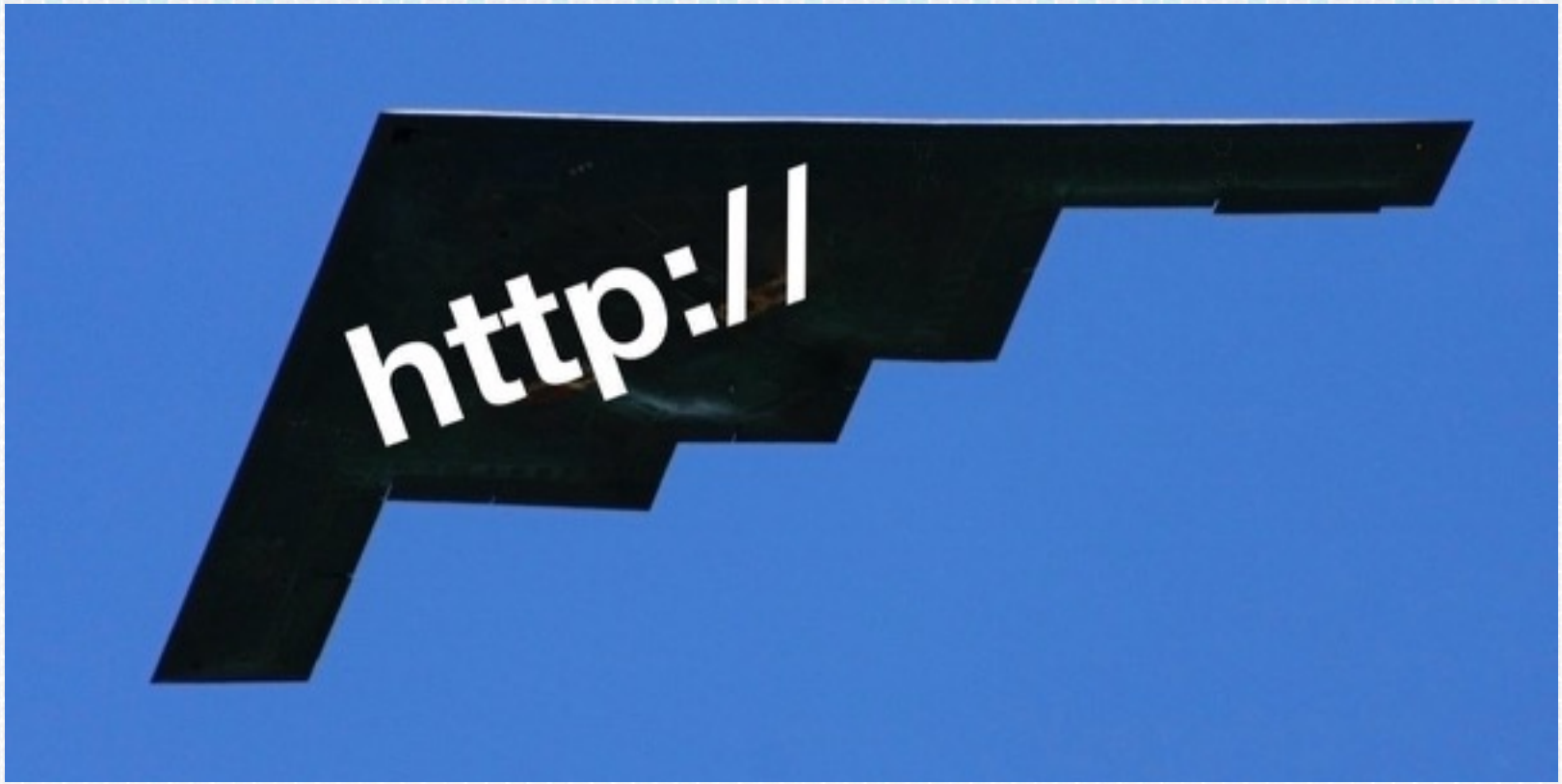
RSAConference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: MASH-F02

