RSA®Conference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: ANF-R02

The Newest Piece of Defense-In-Depth:

Social Media & DNS

Evan Blair

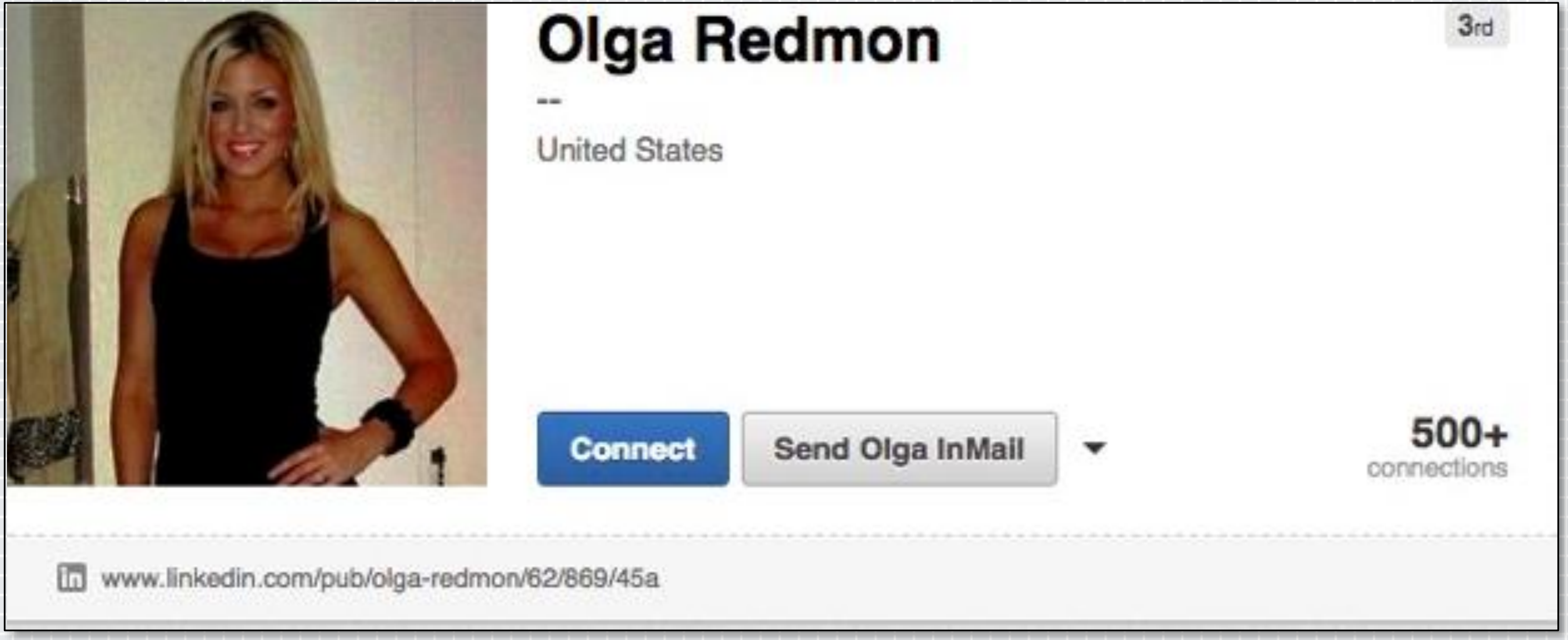
COO
ZeroFOX
@EvanLBlair

Andrew Hay

Head of Research
OpenDNS
@andrewsmhay

#RSAC

It was nice to meet you at RSA…



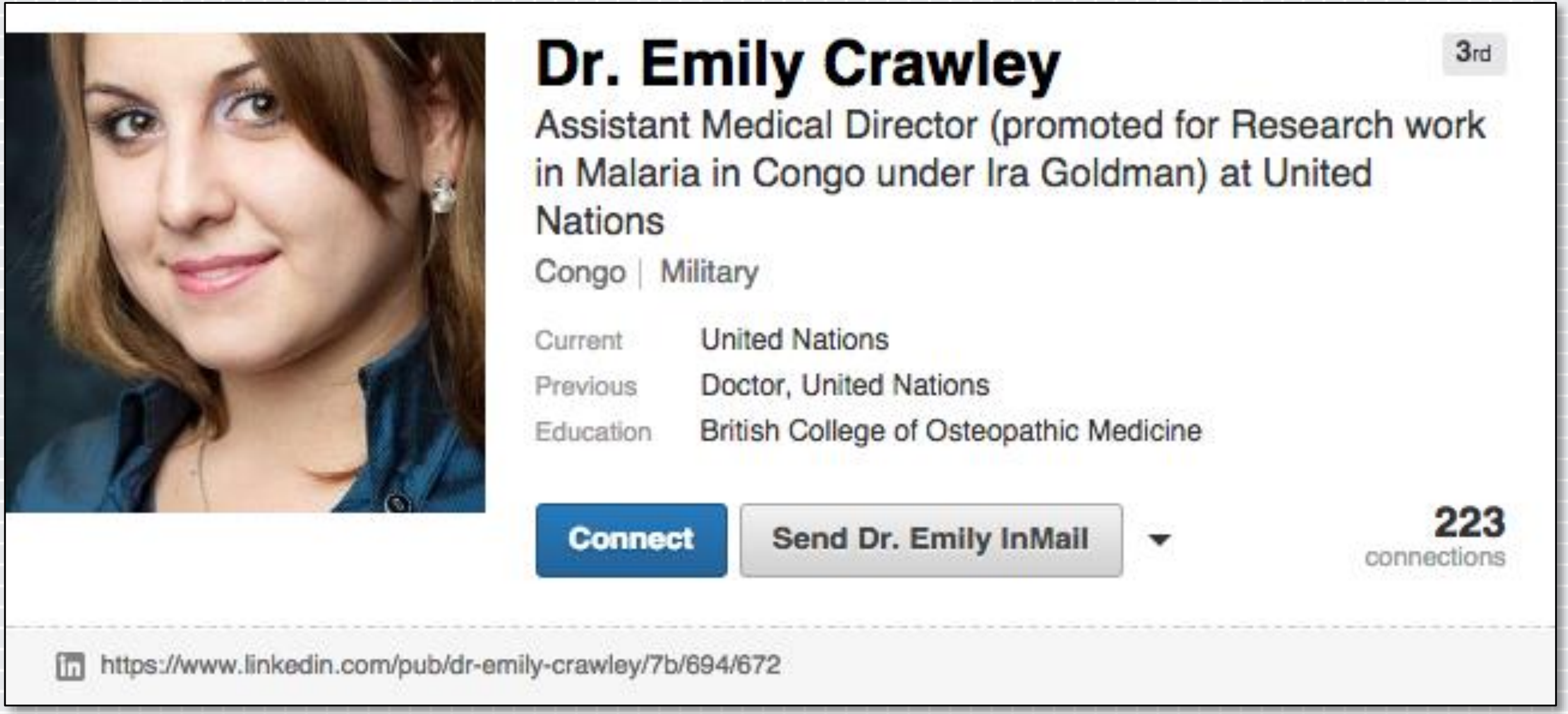
Olga Redmon

--

United States

www.linkedin.com/pub/olga-redmon/62/869/45a

It was nice to meet you at RSA…



Dr. Emily Crawley

3rd

Assistant Medical Director (promoted for Research work in Malaria in Congo under Ira Goldman) at United Nations

