CTI League Disinformation Readme

Pardon our dust whilst we get set up and work our processes out: if you find things wrong or missing in here, please tell [redacted]/[redacted]/[redacted]

What we do

Mission: this is the Disinformation deployment within the CTI League's Covid19 response. We're here as a community to find, analyse and coordinate responses to Covid19 disinformation incidents as they happen, and where our specialist skills and connections are useful.

Tasks:

- Find new disinformation, work out ways to mitigate or stop it, get information to the people who can do that

Lifecycle of a new rumor:

A new Covid19-related rumour has started online. You've seen it yourself, someone has sent you an example of it, you've seen another group tracking it - there are a bunch of ways to spot something new happening. Now what? **NB each of these steps can be by different people**

1. Tell people
    a. Put a message in slack #3-disinformation, with the artefact you found and a short description. Adding the words [NEW RUMOR] will make it a lot easier to find later
2. Decide whether to start an incident
    a. Do a quick check that it's a rumour. One sighting doesn't make an incident. 15 copies of the same message on Twitter, or 3 friends sending you the same strange DM, and you're probably onto something.
3. If it's significant, start an incident
    a. Give it a name. Names help.
    b. Add a row to the incidents spreadsheet
    c. Create a folder in the googledrive INCIDENTS folder for notes and anything that won't fit into the DKAN

    d. Start adding data to the DKAN

4. Investigate the rumor
    a. Look for related artefacts, accounts, urls, narratives etc
5. Investigate ways to close down the rumor / repeater sites etc.
6. Report on the rumor
    a. add an incident to the MISP instance for this rumor
    b. Write and send notes/reports to the people who can respond
    c. Close down the rumor and move onto the next one (there's always a next one)

More detailed notes on process are in CTI League Disinfo Dataflows

Who we are

People:

- Leads: The person responsible for getting you resources, facetime, stuff fixed etc is [redacted], with [redacted] and [redacted]. They know where to find things, or where to find people who know where to find things, can resolve issues, make decisions etc. [redacted] and [redacted] also designed the AMITT framework that we'll be using for reporting.

- Tech: [redacted] made the disinformation MISP galaxies etc happen. Talk to him about tech and standards. [redacted] kicked the disinformation DKAN into life. Talk to him about data storage and communities.

- We walk among you: we've started this deployment by adding people from two existing disinformation groups: Covid19disinformation (Covid19 disinformation tracking with Atlantic Council) and CogSecCollab (aka CSC, a nonprofit dedicated to making community-driven disinformation response work: you might also know us as Misinfosec). As we work together, we'll all blend together, but as we start out, if you're a disinformation newbie, feel free to grab anyone with one of those tags.

How we coordinate this group:

- Slack:
    - most of our work happens in #3-disinformation
- Googledrive: we've created a googledrive for the team.
    - This is where we store artefacts, notes on incidents etc as we track them down.
    - DM [redacted], [redacted] or [redacted] with an email you're comfortable using for the googledrive.
- DKAN: https://data.cogsec-collab.org - this is where we put any data we find.
    - DM [redacted] or [redacted] to get an account on the DKAN
- MISP: https://covid-19.iglocska.eu - this is where we raise incidents
    - Sign up on the site to get an account

How we coordinate with other groups:

- Responders:
  - MISP: we add to MISP so others can read and act on the incidents in it
  - IRs: we're working on this
- CogsecCollab, Covid19Disinformation:
  - will feed in any incidents they find
  - https://misp.cogsec-collab.org/ - the CogSecCollab MISP instance

Tools and help

We've started a bunch of how-to notes at https://github.com/cogsec-collaborative/documentation They're in CogsecCollab because multiple teams need them. If you need a how-to, please ask; if you can write one, please write (we'll take it in any form, just so long as we get the information out to people who need it);

If a note is specific to CTI League or this deployment , please add it to this googledrive instead. We have to assume we're in an adversarial environment here.

Getting yourself started

Get yourself set up on the tech we use

- DM [redacted], [redacted] or [redacted] an email you're happy to use with the googledrive
- Ask [redacted] for an account on the DKAN
- Sign up for MISP

SAy hi in slack channel #3-disinformation

FAQs

Questions:

- Q: Do we just cover Covid19? Mostly, but it's okay to include other topics if they're part of this immediate timespan. TL;DR: we do care about disinformation around current events. We're not so concerned about people talking about aliens.