Website counterintelligence: Leveraging web logs to gather intelligence

Lance Cottrell

Chief Scientist
Ntrepid - Passages
@LanceCottrell


http://

Anonymity is hard

Everything is tracked

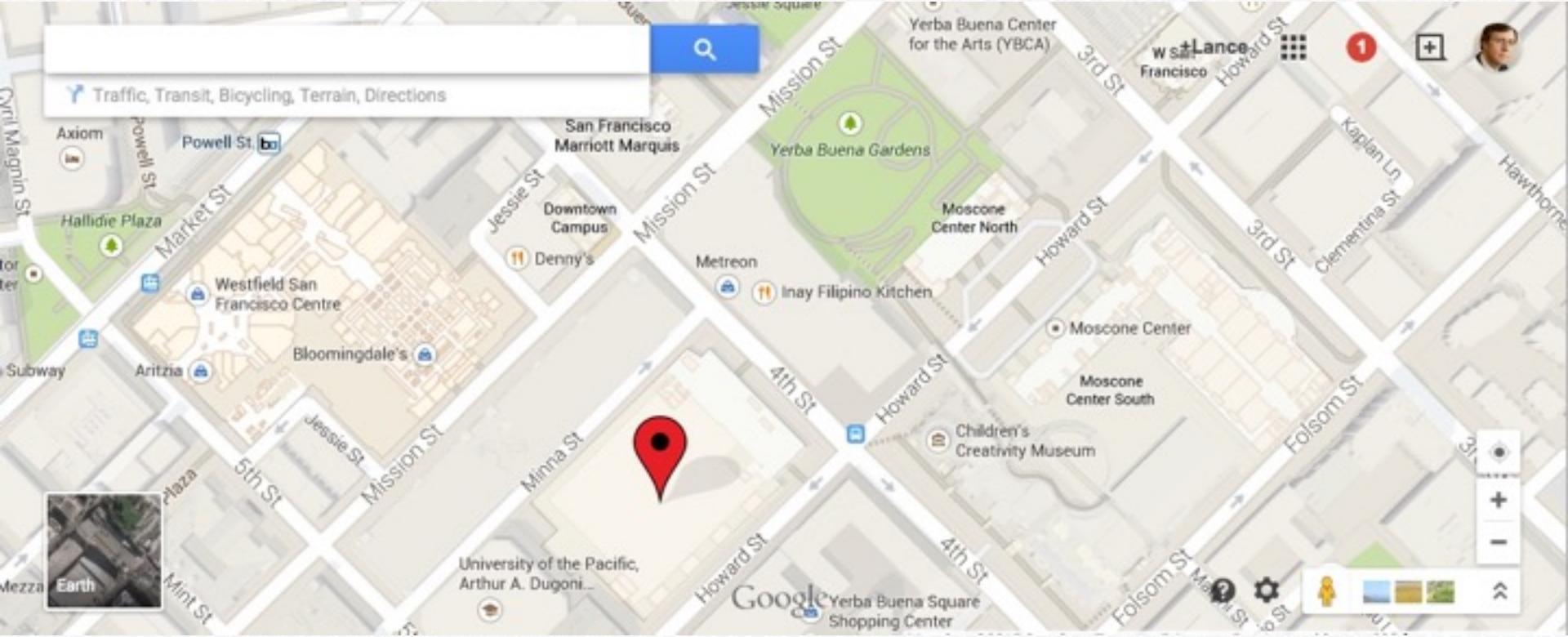
All the time

Everywhere

How Anonymity Fails

- Cookies
- IP
- Traceroute
- History
- Fingerprint
- Human Error
- Behavior

Google Uses Behavior



RSA Conference 2015

San Francisco | April 20-24 | Moscone Center

What can you learn from your logs?