Congo | Military

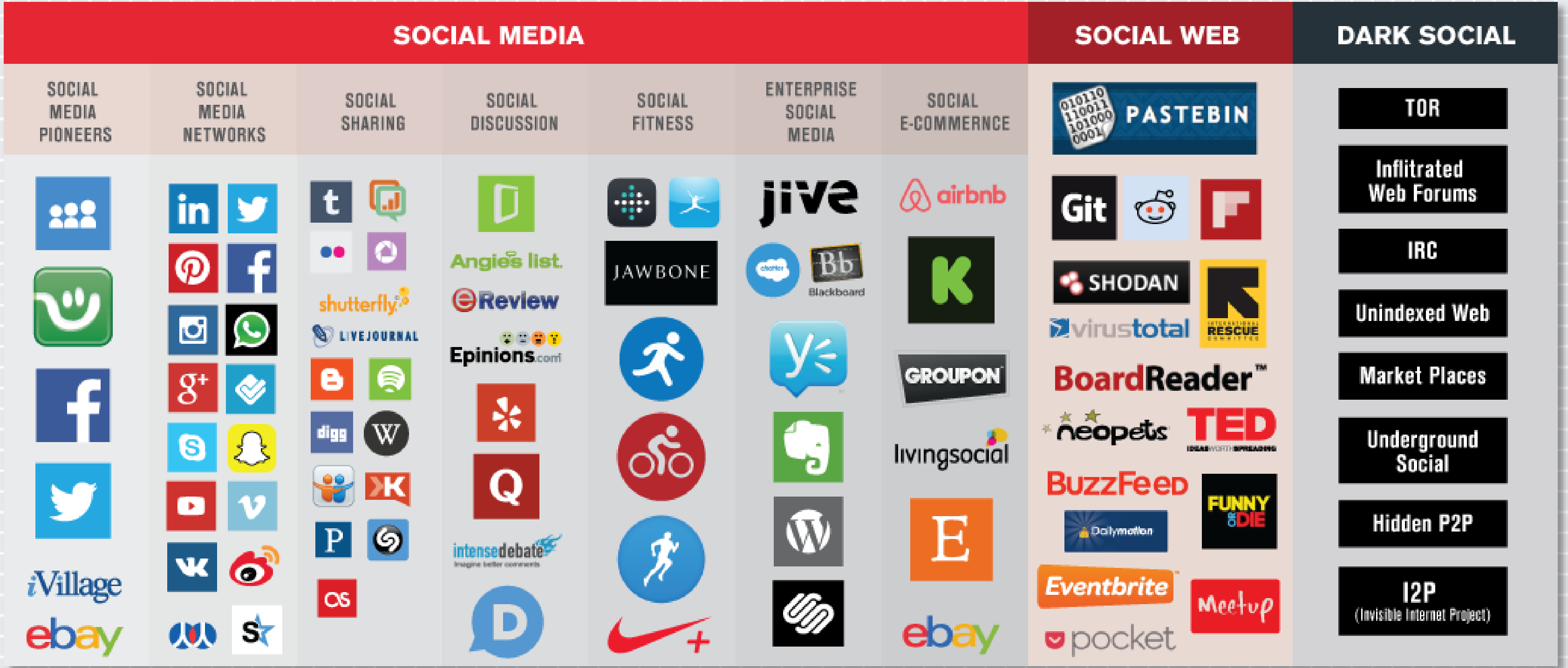
Current	United Nations
Previous	Doctor, United Nations
Education	British College of Osteopathic Medicine

223 connections

https://www.linkedin.com/pub/dr-emily-crawley/7b/694/672

Social media is growing

Social media is growing



SOCIAL MEDIA

SOCIAL MEDIA PIONEERS

SOCIAL MEDIA NETWORKS

SOCIAL SHARING

SOCIAL DISCUSSION

SOCIAL FITNESS

ENTERPRISE SOCIAL MEDIA

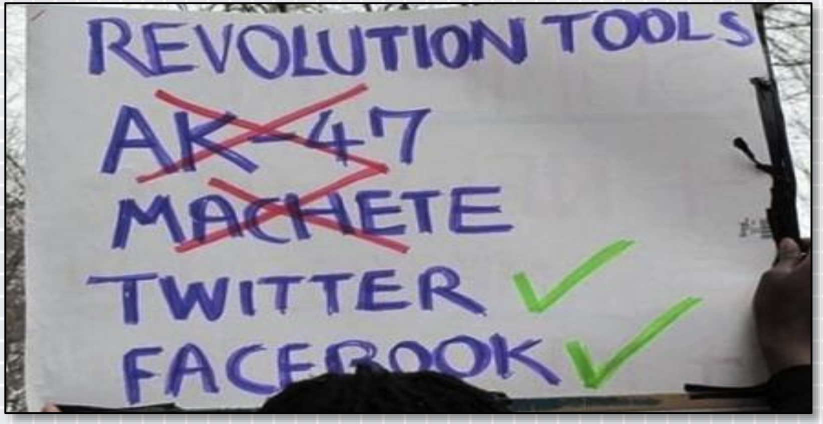
SOCIAL E-COMMERNCE

SOCIAL WEB

DARK SOCIAL

- TOR
- Inflitrated Web Forums
- IRC
- Unindexed Web
- Market Places
- Underground Social
- Hidden P2P
- I2P (Invisible Internet Project)

Communication (R)evolution



New information security challenges

THE SCALE

74% of WORLDWIDE INTERNET USERS HAVE ACTIVE SOCIAL PROFILES

THE TRUST

39% of SOCIAL NETWORK USERS HAVE ACCEPTED FRIEND REQUESTS FROM PEOPLE THEY DONT KNOW

THE VISIBILITY

0 VISIBILTY TO TRADITIONAL ENTERPRISE SECURITY INFRASTRUCTURE

Some of The Bad Stuff

SOCIAL MALWARE & PHISHING

IMPERSONATIONS

ATTACK PLANNING

SOCIAL ENGINEERING

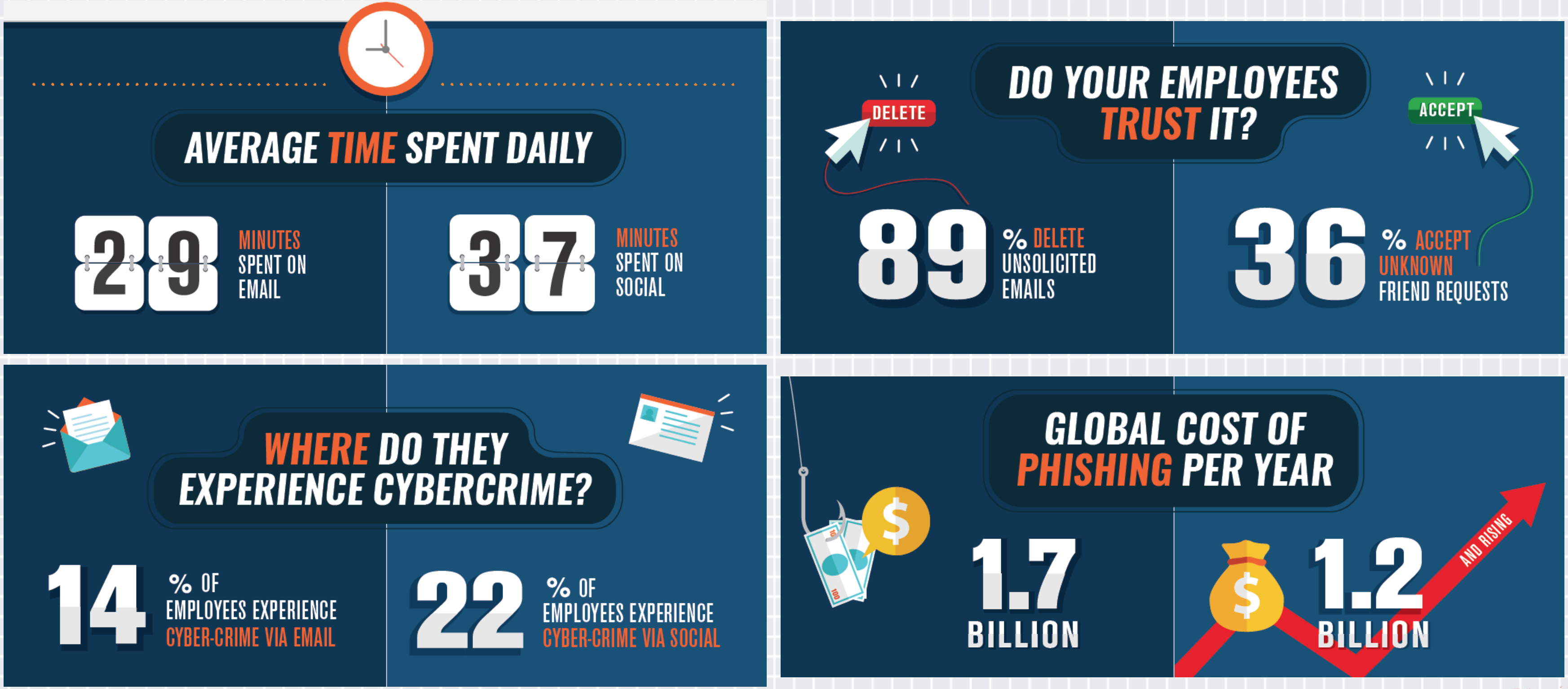
PROPAGANDA

ACCOUNT TAKEOVER

INFORMATION LEAKAGE

TREND HIJACKING

Social vs. Email



AVERAGE TIME SPENT DAILY

29 MINUTES SPENT ON EMAIL

37 MINUTES SPENT ON SOCIAL

DO YOUR EMPLOYEES TRUST IT?

89 % DELETE UNSOLICITED EMAILS

36 % ACCEPT UNKNOWN FRIEND REQUESTS

WHERE DO THEY EXPERIENCE CYBERCRIME?

