Threat Intelligence on the Cheap

OWASP Los Angeles
May 24, 2017

Shane MacDougall

InfoSec Drone

Disclaimer

- These are my opinions only, and do not reflect on my employers
- I am not endorsing these resources, I am simply presenting them as players in the field
- YMMV
- Use these resources at your own risk

About Me

- Shane MacDougall
- Been an InfoSec professional since 1987
- Started as a pentester for KPMG
- Areas of interest include social engineering, threat intelligence, OSINT, machine learning and sentiment analysis
- Powerpoint Ninja

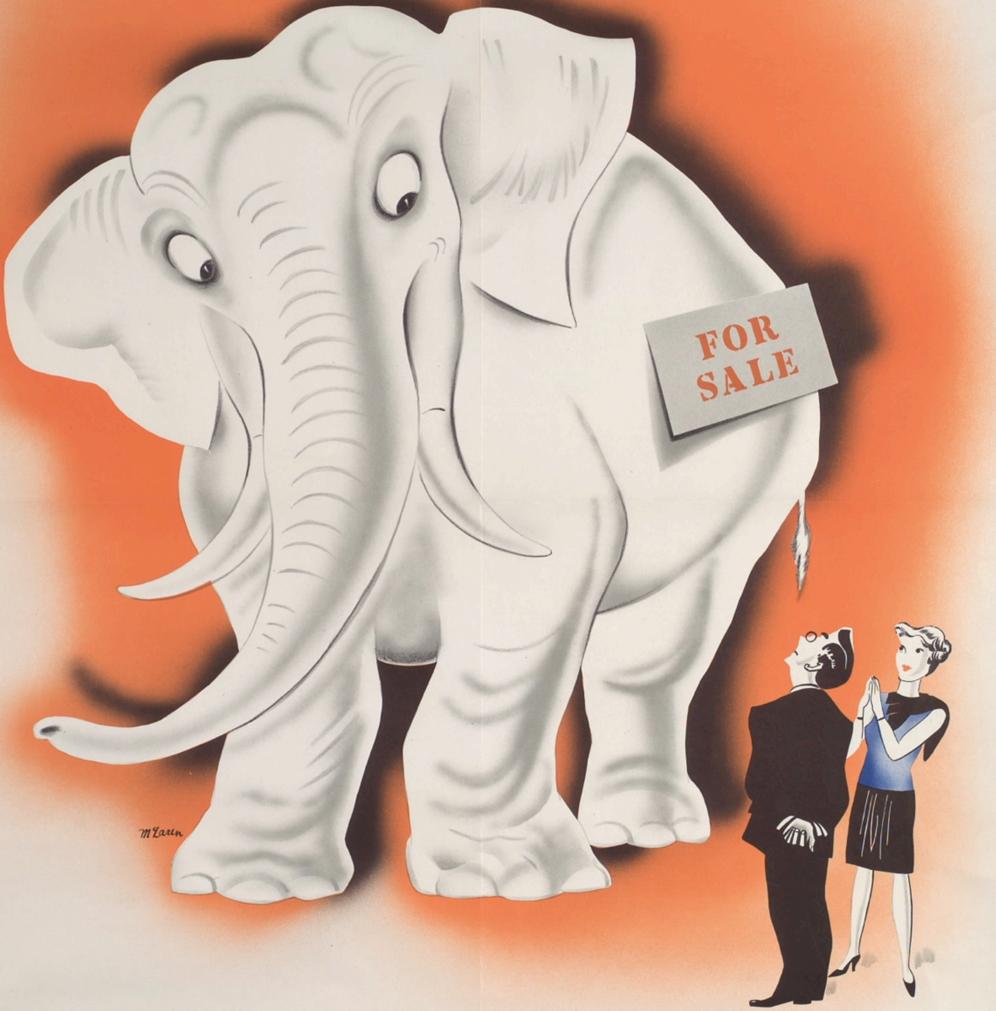
Why This Talk?

- I’ve seen many organizations spend tremendous amounts of money on TI infrastructure
- Most of the outlay could have been easily deployed via DIY
- Cost of TI > 1-3 SOC analysts

What Is Threat Intelligence

- Do you need to be able to reverse malware?
- Do you have attackers dedicated to your particular enterprise?
- Are you in the financial industry? Military?
- Do you have compliance requirements?
- Dollar amount loss
- Do you need Team Cymru feeds or iSight or iDefense or similar high $$$ intelligence?

If you don't need it...



DON'T BUY IT

ISSUED BY THE DIRECTOR OF PUBLIC INFORMATION, UNDER AUTHORITY OF HON. J. T. THORSON, MINISTER OF NATIONAL WAR SERVICES, OTTAWA

EC1

Printed in Canada

What TI Do You Need?

- Needs will vary by your threat model
- User facing versus B2B
- Fraudulent transactions vs hacking attacks
- Volume of transactions
- Need for automation

What Is Threat Intelligence?

What Is Threat Intelligence

- Actionable intelligence on threat actors
- UK Center for Protection of National Infrastructure defines 4 types:
  - Strategic (high level info on changing risk)
  - Technical (attacker methodologies, tools, tactics)
  - Tactical (indicators of compromise)
  - Operational (details on attacks)

What Is Threat Intelligence

- Can include:
  - Indicators of compromise
  - IP address
  - Payloads
  - Device information
  - IP intelligence
  - Phone number
  - Forum posts

What Is Threat Intelligence

- Can include:
  - Attacker’s country
  - Device fingerprint
  - File hash
  - URL
  - TTP (tactics, techniques, procedures)
  - Etc etc etc etc etc

What Is Threat Intelligence

- No One Size Fits All
- YOU need to define what TI means to YOUR organization
- Do not fall into the trap of adopting what others are doing
- Roll your own for your environment
- Make sure expectations/understandings of keyholders are realistics and helpful

What Is Threat Intelligence

- Data without context is just data
- Threat intelligence with no association to your organization is (mostly) useless
- Without a proper platform your data might be useless (or at least not optimally staged)
- Do you want to adopt a TI format (TAXII, STIX, IODEF, etc etc etc)
- Determine your needs/platform/format before you begin or else…

YOU'RE GOING TO
HAVE A BAD TIME

Threat Intelligence Frameworks

Threat Intelligence Frameworks

- You need a framework
- TI data comes in a multitude of formats
- Different distribution methods
- You need the ability to take disparate datasets and converge them into usable and actionable intelligence

CIF

- CIF (Collective Intelligence Framework)
- REN-ISAC project
- Aggregates private and public feeds
- CLI and RESTful API
- Comes pre-configured with feeds
- V3 “The Bearded Avenger”
- http://csirtgadgets.org/
- https://github.com/csirtgadgets/bearded-avenger

