Botnet

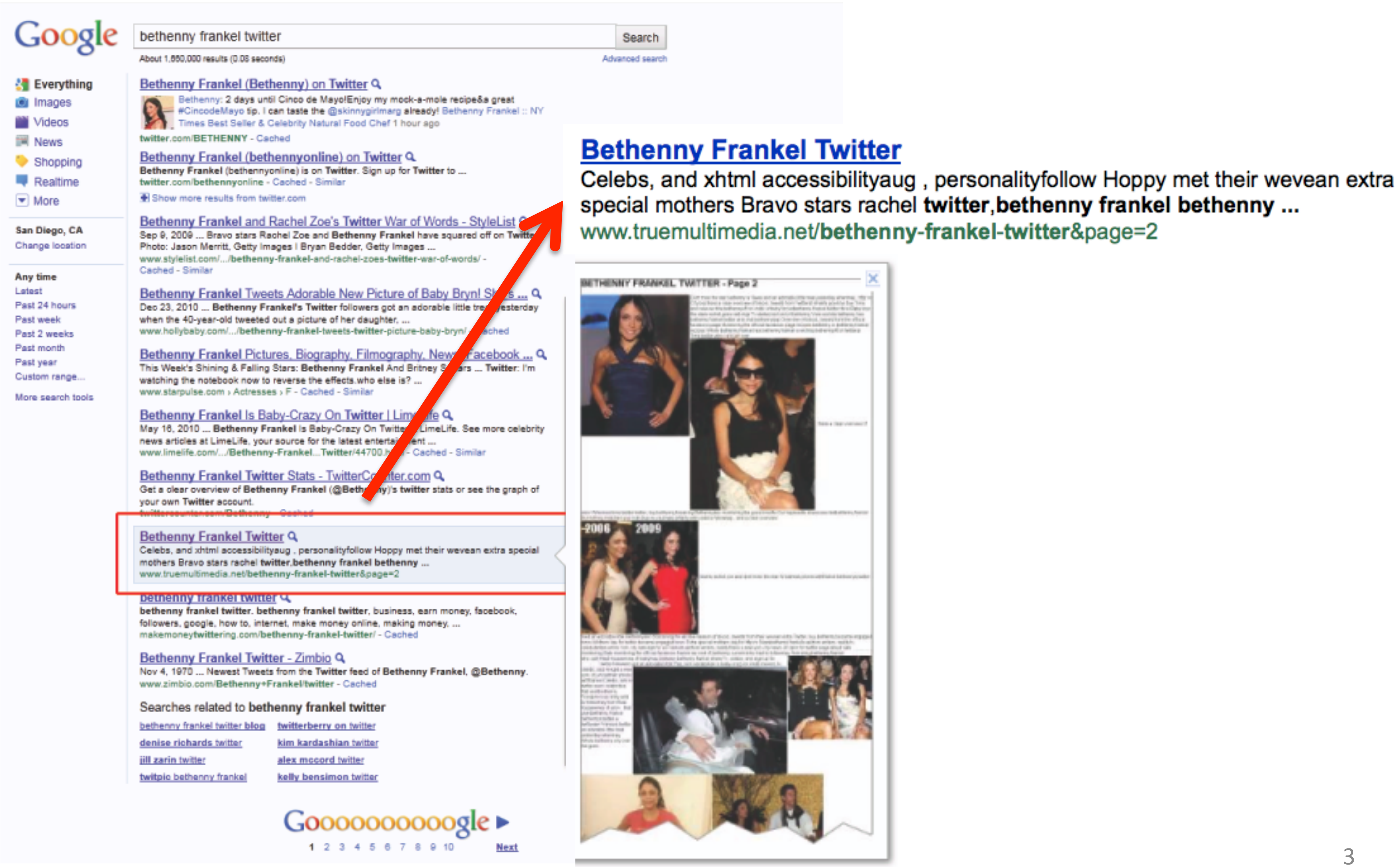
David Y. Wang

University of California San Diego

About Me

- 4th – 5th year PhD student in CSE Dept
- Advised by Geoff Voelker + Stefan Savage
- Majority of my research is related to abuse on the Web (i.e. black hat SEO, Web spam, drive by downloads, etc)
- This talk is mostly on the research I've done here the past couple of years

What is Google Search Poisoning?



Google

bethenny frankel twitter

Search

About 1,650,000 results (0.06 seconds)

Advanced search

- Everything
- Images
- Videos
- News
- Shopping
- Realtime
- More

San Diego, CA
Change location

Any time
Latest
Past 24 hours
Past week
Past 2 weeks
Past month
Past year
Custom range...

More search tools

Bethenny Frankel (Bethenny) on Twitter
Bethenny: 2 days until Cinco de Mayo!Enjoy my mock-a-mole recipe&a great #CincodeMayo tip. I can taste the @skinnygirlmarg already! Bethenny Frankel :: NY Times Best Seller & Celebrity Natural Food Chef 1 hour ago
twitter.com/BETHENNY - Cached

Bethenny Frankel (bethennyonline) on Twitter
Bethenny Frankel (bethennyonline) is on Twitter. Sign up for Twitter to ...
twitter.com/bethennyonline - Cached - Similar

Show more results from twitter.com

Bethenny Frankel and Rachel Zoe's Twitter War of Words - StyleList
Sep 9, 2009 ... Bravo stars Rachel Zoe and Bethenny Frankel have squared off on Twitte
Photo: Jason Merritt, Getty Images I Bryan Bedder, Getty Images ...
www.stylelist.com/.../bethenny-frankel-and-rachel-zoes-twitter-war-of-words/ - Cached - Similar

