No Fuss FOSS

Free and Open Source SOC

TheHive
thinkst
applied research
VirusTotal
yara
Cortex
CyberChef
Talos

Why a FOSS?

Security products are expensive

- It can be hard to get budget for new products.
- If you have some time and skills though you can replicate 80%+ of the big price tag products with open source

How do we build a FOSS?

Quality open source projects

Open source versions of vendor products

Free subscription level to security services

What do we need?

- At least 1 server(VM, physical, or cloud)
- Some scripting capabilities
  - I use bash and python in my implementation
- (Free) Subscription to various security services
- A few email accounts

TheHive

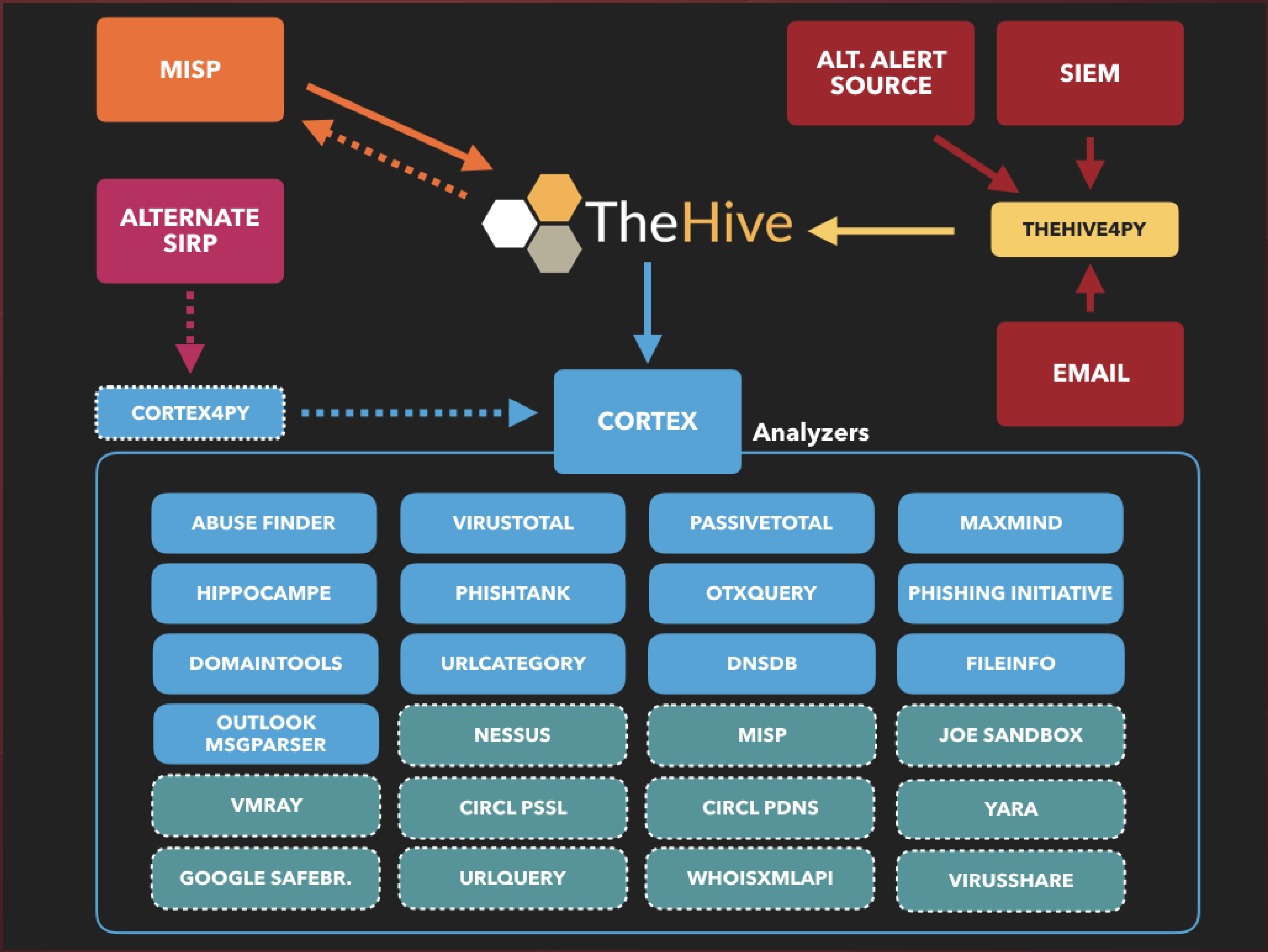
Open source project

- SoC ticketing, noting, and centralized database for incident reporting, tracking, and investigating.
- Web front end
- Elasticsearch DB backend

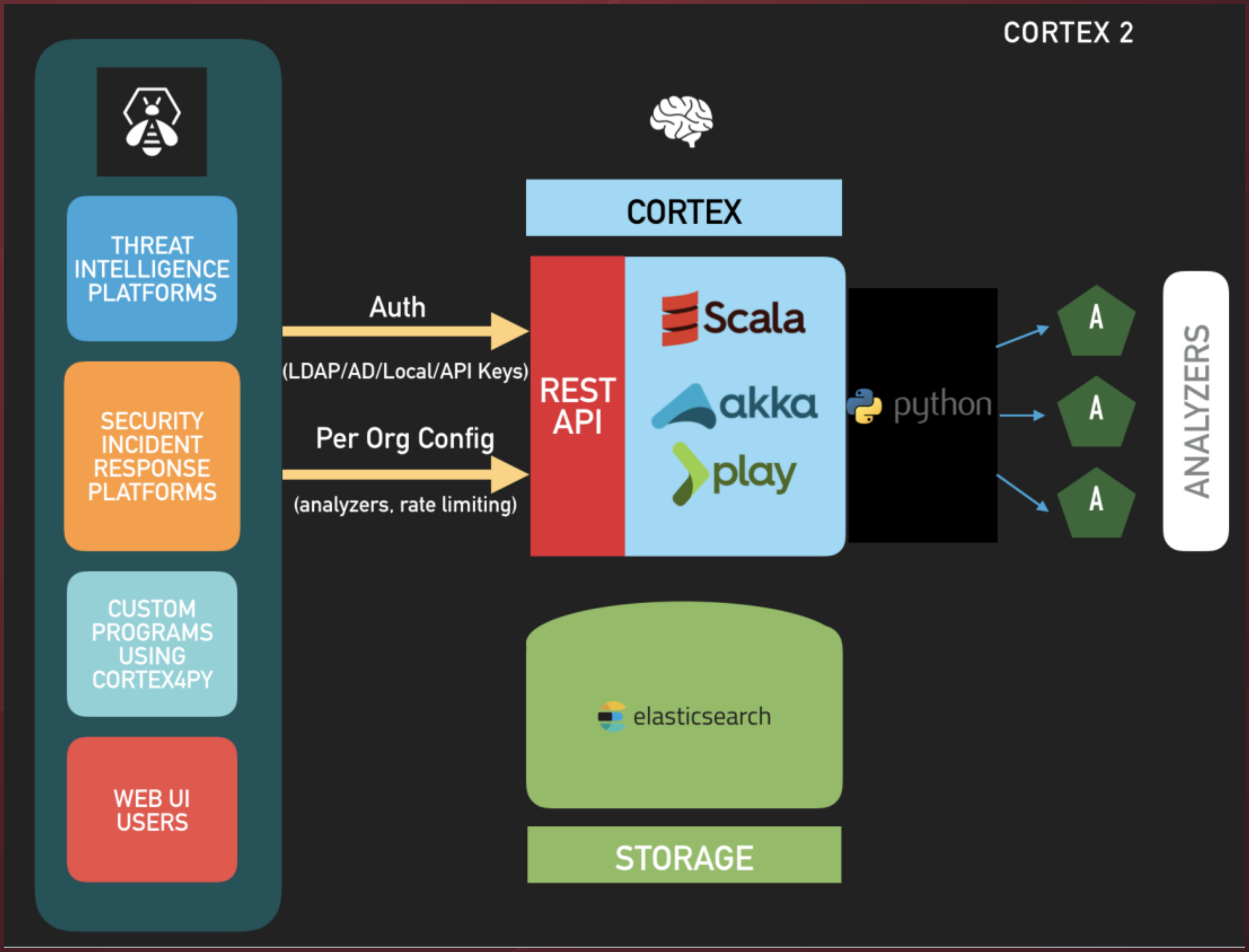
Cortex

- Companion to TheHive
  - Comprised of analyzers that you can run against ‘observables’
  - Can be run independent
  - You can create your own analyzers in python using api’s