MISP

- Malware Information Sharing Platform (& Threat Sharing)
- http://www.misp-project.org/
- Widely used
- Originally used by NATO
- Active community

CRITS

- Collective Research Into Threats
- https://crits.github.io
- Open source project from MITRE
- Widely used
- Very active community

Open Threat Exchange

- AlienVault
- Claims to be the world’s largest crowd-sourced security platform
- 26000+ users
- 1,000,000 potential threats daily
- https://otx.alienvault.com

Threat Intelligence Has Limitations

- You find out a malware package is unique to your company. What now?
- You have an attacker IP address from China
- Is your attacker Chinese?
- You gonna call the Chengdu Police Dept?
- Amount of time you expend needs to have a comparable ROI

Internal vs External

- Internal – leveraging internal information to identify attackers/threat actors (free - sorta)
- External – lists, services (from free to very, very, very not free $$$$$)

Internal

- Firewall logs
- SIEM logs
- Antivirus
- Honeypots
- Incident data
- Device fingerprinting
- Main costs: Storage and processing

Client SideThreat Intelligence

- From our webapp we can do fingerprinting
- This can be especially useful when your threat model is focused primarily on fraud
- Useful but needs correlation

Passive Fingerprinting

- Passive:
  - We don’t query the client
  - We examine TCP/IP traffic, OS fingerprints
  - nmap –o
  - - - osscan-limit
  - - -fuzzy

Active Fingerprint

- We actively query the browser
- Need JavaScript or other similar client-side scripting language to harvest
- Different web clients will yield different fingerprints
- That said, they will likely just rotate through a few clients, so repeated attacks can be detected

Browser/Device Fingerprinting

- Browser information
  - User Agent
  - HTTP_ACCEPT (content types)
  - Browser Plugins
  - Screen size (big one)
  - Fonts
  - Time Zone
  - Cookie information

Browser/Device Fingerprinting

- Device information
  - MAC address (this one DOES get changed)

Browser/Device Fingerprinting

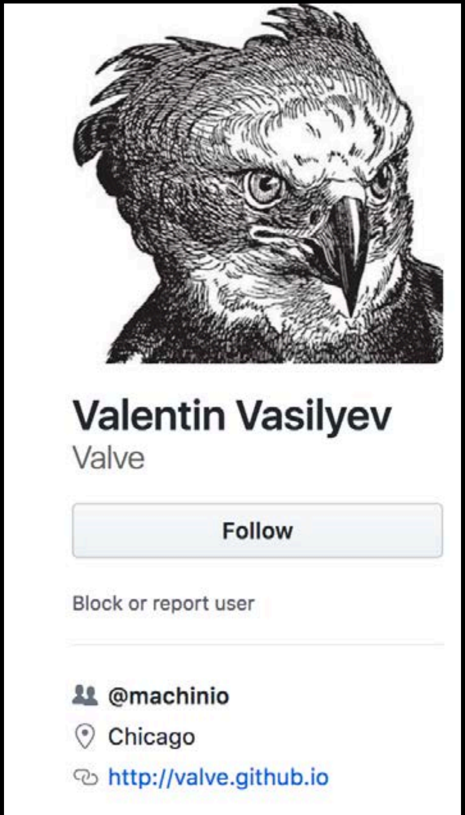
- These combined give us many many many digits worth of uniqueness
- Yes, they can disable JavaScript (enjoy your surfing) – but how frequently do you see that?
- NoScript will save your butt – and nobody uses it
- Mobile devices a lot less unique to fingerprint

Browser/Device Fingerprinting

- It’s still not that difficult to do.
- Don’t believe me?
- Google “buy adult diapers los angeles”
- Now go to Facebook/Amazon
- Enjoy your banner ads for the next five years.

fingerprintjs

- https://github.com/Valve/fingerprintjs2
- Valentin Vasilyev (Valve)



