

BlackHat Abu Dhabi 2011: Fun with Google Custom Searches

Intelligence, Secrets & Leaks

Jamal Bandukwala

11/18/2011

<http://infosecmindstorm.blogspot.com/>

Contents

Google Custom Searches- Background	3
The Open Source Intelligence Deep Web Search	3
Pastebin and collaborative tools intelligence web search.....	9
Social Networking Search	19
Invisible Attacks	24
Final Thoughts/ Conclusion.....	25
About the Author	25
Works Cited.....	26

Google Custom Searches- Background

Google offers a program that allows developers/ users to create their own custom search engines. The Custom search option allows interested parties to be up and running in minutes using a wizard interface along with more advanced options to further customize or fine tune their searches as per their needs (Google Custom Search Developers Guide, Introduction). In this case Google does the heavy lifting and allows the custom search owner to focus on developing/ creating their content/ search list. When using Custom Searches the user/ search creator can choose to either host the code themselves, or allow Google to do it for them. Advanced options of note include the ability to fine tune search results by removing items from the search (while leaving the site in question on the list), promoting search results and on-demand indexing. These enable the user to retrieve search results from newly added sources in a shorter time frame (Improved On Demand Indexing, Google Custom Search Blog).

When a user carries out a traditional Google search, he/she can sometimes end up with very large numbers of hits, most of which are not relevant to what they are looking for and when they try to use advanced operators the user is restricted to going through one source at a time. My custom searches allow an analyst/ researcher to peruse multiple relevant sources at the same time. I have put together three different custom searches/ engines; each of these searches goes through different types of online sources/ content and consequently provides different types of information/ intelligence. This paper will examine the type of information each of these searches goes through, how they can be used, and the types of information one can get from them.

The Open Source Intelligence Deep Web Search

(<http://www.google.com/cse/home?cx=013791148858571516042:eygbr9xc-ys>)

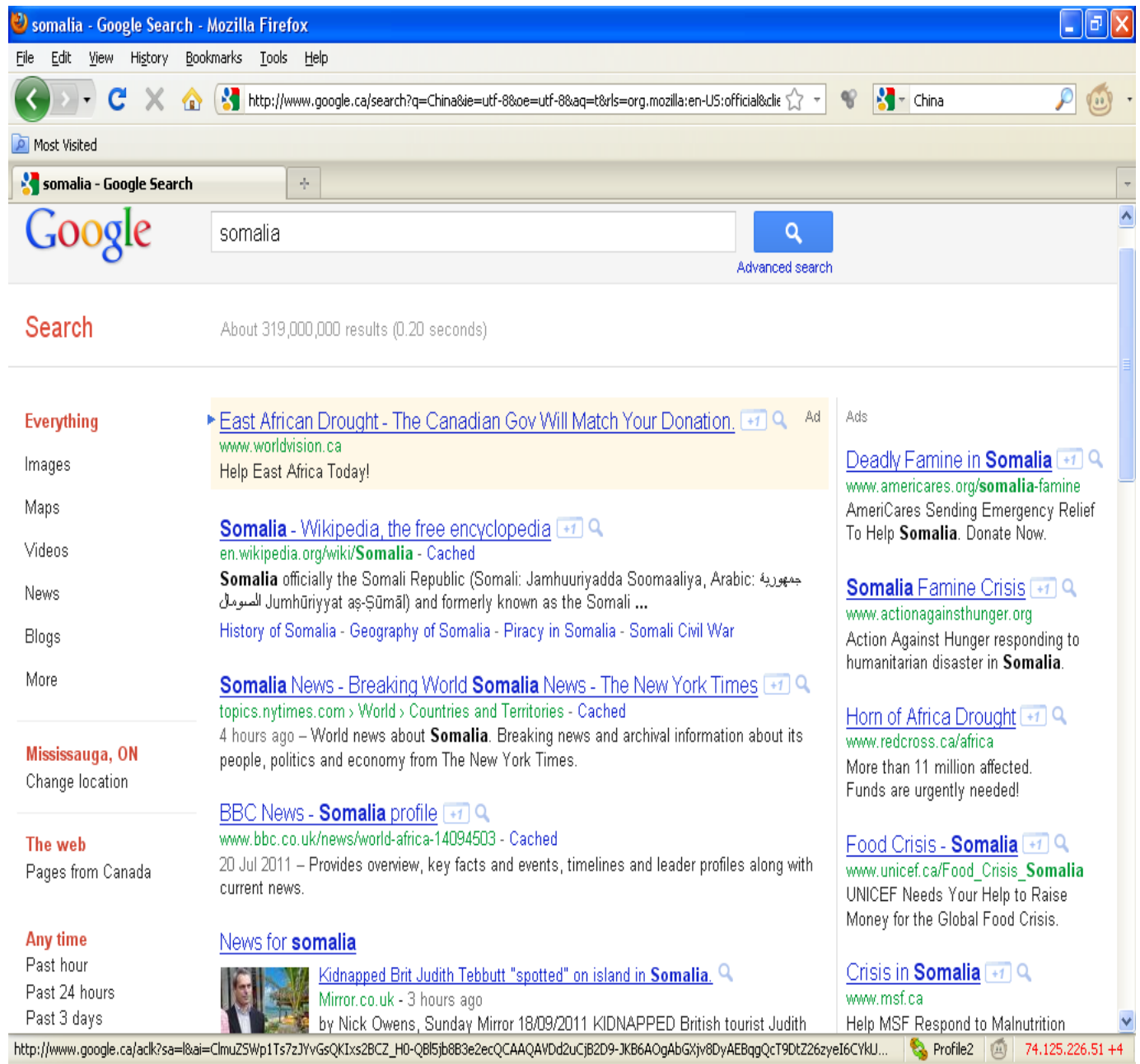
Open Source Intelligence (OSINT) is a form of intelligence gathering from open sources. Open sources refers to publically available information as opposed to covert information. This includes everything from media like newspapers, TV, web content (blogs, wikis, among others), satellite images, public databases, academic journals/ conference info and any other publically available information. In 2006 the Washington Times had an article discussing how OSINT was becoming increasingly important. I find that the following lines were really significant:

“A Defense Department official said Chinese military bloggers have become a valuable source of intelligence on Beijing’s secret military buildup. For example, China built its first Yuan-class attack submarine at an underground factory that was unknown to U.S. intelligence until a photo of the submarine appeared on the Internet in 2004.” (Washington Times)

