

OSINT
workshop -
finding secrets
online

or, How I Learned to
Stop Worrying and Love
my privacy

\$ whoami

Brett Calderbank

-
- ## All-round cool guy
-
- ## Security engineer @ MSP
-
- ## **Hundreds** of twitter followers... at least **dozens**
-
-
- ## Shameless plug: @odin_the_mighty on twitter
- ## Connect with me on LinkedIn if that's your kinda thing:
- <https://www.linkedin.com/in/brettcalderbanks/>

\$ cat /opt/this_talk

- ## Quick n' rough intro to OSINT
-
- ## Introduce you to how different kinds of people potentially use OSINT
-
- ## How we can (and do) use it in information security
-
- ## Not an intro to things like the Overton window, memetics, ACE, or anything potentially SOCINT and such </3

What even is OSINT?

Open-source intelligence (OSINT) is data collected from publicly available sources to be used in an intelligence context.

“Open” meaning Overt.



Adjective [[edit](#)]

overt (*not comparable*)

1. Open and not secret nor concealed.

Just checking, you know what I mean by INTEL right?

- Intelligence is simply put: any information that can be, or is, useful to inform.



This DOESN'T mean that that INTEL is 'intelligent'...



Different types of OSINT

• Shout-out to Wikipedia:

- **Media:**, print [newspapers](#), [magazines](#), [radio](#), and [television](#) from across and between countries.
- **Internet**, online publications, [blogs](#), [discussion groups](#), citizen media (i.e. – cell phone videos, and user created content), [YouTube](#), and other social media websites (i.e. – [Facebook](#), [Twitter](#), [Instagram](#), etc.). This source also outpaces a variety of other sources due to its timeliness and is easily accessible.
- **Public Government Data**, public government reports, budgets, hearings, telephone directories, press conferences, websites, and speeches. Although this source comes from an official source they are publicly accessible and may be used openly and freely.
- **Professional and Academic Publications**, information acquired from [journals](#), conferences, symposia, [academic papers](#), dissertations, and theses.
- **Commercial Data**, [commercial imagery](#), financial and industrial assessments, and databases.
- **Grey Literature**, technical reports, preprints, patents, working papers, business documents, unpublished works, dissertations, and newsletters.

jivoi / [awesome-osint](#)

<> Code

! Issues 0

🔗 Pull requests 1

📁 Projects 0

📖 Wiki

📊 Insights

🧠 A curated list of amazingly awesome OSINT

[awesome-list](#)

[osint](#)

[website](#)

#osint

Who are we talking about?

Tin foil hats on now!



Foreign governments

- US to close CIA division's UK intelligence monitoring unit
- <https://www.ft.com/content/99ede9cc-b582-11e7-aa26-bb002965bce8>

FINANCIAL TIMES myFT

Central Intelligence Agency [+ Add to myFT](#)

US to close CIA division's UK intelligence monitoring unit

Decision ends 7 decades of collaboration with BBC at Caversham Park



The CIA's Open Source Enterprise has been run out of Caversham Park, the Berkshire stately home, since 1943 © Charlie Bibby/FT

[Twitter](#) [Facebook](#) [LinkedIn](#) 12 [Print](#) [Save](#)

Local governments

- <https://www.cpni.gov.uk/who-we-work>
- <https://www.ncsc.gov.uk/information/global-targeting-enterprises-managed-service-providers>

Key points

- *Collaboration between the NCSC, PwC and BAE has led to the discovery of a sustained and global cyber campaign*
- *A known cyber actor using previously documented intrusion tools has targeted major international Managed Service Providers (MSPs) since at least May 2016*
- *We assess the ultimate targets are customers of these MSPs*
- *The activity we are aware of likely represents only a small proportion of the total malicious activity; we are still working to establish the scale of the activity*
- *Compromises could affect government or industry supply chains; we will update our assessment when more information becomes available*
- *We have no evidence to suggest these actors are targeting the general public or SMEs*

Business intelligence

- https://twitter.com/Daniel_Holman/status/917989507454197765

- How can open source intelligence and risk scoring be applied to my business?