Valentin Vasilyev

Valve

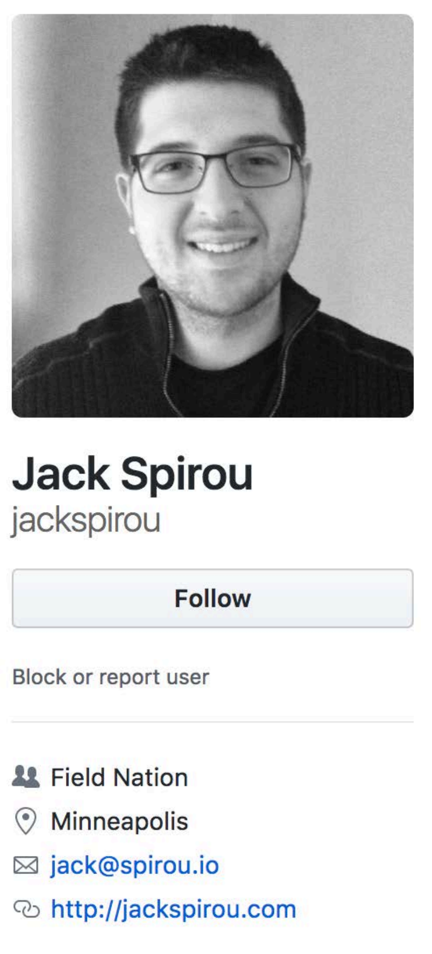
@machinio

Chicago

http://valve.github.io

clientjs

- https://github.com/jackspirou/clientjs
- Jack Spirou
- https://clientjs.org/

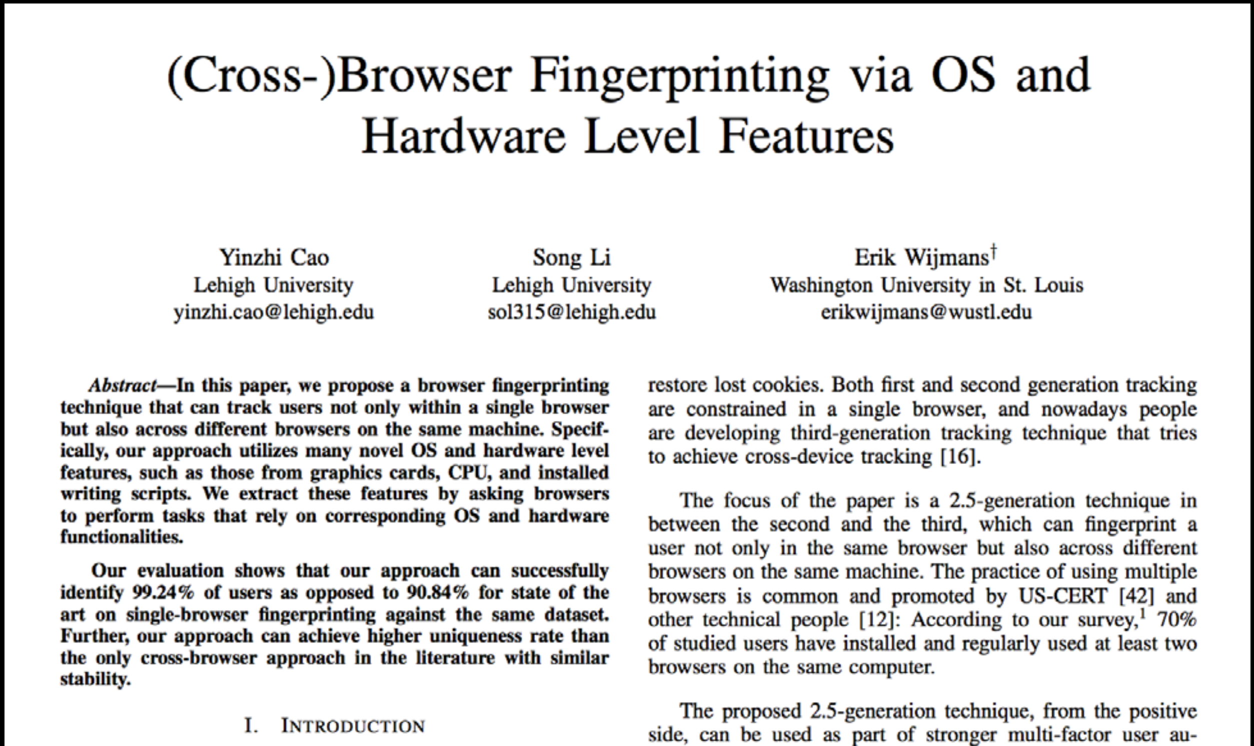


Jack Spirou
jackspirou

Field Nation
Minneapolis
jack@spirou.io
http://jackspirou.com

Browser/Device Fingerprinting

- Cross-browser tracking now deployable
- http://yinzhicao.org/TrackingFree/crossbrowsertracking_NDSS17.pdf



(Cross-)Browser Fingerprinting via OS and Hardware Level Features

Yinzhi Cao
Lehigh University
yinzhi.cao@lehigh.edu

Song Li
Lehigh University
sol315@lehigh.edu

Erik Wijmans[†]
Washington University in St. Louis
erikwijmans@wustl.edu

***Abstract*—In this paper, we propose a browser fingerprinting technique that can track users not only within a single browser but also across different browsers on the same machine. Specifically, our approach utilizes many novel OS and hardware level features, such as those from graphics cards, CPU, and installed writing scripts. We extract these features by asking browsers to perform tasks that rely on corresponding OS and hardware functionalities.**

Our evaluation shows that our approach can successfully identify 99.24% of users as opposed to 90.84% for state of the art on single-browser fingerprinting against the same dataset. Further, our approach can achieve higher uniqueness rate than the only cross-browser approach in the literature with similar stability.

I. Introduction

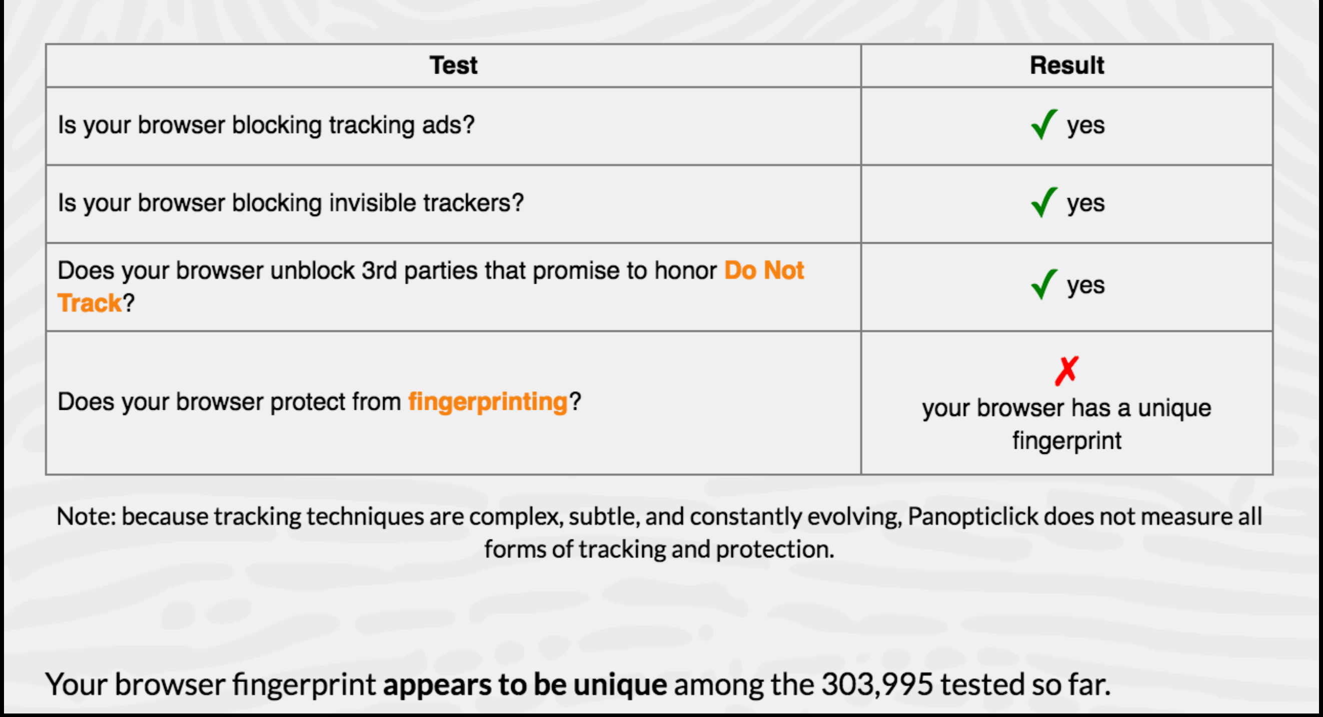
restore lost cookies. Both first and second generation tracking are constrained in a single browser, and nowadays people are developing third-generation tracking technique that tries to achieve cross-device tracking [16].

The focus of the paper is a 2.5-generation technique in between the second and the third, which can fingerprint a user not only in the same browser but also across different browsers on the same machine. The practice of using multiple browsers is common and promoted by US-CERT [42] and other technical people [12]: According to our survey,[1] 70% of studied users have installed and regularly used at least two browsers on the same computer.