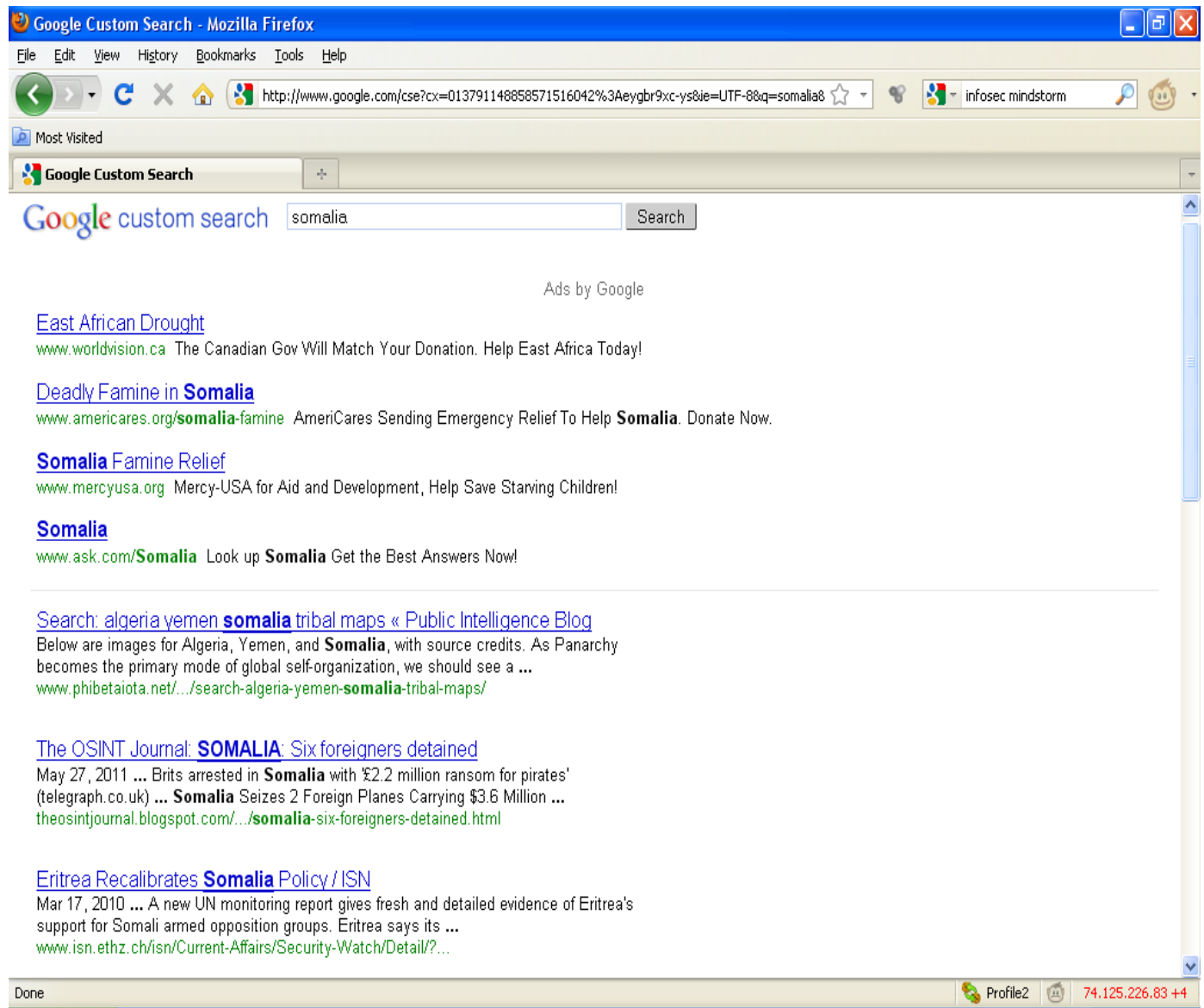
In this case, I have put together a customized Google search that runs against a large list of Open source intelligence sources (which I have compiled and actively maintain); examples of the sites in this search include <http://boardreader.com>, <http://www.deepwebtech.com> and <http://www.turbo10.com/> (Open Source Intelligence Deep Web Search, Infosec Mindstom).

As we are using Google to run against a specified list of sites that includes a variety of intelligence sources ranging from Chinese military bloggers to specialized sites that query various open databases this provides very different results from a regular Google search. A good example of this is if an analyst is looking for information on Somalia and types this term into a regular Google search they get over 319 million results (Screenshot A) most of which are not relevant to them. The same term run through the OSINT Deep Web Search generates very different results as can be seen in Screenshot B. In another attempt, I typed in “RBC Capital Markets” and came across a listing of individuals who were potentially employed, or were affiliated in some way with RBC Capital Markets, the search and listing can be seen in Screenshots C and D. This sort of information could be very useful for a penetration tester, or for someone who wanted to launch a spear phishing attack targeting specific individuals at an organization. As one can see the OSINT search makes it easier for analysts/ researchers to locate relevant information and reduces some of the false positives that come with traditional searches; this particular custom search is especially useful for acquiring political, economic and related intelligence.

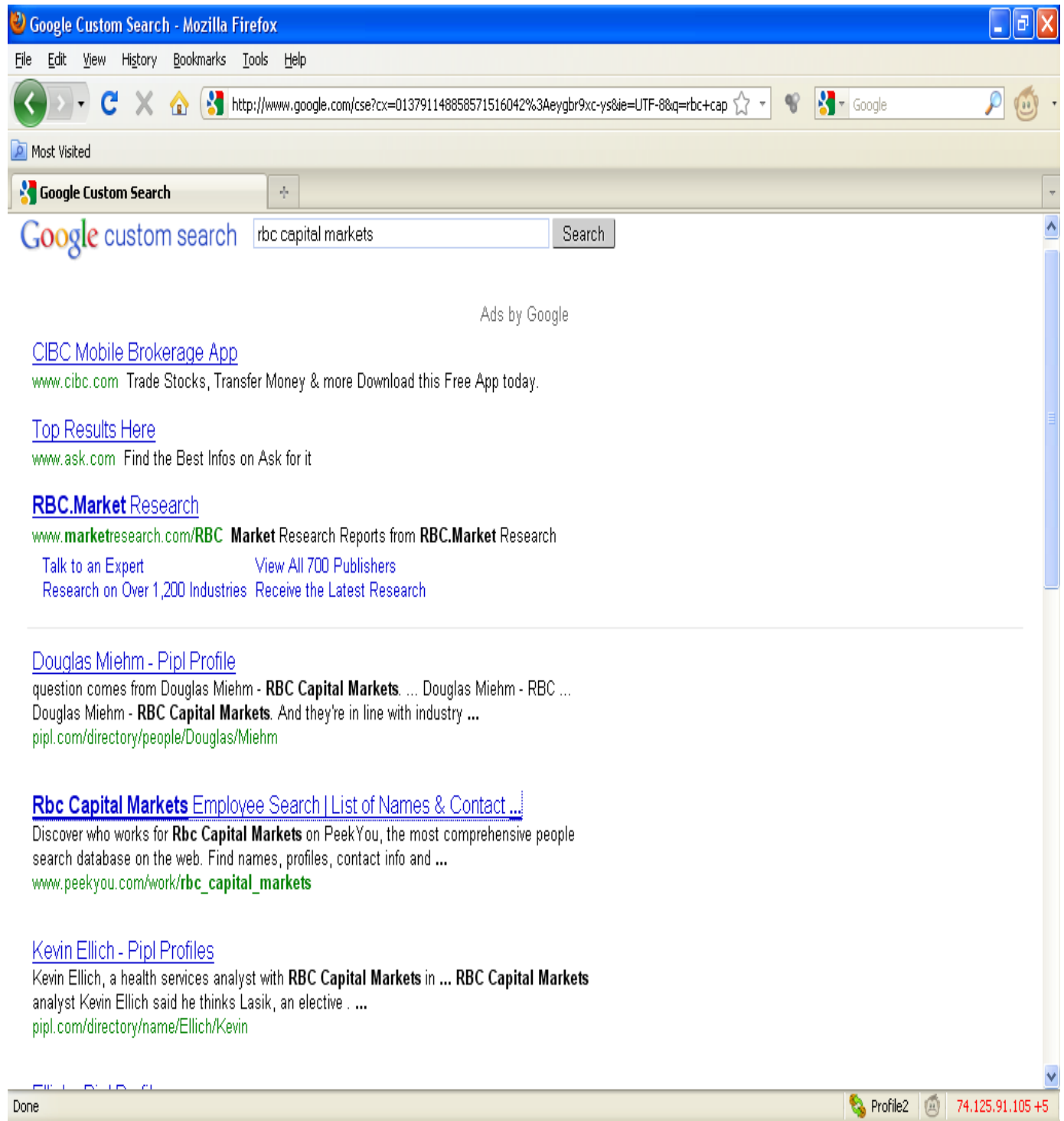
Screenshot A



Screenshot B



Screenshot C



Screenshot D








Rbc Capital Markets Employee Search | List of Names & Contact info for Rbc Capital Markets at PeekYou - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.peakyou.com/work/rbc_capital_markets

Most Visited

Google Custom Search Rbc Capital Markets Employee S...