TheHive/Cortex Stack



TheHive/Cortex Stack



Canaries

- While thinkst sells commercial products they offer Open Source version of many of their tools
  - Open Canary - kind of honeypot
  - Canary tokens - alerting base on honeyfiles

‘Intelligence’

- Use both open source and free intel
  - Talos Inteligence
  - Cymon
  - Urlscan.io
  - Phishtank
  - Openphish
  - Alienvault OTX
  - Threatconnect
  - Passivetotal / riskiq

Feed tools to TheHive

- UrlScan2Hive
- Imap2thehive

Scanning

While traditional AV can be useful to run standard on endpoints step up you response/hunt capabilities with custom signatures for your environment.

- ClamAV - Sigtool
- Yara - yarGen

  Deploy with scripts
- Blazescan
- Minerchk

Sandboxes

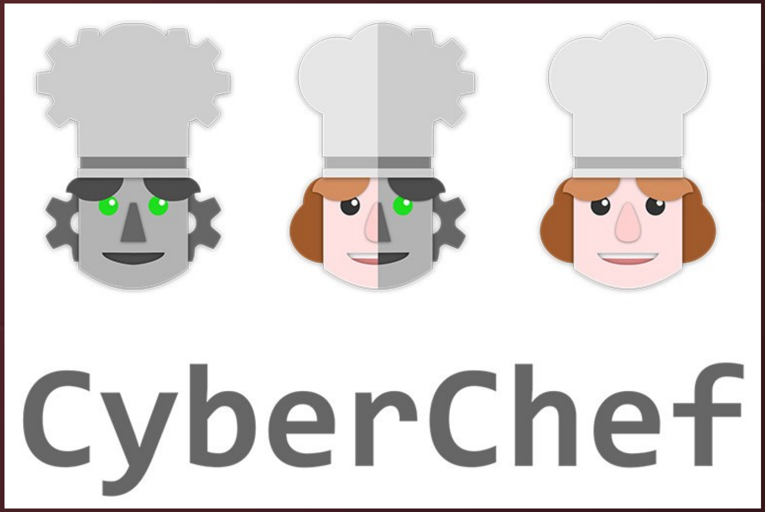
While you can totally go out and build a cuckoo sandbox or other sandbox solution, let’s use some easy and free services to get started.

- Virus total
- Reverse.it / Hybrid Analysis

Infosec Swiss Army tool

Cyberchef

- Great tool full of many easy to use utilities
- Counting, Extracting, beautifying
- Conversion between formats
- Deobfuscation



Other online options:

https://www.unphp.net/

https://www.javascriptdeobfuscator.com/

Slides posted to laskowski-tech.com

Resources TheHive tools

- TheHive https://github.com/TheHive-Project/TheHive
- Cortex https://github.com/TheHive-Project/Cortex
- Hive4py https://github.com/TheHive-Project/TheHive4py
- Cortex4py https://github.com/TheHive-Project/Cortex4py

Resources 2

Canaries

- Open Canary
  https://github.com/thinkst/opencanary
  - Setup guide
    - https://laskowski-tech.com/2017/12/19/setting-up-a-honeypot-using-opencanary/
- Canarytokens
  https://canarytokens.org/generate

Resources 3

Scanning

- ClamAV, Clamscan, sigtool https://www.clamav.net/downloads
- Yara https://virustotal.github.io/yara/
- yarGen https://github.com/Neo23x0/yarGen

Resources 4

Cyberchef

- https://github.com/gchq/CyberChef

My scripts and sigs:

https://github.com/Hestat/minerchk

https://github.com/Hestat/blazescan

https://github.com/Hestat/lw-yara

https://github.com/Hestat/vt.py

https://github.com/Hestat/cryptojacking-scanner

Services

https://www.reverse.it/

https://virustotal.com

https://www.phishtank.com/

https://urlscan.io/

https://www.openphish.com/

https://otx.alienvault.com

https://cymon.io/

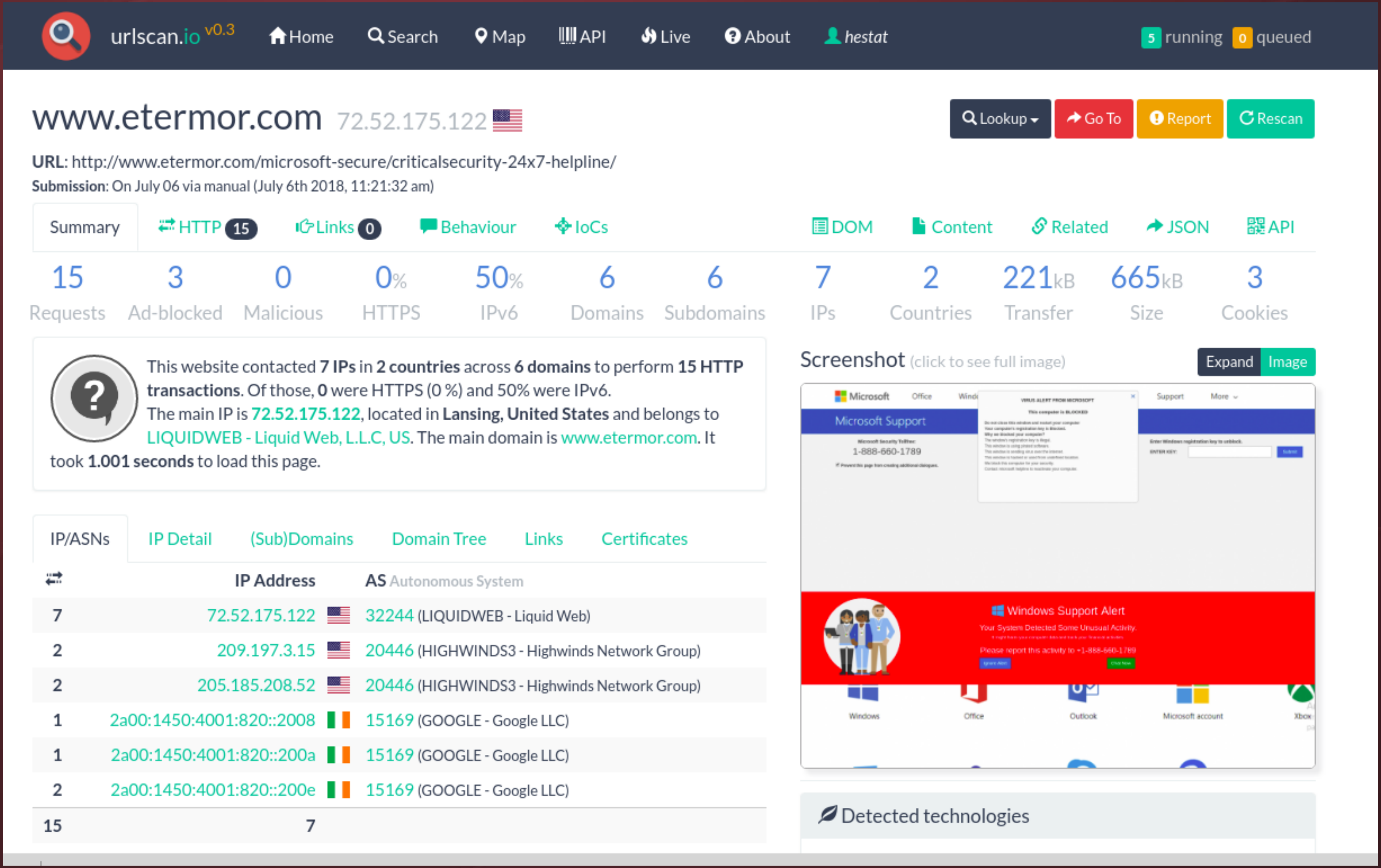
https://threatconnect.com/

https://www.talosintelligence.com/

https://community.riskiq.com/

Demonstration

- https://urlscan.io/result/91610b1f-4548-466e-b058-ac9290ab83fc/



www.etermor.com 72.52.175.122

URL: http://www.etermor.com/microsoft-secure/criticalsecurity-24x7-helpline/
Submission: On July 06 via manual (July 6th 2018, 11:21:32 am)