The proposed 2.5-generation technique, from the positive side, can be used as part of stronger multi-factor user au-

Browser/Device Fingerprinting

- EFF Panopticlick
- https://panopticlick.eff.org



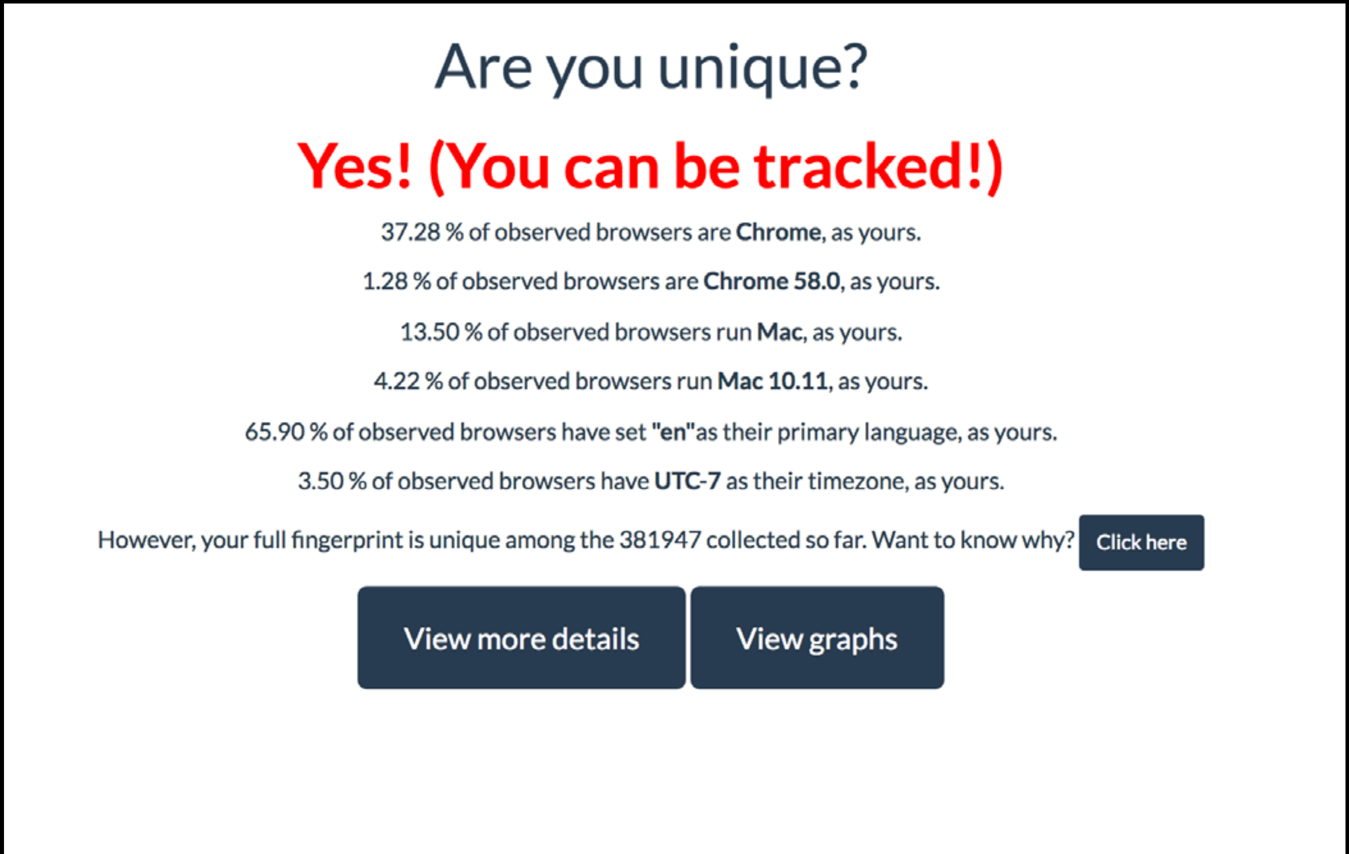
Test	Result
Is your browser blocking tracking ads?	✓ yes
Is your browser blocking invisible trackers?	✓ yes
Does your browser unblock 3rd parties that promise to honor **Do Not Track**?	✓ yes
Does your browser protect from **fingerprinting**?	✗ your browser has a unique fingerprint

Note: because tracking techniques are complex, subtle, and constantly evolving, Panopticlick does not measure all forms of tracking and protection.

Your browser fingerprint **appears to be unique** among the 303,995 tested so far.

Am I Unique?

- https://amiunique.org/



Are you unique?

Yes! (You can be tracked!)

37.28 % of observed browsers are **Chrome**, as yours.

1.28 % of observed browsers are **Chrome 58.0**, as yours.

13.50 % of observed browsers run **Mac**, as yours.

4.22 % of observed browsers run **Mac 10.11**, as yours.

65.90 % of observed browsers have set **"en"**as their primary language, as yours.

3.50 % of observed browsers have **UTC-7** as their timezone, as yours.

However, your full fingerprint is unique among the 381947 collected so far. Want to know why?

External Sources

Best TI Resource Of All

Best Network…

- Is your social network
- Peers in your industry
- People you can call up and ask if they’ve seen/heard information that can help
- People who can ask other people
- Lean on your friends

Breach Detection

- Majority of organizations don’t discover breaches internally
- 5-6 months on average before detection
    - Osterman Research

Pastebin (and friends)

- Pastebin alerts
- Pastemonitor (pastemonitor.com)
- https://github.com/cvandeplas/pystemon
- Many others

Breach Alerting

- Haveibeenpwned.com
- Breachalarm.com
- Hacked-emails.com

- Honeypots (internal)

Reddit

- https://www.reddit.com/r/threatintel/
- https://www.reddit.com/r/security/
- https://www.reddit.com/r/AskNetsec
- https://www.reddit.com/r/netsec/
- https://www.reddit.com/r/hacking/
- https://www.reddit.com/r/infosec/
- https://www.reddit.com/r/malware/
- https://www.reddit.com/r/pwned
- https://www.reddit.com/r/ReverseEngineering

Twitter

- Top resource for threat intelligence
- Most active infosec community anywhere online
- Noisy
- Data overload
- Prepare for the drama llama
- YMMV

Twitter

- Your lists are your friend
- Other people’s lists are your friend
- Outside of data feeds (which we will soon discuss), most of the valuable information needs to be processed manually
- Very time consuming…
- Get emotionally vested
- DRAMA!!!!!