	Philip Hintze New York, NY Rbc Capital Markets	1
	Hillary Christiansen Vienna, VA Arlington, VA Rbc Capital Markets - Apollo Housing Capital	1
	Jeffrey Greiner Greenwood, MN Rbc Capital Markets	1
	Sarah L. Barnett 35 yrs, butterflypryncess Aztec, NM Oakland, CA Daly City, CA Rbc Capital Markets	3
	Troy Maxwell Toronto, ON Managing Director & Chief Financial Officer	1
	Jill Gardiner Vancouver, BC Rbc Capital Markets	1
	Amy M. Baldwin 32 yrs Pleasant Hill, CA Robertson Stephens Rbc Capital Markets Assistant ...	2

make a quizmore quizzesgrab code theatre and Walt Disney World take this quiz Physical Therapist Aid moody Self Employed design creative team player english Social Worker its all about donnie brosko University of Maryland boston legel PERSONAL TRAINER i watch bet and espn Prince Georges Community College Artist

Top Searches

- Piracy
- Terrorism
- "tanya Tripi-weiss"
- List Of Rbc Capital Markets Employees
- Aura Reinhard
- List Of Employees Rbc
- Rbc Cm Employee
- Rbccm Employee Directory
- Tanya Tripi-weiss
- Rbc Capital Markets New York Employee Directory

Find us on Facebook

PeekYou - Free People Search

59,929 people like PeekYou - Free People Search.

Transferring data from in.getclicky.com...

Profile2 38.108.107.11

Pastebin and collaborative tools intelligence web search

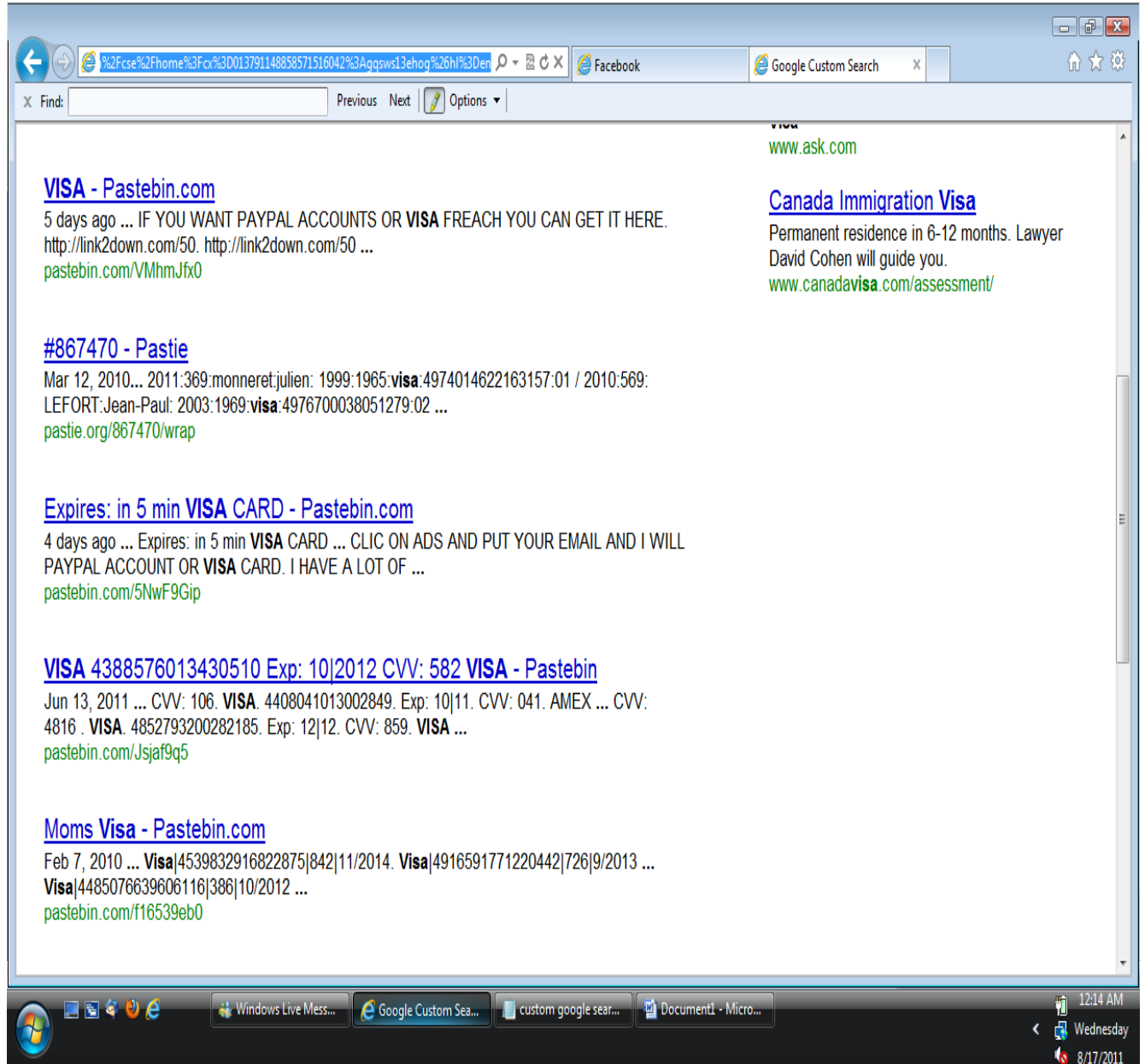
(<http://www.google.com/cse/home?cx=013791148858571516042:gqsws13ehog&hl=en>)

What is a pastebin? A pastebin is a site that allows users to post snippets of text for others to view; different pastebin sites can be targeted towards different audiences (Wikipedia, Pastebin). This is different from twitter, as twitter has a fixed limit of characters per communication while pastebin sites do not. While pastebin sites do have legitimate uses, a number of pastebin sites are also used to post spam and also by various parties (including Anonymous and Lulzsec) to leak/ post information (Zeltser, The Use of Pastebin for Sharing Stolen Data).

The pastebin intelligence search goes through more than twenty different pastebin sites, ranging from popular sites like pastebin.com to some more obscure sites like <http://piratepad.net>. The list of sites is regularly updated, but is not available to the public as it is confidential; more examples of the sites being searched can be found on my blog (Pastebin and Collaborative Tools Web Search, Infosec Mindstorm). I tried a number of searches with this custom search engine and got back some rather surprising results. The searches resulted in everything from credit card numbers, leaked databases, compromised sites and even travel itineraries and passport information.