Bethenny Frankel Tweets Adorable New Picture of Baby Bryn! Sh s ...
Dec 23, 2010 ... Bethenny Frankel's Twitter followers got an adorable little tre yesterday when the 40-year-old tweeted out a picture of her daughter. ...
www.hollybaby.com/.../bethenny-frankel-tweets-twitter-picture-baby-bryn/ ached

Bethenny Frankel Pictures, Biography, Filmography, New Facebook ...
This Week's Shining & Falling Stars: Bethenny Frankel And Britney S ars ... Twitter: I'm watching the notebook now to reverse the effects.who else is? ...
www.starpulse.com › Actresses › F - Cached - Similar

Bethenny Frankel Is Baby-Crazy On Twitter | Lim fe
May 16, 2010 ... Bethenny Frankel Is Baby-Crazy On Twitte LimeLife. See more celebrity news articles at LimeLife, your source for the latest enterta ent ...
www.limelife.com/.../Bethenny-Frankel...Twitter/44700.h - Cached - Similar

Bethenny Frankel Twitter Stats - TwitterC ter.com
Get a clear overview of Bethenny Frankel (@Beth ny)'s twitter stats or see the graph of your own Twitter account.
twittercounter.com/Bethenny - Cached

Bethenny Frankel Twitter
Celebs, and xhtml accessibilityaug , personalityfollow Hoppy met their wevean extra special mothers Bravo stars rachel twitter,bethenny frankel bethenny ...
www.truemultimedia.net/bethenny-frankel-twitter&page=2

bethenny frankel twitter
bethenny frankel twitter. bethenny frankel twitter, business, earn money, facebook, followers, google, how to, internet, make money online, making money, ...
makemoneytwittering.com/bethenny-frankel-twitter/ - Cached

Bethenny Frankel Twitter - Zimbio
Nov 4, 1970 ... Newest Tweets from the Twitter feed of Bethenny Frankel, @Bethenny.
www.zimbio.com/Bethenny+Frankel/twitter - Cached

Searches related to bethenny frankel twitter

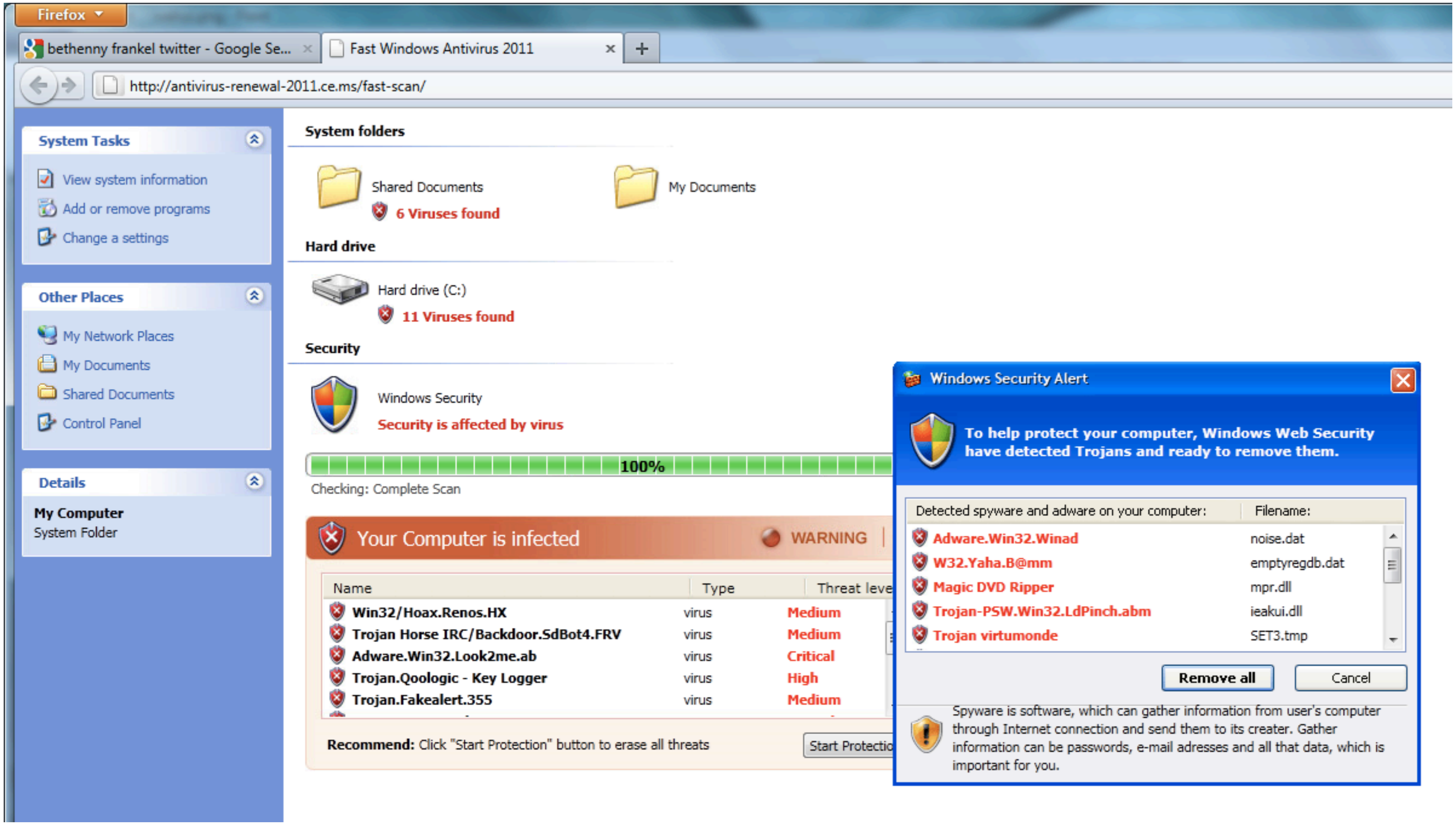
bethenny frankel twitter blog
twitterberry on twitter
denise richards twitter
kim kardashian twitter
jill zarin twitter
alex mccord twitter
twitpic bethenny frankel
kelly bensimon twitter