HoneyPots

- Golden
- A must have for any environment
- Internal yield real time/near real-time intelligence
- Free / Paid
- New hotness

HoneyPots

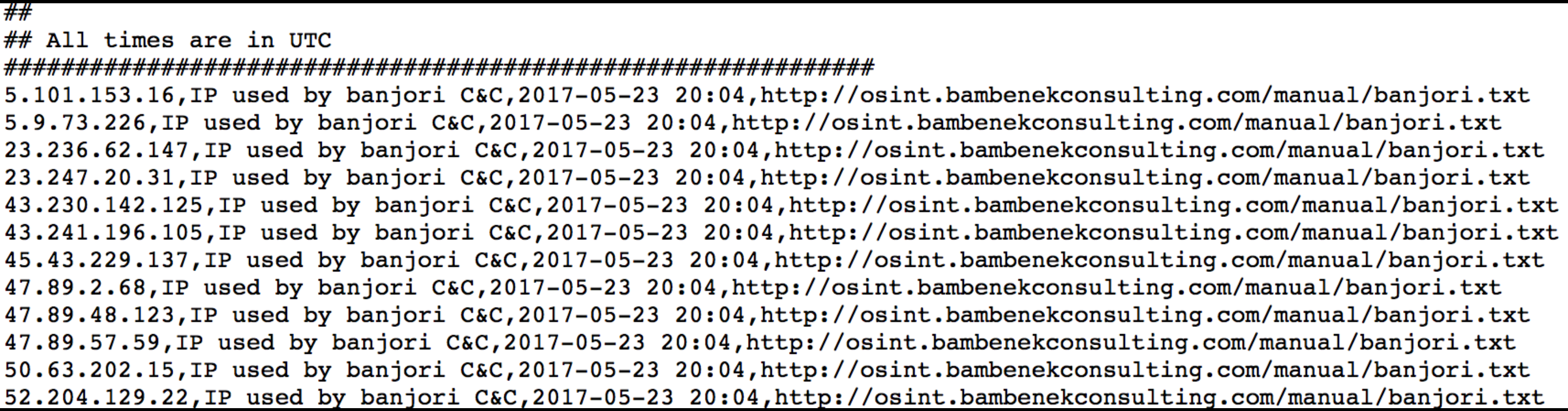
- External
- Twitter feeds
- My list: https://bitbucket.org/tactical_intel/honeypots
- Normalizing data is a PITA
- RegEx are your friend

My Favorites

- @suspectnetworks
- @webironbots
- @idahohoneypot
- @volipban
- @openblacklist
- @honeypylog
- @honeyfog
- @netmenaces
- @evilafoot
- @openblacklist
- @gosint2
- @malware_traffic
- @honeypoint
- @honeypotlog
- @atma_es
- @internetbadness
- @eis_bfb *
- @olaf_j *
- @pancak3lullz **

Bambinek C&C List

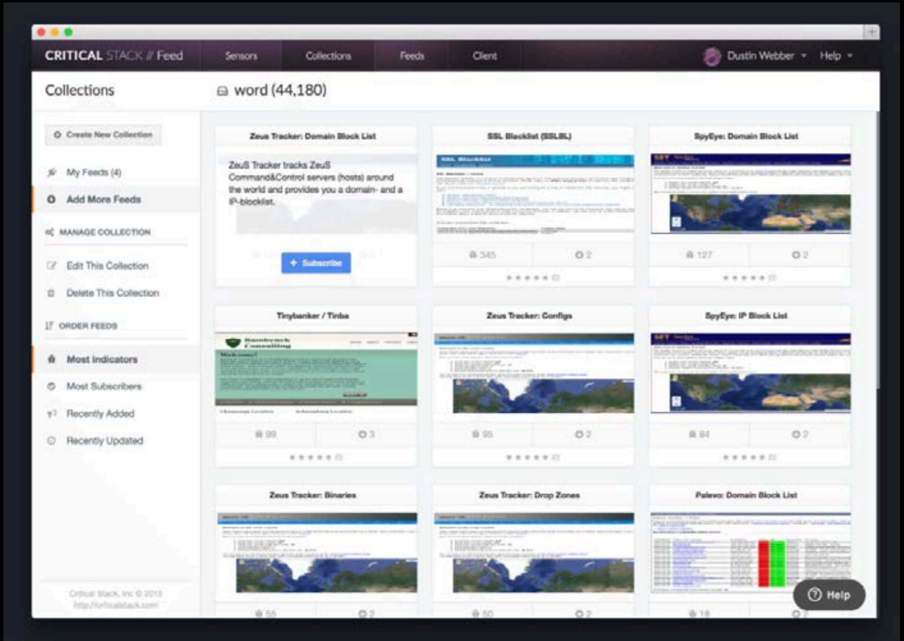
- http://osint.bambenekconsulting.com/feeds/c2-ipmasterlist.txt
- List of C2 IP addresses



```
##
## All times are in UTC
#############################################################
5.101.153.16,IP used by banjori C&C,2017-05-23 20:04,http://osint.bambenekconsulting.com/manual/banjori.txt
5.9.73.226,IP used by banjori C&C,2017-05-23 20:04,http://osint.bambenekconsulting.com/manual/banjori.txt
23.236.62.147,IP used by banjori C&C,2017-05-23 20:04,http://osint.bambenekconsulting.com/manual/banjori.txt
23.247.20.31,IP used by banjori C&C,2017-05-23 20:04,http://osint.bambenekconsulting.com/manual/banjori.txt
43.230.142.125,IP used by banjori C&C,2017-05-23 20:04,http://osint.bambenekconsulting.com/manual/banjori.txt
43.241.196.105,IP used by banjori C&C,2017-05-23 20:04,http://osint.bambenekconsulting.com/manual/banjori.txt
45.43.229.137,IP used by banjori C&C,2017-05-23 20:04,http://osint.bambenekconsulting.com/manual/banjori.txt
47.89.2.68,IP used by banjori C&C,2017-05-23 20:04,http://osint.bambenekconsulting.com/manual/banjori.txt
47.89.48.123,IP used by banjori C&C,2017-05-23 20:04,http://osint.bambenekconsulting.com/manual/banjori.txt
47.89.57.59,IP used by banjori C&C,2017-05-23 20:04,http://osint.bambenekconsulting.com/manual/banjori.txt
50.63.202.15,IP used by banjori C&C,2017-05-23 20:04,http://osint.bambenekconsulting.com/manual/banjori.txt
52.204.129.22,IP used by banjori C&C,2017-05-23 20:04,http://osint.bambenekconsulting.com/manual/banjori.txt
```

Critical Stack Intel

- Aggregated and parsed by Critical Stack and ready to deploy to BRO IDS
- You specify which feeds to deploy
- https://intel.criticalstack.com/



ZeuS Tracker tracks ZeuS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist.