#RSAC

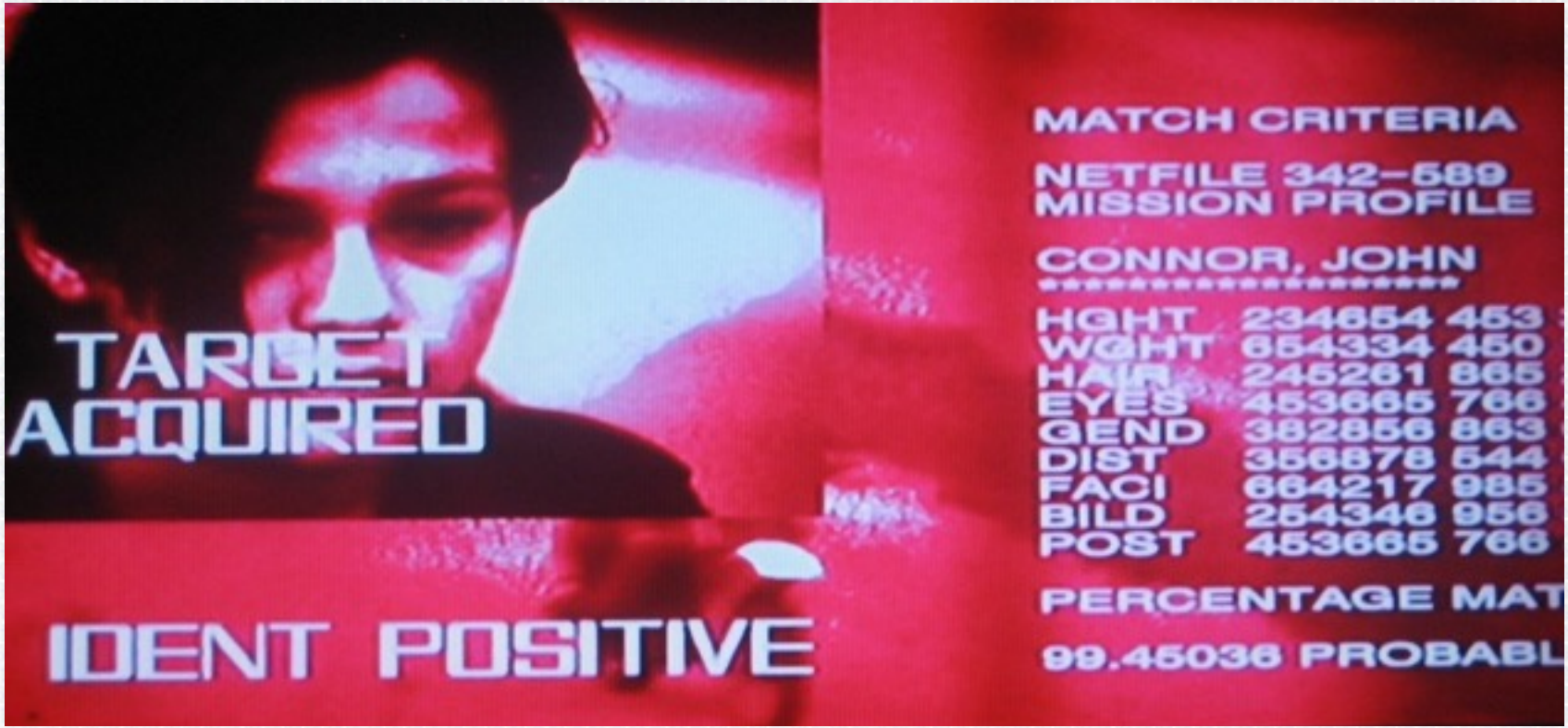
Let's put me under the microscope

Angel Investing

New Product R&D

Doing unto others

Step 1: Identify visitors so you can track them



Direct Identification from the IP

Reverse DNS

```
$ host 107.77.92.56

Host 56.92.77.107.in-addr.arpa. not found: 3(NXDOMAIN)
```

Whois

```
$ whois 107.77.92.56

NetRange:       107.64.0.0 - 107.127.255.255
CIDR:           107.64.0.0/10
NetName:        ATT-MOBILITY-LLC
NetHandle:      NET-107-64-0-0-1
Parent:         NET107 (NET-107-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   AT&T Mobility LLC (ATTMO-3)
RegDate:        2011-02-04
Updated:        2012-03-20
```

Solicited Identification

- Newsletter
- Webinar registration
- White-paper registration
- Account creation