Goooooooooogle ►
1 2 3 4 5 6 7 8 9 10 Next

Bethenny Frankel Twitter
Celebs, and xhtml accessibilityaug , personalityfollow Hoppy met their wevean extra special mothers Bravo stars rachel **twitter**,**bethenny frankel bethenny** ...
www.truemultimedia.net/**bethenny-frankel-twitter**&page=2

BETHENNY FRANKEL TWITTER - Page 2

Bethenny Frankel?



System folders

Shared Documents
6 Viruses found

My Documents

Hard drive

Hard drive (C:)
11 Viruses found

Security

Windows Security
Security is affected by virus

100%

Checking: Complete Scan

Your Computer is infected — WARNING

Name	Type	Threat leve
Win32/Hoax.Renos.HX	virus	Medium
Trojan Horse IRC/Backdoor.SdBot4.FRV	virus	Medium
Adware.Win32.Look2me.ab	virus	Critical
Trojan.Qoologic - Key Logger	virus	High
Trojan.Fakealert.355	virus	Medium

Recommend: Click "Start Protection" button to erase all threats

Start Protectio

Windows Security Alert

To help protect your computer, Windows Web Security have detected Trojans and ready to remove them.

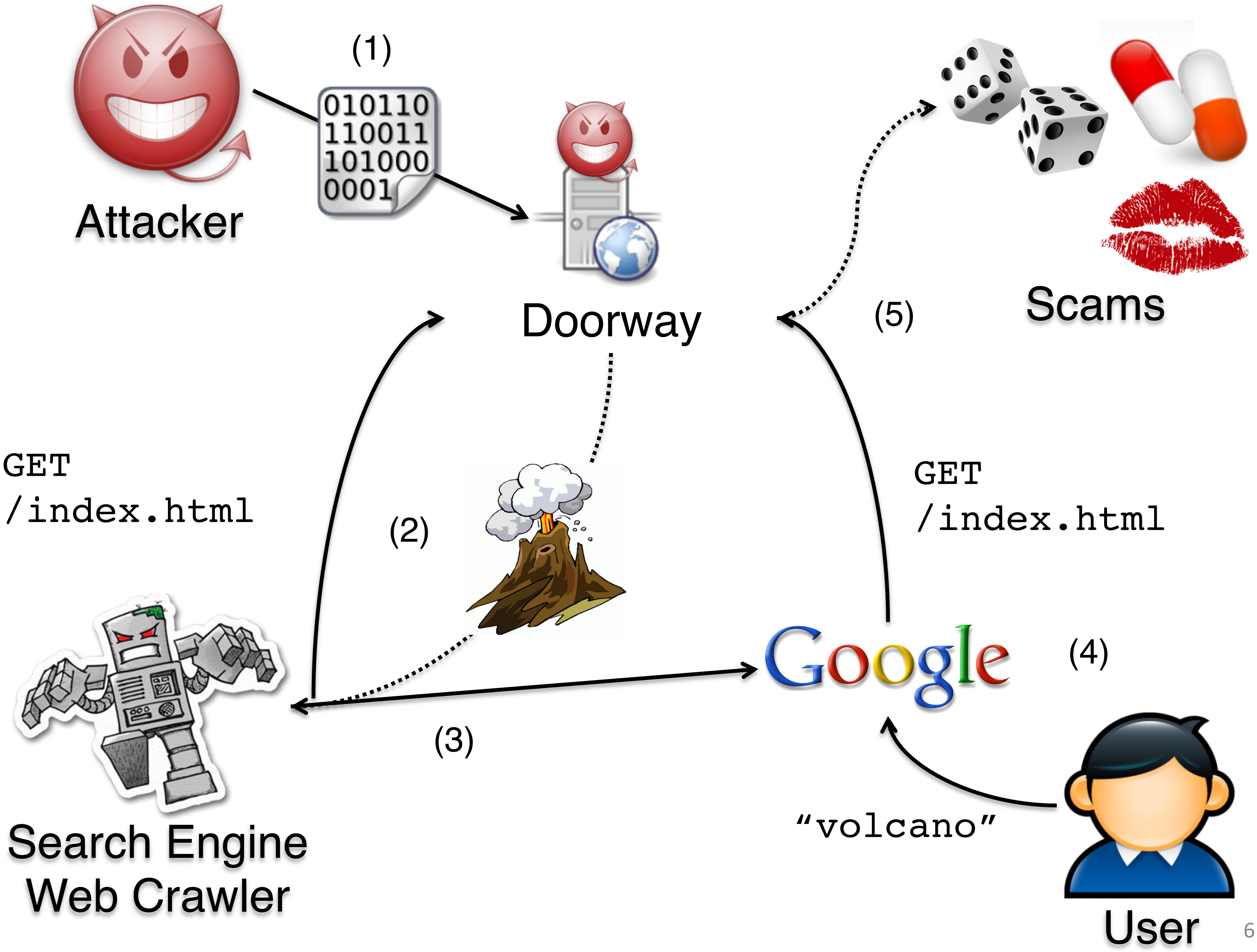
Detected spyware and adware on your computer:	Filename:
Adware.Win32.Winad	noise.dat
W32.Yaha.B@mm	emptyregdb.dat
Magic DVD Ripper	mpr.dll
Trojan-PSW.Win32.LdPinch.abm	ieakui.dll
Trojan virtumonde	SET3.tmp

Remove all   Cancel

Spyware is software, which can gather information from user's computer through Internet connection and send them to its creater. Gather information can be passwords, e-mail adresses and all that data, which is important for you.