15	3	0	0%	50%	6	6	7	2	221kB	665kB	3
Requests	Ad-blocked	Malicious	HTTPS	IPv6	Domains	Subdomains	IPs	Countries	Transfer	Size	Cookies

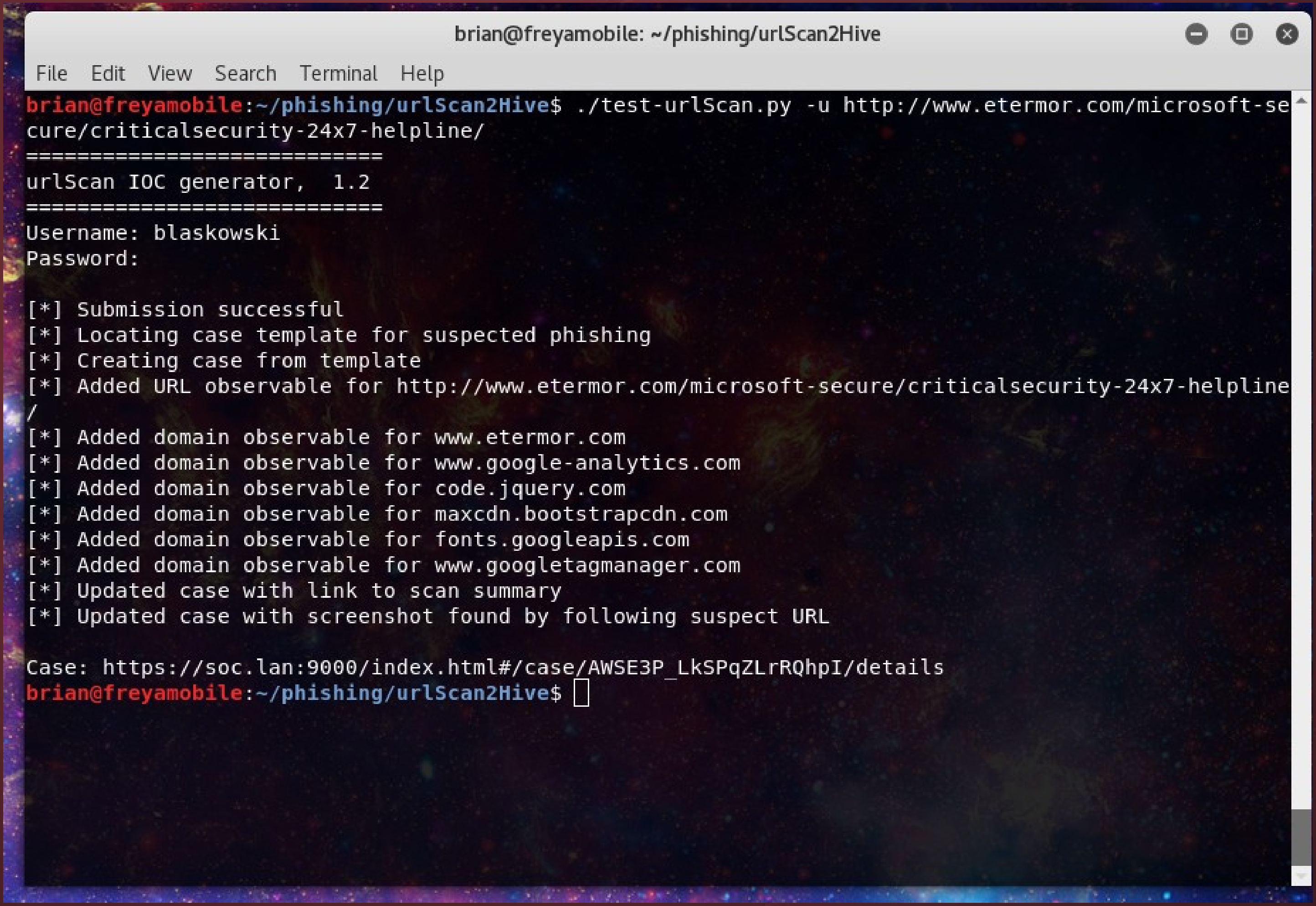
This website contacted **7 IPs** in **2 countries** across **6 domains** to perform **15 HTTP transactions**. Of those, **0** were HTTPS (0 %) and 50% were IPv6. The main IP is 72.52.175.122, located in **Lansing, United States** and belongs to LIQUIDWEB - Liquid Web, L.L.C, US. The main domain is www.etermor.com. It took **1.001 seconds** to load this page.

⇄	IP Address		AS Autonomous System
7	72.52.175.122	🇺🇸	32244 (LIQUIDWEB - Liquid Web)
2	209.197.3.15	🇺🇸	20446 (HIGHWINDS3 - Highwinds Network Group)
2	205.185.208.52	🇺🇸	20446 (HIGHWINDS3 - Highwinds Network Group)
1	2a00:1450:4001:820::2008	🇮🇪	15169 (GOOGLE - Google LLC)
1	2a00:1450:4001:820::200a	🇮🇪	15169 (GOOGLE - Google LLC)
2	2a00:1450:4001:820::200e	🇮🇪	15169 (GOOGLE - Google LLC)
15	7		

Screenshot (click to see full image)