Emerging Threats

- Emerging Threats Firewall Rules
  - Collection of rules for various firewalls (pfsense, iptables, etc)
  - http://rules.emergingthreats.net/fwrules/
- Emerging Threats IDS Rules
  - Collection of Snort and Suricata rules for blocking or alerting
  - http://rules.emergingthreats.net/blockrules/

HailATaxii

- A free repository of Open Source threat intelligence feeds in STIX format
- Over 825k+ indicators

Firehol.org

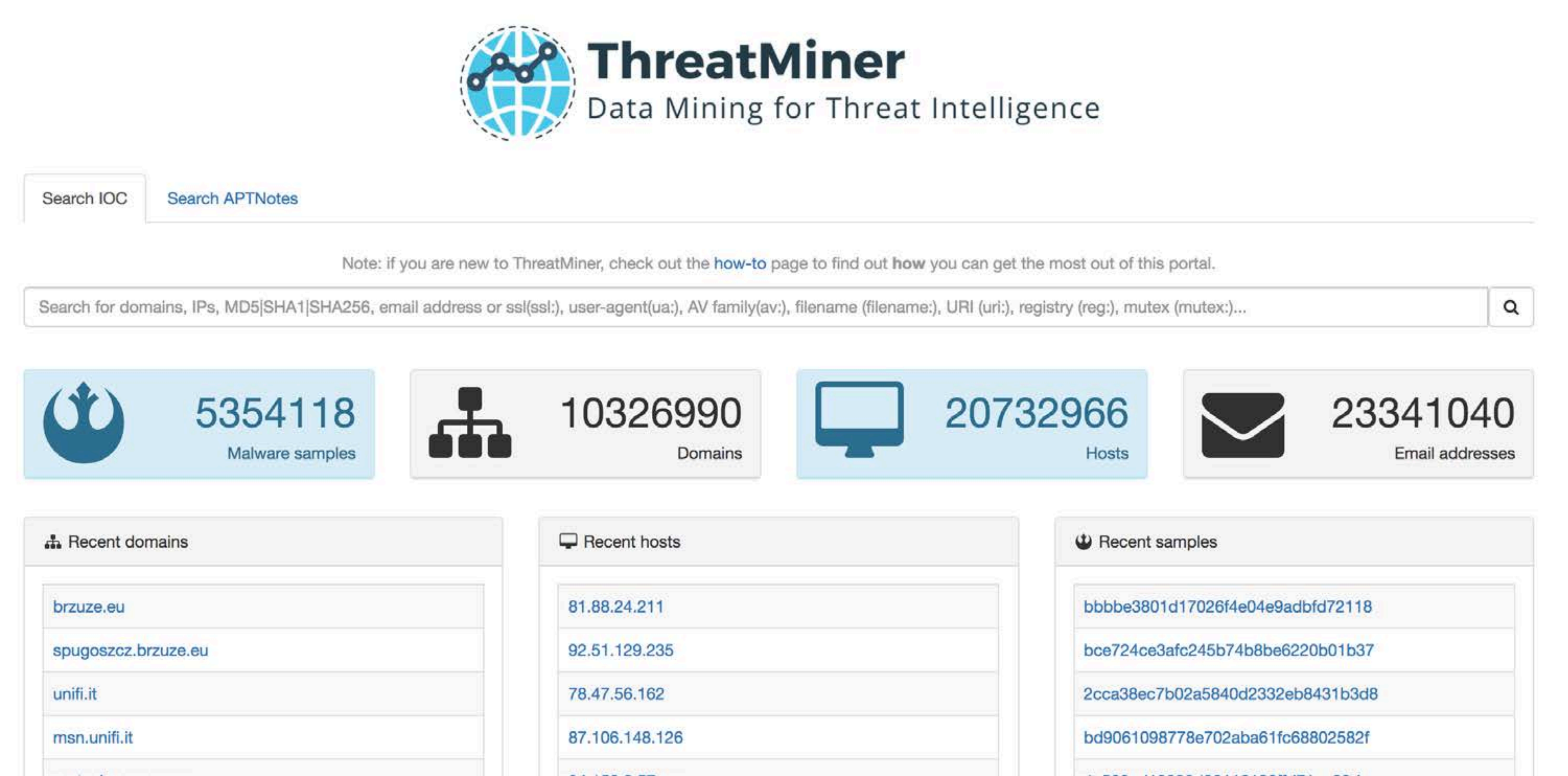
- http://iplists.firehol.org/
- TONS of feeds (400+)
- Attack/abuse/malware/botnets/C2
- Click a link and then download the corresponding github file
- Constantly maintained
- Collection of tons of sources
- Firehol and Fireqos languages

c1fapp.org

- Feed aggregator
- Private and open source feeds included
- Nice interface
- Minimal feeds for free source
- Takes a while to get activated

ThreatMiner

- https://www.threatminer.org/



ThreatMiner
Data Mining for Threat Intelligence

Search IOC | Search APTNotes

Note: if you are new to ThreatMiner, check out the how-to page to find out **how** you can get the most out of this portal.

Search for domains, IPs, MD5|SHA1|SHA256, email address or ssl(ssl:), user-agent(ua:), AV family(av:), filename (filename:), URI (uri:), registry (reg:), mutex (mutex:)...