4 Aggressive Tricks for Identification

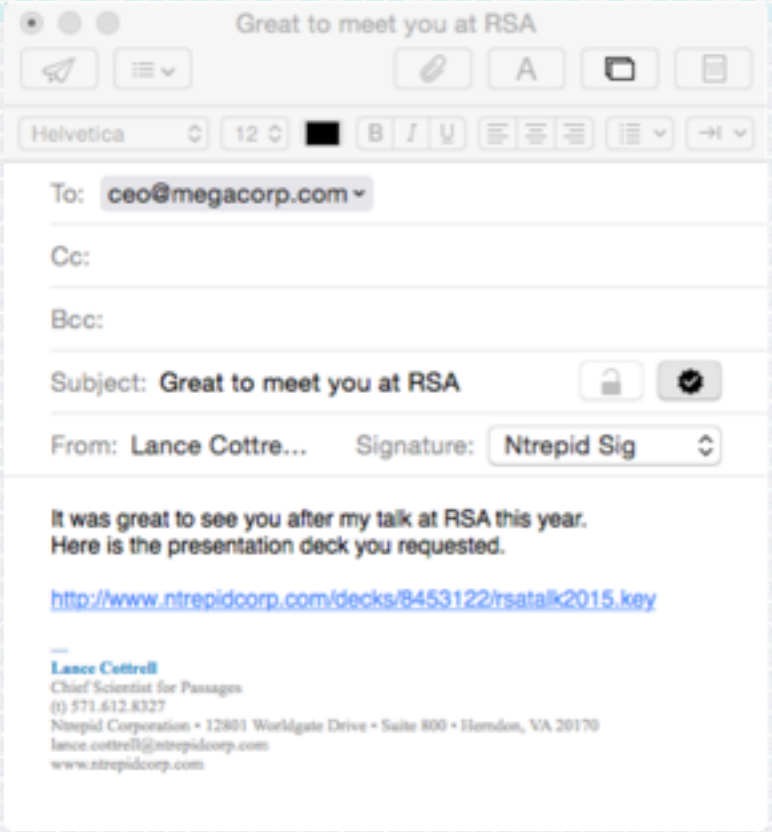
1. Targeted Social Media links
2. “Phishing” email
3. Social Engineer for Corp IP blocks
4. HTML Bug in email

Targeted Social Media Links

- Create unique URL for some content.
  - http://yourcorp.com/white-paper.pdf?unique=12345678
- Share content with just the target
- Link IP addresses with the unique ID / target

“Phishing” Email

- As before, create unique URL for some interesting content.
- Send email with link to enticing content
- Link recipients with the unique ID / target