As an example I typed in “VISA” in the pastebin custom search and came across various Visa numbers posted online and various individuals offering to sell credit card related information as can be seen in both Screenshot E and Screenshot F.

Screenshot E



Screenshot F

|| VISA | AMEX | MASTERCARD | DISCOVER | Huge List! | | - Pastebin.com - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://pastebin.com/k52W1Qv

Most Visited

Google Custom Search

|| VISA | AMEX | MASTERCARD | DISCOVER | Huge List! | |

BY: A GUEST | SEP 1ST, 2011 | SYNTAX: NONE | SIZE: 21.82 KB | VIEWS: 229 | EXPIRES: NEVER

COPY TO CLIPBOARD | DOWNLOAD | RAW | EMBED | REPORT ABUSE

Like

MY PASTES

PUBLIC PASTES

Untitled 4 sec ago

Childrens.Hospital.US.S... 10 sec ago

Untitled 10 sec ago

Readiris Pro v12.0.1.10... 12 sec ago

saberooc 18 sec ago

Untitled 16 sec ago

Christie McCarthy - Cau... 19 sec ago

Christie McCarthy - Fai... 19 sec ago

LAYOUT WIDTH

Life? Love? Future? Get your answers

Done Profile2 184.154.125.14

1. For more, please visit: <http://ughackerzworld.blogspot.com/>

2. If you would like to purchase, please email; zuchiro@live.com

3. Hacking supplies updated hourly!

4.

5. ANASTAS HACKETT|4852470003787401|08|11|042|229-19 MERRICK BLVD, 313|LAURELTON|11413|New York|US|7187491152|

6. Ae Young Lee|4147202046962146|12|11|109|350 S 200 W, Apt C308|Salt Lake City|84101|Utah|US|8018331261|

7. Jermaine Burbridge|4185868003847083|11|11|408|7200 sw 4th ct.|North Lauderdale|33068|Florida|US|9549074995|

8. Carol Little|4266841197606583|11|11|583|215 Ninth Av|La Grange|60525|Illinois|US|708-354-8637|

9. Mark Royal|4640188001228650|10|11|464|314 E Cairo Dr|Tempe|85282|Arizona|US|480 760-5586|

10. Thyra Romito|4147202014300568|10|11|162|125 Lakeview Drive #701|Bloomington|60108|Illinois|US|630-570-3666|

11. randy kendrick|4128004052956282|01|12|762|3964 E. paradise view dr|paradise valley|85253|Arizona|US|6029546262|

12. Greg Leach|4388576016657762|01|12|719|855 Sand Ave|Eugene|97401|Oregon|US|541-746-2110

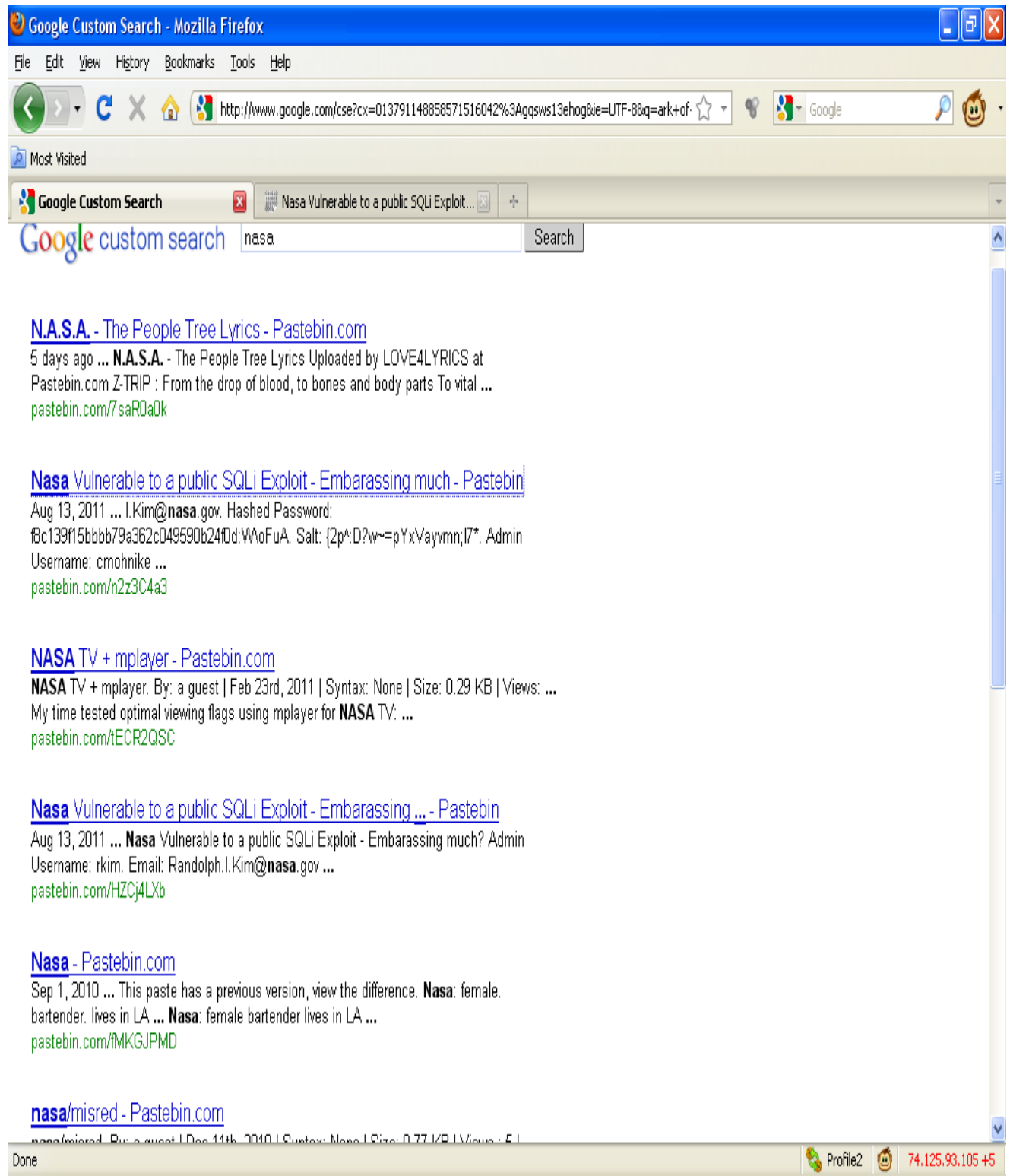
13. Don Gonzales|4712037340968646|12|11|422|41 Forest Drive|Mansfield|76063|Texas|US|817-456-1021

14. martha walker|4147202039291958|12|11|047|22118 miller ridge rd.|los gatos|95033|California|US|408-395-5306

15. Barry Taylor|1962-07-21|USA|TX|75154|RED OAK|402 Prah Rd |Red Oak TX 75154|TAYLOR

I then tried searching for NASA and came across posts claiming that some NASA sites were vulnerable to a public SQLi exploit and had potentially been compromised, the search and results can be seen in both Screenshot G and Screenshot H. I was really surprised when I got similar results when I searched for Police and Air Force as well (different states/ countries police and air force sites). This is significant because I simply typed in these terms and came across these postings; I was not actively seeking compromised sites.