Detected technologies

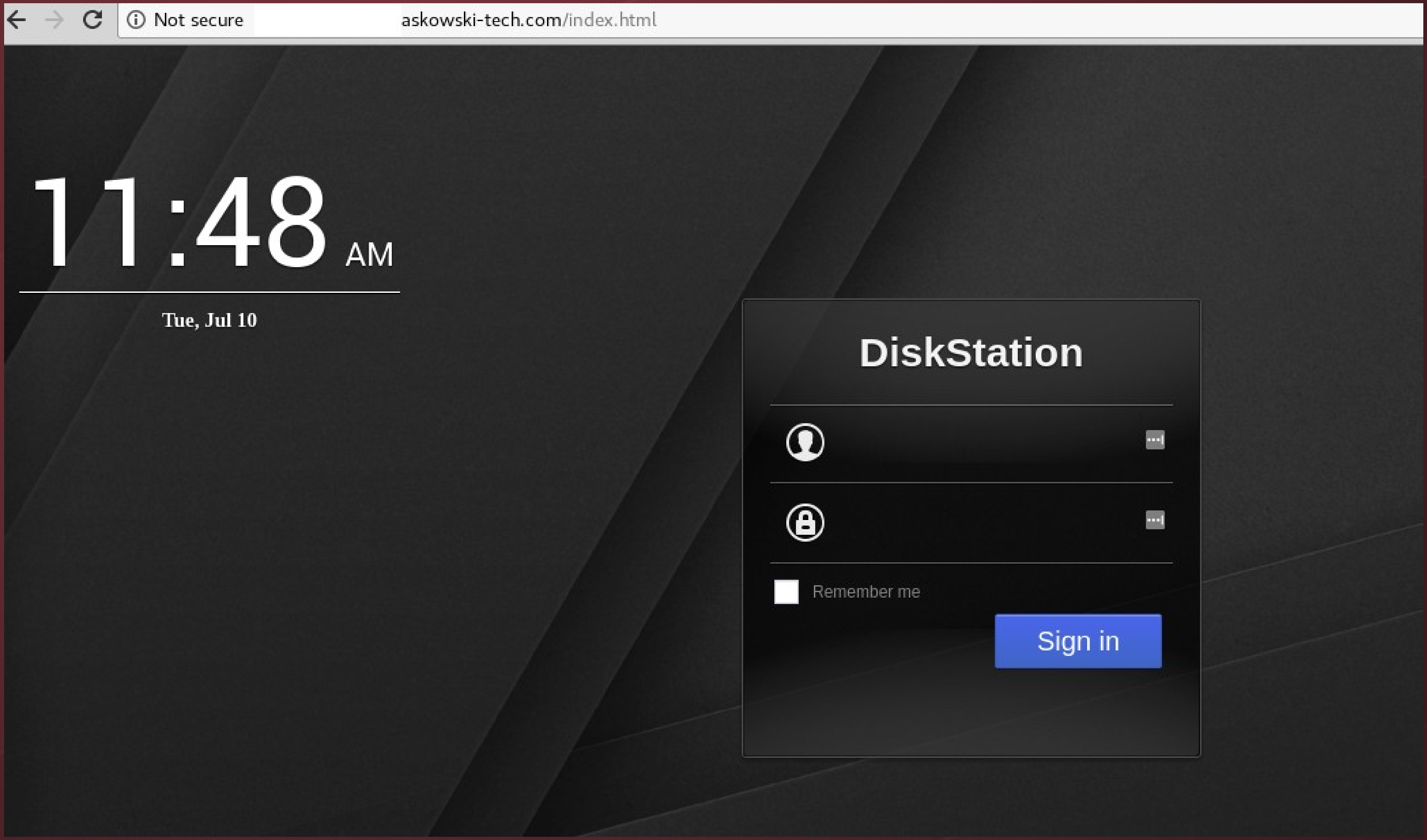
Demonstration



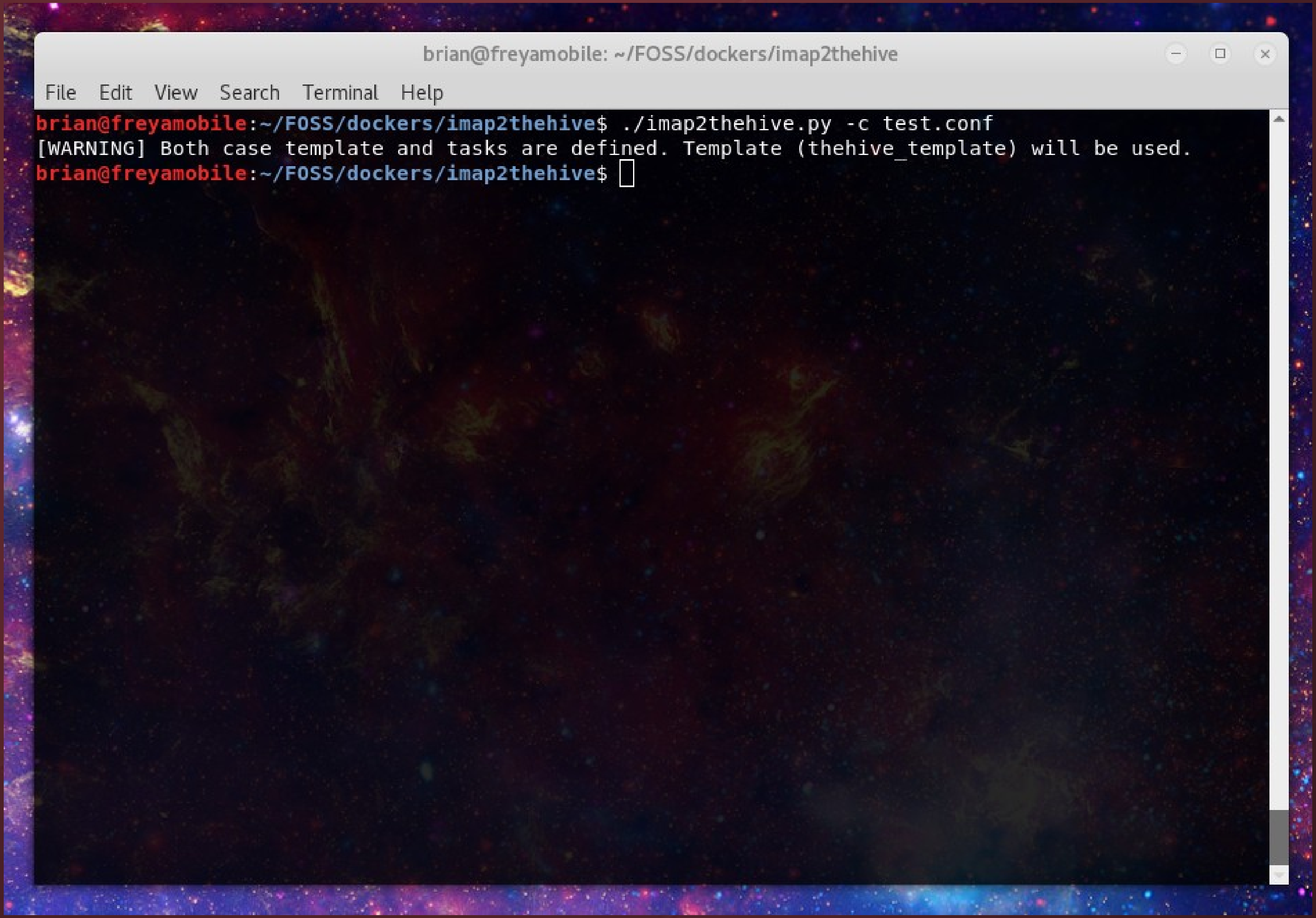
brian@freyamobile: ~/phishing/urlScan2Hive
File Edit View Search Terminal Help

```
brian@freyamobile:~/phishing/urlScan2Hive$ ./test-urlScan.py -u http://www.etermor.com/microsoft-se
cure/criticalsecurity-24x7-helpline/
============================
urlScan IOC generator,  1.2
============================
Username: blaskowski
Password:

[*] Submission successful
[*] Locating case template for suspected phishing
[*] Creating case from template
[*] Added URL observable for http://www.etermor.com/microsoft-secure/criticalsecurity-24x7-helpline
/
[*] Added domain observable for www.etermor.com
[*] Added domain observable for www.google-analytics.com
[*] Added domain observable for code.jquery.com
[*] Added domain observable for maxcdn.bootstrapcdn.com
[*] Added domain observable for fonts.googleapis.com
[*] Added domain observable for www.googletagmanager.com
[*] Updated case with link to scan summary
[*] Updated case with screenshot found by following suspect URL

Case: https://soc.lan:9000/index.html#/case/AWSE3P_LkSPqZLrRQhpI/details
brian@freyamobile:~/phishing/urlScan2Hive$ 
```