1. Credit Risk

Financial institutions rely on credit databases to make decisions about whether to provide credit. By looking at what a person or organisation has said or has been said about them online, a risk score can be generated to provide an additional objective measure of credit risk.

2. Cyber Risk

The information available online about your company, its infrastructure and its people will be used by attackers as inputs into cyber attacks. A risk score can be generated based on the type and volume of information available.

3. Third Party Risk

Your suppliers have privileged access to your people, data and infrastructure. You rely on them to provide the inputs that you need to run your business. By looking at the behaviours of the supplier's executives and what is being said about them and their company online, a risk score can be generated to help identify areas of concern.

4. Employment Screening and Ongoing Monitoring

Your employees have access to your most sensitive data, and represent your business. By assessing a candidate's online behaviour, you can generate a risk score that will help guide the interview process.

Once an employee joined your organisation, you can protect your assets by monitoring online behaviour. Depending on the organisations risk tolerance, risk scores above the tolerance can be turned into alerts for action by your security team.

and (most importantly) us!

- https://en.wikipedia.org/wiki/Cyber_threat_intelligence

According to CERT-UK **cyber threat intelligence** (CTI) is an "elusive"^[1] concept. While cyber security comprises the recruitment of IT security experts, and the deployment of technical means, to protect an organization's critical infrastructure, or intellectual property, CTI is based on the collection of intelligence using **open source intelligence** (OSINT), **social media intelligence** (SOCMINT), **human intelligence** (HUMINT) or intelligence from the **deep and dark web**. CTI's key mission is to research and analyze trends and technical developments in three areas:

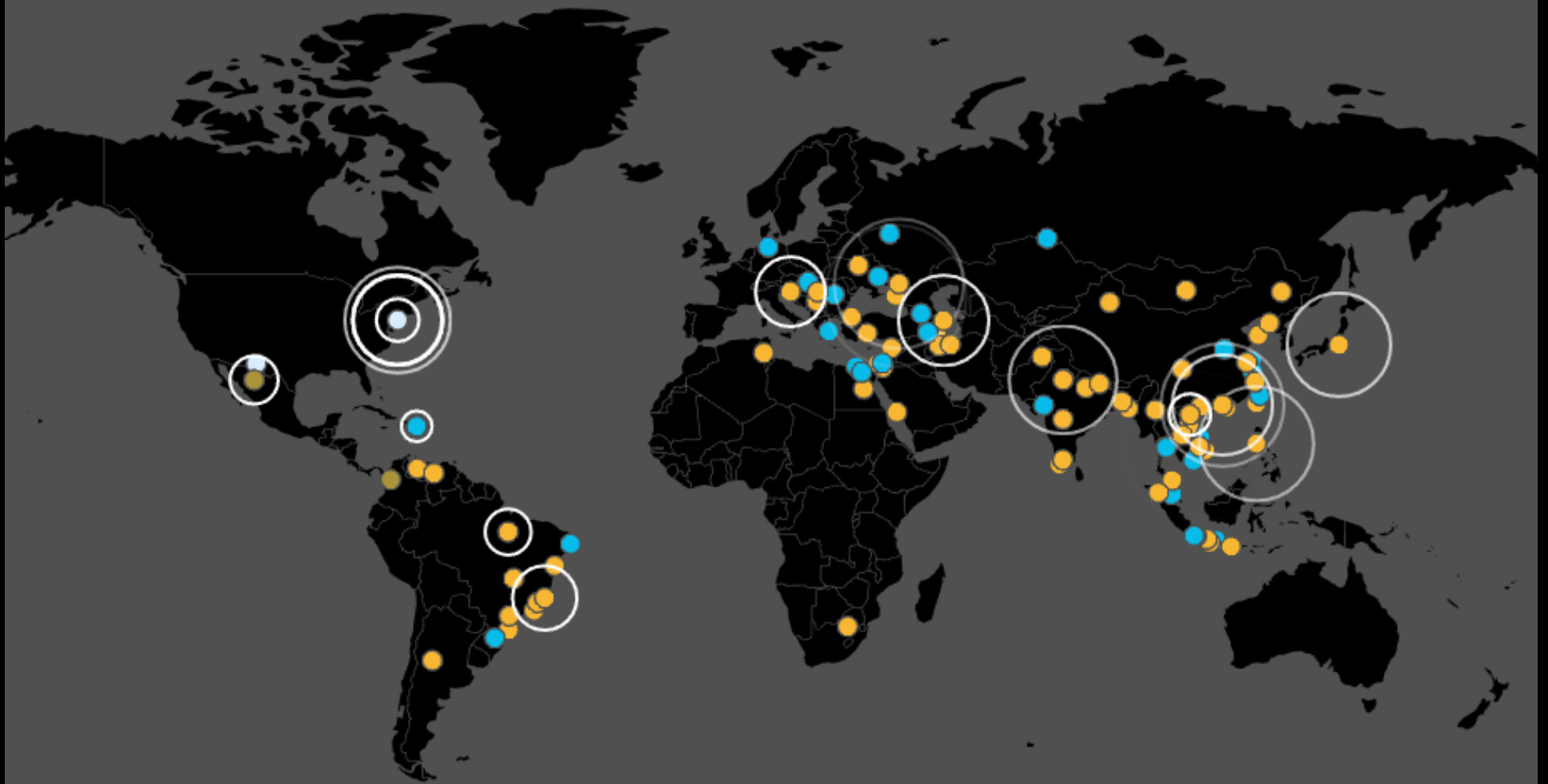
- Cyber crime
- Cyber hactivism
- Cyber espionage (**advanced persistent threat** or APT)