Screenshot G



Screenshot H

Nasa Vulnerable to a public SQLi Exploit - Embarrassing much? Admin Username: - Pastebin.com - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://pastebin.com/HZCj4LXb

Most Visited

Google Custom Search

Nasa Vulnerable to a public SQLi E...

BY: A GUEST | AUG 13TH, 2011 | SYNTAX: NONE | SIZE: 0.62 KB | VIEWS: 45 | EXPIRES: NEVER

COPY TO CLIPBOARD | DOWNLOAD | RAW | EMBED | REPORT ABUSE

Predictions! Compatibility! Games! And More!

ASTROLOGY.COM

```
1. Nasa Vulnerable to a public SQLi Exploit - Embarrassing much?
2.
3. Admin Username: rkim
4. Email: Randolph.I.Kim@nasa.gov
5. Hashed Password: f8c139f15bbbb79a362c049590b24f0d:W\oFuA
6. Salt: {2p^:D?w~=pYxVayvmn;17*
7.
8. Admin Username: cmohnike
9. Email: MohnikCC@nv.doe.gov
10. Hashed Password: 6c6e2b5e36846c2aee99b1c6ell194f63
11. Salt: )~#FJj:zQ^52q:SF{&5MDCILiPi2S=
12.
13. - If shit like this is vulnerable to public exploits, imagine whats vulnerable to private 0days :) -
14.
15. [+] TriCk - TeaMp0isoN
16. [+] Shoutouts: iN^SaNe - Hex00010 - MLT
17.
18. Twitter:
19. @TeaMp0isoN_
20.
21. **NOTE: A joint #TeaMp0isoN & #Anonymous Operation is about to hit the interwebs soon **
```

MY PASTES

PUBLIC PASTES

Untitled 4 sec ago

ABIX v6.67.03 Bilanguag... 12 sec ago

Untitled 17 sec ago

Untitled 23 sec ago

Untitled 30 sec ago

Untitled 29 sec ago

Untitled 35 sec ago

Untitled 41 sec ago

LAYOUT WIDTH

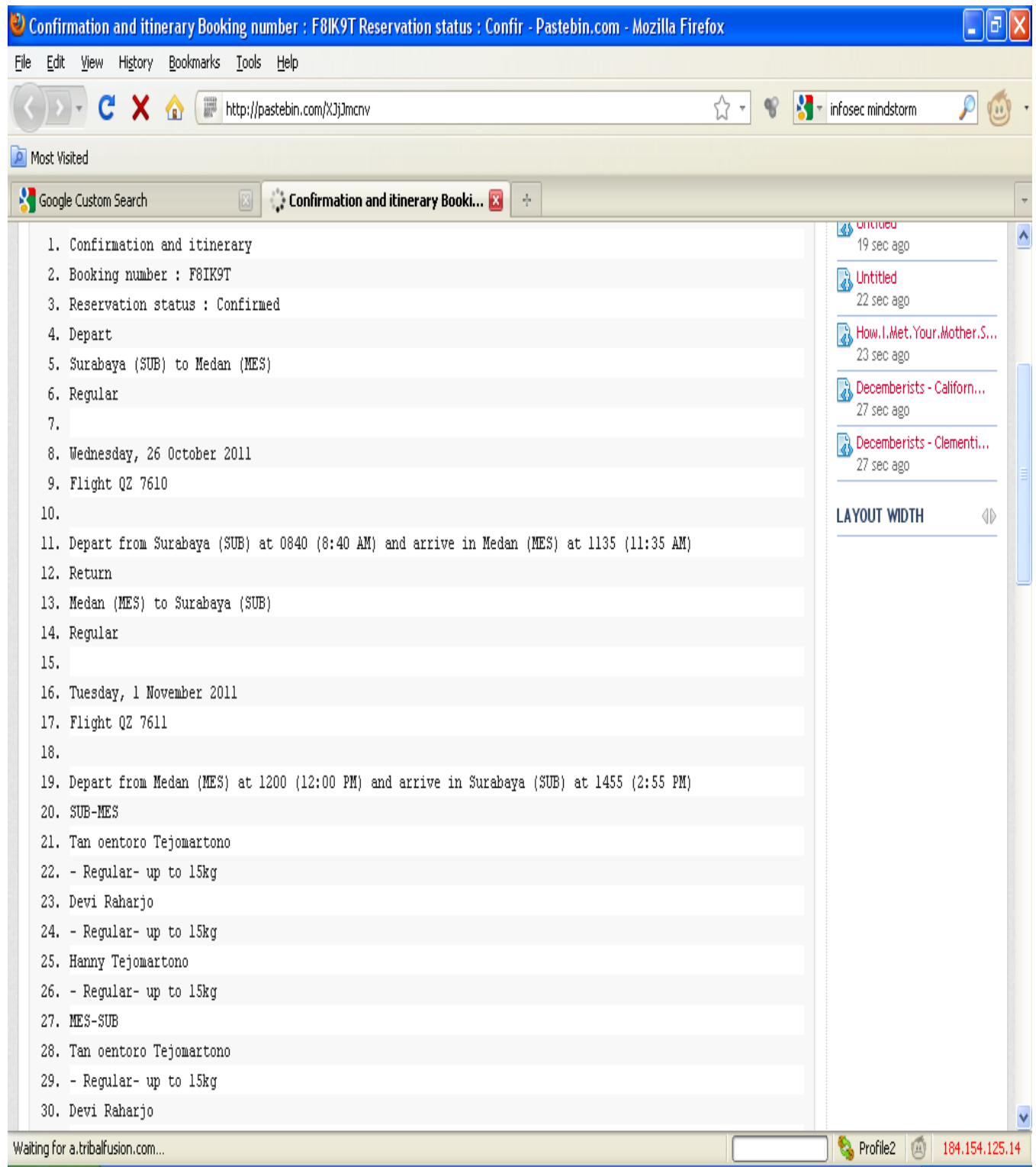
Predictions! Compatibility! Games! And More!

Done

Profile2 184.154.125.14

As a final example I typed in passport number and came across several trip bookings that included everything from travel itineraries, flight booking numbers, airline ticket numbers and passport information. In some cases the information was for upcoming travel dates and a malicious party would have been able to interrupt a person's travel plans, by attempting to cancel or reschedule flights, hotel bookings and other plans. In other cases the itineraries and information were for trips that had already taken place, a malicious party could still have attempted to use this information to take over an identity, you can see examples of this in Screenshot I and Screenshot J. The reader can see that the pastebin search generates a lot of results relating to exposed and leaked information; this same tool can also be used to get a better understanding of some of the risks an organization faces and take the necessary actions to counter these. As an example if an organization suspects that one of their members is leaking or stealing information, they can setup a honeytrap and monitor the pastebin engine for specific keywords or terms.

Screenshot I-1



Screenshot I-2

Confirmation and itinerary Booking number : F8IK9T Reservation status : Confir - Pastebin.com - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://pastebin.com/XJjmcnv

Most Visited

Google Custom Search Confirmation and itinerary Book...