Demonstration



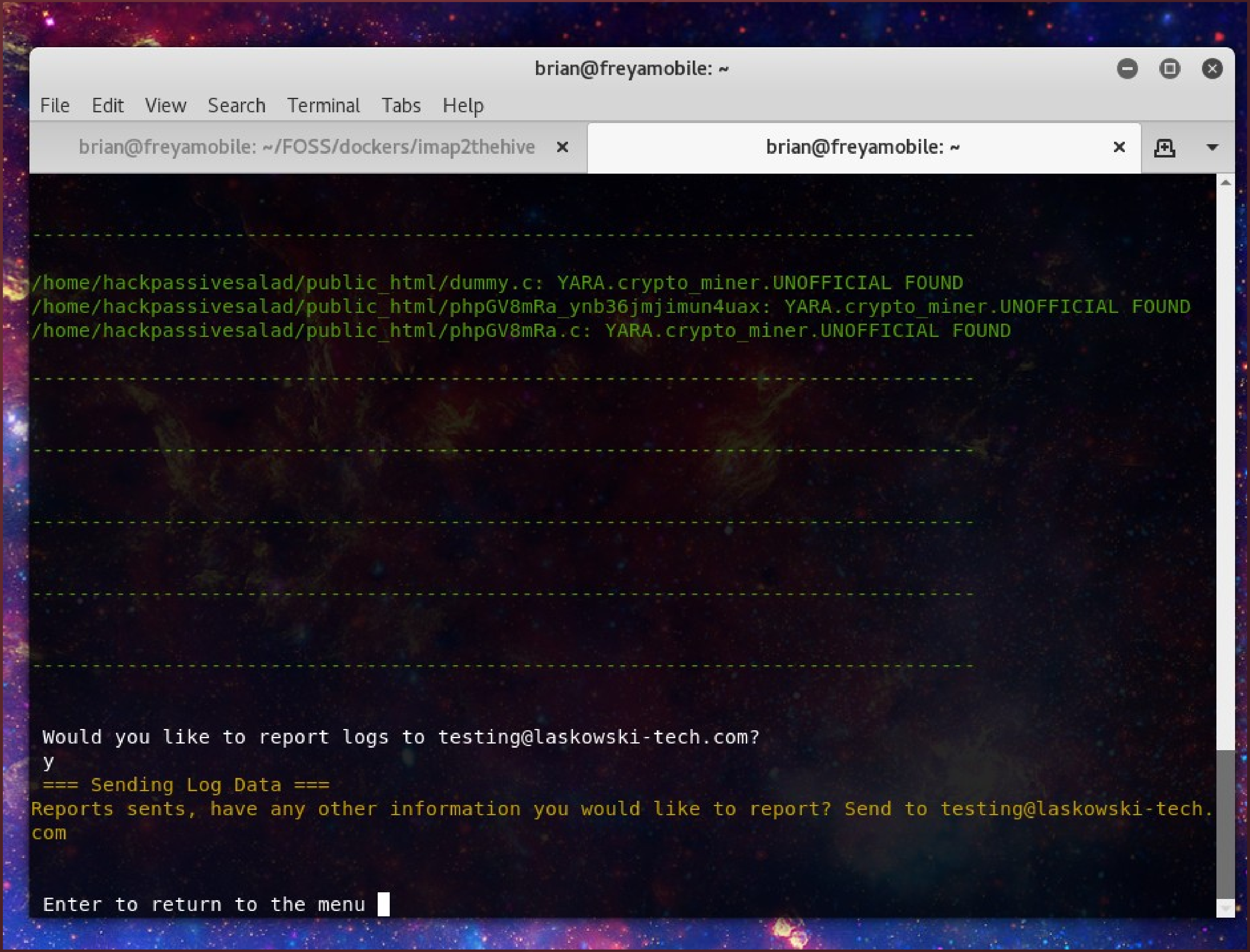
Demonstration



brian@freyamobile: ~/FOSS/dockers/imap2thehive
File Edit View Search Terminal Help

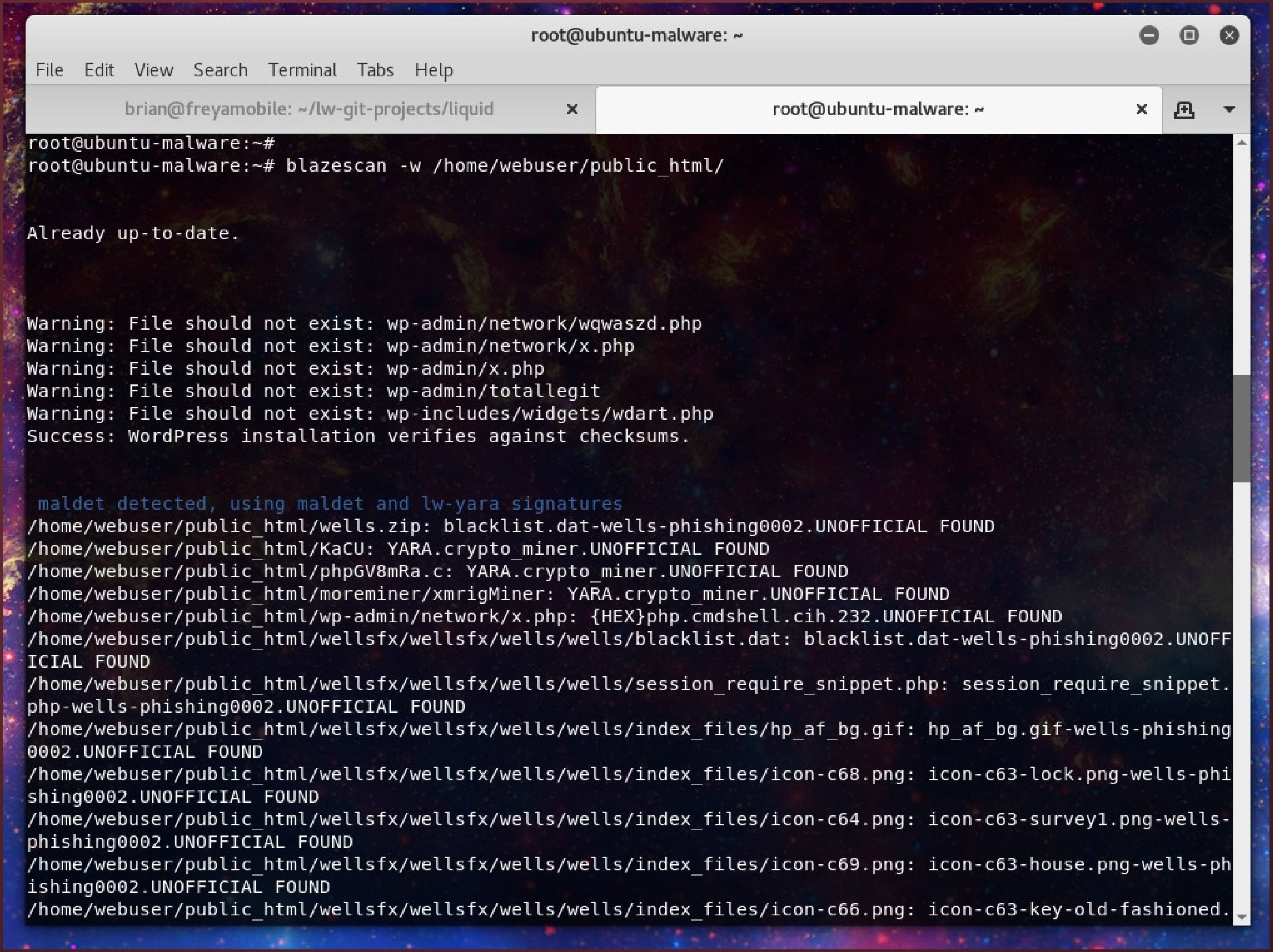
```
brian@freyamobile:~/FOSS/dockers/imap2thehive$ ./imap2thehive.py -c test.conf
[WARNING] Both case template and tasks are defined. Template (thehive_template) will be used.
brian@freyamobile:~/FOSS/dockers/imap2thehive$ 
```

Demonstration


brian@freyamobile: ~
File Edit View Search Terminal Tabs Help
brian@freyamobile: ~/FOSS/dockers/imap2thehive
brian@freyamobile: ~