Those accumulated data based on research and analysis enable states to come up with preventive measures in advance. Considering the serious impacts of cyber threats, CTI has been raised as an efficient solution to maintain international security.

- <http://osint.bambenekconsulting.com/feeds/>

Why do we even care?

-
-
- ## It affects every single one of us 24/7/365
-
- ## From directly in our jobs and social lives, to international relations and military operations
-
- ## For example...



Country	Botnet
 Mexico	nivdort
 Brazil	sality4
 United States	mirai
 Viet Nam	sality4
 Dominican Republic	sality3

- <http://www.bbc.co.uk/news/world-europe-41510592>

- **Russian soldiers face ban on selfies and blog posts**

- ⌚ 5 October 2017 | Europe

f t n ✉ Share

Bad OPSEC, and staying up-to-date!

- <https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/>

ANDY GREENBERG SECURITY 10.20.17 05:45 PM

**THE REAPER IOT BOTNET HAS
ALREADY INFECTED A MILLION
NETWORKS**

Where can we use this?

- ## To practice good OPSEC/privacy
- By having a good understanding of our footprint we can be in control of what “bad” people can see and use against us.
- ## Business intelligence
- Businesses can take advantages by being aware of, and adapting to, public perceptions and usage of their products as well as changing to meet demand.
- ## Threat intelligence

Us lot in security can take advantage of sharing different information and data sets – to help up work on anything from exploit development, to research, to the whole suite of blue and red teaming skills.