5354118	Malware samples
10326990	Domains
20732966	Hosts
23341040	Email addresses

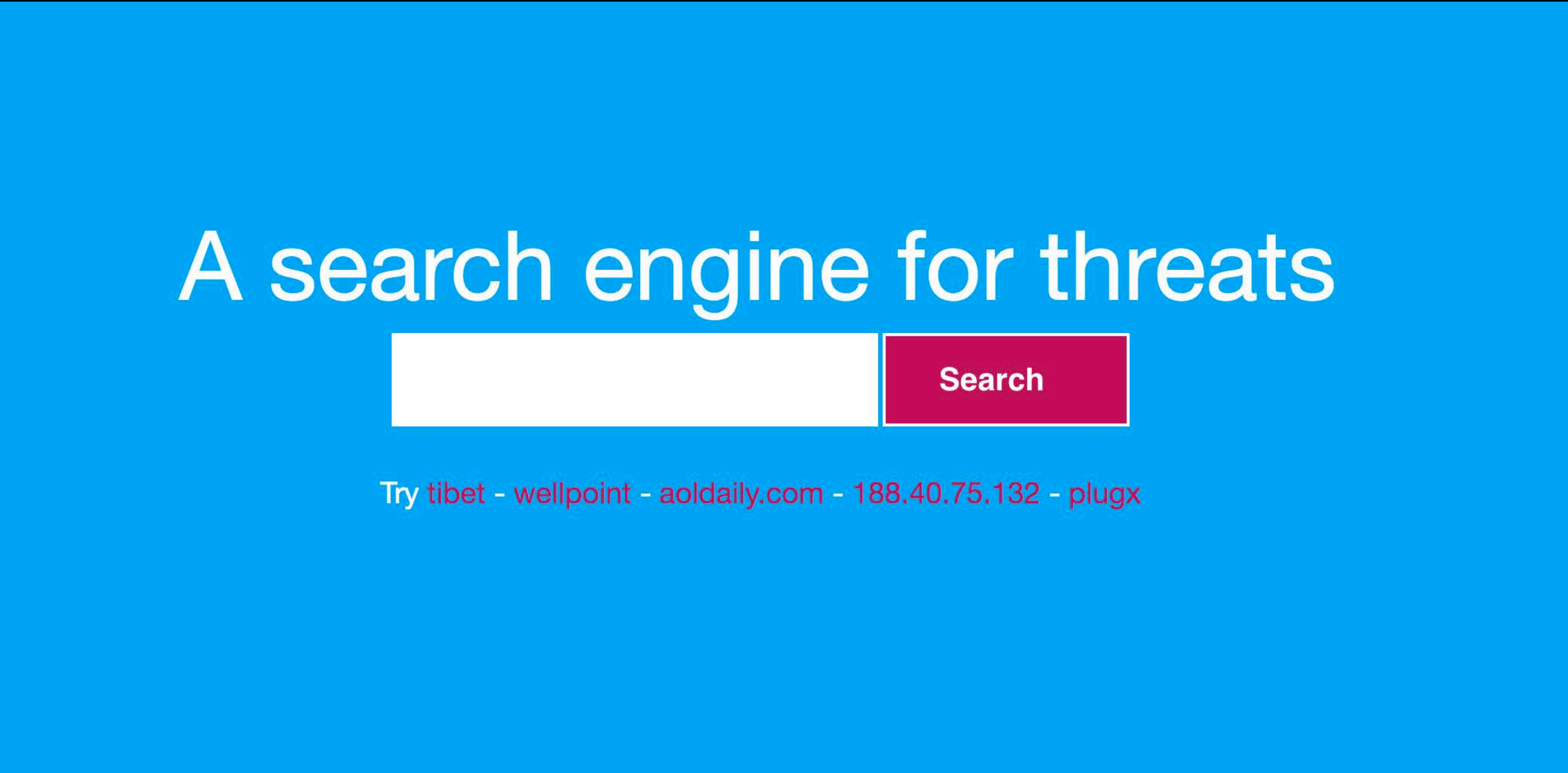
Recent domains	Recent hosts	Recent samples
brzuze.eu	81.88.24.211	bbbbe3801d17026f4e04e9adbfd72118
spugoszcz.brzuze.eu	92.51.129.235	bce724ce3afc245b74b8be6220b01b37
unifi.it	78.47.56.162	2cca38ec7b02a5840d2332eb8431b3d8
msn.unifi.it	87.106.148.126	bd9061098778e702aba61fc68802582f

ThreatMiner

- You can search:
  - Domains
  - IP’s
  - Hashes
  - Email
  - SSL info
  - Filenames, mutex strings
  - User Agents
  - Registry Key Strings
  - and more….

ThreatCrowd

- https://www.threatcrowd.org/



A search engine for threats

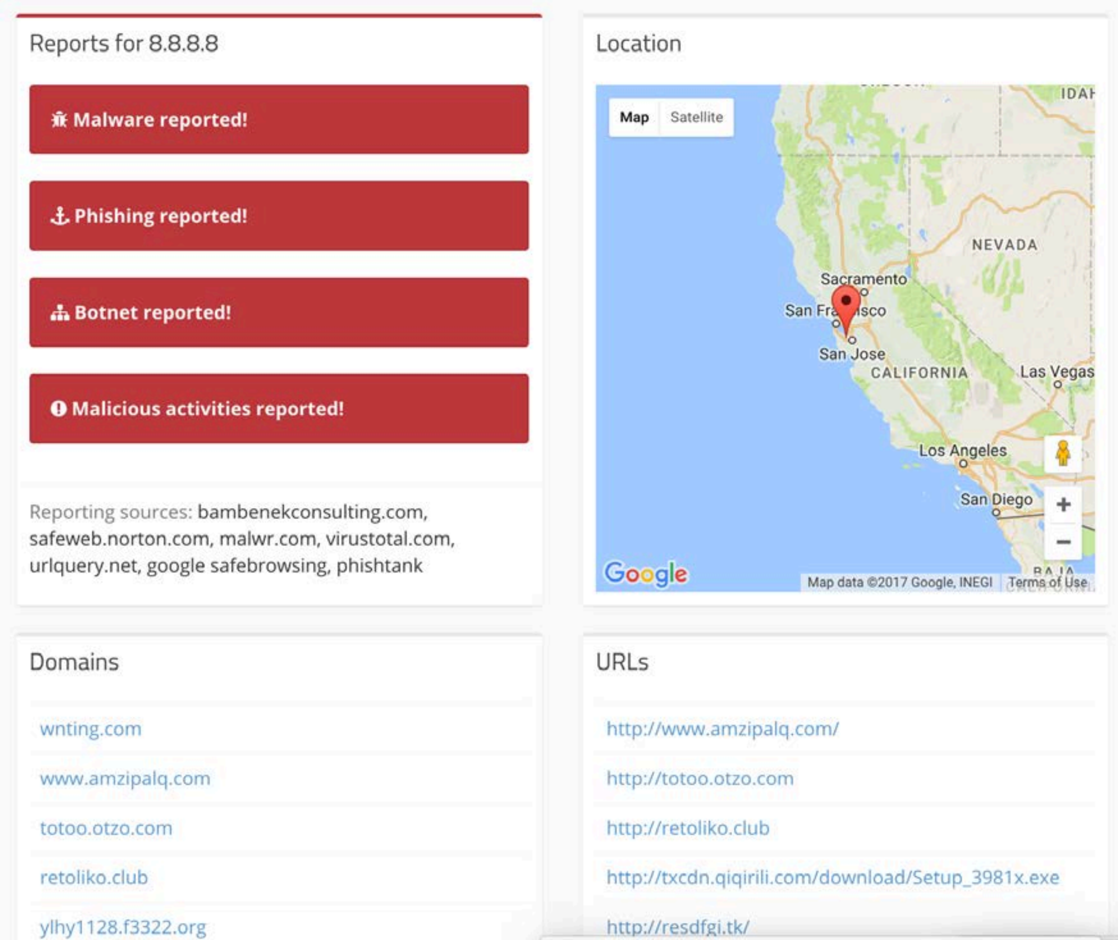
Try tibet - wellpoint - aoldaily.com - 188.40.75.132 - plugx

Autoshun.org

- 2000 malicious IP addresses
- wget/curl/API
- 30 minute time limit
- Has Snort plugin
- P0f (OS fingerprinting) plugin

Cymon

- https://www.cymon.io



Reports for 8.8.8.8

Malware reported!