14 % OF EMPLOYEES EXPERIENCE CYBER-CRIME VIA EMAIL

22 % OF EMPLOYEES EXPERIENCE CYBER-CRIME VIA SOCIAL

GLOBAL COST OF PHISHING PER YEAR

1.7 BILLION

1.2 BILLION

Connectivity Breeds Vulnerability

Mobile Business/BYOD

Proactive & Intelligent Protection

Detection

- Detecting malicious activity on your network is hard
- Detecting malicious activity targeting your users **OUTSIDE OF YOUR NETWORK** is even harder
- Difficult to monitor **ALL** possible communication **VECTORS** and data transmission **MEDIUMS**

TYPHOID CARRIER →
← ANY FOOD NOT COOKED AFTER PREP-ARATION
IN THIS MANNER THE FAMOUS "TYPHOID MARY" INFECTED FAMILY AFTER FAMILY

Attribution, Motive, and Extent

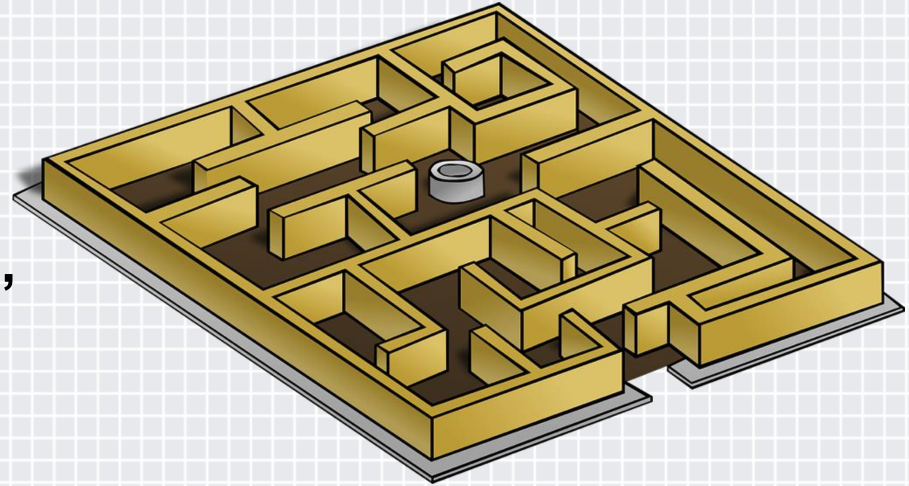
- More difficult still to determine **ATTRIBUTION**, **MOTIVE**, and **EXTENT**
  - **TARGETED** or **OPPORTUNISTIC** attack?
  - **CARELESS/CLICK-HAPPY** employee or **MALICIOUS INSIDER**?
  - **ISOLATED INCIDENT** or **LONG RUNNING** campaign?

Links, Links, Links

- The number of social sites is **GROWING**
  - Social communications (e.g. Twitter)
  - Social engagement (e.g. Facebook)
  - Social sharing (e.g. Instagram)
  - Blogging (e.g. Wordpress)
- With them, the number of embedded URLs

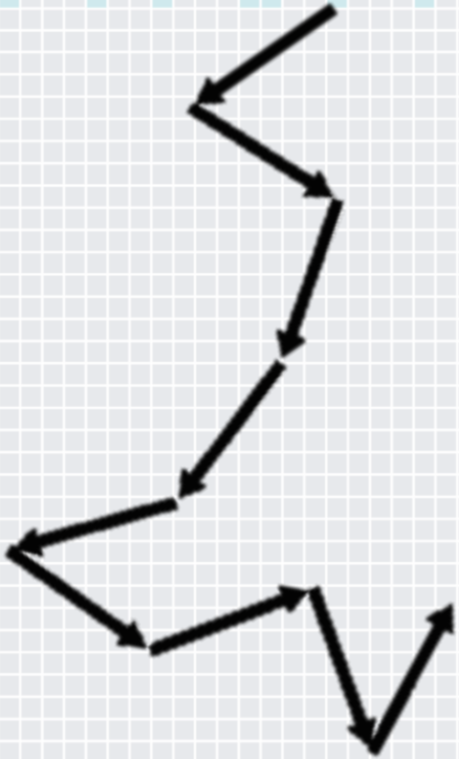
Moving At The Speed of Social

- **With more URLs, comes more creativity from malicious actors**
- **The obfuscation of malicious sites is increasing**
  - e.g. using URL shorteners
- **Employing “confusion tactics” is commonplace**
  - e.g. fonts, spelling, etc.

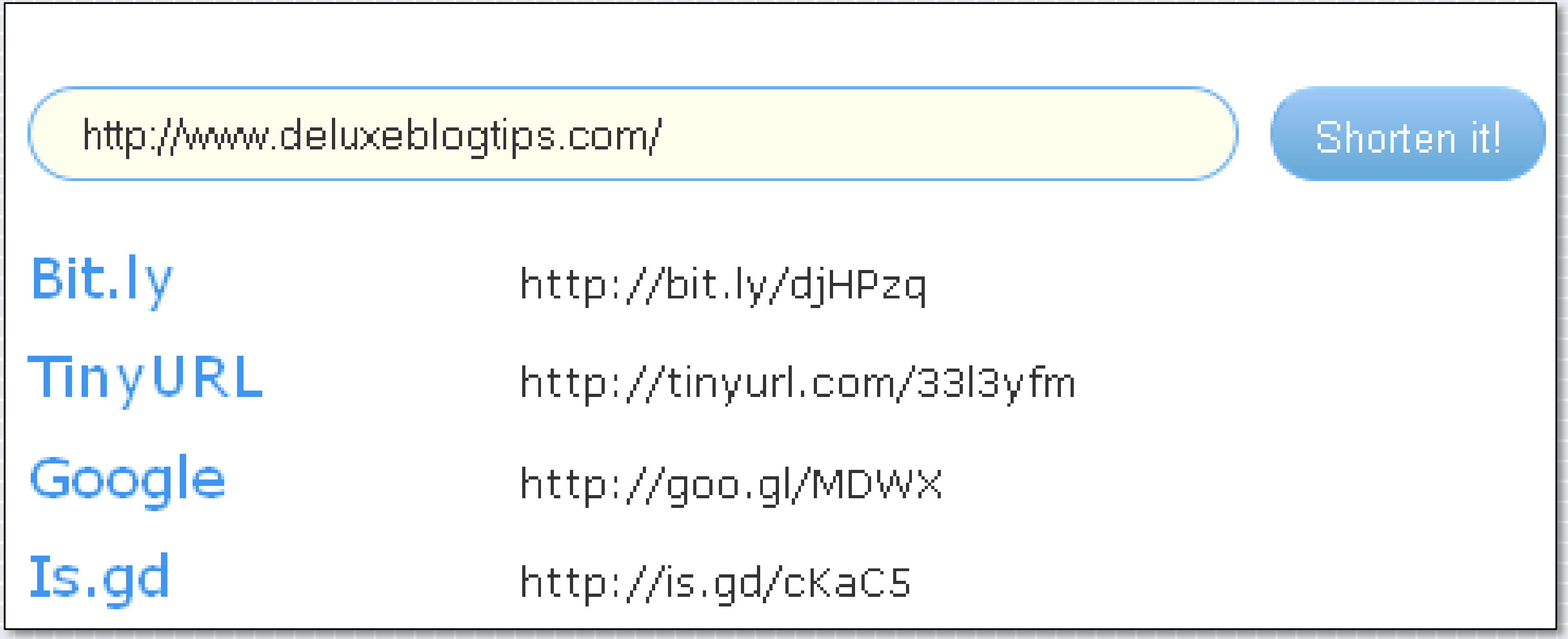


Avoiding Typhoid Mary

- Let’s take a look at some **DNS TRAFFIC** that you could expect to see via popular social media channels
- At the **VERY LEAST** you should be able to **MAKE MORE INFORMED DECISIONS**