32. Hanny Tejomartono
33. - Regular- up to 15kg
34. Guest information
35. Guest 1: Tan oentoro Tejomartono
36. Nationality: Indonesia
37. Date of Birth: 08/04/1954
38. Identification/Passport number: 3573050408540001
39. Issuing Country: Indonesia
40. Expiration Date: 08/04/2015
41.
42. Guest 2: Devi Raharjo
43. Nationality: Indonesia
44. Date of Birth: 04/06/1957
45. Identification/Passport number: 3573054604570001
46. Issuing Country: Indonesia
47. Expiration Date: 04/06/2015
48.
49. Guest 3: Hanny Tejomartono
50. Nationality: Indonesia
51. Date of Birth: 09/24/1988
52. Identification/Passport number: 3573056409880006
53. Issuing Country: Indonesia
54. Expiration Date: 09/24/2012
55.
56. Booking contact
57. verryadi harsono
58. Address 1: PBI J2 no 5, malang, Jawa Timur 65125, Indonesia
59. Business phone:
60. Home phone:
61. Mobile phone: 6281555729199

SHARE PASTEBIN

3k

+1

Read cdn5.tribalfusion.com

Profile2 184.154.125.14

Screenshot J

DO-NOT-REPLY@STATE.GOV on Monday U.S. DoS - CEAC Confirmation (AA001PSIEJ) Dea - Pastebin.com - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://pastebin.com/8GBYQ7i6

Most Visited

Google Custom Search

DO-NOT-REPLY@STATE.GOV on M...

PASTEBIN | #1 PASTE TOOL SINCE 2002

CREATE NEW PASTE | TOOLS | API | ARCHIVE | FAQ

010110
110011
101000
0001

PASTEBIN

Follow @pastebin

search...

CREATE NEW PASTE | TRENDING PASTES

SIGN UP | LOGIN | MY SETTINGS | MY PROFILE

Untitled

BY: A GUEST | SEP 2ND, 2011 | SYNTAX: NONE | SIZE: 0.64 KB | VIEWS: 35 | EXPIRES: NEVER

COPY TO CLIPBOARD | DOWNLOAD | RAW | EMBED | REPORT ABUSE

Predictions! Compatibility! Games! And More!

Always Free!

ASTROLOGY.COM

1. DO-NOT-REPLY@STATE.GOV on Monday

2. U.S. DoS - CEAC Confirmation (AA001PSIEJ)

3. Dear Applicant, Thank you for being a valued U.S. Consular Electronic Application Center (CEAC) customer. Your electronic Visa application has been submitted. Name Provided: VUONG, DUNG Nationality: VIETNAM Passport Number: B2204389 Completed On: 04 JULY 2011 02:46:00 EST Confirmation #: AA001PSIEJ YOUR CONFIRMATION PAGE IS ATTACHED TO THIS EMAIL IN A PDF FILE! You must follow the instructions on the confirmation page in order for the U.S. Department of State to continue processing your visa application. HOW TO PRINT YOUR Confirmation Page: 1. DOUBLE CLICK on the attached

RAW Paste Data

CREATE NEW PASTE | CREATE NEW VERSION OF THIS PASTE

DO-NOT-REPLY@STATE.GOV on Monday

U.S. DoS - CEAC Confirmation (AA001PSIEJ)

Dear Applicant, Thank you for being a valued U.S. Consular Electronic Application Center (CEAC) customer. Your electronic Visa application has been submitted. Name Provided: VUONG, DUNG Nationality: VIETNAM Passport Number: B2204389 Completed On: 04 JULY 2011 02:46:00 EST

MY PASTES

PUBLIC PASTES

CMasterFarmer
1 sec ago

Untitled
2 sec ago

Deborah Cox - It's Ov...
3 sec ago

Deborah Cox - Just When...
3 sec ago

Deborah Cox - Things Ju...
3 sec ago

Untitled
7 sec ago

Untitled
8 sec ago

Untitled
11 sec ago

LAYOUT WIDTH

Predictions!

Done

Profile2 184.154.125.14

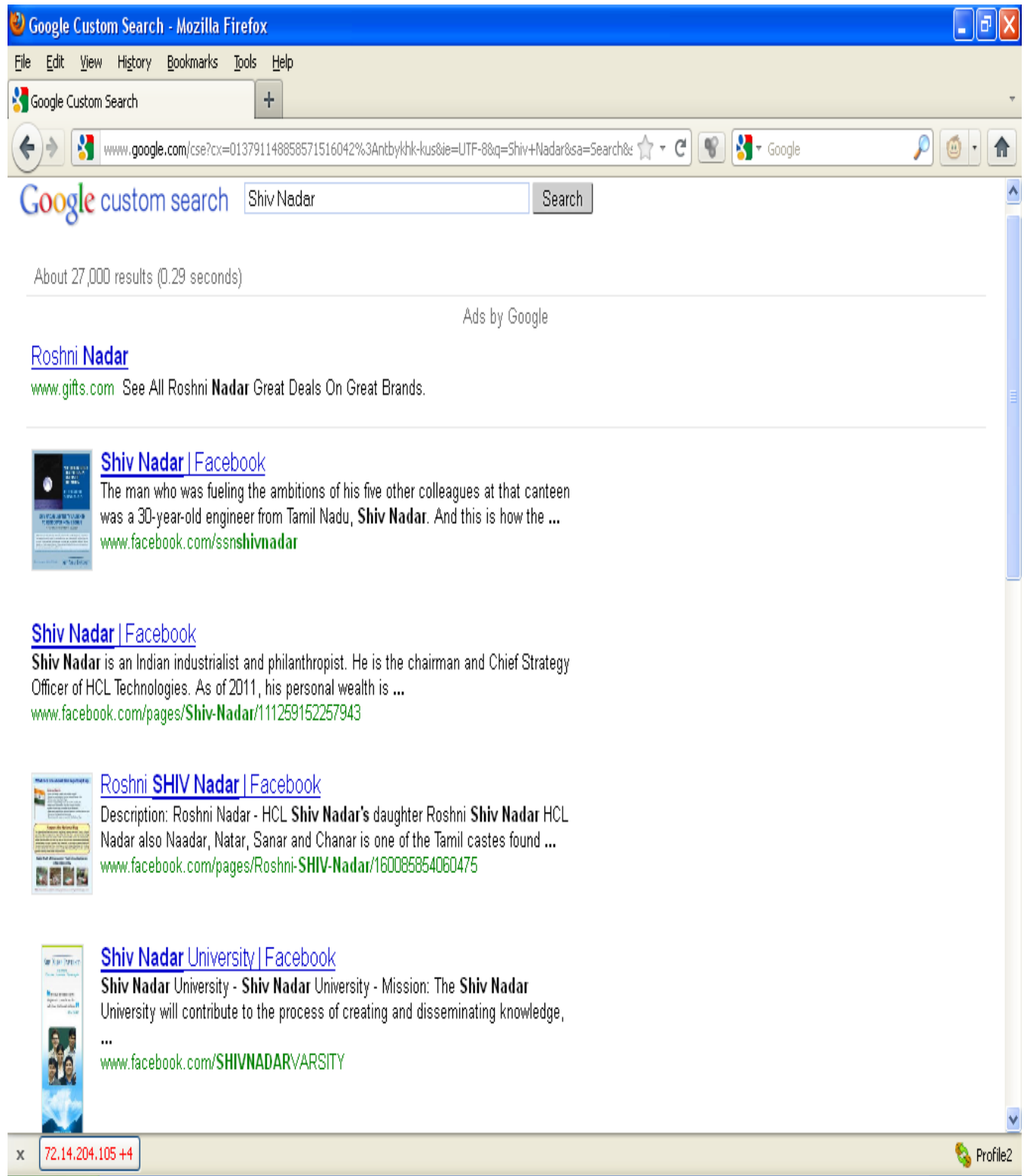
Social Networking Search

(<http://www.google.com/cse/home?cx=013791148858571516042:ntbykhk-kus>)