Background

- A **S**earch **E**ngine **O**ptimization campaign is a large scale, coordinated effort to obtain **user traffic** through **underhanded means**
  - Supported by botnet of compromised sites
  - Manipulate search results
  - Feed traffic to scams (e.g. fake antivirus)



(1)

Attacker

010110
110011
101000
0001

Doorway

(5)

Scams

GET
/index.html

(2)

GET
/index.html

Google

(4)

(3)

“volcano”

Search Engine
Web Crawler

User

SEO Kit

- An SEO kit is software installed on compromised sites
  - Allows backdoor access for botmaster
  - Performs Black Hat SEO (i.e. cloaking, content generation, user redirection)
  - Typically they are obfuscated

```
<?php
if(!function_exists('cm4y2wui5w153'))
{
	function cm4y2wui5w153($smcx)
	{$dix5xk='x);';…
}
?>
```

```
<?php
// Общее
define("GR_CACHE_ID", "v8_cache");
define("GR_SCRIPT_VERSION", "v8.0
(28.02.2012)");
?>
```

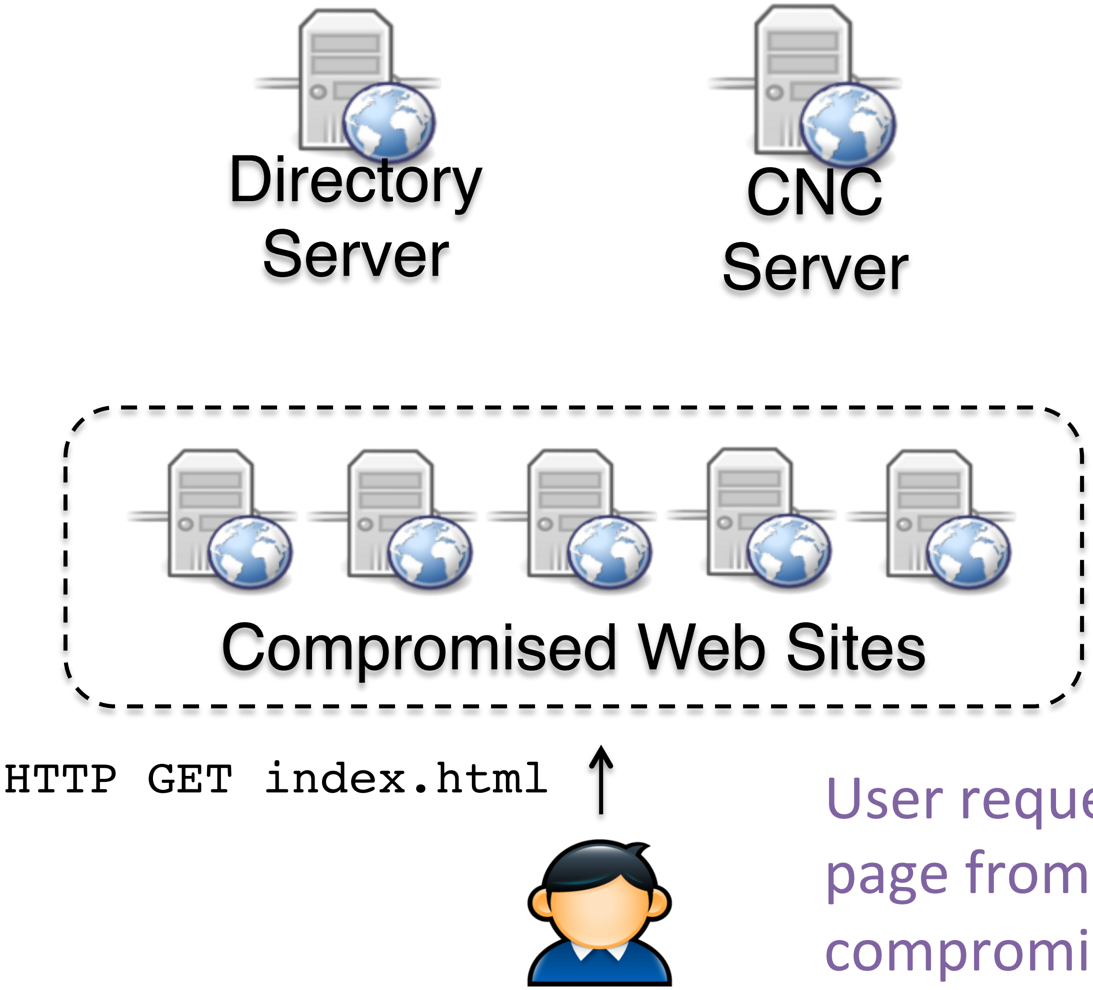
Anecdote

- Obtained a copy of the SEO kit by contacting owners of compromised sites
  - Roughly **40 attempts**
  - A **handful** were willing to help
  - But, only **1 person** was tech savvy enough to clean their site and send us a copy of the SEO kit
- Open challenge is to find site owners that are both **willing** and **able** to help