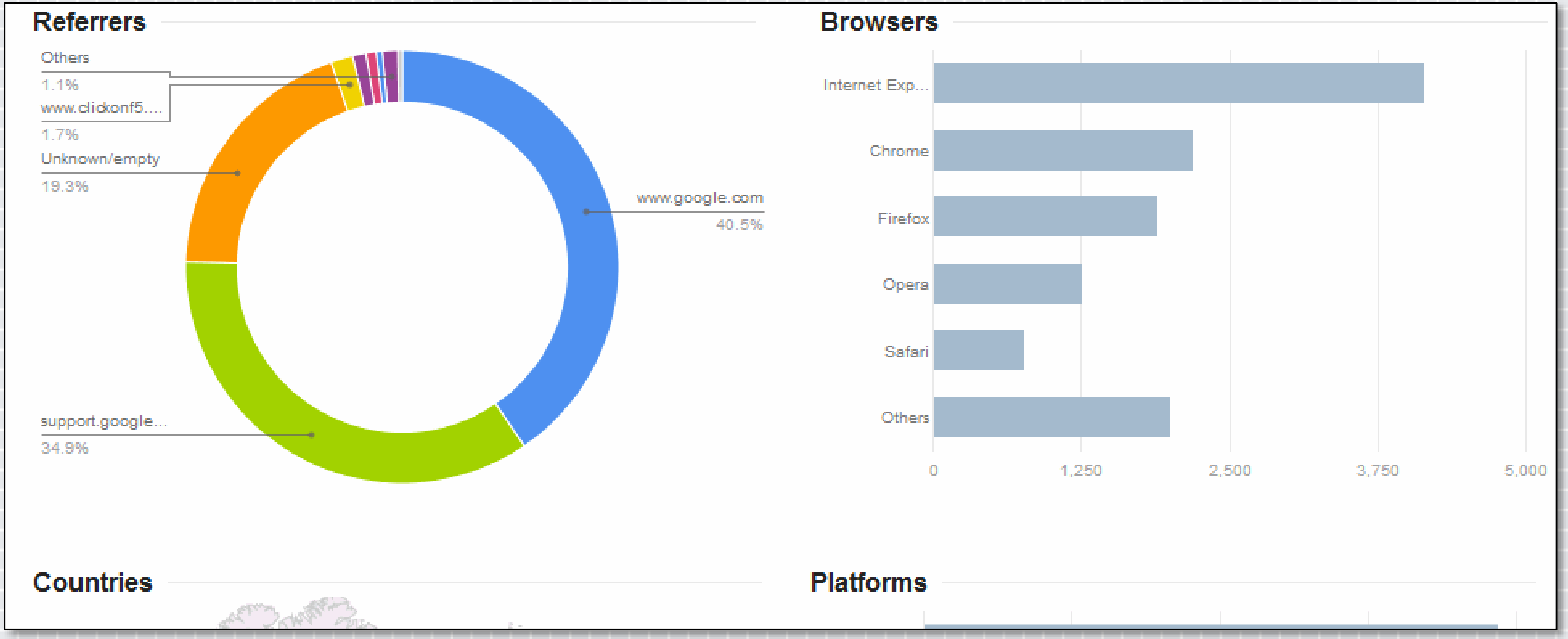
Example 1 – URL Shorteners



http://www.deluxeblogtips.com/

Bit.ly	http://bit.ly/djHPzq
TinyURL	http://tinyurl.com/33l3yfm
Google	http://goo.gl/MDWX
Is.gd	http://is.gd/cKaC5

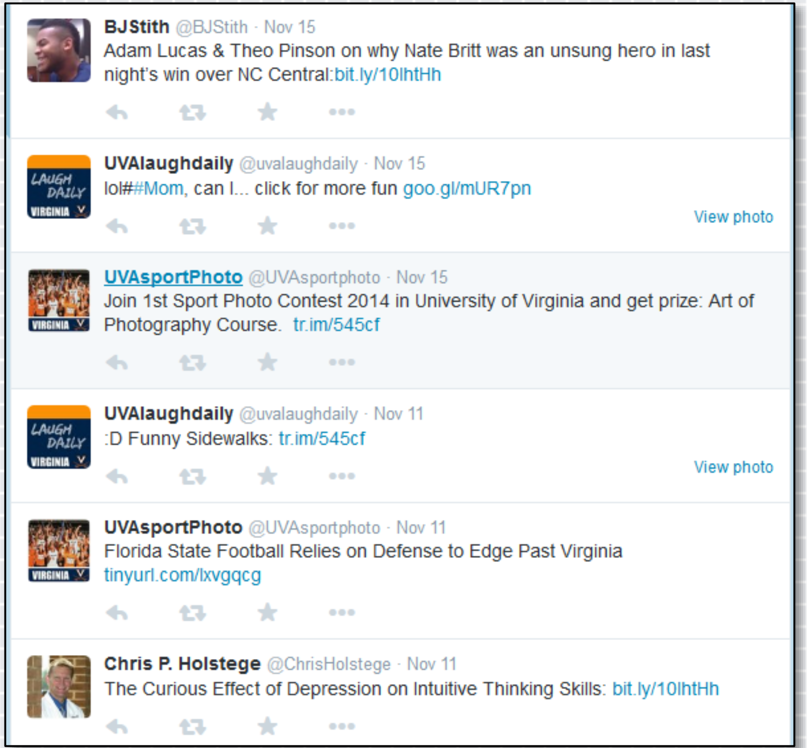
Example 1 – URL Shorteners (continued…)



Example 1 – URL Shorteners (continued…)

- URL shorteners are deterministic, thus the same URL gets encoded to the same shortened URL every time

- Run a discovered attack URL through every URL shortener, and then search for that URL through Google.



BJStith @BJStith · Nov 15
Adam Lucas & Theo Pinson on why Nate Britt was an unsung hero in last night's win over NC Central:bit.ly/10lhtHh

UVAlaughdaily @uvalaughdaily · Nov 15
lol##Mom, can I... click for more fun goo.gl/mUR7pn
View photo

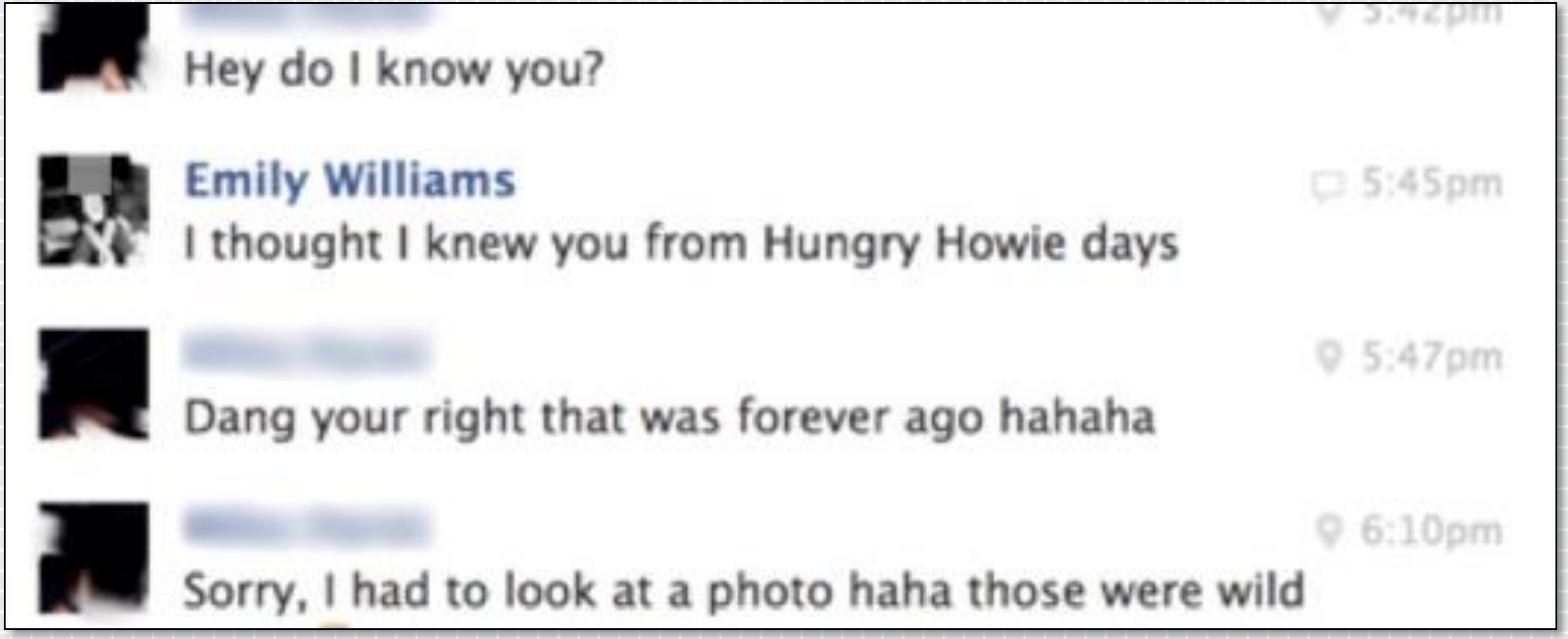
UVAsportPhoto @UVAsportphoto · Nov 15
Join 1st Sport Photo Contest 2014 in University of Virginia and get prize: Art of Photography Course. tr.im/545cf

UVAlaughdaily @uvalaughdaily · Nov 11
:D Funny Sidewalks: tr.im/545cf
View photo

UVAsportPhoto @UVAsportphoto · Nov 11
Florida State Football Relies on Defense to Edge Past Virginia tinyurl.com/lxvgqcg

Chris P. Holstege @ChrisHolstege · Nov 11
The Curious Effect of Depression on Intuitive Thinking Skills: bit.ly/10lhtHh

Example 2 – Spear Phishing .. (continued…)



[redacted] 5:42pm

Hey do I know you?