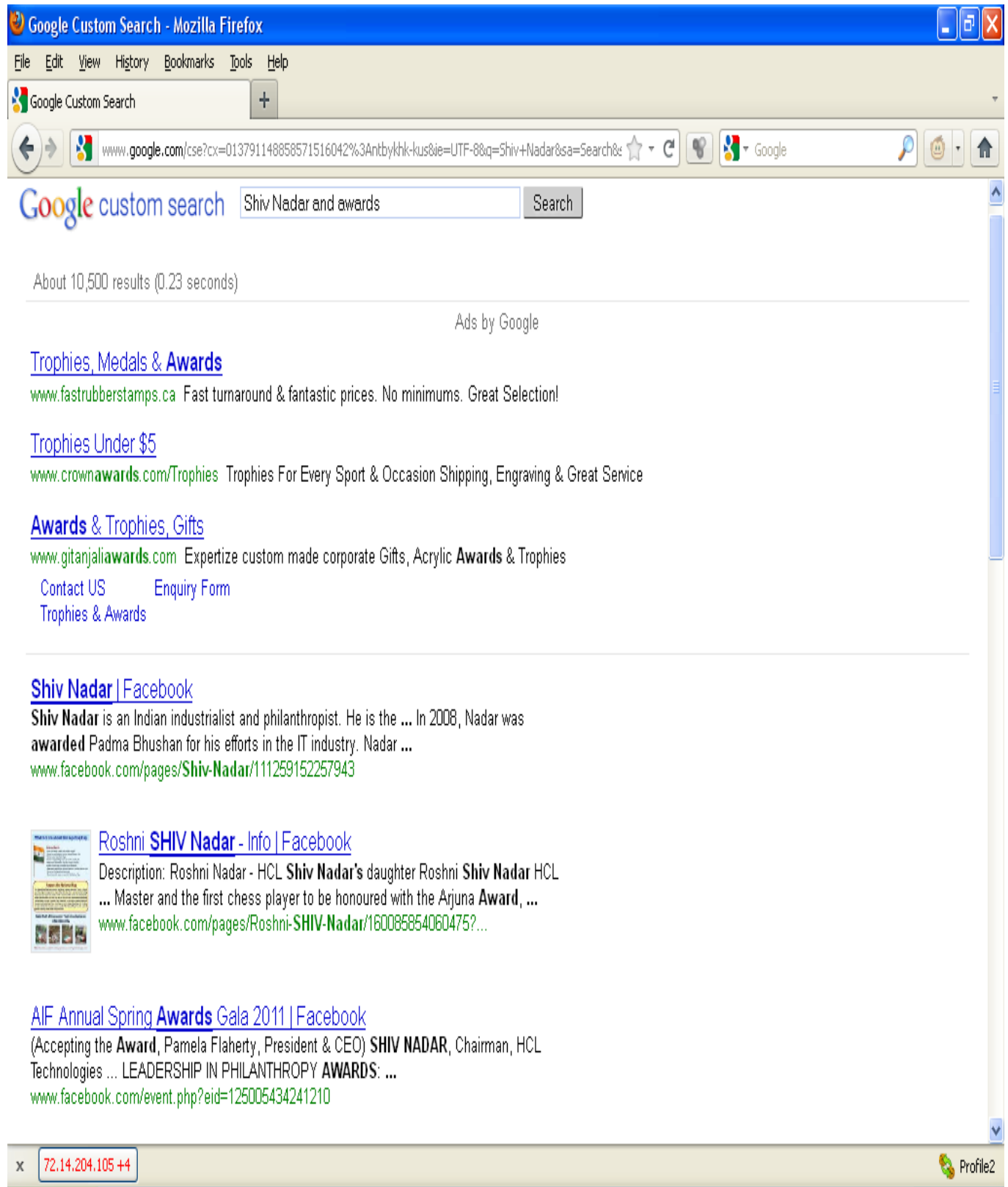
There are currently more than sixty social networking sites that are run through this custom search, examples include flickr, linkedin, facebook and Hi5. The list of sites is regularly updated but is not available to the public as it is confidential; further examples of the sites being searched can be found on my blog (Social Networking Intel/ Footprint Web Search, Infosec Mindstorm). My search attempts generated everything from an individual's personal social media page, to events where they were attending or volunteered at. I also came across individuals who worked at their organizations or people who knew them personally/ friends.

This search is very useful for reconnaissance related activities, intelligence gathering and finding social engineering targets and opportunities. One thing that really surprised me was the amount of information I was able to obtain on certain individuals even if they did not have a social media presence themselves. In some cases there was enough information for me to potentially engineer a meeting with the individual or get an introduction to the person in question. A good example of this is a search I ran on Shiv Nadar a well known multi-billionaire Indian industrialist and philanthropist (Wikipedia, Shiv Nadar). While I was unable to locate a social media page for Mr. Nadar, I was able to get information on events he volunteered at or was involved with as seen in Screenshots K and L.

Screenshot K-1



Screenshot K-2



Screenshot L -1

AIF Annual Spring Awards Gala 2011 | Facebook - Mozilla Firefox

File Edit View History Bookmarks Tools Help


http://www.facebook.com/event.php?eid=125005434241210&ref=nf

Most Visited

Google Custom Search

AIF Annual Spring Awards Gala 2011

Share · Public Event



Time Wednesday, June 8 · 6:00pm - 9:00pm

Location [Cipriani Club 55](#)
55 Wall Street
New York, NY

Created By [American India Foundation](#)

More Info HONORING:

CITI FOUNDATION
(Accepting the Award, Pamela Flaherty, President & CEO)
SHIV NADAR, Chairman, HCL Technologies

LEADERSHIP IN PHILANTHROPY AWARDS:

SURI SEHGAL, Ph.D.
Chairman, Sehgal Family Foundation
Chairman, Institute of Rural Research & Development

RAJ B. VATTIKUTI
Chairman, Vattikuti Ventures

ROMESH WADHWANI
Founder & Chairman, Symphony Technology Group

PERFORMANCE BY GRAMMY NOMINEE
CHANDRIKA KRISHNAMURTHY TANDON

MISTRESS OF CEREMONIES
TINKU JAIN

Done Profile2 69.171.228.14

Screenshot L -2

AIF Annual Spring Awards Gala 2011 - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Google Custom Search x AIF Annual Spring Awards Gala 2011 x +

www.facebook.com/event.php?eid=125005434241210

facebook Search Jamal Bandukwala Find Friends Home

More Info HONORING:

CITI FOUNDATION
(Accepting the Award, Pamela Flaherty, President & CEO)
SHIV NADAR, Chairman, HCL Technologies

LEADERSHIP IN PHILANTHROPY AWARDS:

SURI SEHGAL, Ph.D.
Chairman, Sehgal Family Foundation
Chairman, Institute of Rural Research & Development