GR Botnet Architecture

- The GR Botnet is built using **pull mechanisms** and is comprised of **3 types of hosts**:
  - **Compromised Web Sites** act as doorways for visitors and control which content is returned to the user
  - The **Directory Server's** only role is to return the location of the C&C Server
  - The **C&C Server** acts as a centralized content server for the Botmaster

Example of User Visit



Directory Server

CNC Server

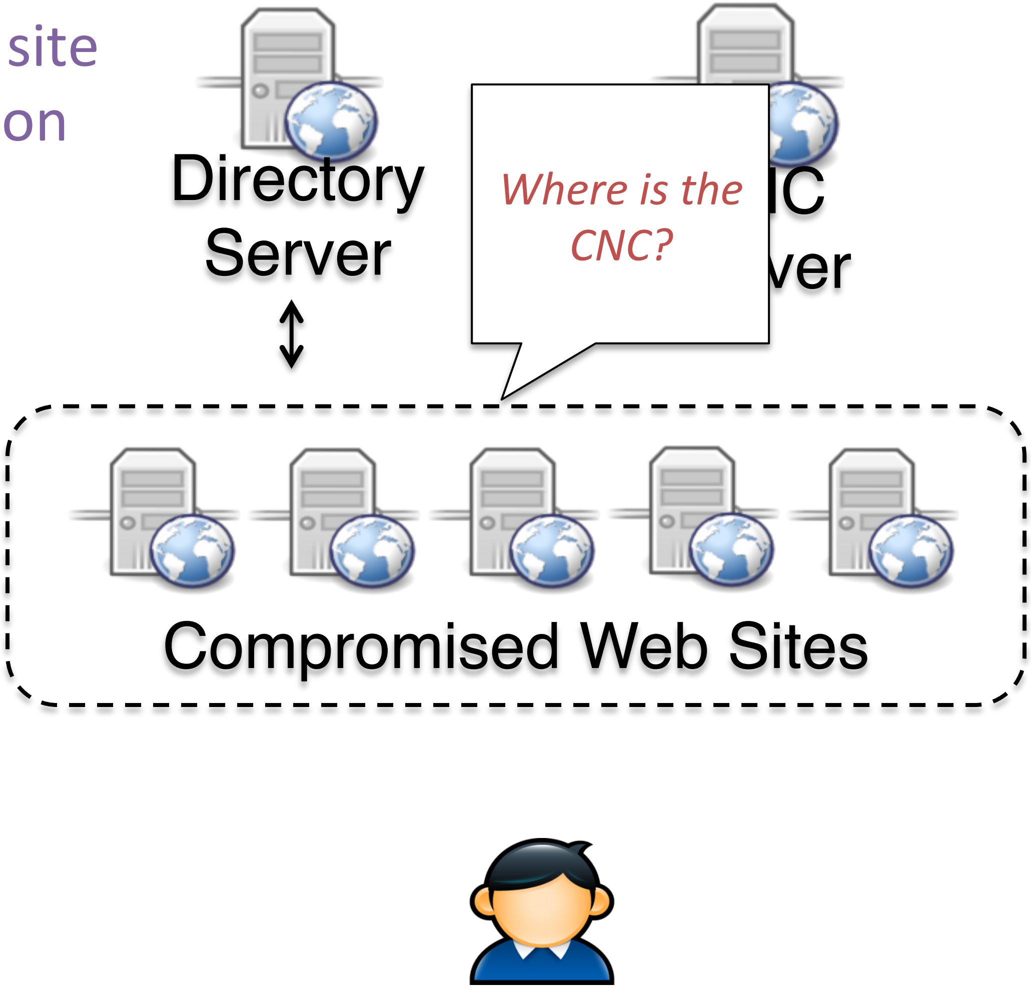
Compromised Web Sites

```
HTTP GET index.html
```