Emily Williams 5:45pm

I thought I knew you from Hungry Howie days

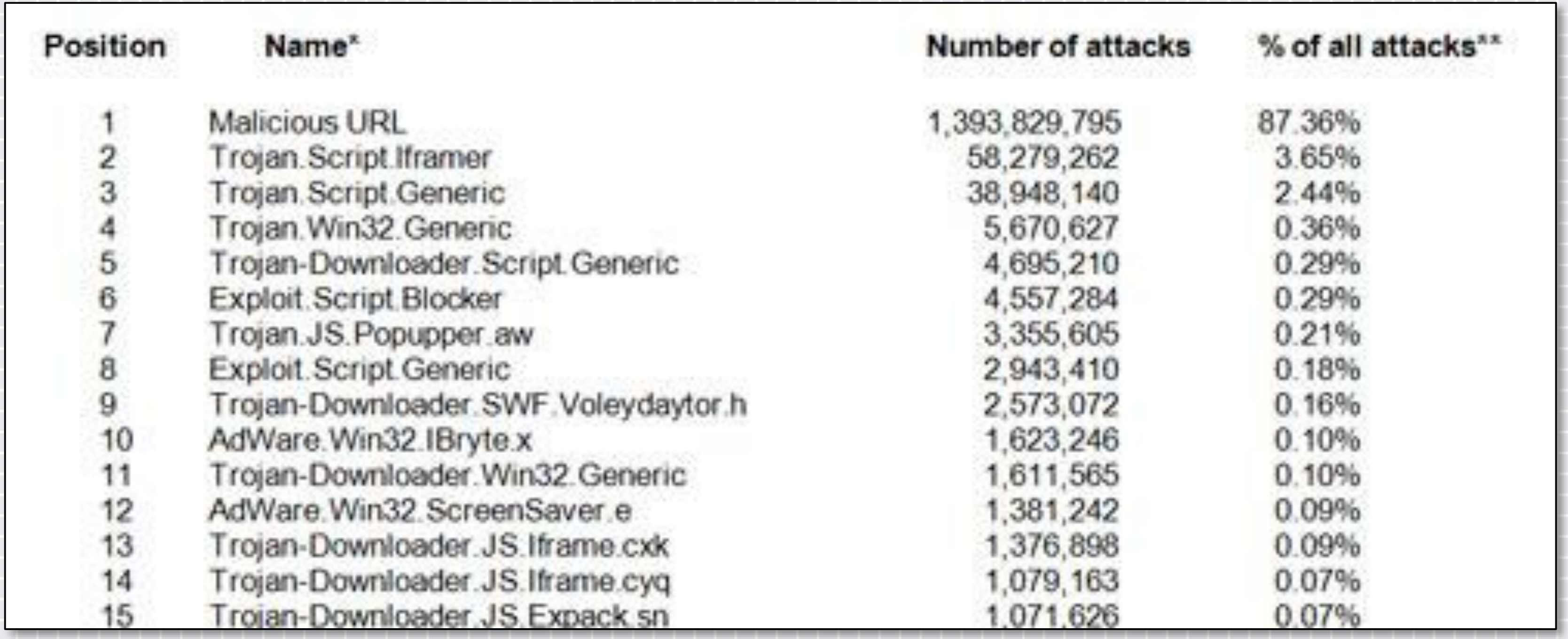
[redacted] 5:47pm

Dang your right that was forever ago hahaha

[redacted] 6:10pm

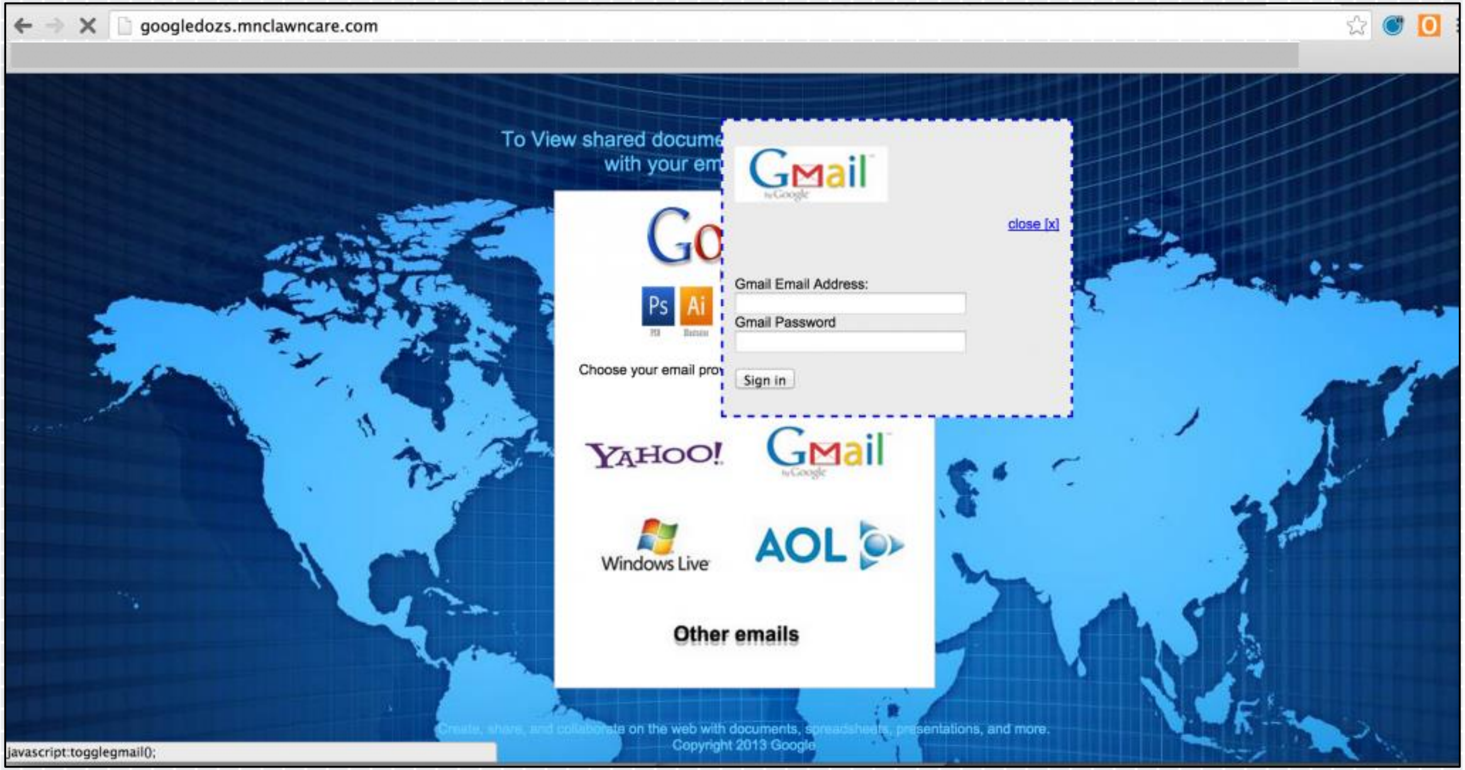
Sorry, I had to look at a photo haha those were wild

Example 2 – Spear Phishing .. (continued…)



Position	Name*	Number of attacks	% of all attacks**
1	Malicious URL	1,393,829,795	87.36%
2	Trojan.Script.Iframer	58,279,262	3.65%
3	Trojan.Script.Generic	38,948,140	2.44%
4	Trojan.Win32.Generic	5,670,627	0.36%
5	Trojan-Downloader.Script.Generic	4,695,210	0.29%
6	Exploit.Script.Blocker	4,557,284	0.29%
7	Trojan.JS.Popupper.aw	3,355,605	0.21%
8	Exploit.Script.Generic	2,943,410	0.18%
9	Trojan-Downloader.SWF.Voleydaytor.h	2,573,072	0.16%
10	AdWare.Win32.IBryte.x	1,623,246	0.10%
11	Trojan-Downloader.Win32.Generic	1,611,565	0.10%
12	AdWare.Win32.ScreenSaver.e	1,381,242	0.09%
13	Trojan-Downloader.JS.Iframe.cxk	1,376,898	0.09%
14	Trojan-Downloader.JS.Iframe.cyq	1,079,163	0.07%
15	Trojan-Downloader.JS.Expack.sn	1,071,626	0.07%

Example 3 – Fraudulent Websites



googledozs.mnclawncare.com

To View shared docume
with your em

Choose your email prov

Gmail Email Address:

Gmail Password

Sign in

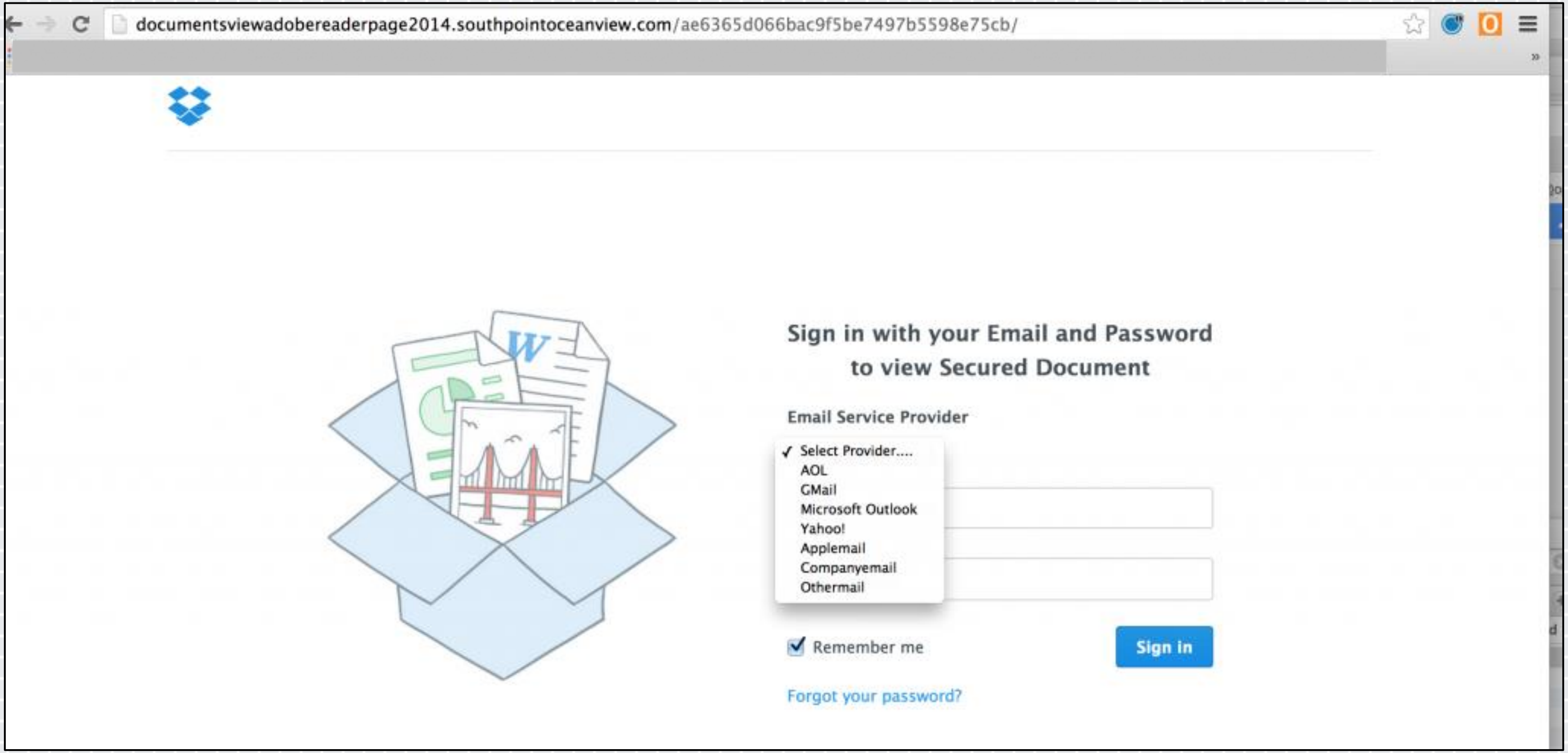
close [x]

Other emails

Create, share, and collaborate on the web with documents, spreadsheets, presentations, and more.
Copyright 2013 Google

javascript:togglegmail();

Example 3 – Fraudulent Websites

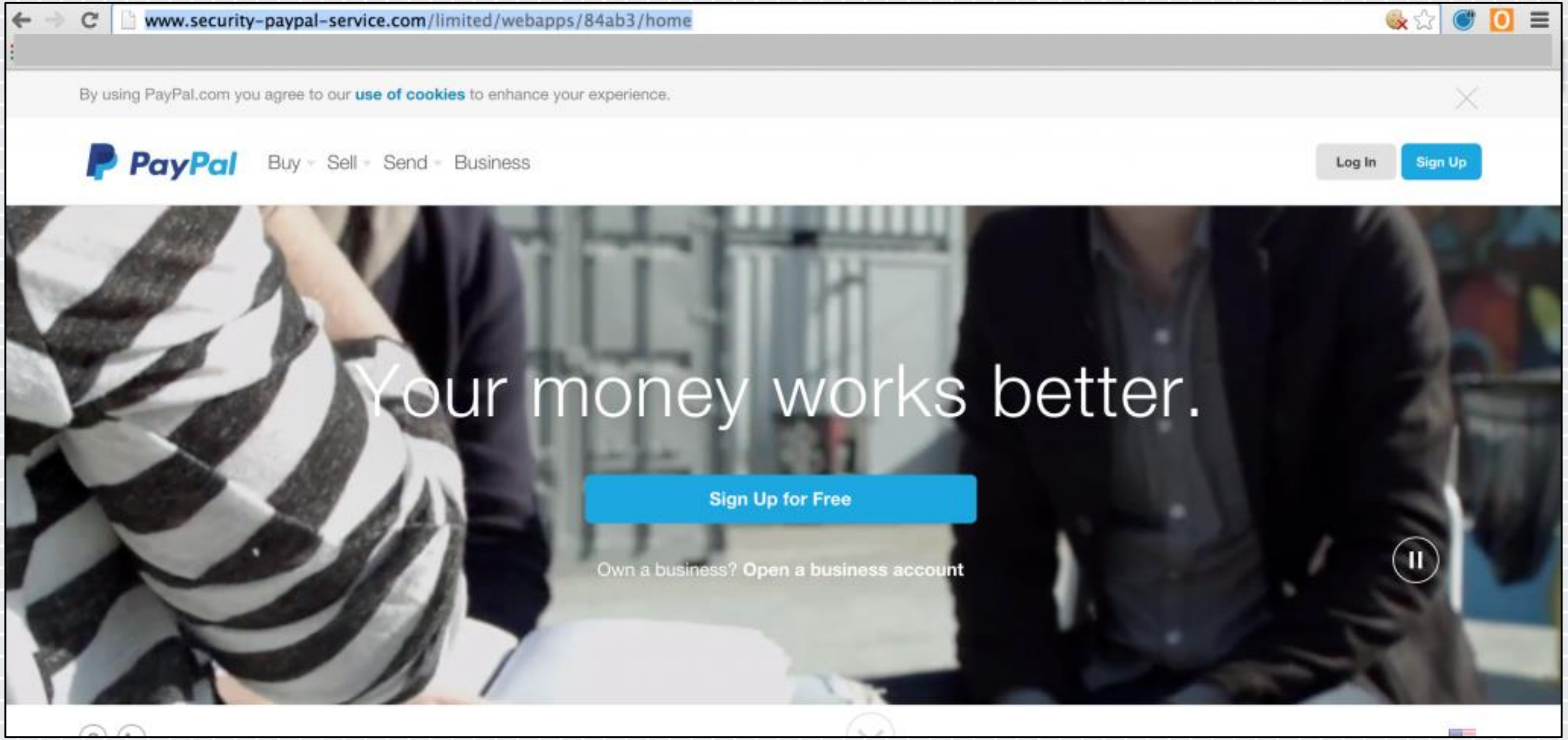


documentsviewadobereaderpage2014.southpointoceanview.com/ae6365d066bac9f5be7497b5598e75cb/

Sign in with your Email and Password
to view Secured Document

Email Service Provider

Example 3 – Fraudulent Websites



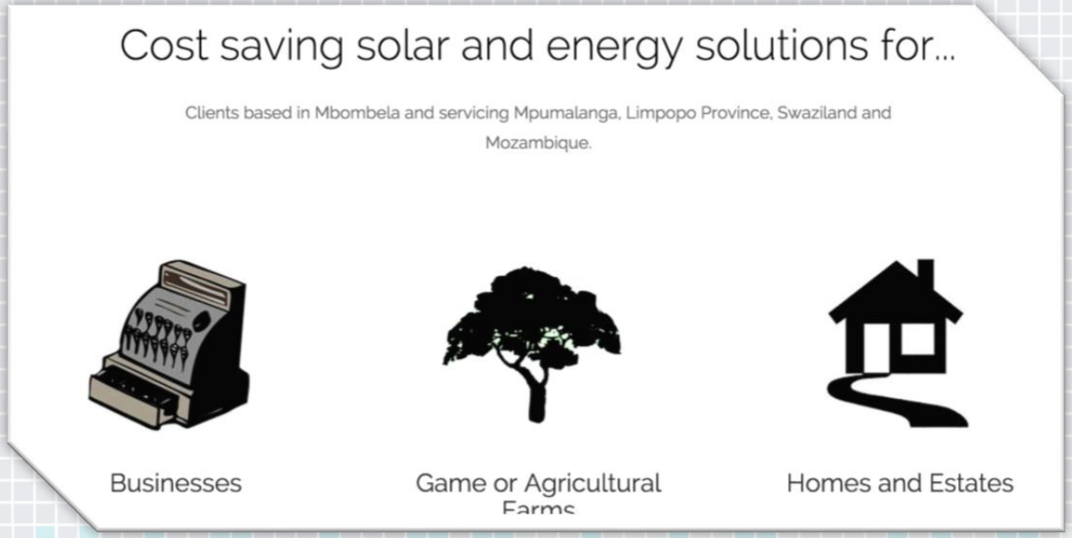
www.security-paypal-service.com/limited/webapps/84ab3/home

By using PayPal.com you agree to our **use of cookies** to enhance your experience.