RAJ B. VATTIKUTI
Chairman, Vattikuti Ventures

ROMESH WADHWANI
Founder & Chairman, Symphony Technology Group

PERFORMANCE BY GRAMMY NOMINEE
CHANDRIKA KRISHNAMURTHY TANDON

MISTRESS OF CEREMONIES
TINKU JAIN
TV Host, Namaste America

GALA CO CHAIRS:

RAVI AKHOURY, Akhoury Foundation
ARUN & ASMITA BHATIA, The Arun & Asmita Bhatia Family Foundation
SANT & VIKRAM CHATWAL, Chairman & CEO, Hampshire Hotels and Resorts;
President, Vikram Chatwal Hotels
PRADEEP KASHYAP & FAMILY
ATUL C. KHANNA
MARTIN LIPTON, Founding Partner, Wachtell, Lipton, Rosen & Katz
VICTOR & TARA MENEZES, Senior Advisor, New Silk Route
ANIL K. MONGA, CEO, Victory International (USA), LLC
ARVIND RAGHUNATHAN, CEO, Roc Capital Management
RAVI REDDY, Co-Founder & Managing Partner, Think Capital LLC

Sponsored See All

Best Smartphone Gadgets
smartphoneappreviews.biz

New and Latest Mobile Cell Phone Gadgets, Applications, Software, Games, Smartphone Phone Accessories and more

Free Rich Dad® Workshop

Don't miss the opportunity to attend this free Learn to be Rich workshop from the author of Rich Dad. Greater Toronto Area Dec 6-15

Mosheta Salon & Spa

\$10 WOMENS HAIR CUT
Sr Stylist- with purchase of shampoo and conditioner call 416 928 0228 www.mosheta.com

119 people like Mosheta Salon & Spa- Young Street 416-928-0228.

Ride With Purpose
conquercancer.ca

Register for the most important ride of your life. The Enbridge Ride to Conquer Cancer®, the largest cycling fundraiser in Canada.

Chat (5)

66.220.149.11 Profile2

The screenshots posted above (K and L) are very significant because they tell us that Mr. Nadar is involved with America India foundation. The screenshots also indicate that this organization held its annual Springs Awards Gala on June 08 2011 at the Cipriani Club 55 in New York City and that Mr. Nadar was one of the key people being honoured. In addition to this, one also learns that Mr. Nadar is the Chairman of HCL Technologies and the researcher/ analyst also gets the names of numerous other prominent individuals who are also heavily involved in this event and as a consequence likely know Mr. Nadar. This sort of information is very useful for a malicious actor who wants to send out a highly customized spear phishing attack targeting Mr. Nadar or any of the other individuals on that page. In addition to this the information available also allows individuals to create/ engineer opportunities to meet Mr. Shiv Nadar or any of the other individuals listed on this event. An individual could potentially do this by choosing to get involved with the organization or by using a social engineering attack, for instance claiming to have been at the Awards event and having been introduced to these individuals attempting to follow up and meet with them.

Invisible Attacks

While Google Custom Searches can be an excellent reconnaissance tool and are very useful in gathering potential targets for penetration tests, they can be used for other purposes as well. A custom search (with a user's own hit list) can also be used to quickly scan whether any external facing web based applications have been infected/ compromised. Hypothetically Google custom searches could also be used to launch 'invisible' attacks, the scenario listed below is a good illustration of this.

A malicious party could potentially hijack an existing researcher's identity and offer a custom search targeted at a very specific audience, for instance providing computer fraud statistics to a select group of senior executives or personnel. If a malicious party attempts to provide a service to a very small group of select individuals, there is a smaller chance of them being detected prior to launching an attack. The attacker could use the search to provide legitimate results most of the time and by doing so build a level of trust into the search engine; once they have sufficient trust built in, they could enter a temporary site into the engine using a service like tiny-url and then with the custom searches in built capabilities promote the results from the newly entered malicious site to the top of the list. The idea here is that the malicious actor would select a piece of malware suited to their requirements that can be stealthily installed and that does not generate a lot of noise. The actor would promote the malicious url for a short period of time, possibly as little as a few hours and then remove the url from the custom search altogether. This is extremely significant because using a temporary link makes it challenging for individuals/ teams to identify the source of the infection and depending on the behavior of the malware to determine whether the malicious code is in their environment at all. In addition to this by targeting a very select group of personnel (small scale) and using what appears to a trusted/ legitimate source of information this can also complicate matters in trying to obtain samples and identify the malware in question.

Final Thoughts/ Conclusion

As one can see Google offers a great deal of flexibility with their custom searches and opens a whole new realm of possibilities for the security and intelligence communities. One can clearly find a lot of information (with the right searches) including things like credit card numbers, and passport information. It is significant to note that even if you do not have your own social media/ web 2.0 presence, others in your network can release information about you or your activities on the web. Individual pieces of information by themselves may not mean much or even appear relevant but gathering all these pieces of information together can release a much bigger picture and allow an analyst/ user to get a better understanding of an individual or a situation. The information available in various locations on the internet may make it possible to engineer/ create opportunities for meetings with various individuals including political and business power brokers.

Running the appropriate searches generates useful political, social, economic and related intelligence and can be used to possibly obtain information on upcoming threats (both internet based and others) and take the appropriate actions to combat these. Organizations or other entities can even use these customized searches with a honeytrap if they suspect that an individual is leaking/ stealing their information. They can do this by leaking fake information in their organizations and watching to see if they become available via the Pastebin Custom search (or others). To conclude a lot of information is available to an analyst/ user with the right searches and the right content; while some of the information found can be disheartening these same searches can also be used to gather intelligence, anticipate and counter possible threats to an organization. It would appear that the custom search engine owner/ creator and the individual using the searches are both only limited by the content in the search engine and their imagination.

About the Author

Jamal Bandukwala is a security professional at a major financial institution. He is also a blogger and independent security researcher with a variety of infosec interests including Google hacking, Open Source Intelligence & pen testing among others. His personal research and musings can be found at <http://infosecmindstorm.blogspot.com/>

Works Cited

Bandukwala, Jamal. <http://infosecmindstorm.blogspot.com/> (Last visited, Nov 16 2011)

Google. Google Custom Search APIs and Tools Developer's Guide.
http://code.google.com/apis/customsearch/docs/dev_guide.html (Last visited, Nov 16 2011)

Jiang, Rui, Google. Improved On-Demand Indexing. Google Custom Search Blog.
http://googlecustomsearch.blogspot.com/2011/06/improved-on-demand-indexing.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+blogspot%2FSyga+%28Google+Custom+Search%29 (Last visited, Nov 16 2011)

Shiv Nadar. Wikipedia.com http://en.wikipedia.org/wiki/Shiv_Nadar (Last visited, Nov 16 2011)

Pastebin. Wikipedia.com <http://en.wikipedia.org/wiki/Pastebin> (Last visited, Nov 16 2011)

Washington Times. CIA mines 'rich' content from blogs.
<http://www.washingtontimes.com/news/2006/apr/18/20060418-110124-3694r/> (Last visited, Nov 16 2011)

Zelster, Lenny. Pastebin used for sharing stolen data.
<http://blog.zeltser.com/post/7033873645/pastebin-used-for-sharing-stolen-data> (Last visited, Nov 16 2011)