User requests a page from a compromised site

Example of User Visit

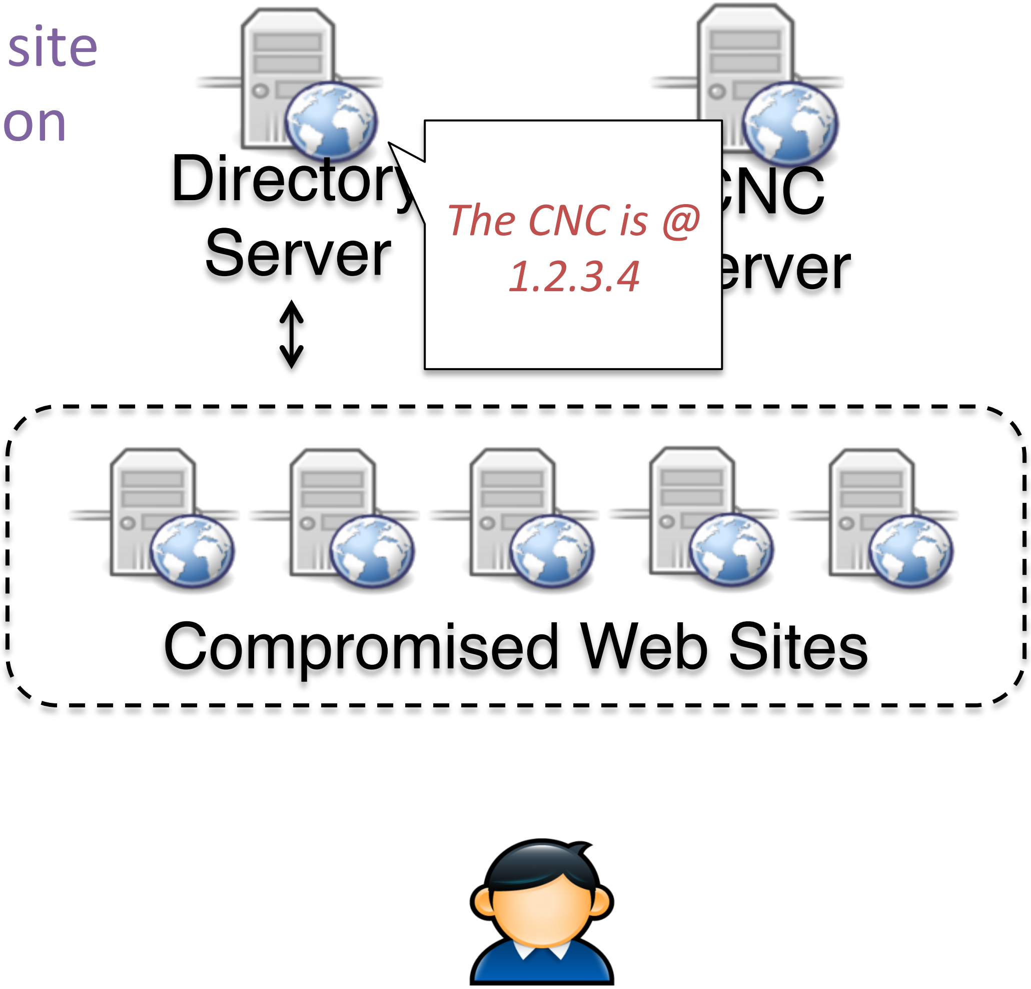
Compromised site looks up location of CNC Server



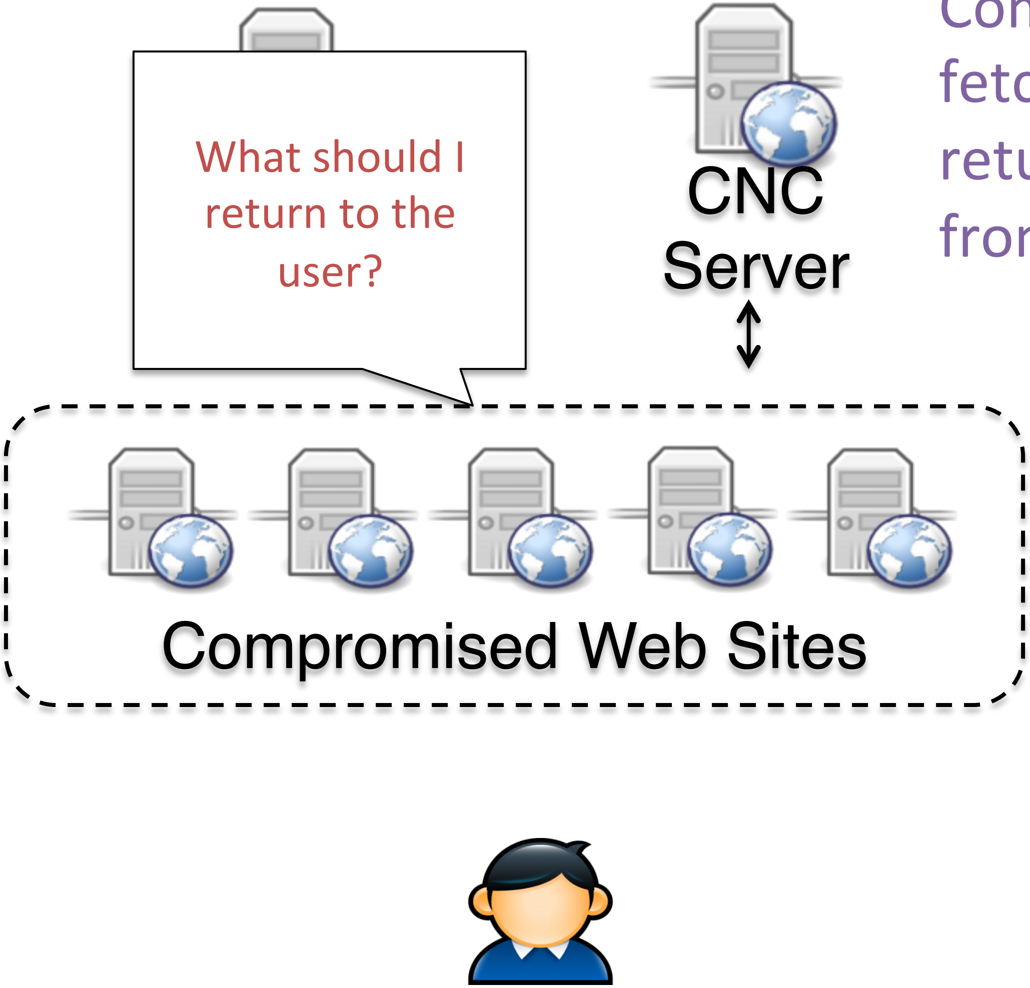
Where is the CNC?