Example 3 – Fraudulent Websites

- Let’s look at a seemingly innocuous domain

gfuel-alternative-energy[.]co[.]za

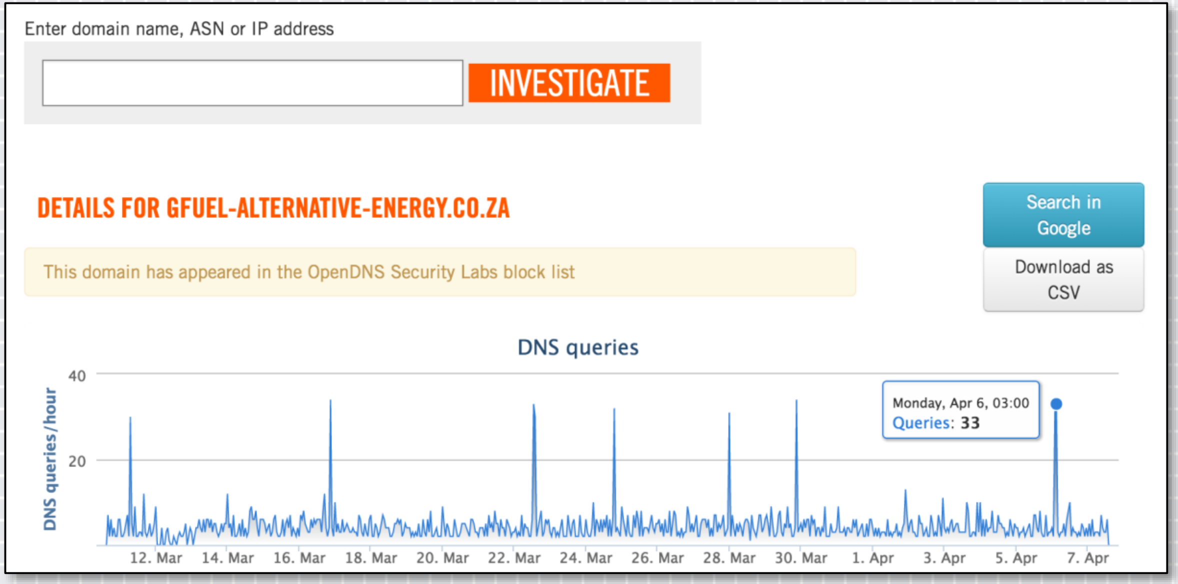


Cost saving solar and energy solutions for...

Clients based in Mbombela and servicing Mpumalanga, Limpopo Province, Swaziland and Mozambique.

Example 3 – Fraudulent Websites

- However, **gfuel-alternative-energy[.]co[.]za**, has previously appeared in the block list



Enter domain name, ASN or IP address

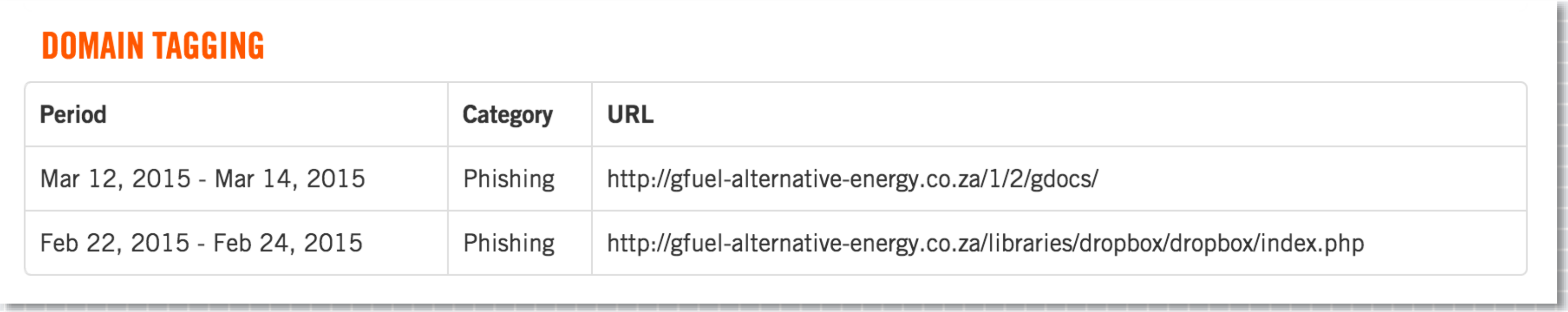
DETAILS FOR GFUEL-ALTERNATIVE-ENERGY.CO.ZA

This domain has appeared in the OpenDNS Security Labs block list

Monday, Apr 6, 03:00
Queries: 33

Example 3 – Fraudulent Websites

- And, gfuel-alternative-energy[.]co[.]za, has previously been tagged as a phishing site

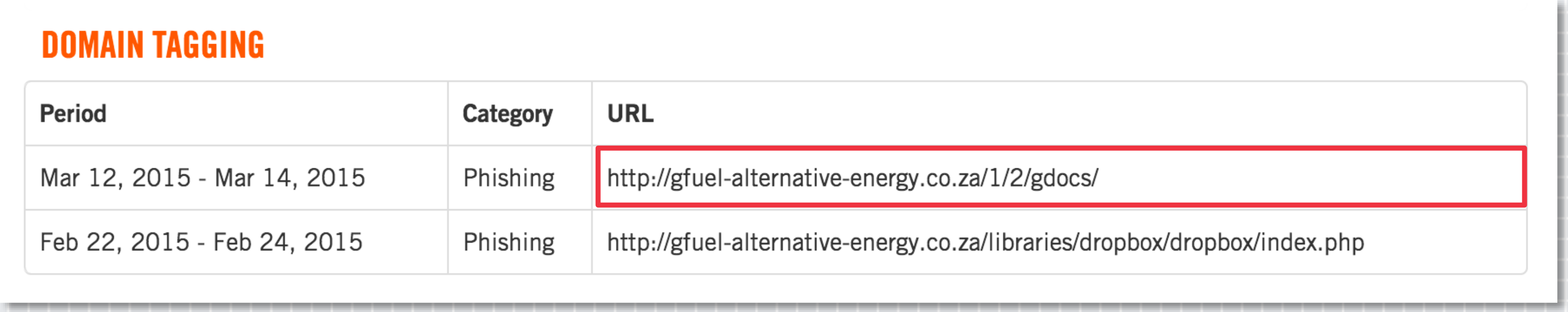


DOMAIN TAGGING

Period	Category	URL
Mar 12, 2015 - Mar 14, 2015	Phishing	http://gfuel-alternative-energy.co.za/1/2/gdocs/
Feb 22, 2015 - Feb 24, 2015	Phishing	http://gfuel-alternative-energy.co.za/libraries/dropbox/dropbox/index.php

Example 3 – Fraudulent Websites

- But everything is fixed now, right?

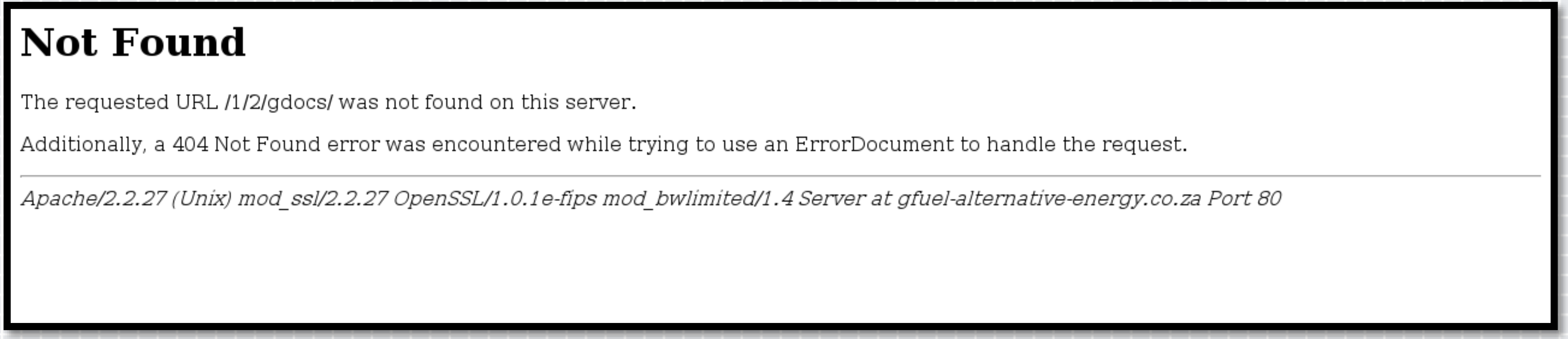


DOMAIN TAGGING

Period	Category	URL
Mar 12, 2015 - Mar 14, 2015	Phishing	http://gfuel-alternative-energy.co.za/1/2/gdocs/
Feb 22, 2015 - Feb 24, 2015	Phishing	http://gfuel-alternative-energy.co.za/libraries/dropbox/dropbox/index.php