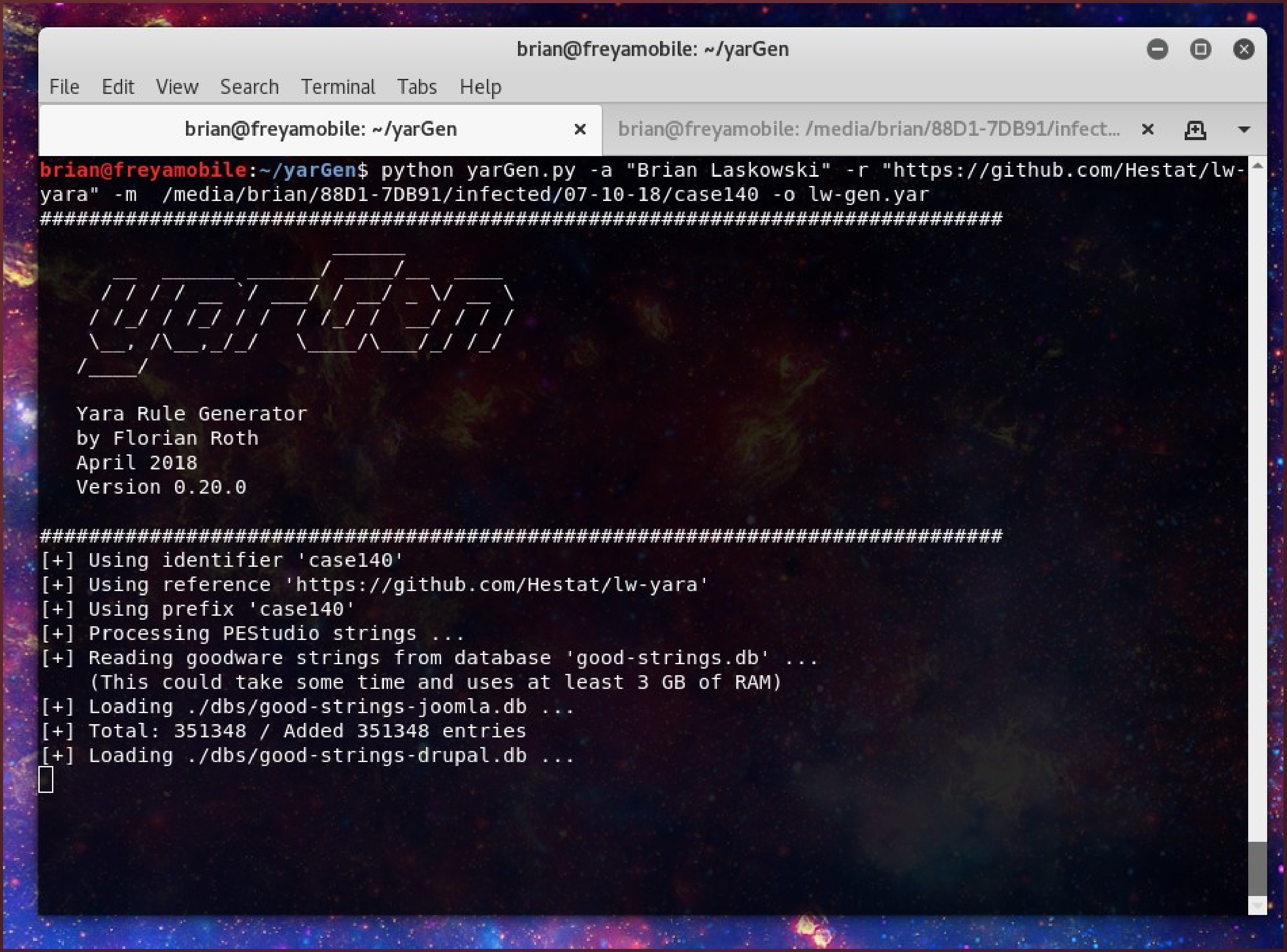
```
--------------------------------------------------------------------------------

/home/hackpassivesalad/public_html/dummy.c: YARA.crypto_miner.UNOFFICIAL FOUND
/home/hackpassivesalad/public_html/phpGV8mRa_ynb36jmjimun4uax: YARA.crypto_miner.UNOFFICIAL FOUND
/home/hackpassivesalad/public_html/phpGV8mRa.c: YARA.crypto_miner.UNOFFICIAL FOUND

--------------------------------------------------------------------------------


--------------------------------------------------------------------------------


--------------------------------------------------------------------------------


--------------------------------------------------------------------------------


--------------------------------------------------------------------------------


 Would you like to report logs to testing@laskowski-tech.com?
 y
 === Sending Log Data ===
Reports sents, have any other information you would like to report? Send to testing@laskowski-tech.
com


 Enter to return to the menu
```

Demonstration



```
root@ubuntu-malware:~#
root@ubuntu-malware:~# blazescan -w /home/webuser/public_html/


Already up-to-date.



Warning: File should not exist: wp-admin/network/wqwaszd.php
Warning: File should not exist: wp-admin/network/x.php
Warning: File should not exist: wp-admin/x.php
Warning: File should not exist: wp-admin/totallegit
Warning: File should not exist: wp-includes/widgets/wdart.php
Success: WordPress installation verifies against checksums.


 maldet detected, using maldet and lw-yara signatures
/home/webuser/public_html/wells.zip: blacklist.dat-wells-phishing0002.UNOFFICIAL FOUND
/home/webuser/public_html/KaCU: YARA.crypto_miner.UNOFFICIAL FOUND
/home/webuser/public_html/phpGV8mRa.c: YARA.crypto_miner.UNOFFICIAL FOUND
/home/webuser/public_html/moreminer/xmrigMiner: YARA.crypto_miner.UNOFFICIAL FOUND
/home/webuser/public_html/wp-admin/network/x.php: {HEX}php.cmdshell.cih.232.UNOFFICIAL FOUND
/home/webuser/public_html/wellsfx/wellsfx/wells/wells/blacklist.dat: blacklist.dat-wells-phishing0002.UNOFF
ICIAL FOUND
/home/webuser/public_html/wellsfx/wellsfx/wells/wells/session_require_snippet.php: session_require_snippet.
php-wells-phishing0002.UNOFFICIAL FOUND
/home/webuser/public_html/wellsfx/wellsfx/wells/wells/index_files/hp_af_bg.gif: hp_af_bg.gif-wells-phishing
0002.UNOFFICIAL FOUND
/home/webuser/public_html/wellsfx/wellsfx/wells/wells/index_files/icon-c68.png: icon-c63-lock.png-wells-phi
shing0002.UNOFFICIAL FOUND
/home/webuser/public_html/wellsfx/wellsfx/wells/wells/index_files/icon-c64.png: icon-c63-survey1.png-wells-
phishing0002.UNOFFICIAL FOUND
/home/webuser/public_html/wellsfx/wellsfx/wells/wells/index_files/icon-c69.png: icon-c63-house.png-wells-ph
ishing0002.UNOFFICIAL FOUND
/home/webuser/public_html/wellsfx/wellsfx/wells/wells/index_files/icon-c66.png: icon-c63-key-old-fashioned.
```