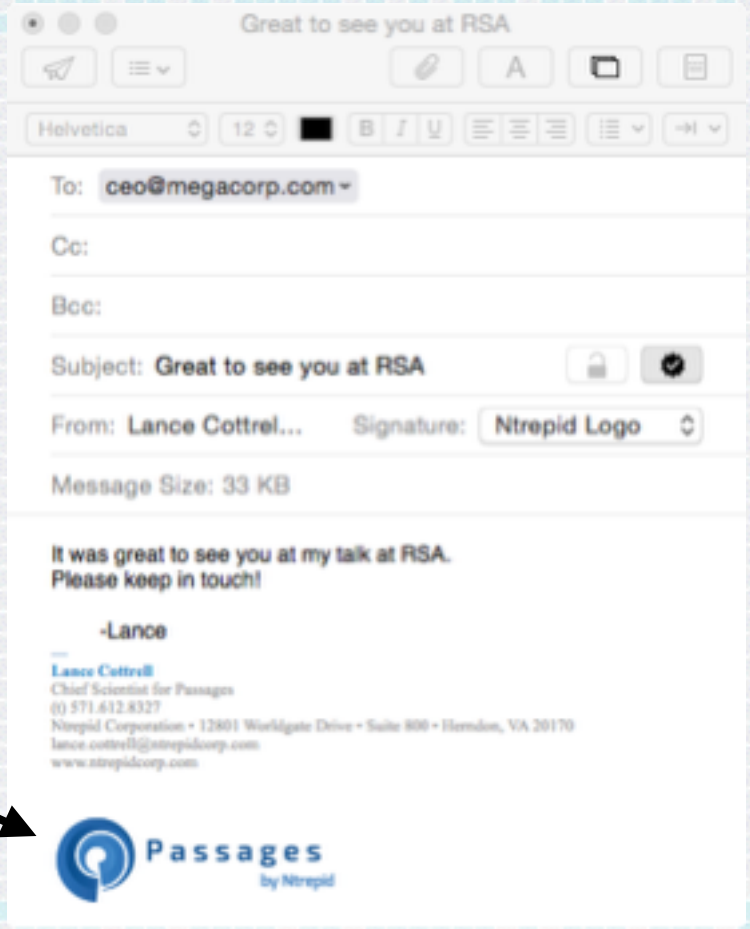


Social Engineer the Corp IP space

HTML Bug in Email

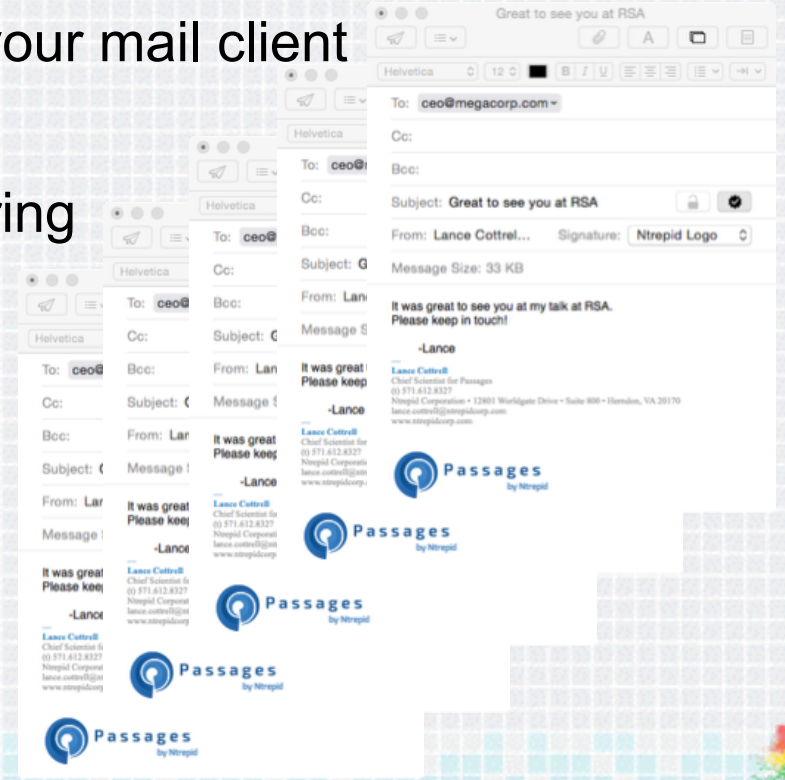
- Completely Automated
- No user action
- Passive with every email you send.

That



Create a Random Signature Tracker

- Create an HTML signature file in your mail client
- Find that signature file
- Add unique tag and identifiable string
- Change every 10 seconds



That looks like…

Signature Image Code

```
<img src="http://ntrepidcorp.com//passages_logo.jpg?
sig_tracker_identifier8290=XXXtnofbXXX">
```

Signature File Updater

```
while (1) {
        $unique = time() . "endmarker";
        `cat $sigCpy | sed \'s/XXXtnofbXX/$unique/g\' > $targetfile`;
        sleep($sleeptime);
}
```

Identify Who Got Which Tracker ID

- Scan sent email folder
- Extract the recipients and the tracker ID from each email
- Note: trackers and email addresses will be many to many

```
foreach unexamined email {
        find the emails containing the marked signatures
        extract the recipient information from the email
        extract the unique ID from the email
        put both in a database
}
```

Connect IPs to IDs

- Scan your web logs
- Extract all the hits on your mail signature image file
- Record the IP addresses which have hit that unique Tracker
- This too can be a many to many relationship

example.com 70.197.23.21 - - [17/Feb/2015:18:23:34 +0000] "GET //siglogo.jpg?sig_tracker_identifier8290=1424138085endmarker HTTP/1.1"

Step 2: Keep track of your target after identification

IP Address

Always there for you

May not be helpful

Cookies

- Cookies (and Super Cookies)
- Yeah….
  - obvious
  - simple
  - effective

Browser Fingerprints

Panopticlick

EFF research project

http://panopticlick.eff.org

Step 3: Pattern Analysis

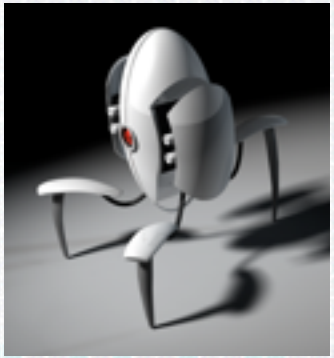
"Textile cone" by Photographer: Richard Ling (richard@research.canon.com.au) - Location: Cod Hole, Great Barrier Reef, Australia. Licensed under CC BY-SA 3.0 via Wikimedia Commons - https://commons.wikimedia.org/wiki/File:Textile_cone.JPG#/media/File:Textile_cone.JPG

Usage Analysis

- Technical details are highly dependent on your particular hosting and analytics platforms.
  - Google Analytics is not granular enough.
  - Logs will likely need post-processing to be most useful