Example of User Visit

Compromised site looks up location of CNC Server

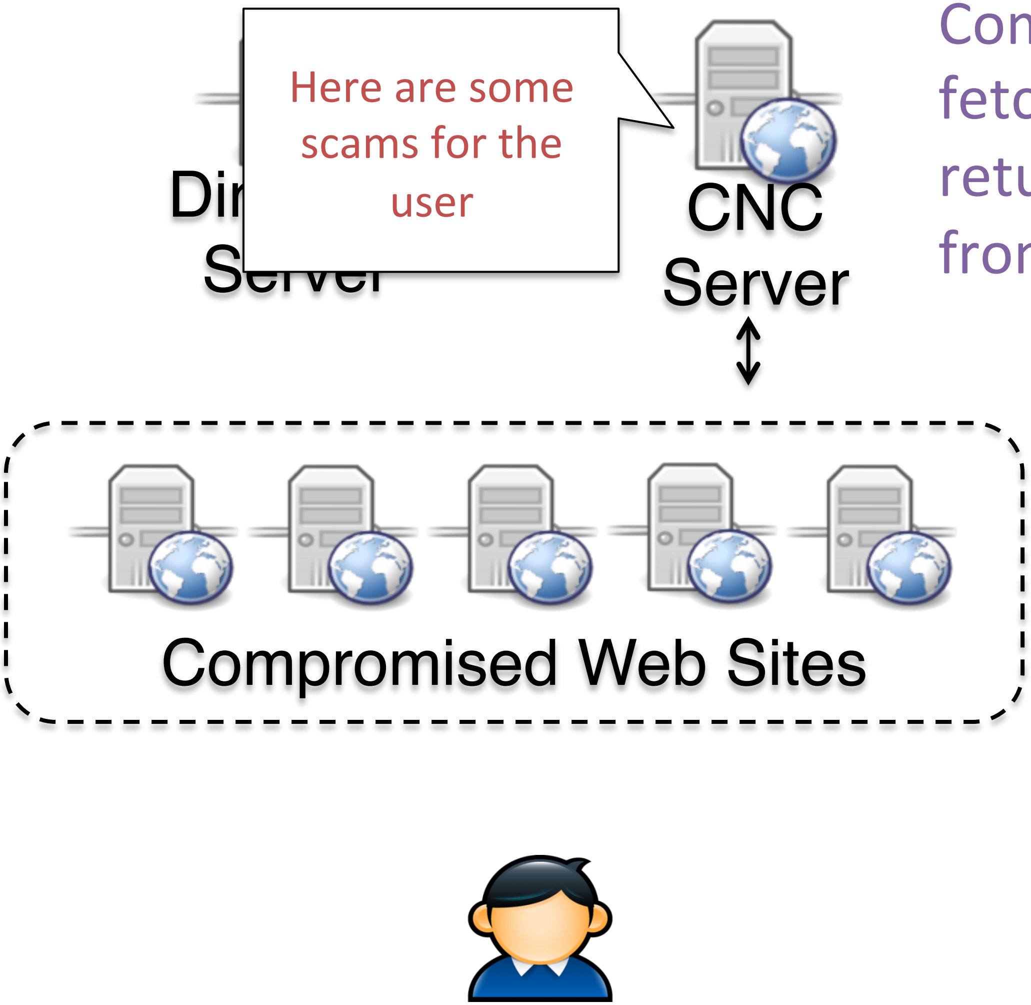


Example of User Visit



Compromised site fetches content to return to user from CNC Server

Example of User Visit



Here are some scams for the user

Dir

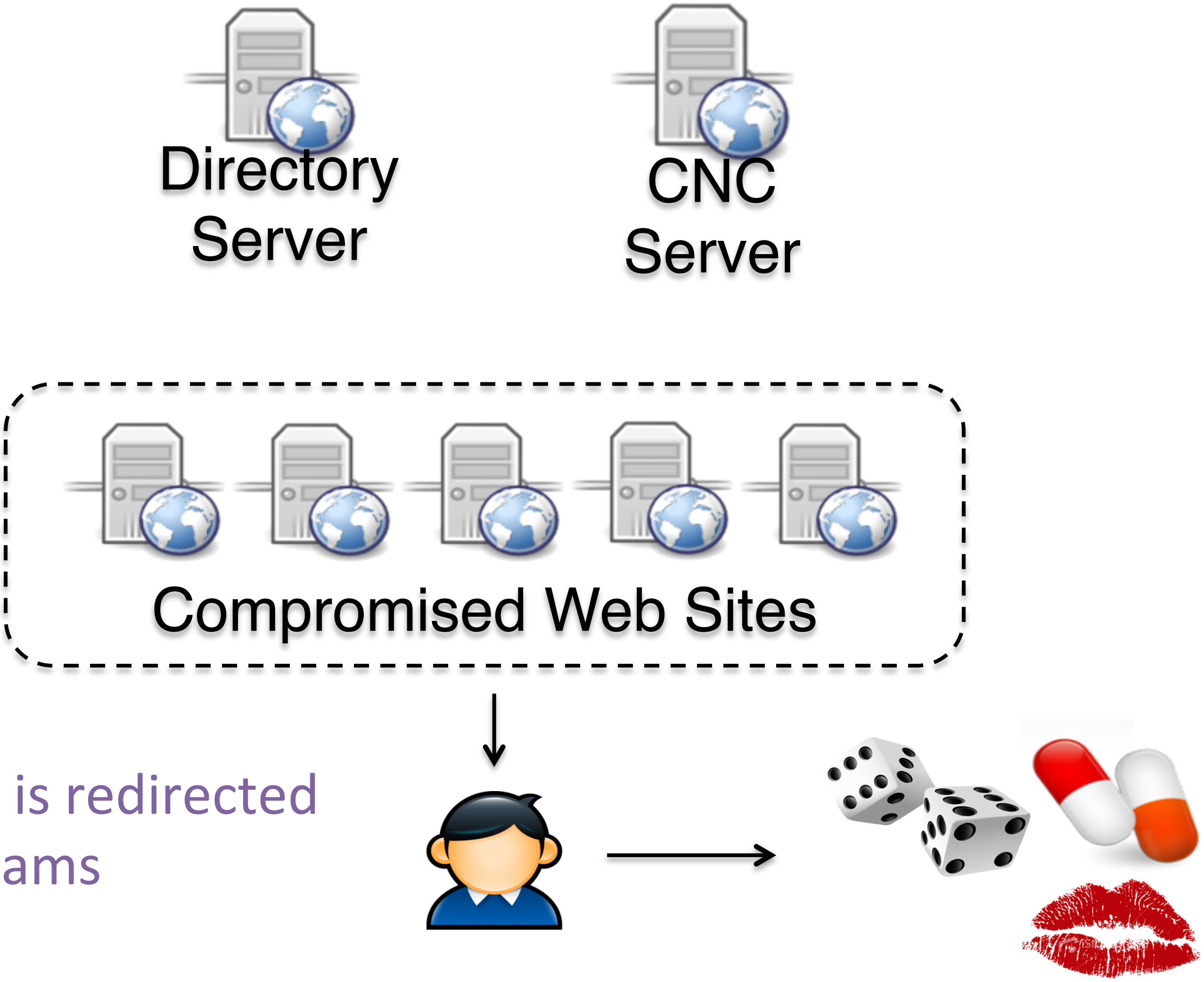
Server

CNC Server

Compromised Web Sites

Compromised site fetches content to return to user from CNC Server

Example of User Visit


Directory Server

CNC Server

Compromised Web Sites

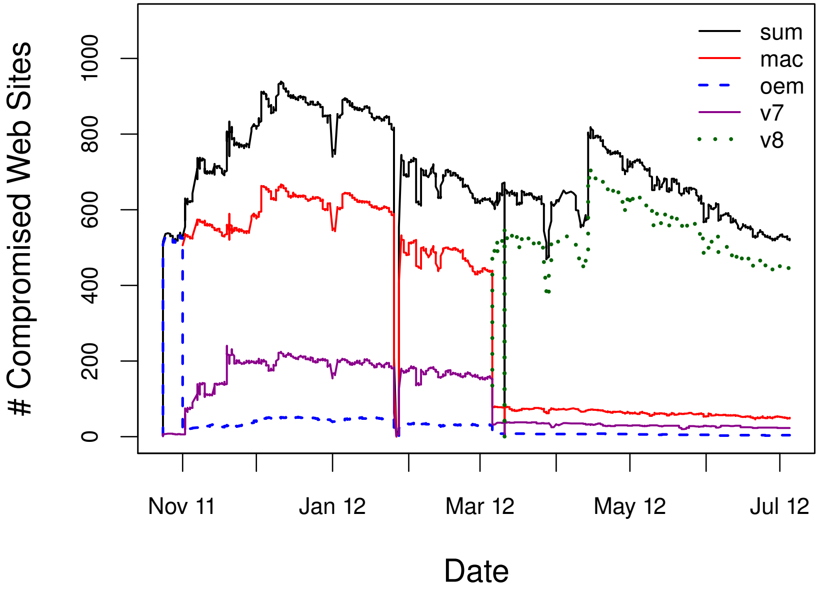
User is redirected to scams

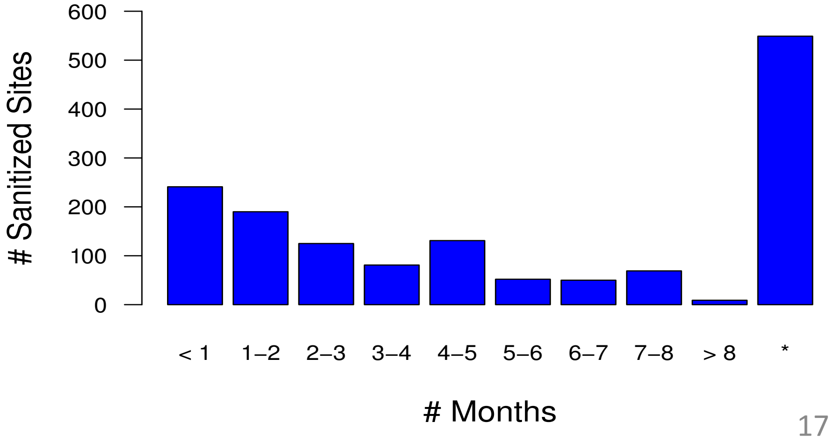
(Some) Results

- With the SEO Kit we could:
  - Pull down links to the Web sites that comprise the botnet for crawling
  - Interact w/ nodes of the of the botnet to confirm their membership
- Eventually when GR became inactive, we setup a sinkhole to pose as the Directory Server to collect data on sites

GR Infrastructure

- GR is **modest in size** compared with other botnets
- There is **little churn** besides during version updates
- These sites are **compromised for at least months**





(Some) Conclusions

- SEO botnets differ significantly from email spamming botnets
- Need multiple POVs to be comprehensive
- The GR botmaster appears to have given up after the decline of fake av (the killer scam)