Example 3 – Fraudulent Websites

- Looks to be taken down



Not Found

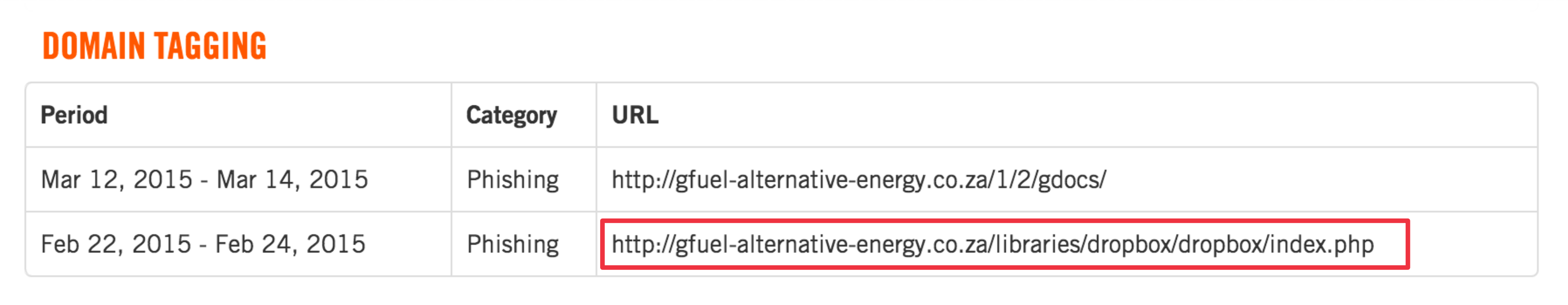
The requested URL /1/2/gdocs/ was not found on this server.

Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request.

Apache/2.2.27 (Unix) mod_ssl/2.2.27 OpenSSL/1.0.1e-fips mod_bwlimited/1.4 Server at gfuel-alternative-energy.co.za Port 80

Example 3 – Fraudulent Websites

- If that one is removed, surely the older one has been removed, right?

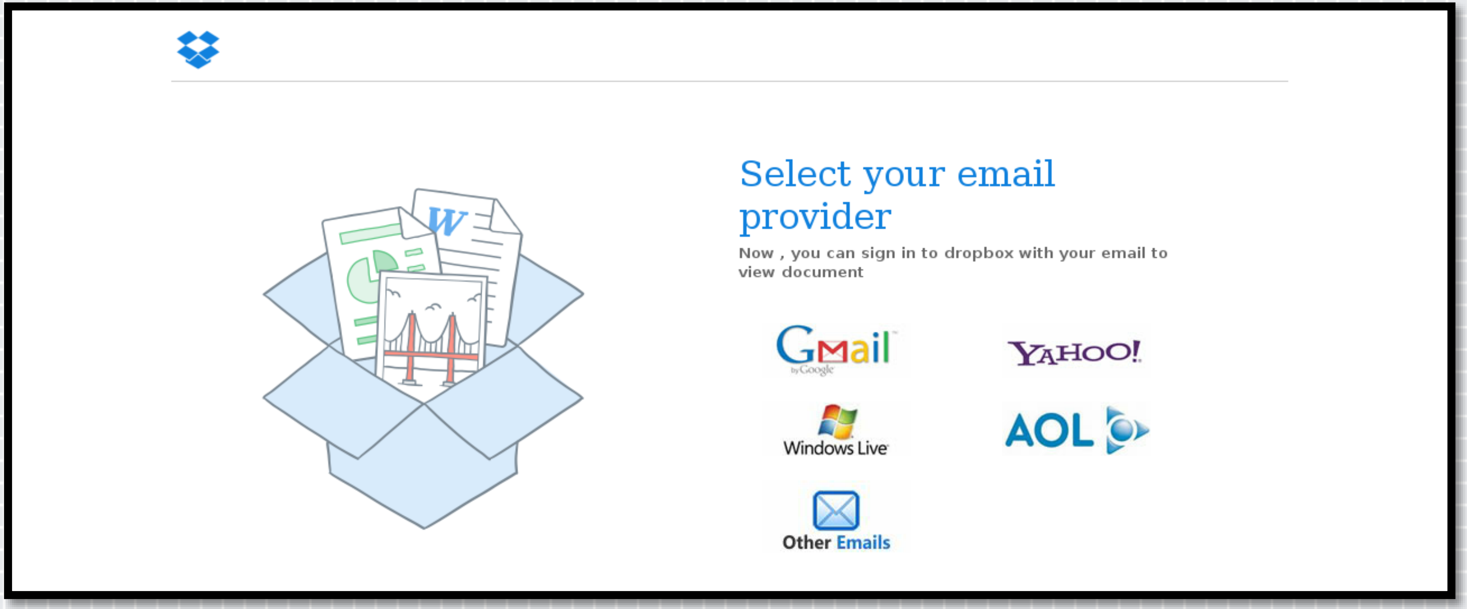


DOMAIN TAGGING

Period	Category	URL
Mar 12, 2015 - Mar 14, 2015	Phishing	http://gfuel-alternative-energy.co.za/1/2/gdocs/
Feb 22, 2015 - Feb 24, 2015	Phishing	http://gfuel-alternative-energy.co.za/libraries/dropbox/dropbox/index.php

Example 3 – Fraudulent Websites

- Maybe not…



Select your email provider

Now , you can sign in to dropbox with your email to view document

The Good News

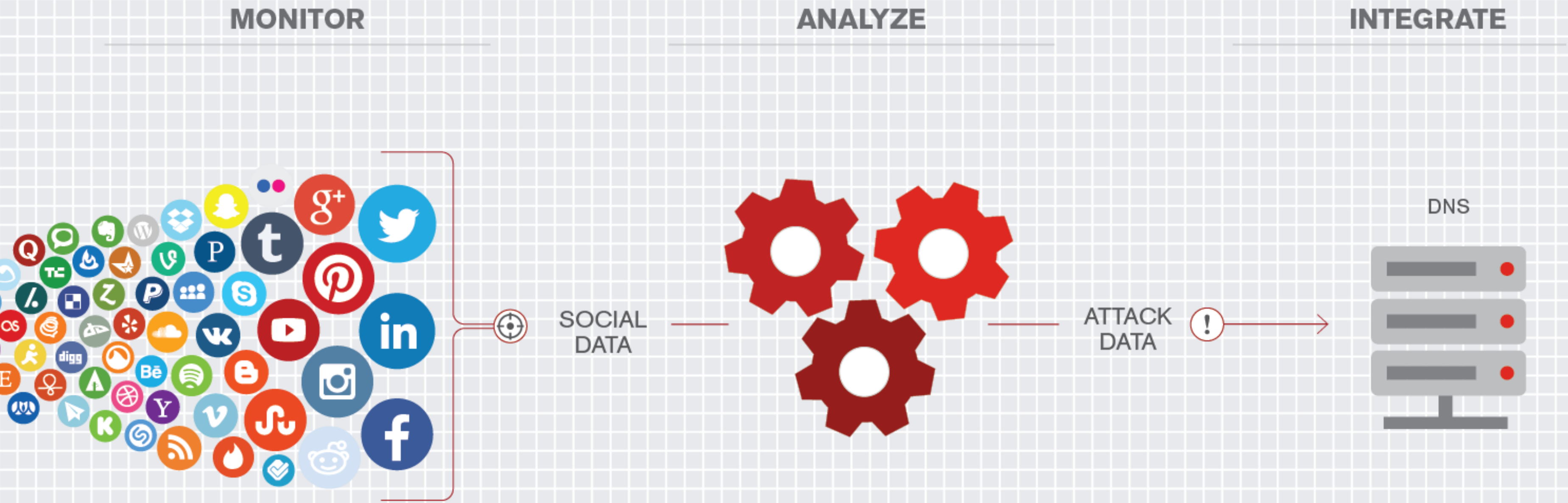
> What enables the wise sovereign and the good general to strike and conquer, and achieve things beyond the reach of ordinary men, is foreknowledge.

--Sun Tzu

The Good News

- For the clever security professional, social media is **a gold mine of publicly-facing, proactive intelligence**
- Social media data can be leveraged to enhance existing security tools
- The newest threat vector is simultaneously the **newest security OSINT repository**
- **Threats are circulated in broad daylight**

Think About it This Way



Your Security Framework Just Got Deeper

- Social media is a robust new layer in any defense-in-depth posture
- **Malicious links** found on social media **means enhanced DNS filters**
- As social media continues to grow, **leverage it to empower your existing DNS framework**

Breaking News April (continued…)

Conclusion

- Defense in depth is more than new boxes on your network
- Need Outside-In for Defense in depth
- Social enables your business & also creates new vulnerability
- Social is either a risk or an ally – **you decide**

Apply

- Does your organization have a security posture to address cyber security threats via social?
- Enable proactive security to minimize exposure to social media threats
- Continue to improve and tune measures based on your organization’s needs to enable a crucial layer of any defense in depth strategy