Create Topic Groups

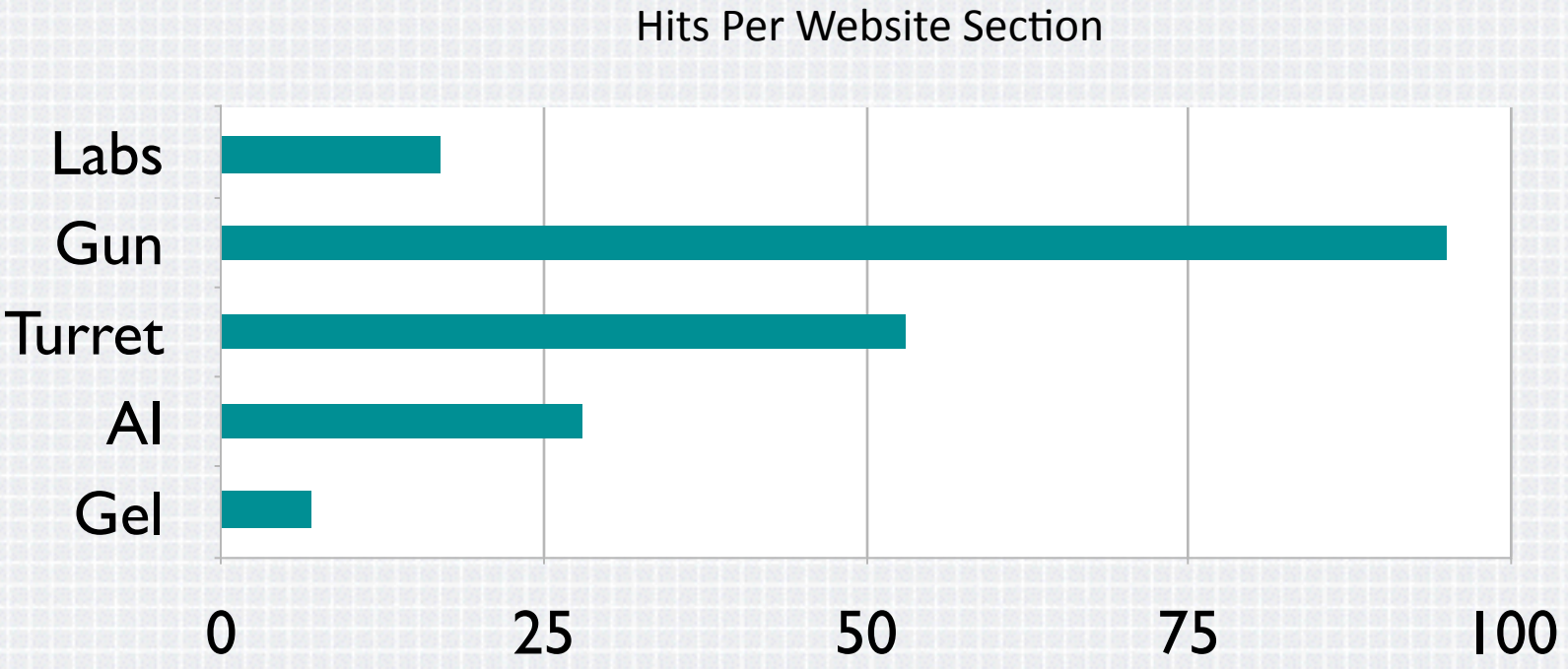
- Group pages and web resources by type and topic
  - Which product / service
  - marketing
  - technical
  - help
  - corp
  - team
  - labs
  - weapons



Examples from our website

- Page Categories
  - Team
  - Media & Events
  - White Papers
  - Support
  - FAQ
- Types of Targets
  - Known Competitors
  - Possible Competitors