Phishing reported!

Botnet reported!

Malicious activities reported!

Reporting sources: bambenekconsulting.com, safeweb.norton.com, malwr.com, virustotal.com, urlquery.net, google safebrowsing, phishtank

Location

Domains

wnting.com

www.amzipalq.com

totoo.otzo.com

retoliko.club

ylhy1128.f3322.org

URLs

http://www.amzipalq.com/

http://totoo.otzo.com

http://retoliko.club

http://txcdn.qiqirili.com/download/Setup_3981x.exe

http://resdfgi.tk/

recon-ng

- By Tim Tomes
- Reconnaissance framework
- Comes with Kali
- My favorite

recon-ng

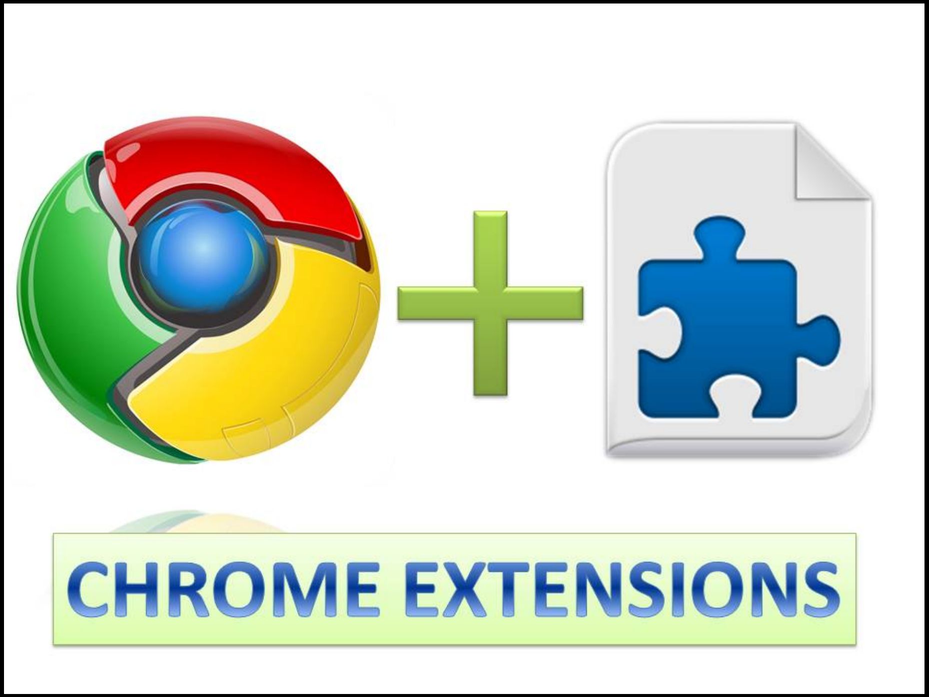
- Terminal based
- Similar structure/commands to Metasploit
- > show modules
- > use recon/domains-contacts/pgp_search
- > show info
- > run

SpiderFoot

- http://spiderfoot.net
- OSINT automation tool
- Windows/Linux
- Another data aggregation/lookup tool
- 50+ hosts

ThreatPinch

- @threatpinch on Twitter
- Chrome extension



Malware

- Many of the aforementioned engines support malware sampling
- VirusTotal (https://virustotal.com)
- Totalhash (https://totalhash.cymru.com)
- Malwr (https://malwr.com/)
- Virus Share (https://virusshare.com/)
- Yara Rules (https://github.com/Yara-Rules/rules)

Malware

- 99% of malware hashes are seen for 58 seconds or less
- Vast majority of malware only seen once

    - Verizon Data Breach Investigations Report, 2016

Maltego

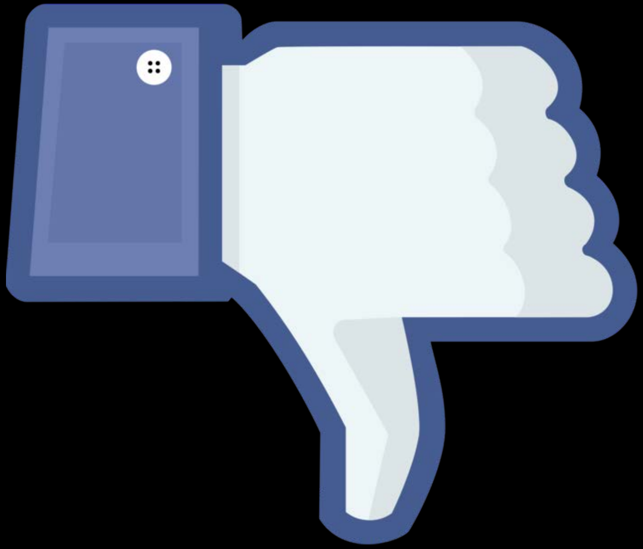
- Industry standard viztool?
- The first. Perhaps the best.
- Easy to write your own transforms
- Free version is fine but doesn’t scale
- Check out CanariProject.com
- Malformity (https://github.com/digital4rensics/Malformity)
- Some of the earlier resources also have maltego transforms (ie @threatcrowd et al)

Crowdsourced TI

- ThreatConnect (TC Open)
  - https://www.threatconnect.com/free/
  - Allows you to see/share intelligence
  - Free tool is limited, but it’s free so…
  - 100+ OSINT feeds
  - Threat/incident/adversary info
  - Intelligence validation w/ other users

Facebook ThreatExchange

- Invite only
- Need to have large web presence
- https://developers.facebook.com/docs/threat-exchange/v2.9



Phishing

- https://www.phishtank.com
- https://openphish.com/

Great TI List

- https://github.com/hslatman/awesome-threat-intelligence
- H/T to Herman Slatman

DarkWeb

- Onerous and time consuming
- Not necessarily worth the investment of time unless high value target IMHO
- IME regular web monitoring yields much more/better intel than DarkWeb
- When it hits, it often hits big
- YMMV

Speed Is Of The Essence

- 84% of phishing sites exist for less than 24 hours
    - Webroot Phishing Threat Trends Report, 2016
- IP reputation sites often rank sites as bad based on badness 6+ months prior

Common Pitfalls

- Oversubscription
  - Data overload is a real thing
  - Irrelevant/unrelated data
- Improper implementation
  - Data deployed to the wrong people
  - Data not acted on
  - Data not validated

TI Efficiencies

- Ways you can reduce costs/increase efficiencies:
  - Reduce archiving (do you really need 2 years worth of data)
  - Focus scope
  - Roll your own

Thank You

- Email: shane@tacticalintelligence.org
- Twitter: @tactical_intel
- Tinder: @infosec-studmuffintop