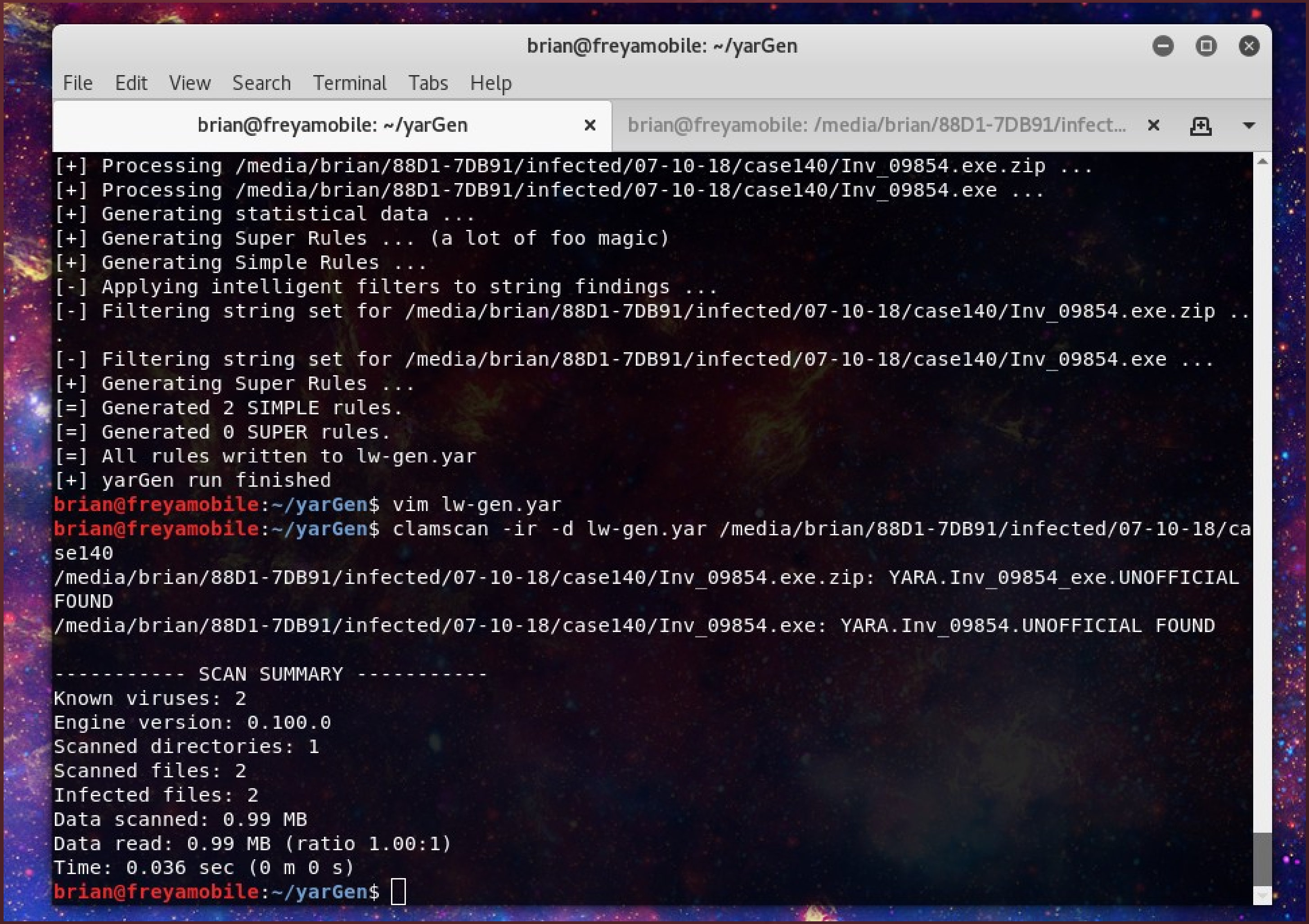
Demonstration



brian@freyamobile: ~/yarGen
File Edit View Search Terminal Tabs Help
brian@freyamobile: ~/yarGen
brian@freyamobile: /media/brian/88D1-7DB91/infect...

```
brian@freyamobile:~/yarGen$ python yarGen.py -a "Brian Laskowski" -r "https://github.com/Hestat/lw-
yara" -m  /media/brian/88D1-7DB91/infected/07-10-18/case140 -o lw-gen.yar
###############################################################################

                        ______
      __  ______ ______/ ____/__  ____
     / / / / __ `/ ___/ / __/ _ \/ __ \
    / /_/ / /_/ / /  / /_/ /  __/ / / /
    \__, /\__,_/_/   \____/\___/_/ /_/
   /____/

   Yara Rule Generator
   by Florian Roth
   April 2018
   Version 0.20.0

###############################################################################
[+] Using identifier 'case140'
[+] Using reference 'https://github.com/Hestat/lw-yara'
[+] Using prefix 'case140'
[+] Processing PEStudio strings ...
[+] Reading goodware strings from database 'good-strings.db' ...
    (This could take some time and uses at least 3 GB of RAM)
[+] Loading ./dbs/good-strings-joomla.db ...
[+] Total: 351348 / Added 351348 entries
[+] Loading ./dbs/good-strings-drupal.db ...
```