Segment statistics

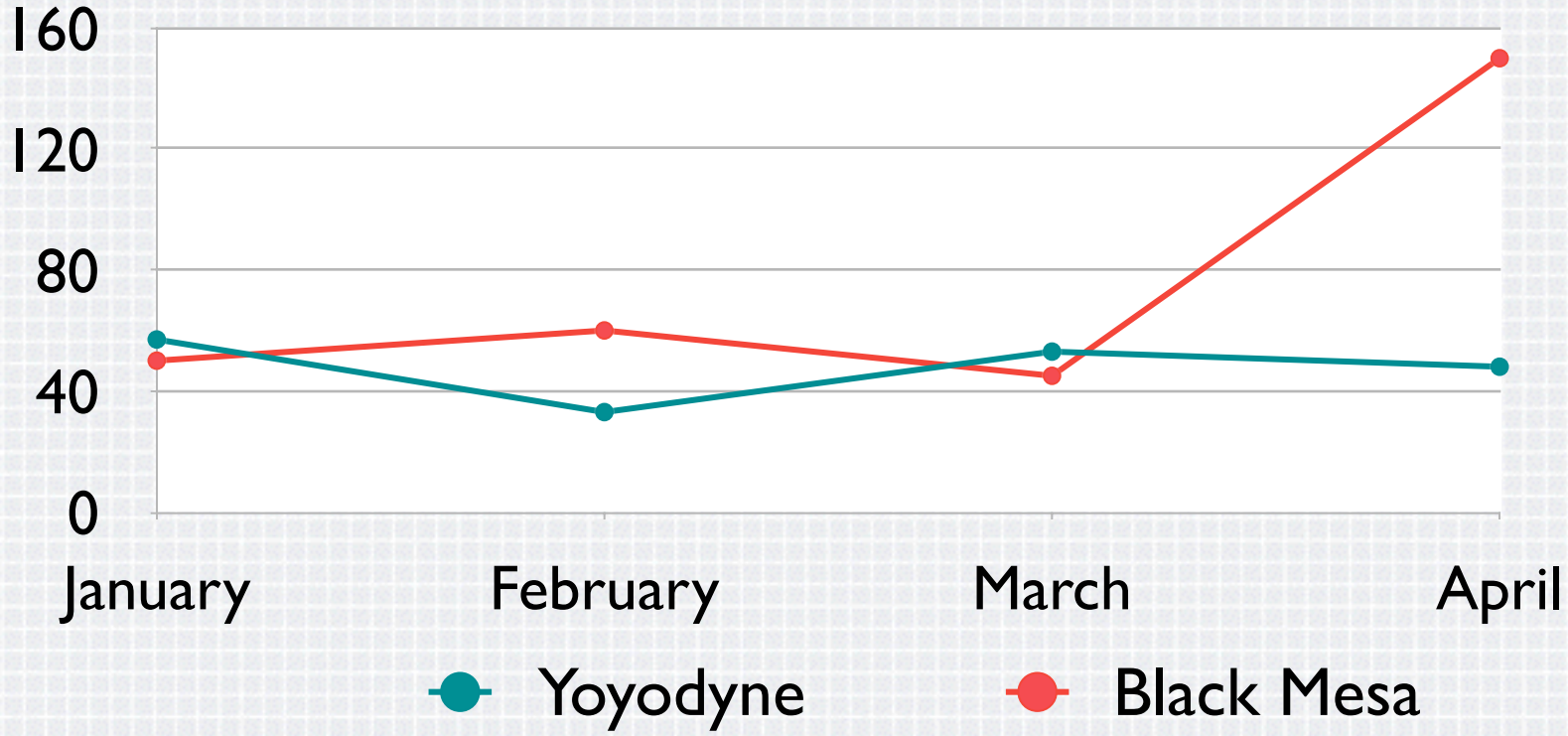


Flag outliers

Who stands out

Black Mesa	Labs	Gun	Turret	AI	Gel
Weapons R&D	2	9	11	3	1
Biologics Lab	6	1	2	4	3
Marketing	8	3	45	10	12
Executives	30	4	12	6	9

Quick and Dirty



How to protect yourself

- Incognito mode in the browser (or better)
- Non-attributed IP address
- Disposable email addresses for registrations
- Turn off auto-download images in email
- Clean VM or iOS for competitive research

Next Steps

- When you get back:
  - Start detailed logging of URL and IP addresses
  - Create groups of web pages based on product and purpose
- In the next few months:
  - Identify Targets for tracking
  - Initiate target acquisition for top priorities
- Within six months you should:
  - Implement tracking bug
  - Automate target acquisition
  - Initiate analysis of data

I Am Not Anonymous

- lance.cottrell@ntrepidcorp.com
- @LanceCottrell
- http://linkedin.com/in/LanceCottrell
- http://ThePrivacyBlog.com
- http://ntrepidcorp.com/blog