-

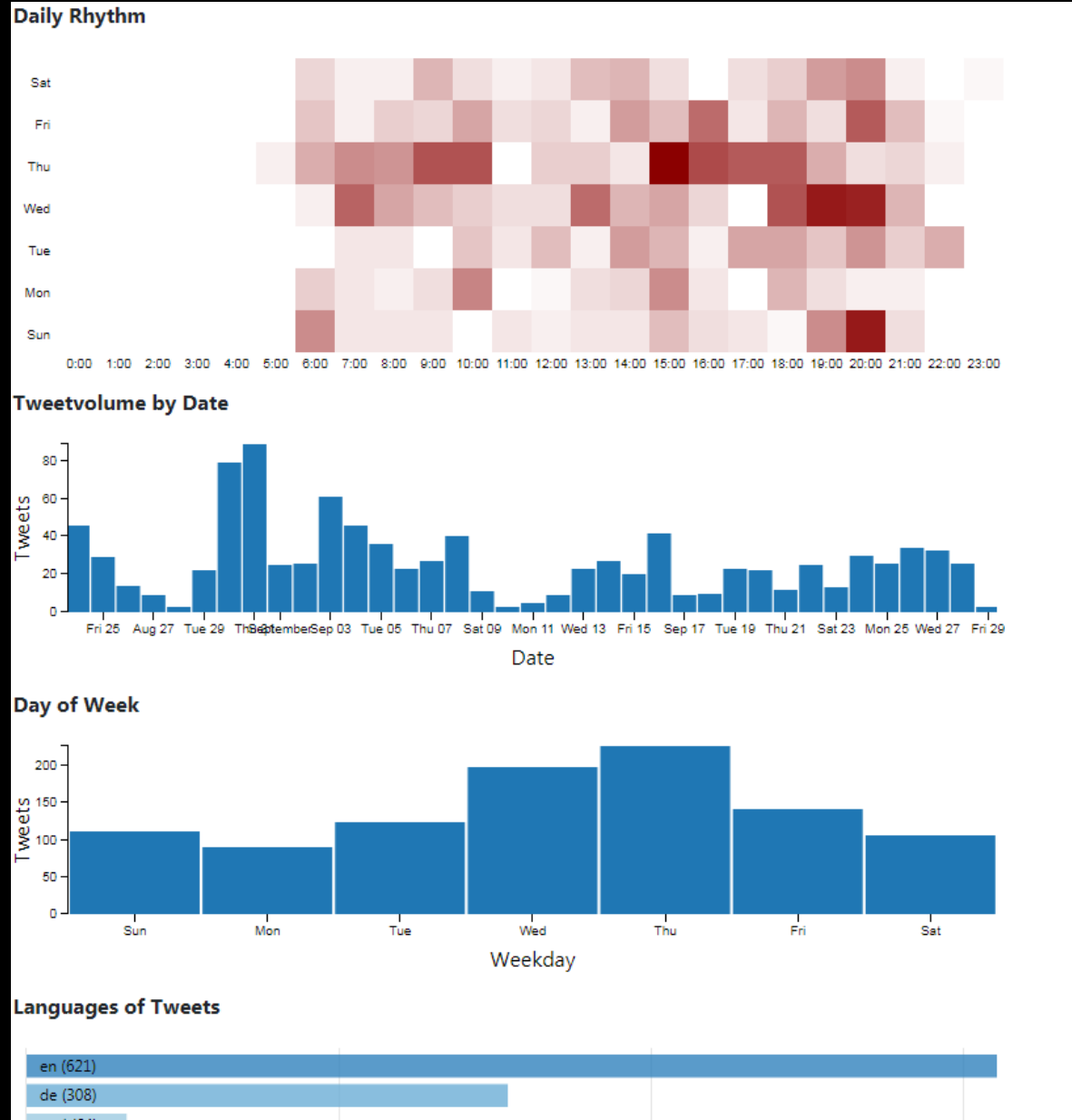
Practice safe SECS



OPSEC
COMSEC
INFOSEC
PERSEC

KEEP IT UNDER WRAPS

- <https://www.poynter.org/news/ultimate-guide-bust-fake-tweeters-video-toolkit-10-steps>
- <https://accountanalysis.lucahammer.com>



What tools do people use?

- <https://github.com/aancw/Belati>
- <https://n0where.net/easy-intelligence-gathering/>
- <https://github.com/smicallef/spiderfoot>



LET'S DO SOMETHING PRACTICAL!

- Courtesy of https://twitter.com/Opes_pwnyan:
- > https://twitter.com/_pentti_1
- > https://twitter.com/_1m4S
- > https://twitter.com/_Come_AndGetMe_
-

```
*****
*
*  _  _  _  _  _  _  _  _  _  _  _  _  _  _  _  _  _  _  _  _  _  _  _
*  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
*  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
*  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
*  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
*
* TheHarvester Ver. 2.7
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*****
```

A few other tools:

- Wayback machine
- Video Downloader
- Maltego
- Instalooter
- Tor/chrome incognito/other browsers

Q&A time!

Thanks for being here!