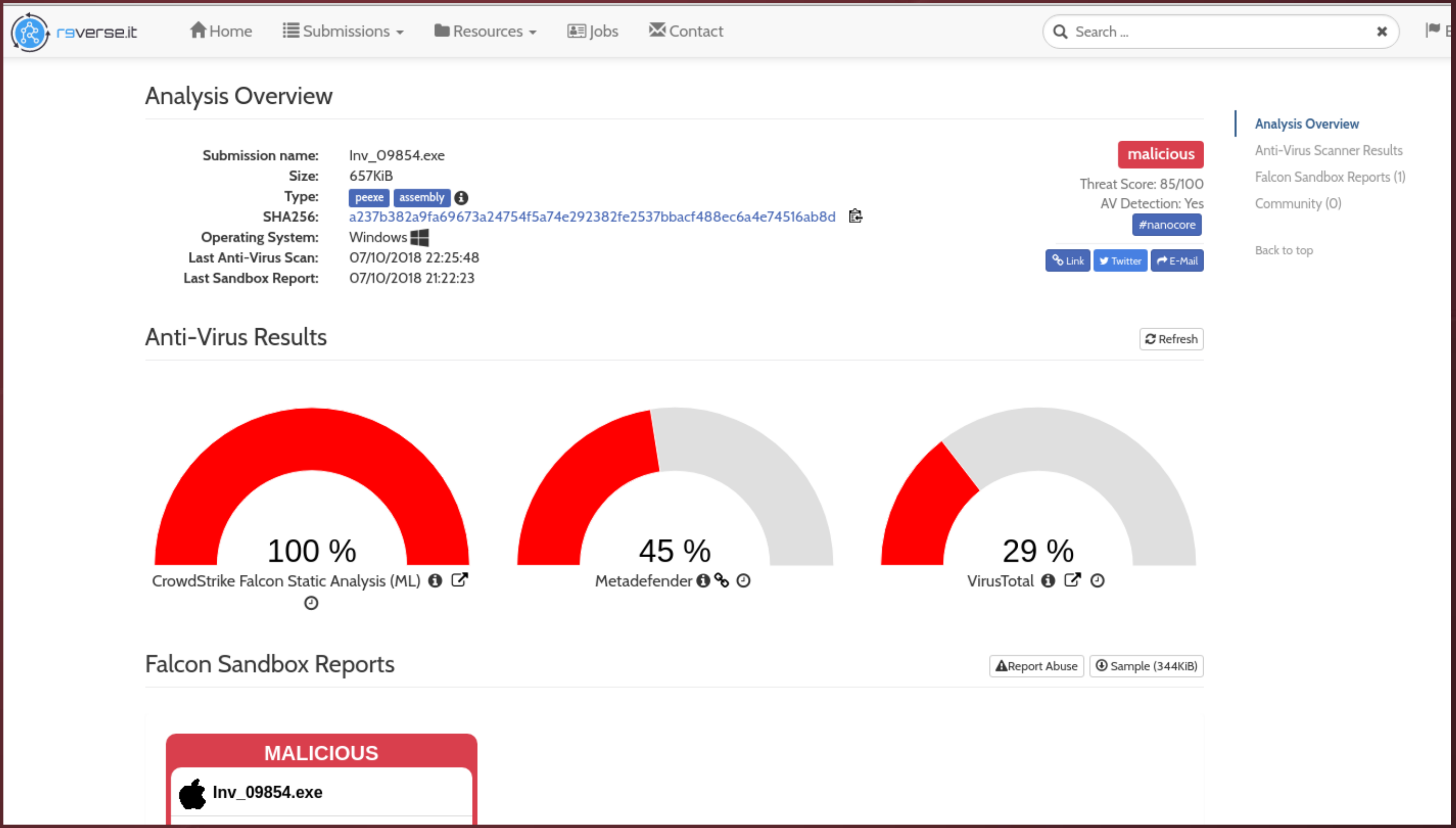
Demonstration



brian@freyamobile: ~/yarGen
File Edit View Search Terminal Tabs Help
brian@freyamobile: ~/yarGen
brian@freyamobile: /media/brian/88D1-7DB91/infect...

```
[+] Processing /media/brian/88D1-7DB91/infected/07-10-18/case140/Inv_09854.exe.zip ...
[+] Processing /media/brian/88D1-7DB91/infected/07-10-18/case140/Inv_09854.exe ...
[+] Generating statistical data ...
[+] Generating Super Rules ... (a lot of foo magic)
[+] Generating Simple Rules ...
[-] Applying intelligent filters to string findings ...
[-] Filtering string set for /media/brian/88D1-7DB91/infected/07-10-18/case140/Inv_09854.exe.zip ..
.
[-] Filtering string set for /media/brian/88D1-7DB91/infected/07-10-18/case140/Inv_09854.exe ...
[+] Generating Super Rules ...
[=] Generated 2 SIMPLE rules.
[=] Generated 0 SUPER rules.
[=] All rules written to lw-gen.yar
[+] yarGen run finished
brian@freyamobile:~/yarGen$ vim lw-gen.yar
brian@freyamobile:~/yarGen$ clamscan -ir -d lw-gen.yar /media/brian/88D1-7DB91/infected/07-10-18/ca
se140
/media/brian/88D1-7DB91/infected/07-10-18/case140/Inv_09854.exe.zip: YARA.Inv_09854_exe.UNOFFICIAL
FOUND
/media/brian/88D1-7DB91/infected/07-10-18/case140/Inv_09854.exe: YARA.Inv_09854.UNOFFICIAL FOUND

----------- SCAN SUMMARY -----------
Known viruses: 2
Engine version: 0.100.0
Scanned directories: 1
Scanned files: 2
Infected files: 2
Data scanned: 0.99 MB
Data read: 0.99 MB (ratio 1.00:1)
Time: 0.036 sec (0 m 0 s)
brian@freyamobile:~/yarGen$
```

Demonstration



Analysis Overview

Submission name: Inv_09854.exe
Size: 657KiB
Type: peexe assembly
SHA256: a237b382a9fa69673a24754f5a74e292382fe2537bbacf488ec6a4e74516ab8d
Operating System: Windows
Last Anti-Virus Scan: 07/10/2018 22:25:48
Last Sandbox Report: 07/10/2018 21:22:23

malicious
Threat Score: 85/100
AV Detection: Yes
#nanocore

Anti-Virus Results

100 %
CrowdStrike Falcon Static Analysis (ML)

45 %
Metadefender

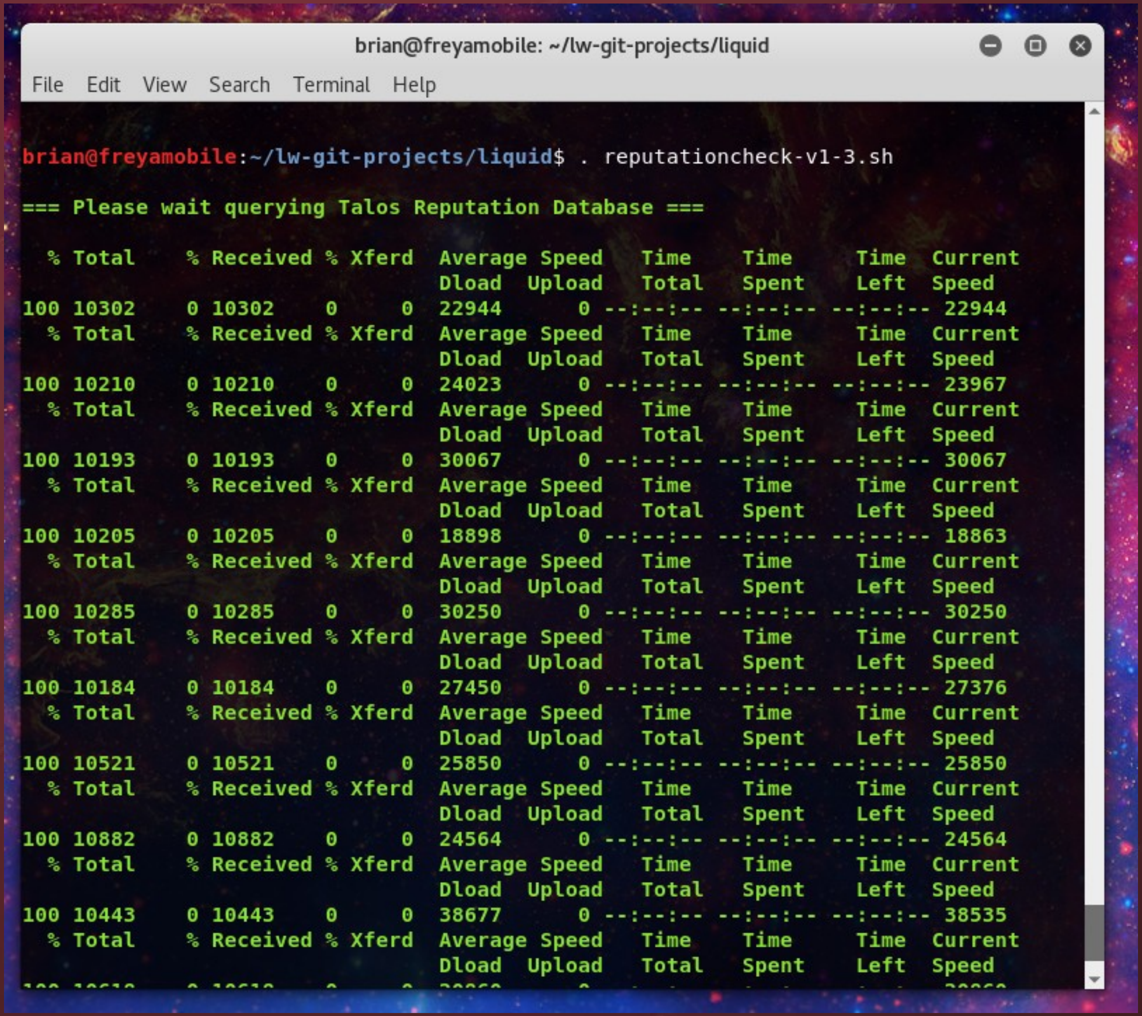
29 %
VirusTotal

Falcon Sandbox Reports

MALICIOUS
Inv_09854.exe

https://www.reverse.it/sample/a237b382a9fa69673a24754f5a74e292382fe2537bbacf488ec6a4e74516ab8d/5b45163a7ca3e15fbc444f34

Demonstration



```
brian@freyamobile:~/lw-git-projects/liquid$ . reputationcheck-v1-3.sh

=== Please wait querying Talos Reputation Database ===

  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 10302    0 10302    0     0  22944      0 --:--:-- --:--:-- --:--:-- 22944
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 10210    0 10210    0     0  24023      0 --:--:-- --:--:-- --:--:-- 23967
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 10193    0 10193    0     0  30067      0 --:--:-- --:--:-- --:--:-- 30067
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 10205    0 10205    0     0  18898      0 --:--:-- --:--:-- --:--:-- 18863
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 10285    0 10285    0     0  30250      0 --:--:-- --:--:-- --:--:-- 30250
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 10184    0 10184    0     0  27450      0 --:--:-- --:--:-- --:--:-- 27376
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 10521    0 10521    0     0  25850      0 --:--:-- --:--:-- --:--:-- 25850
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 10882    0 10882    0     0  24564      0 --:--:-- --:--:-- --:--:-- 24564
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 10443    0 10443    0     0  38677      0 --:--:-- --:--:-- --:--:-- 38535
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
```