Disinformation

General

The CTI League is willing to neutralize any threat in the cyber domain regarding the current pandemic, including disinformation. The mission of this effort is to find, analyse and coordinate responses to Covid19 disinformation incidents as they happen, and where our specialist skills and connections are useful. The TL;DR is that we find and track new disinformation incidents, work out ways to mitigate or stop disinformation incidents, and get information to the people who can do that.

Our Efforts

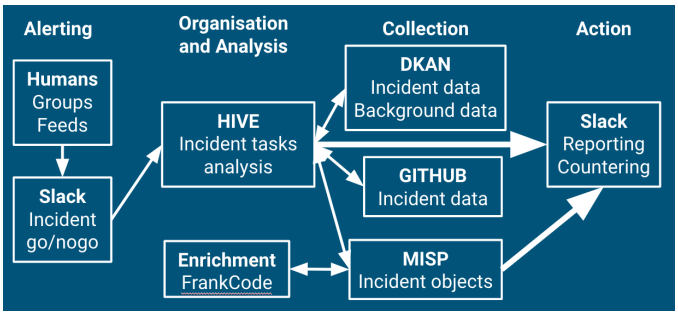
The disinformation team:

- Finds, tracks and responds to disinformation incidents
- Adapts the tech we need to do that better/faster
- Writes the processes and how-tos we need to include more people in our response

Team coordination:

- Slack channel #4-disinformation
- Team discussion/training on zoom Wednesday and Saturday at 4-5 PST / 7-8 EST
- Team README and startup guide
- Team playbook: The Big Book of Disinformation Response

Our Workflows



Disinformation analysis has overlaps with other incident response methods, and we try to keep tools, processes and outputs as similar as possible, and will be reaching out to other CTI League teams to explore connections. Our current process (above) uses HIVE to organise tasks around each disinformation incident and its connections to previous incidents, actors, artefacts etc.

Alerts currently come in from connected disinformation groups (Covid19Disinformation, Covid19Activation), CTI League members, existing feeds etc. and are triaged for volume and relevance before being activated as incidents. The full incident process is described in the Big Book of Disinformation Response, but is a combination of collection, enrichment and analysis of social media artefacts and narratives, with emphasis on TTPs, incident objects and how to report or counter any of these that we find.

We're also working on connected workflows including narrative tracing across incidents, using the tools inside HIVE and MISP.

Our Tech

Our tech stack includes:

- HIVE https://hive.thlab.ninja/: task/project management
- 'Clean' MISP https://covid-19.iglocska.eu: reported objects
- 'Dirty' MISP https://misp.cogsec-collab.org: objects under analysis
- DKAN https://data.cogsec-collab.org: data repository
- github team: kanbans and datastore
- googledrive: team notes