CTI League Disinfo Dataflows

Incident dataflows

Incident Endpoints

Narrative dataflows

Incident dataflows

Scoping

- CTI League is Covid19. Do we just cover Covid19? No - can include politics. Don't care about aliens though.
- Anybody can start an incident, but the group decides what it reports on.

Intel feeds

- Phishing maybe - not much; lots false positives
- Ted team feed
- Phone honeypots
- disinfo@ctlleague.org - reporting hotline
- Feeds potential from other groups - e.g. peacetech from next thursday
- Mitre covid19 feed - might be in wrong direction; needs to be symmetric
- Sniff EuVsDisfo - is slow (narrative based) - SJ's dataset/ data stream list
- Sniff hamilton68 dashboard for themes
- Sniff botnet feeds for themes
- Set up reporting from Facebook, twitter etc
- Ask Facebook for feeds from them

Data suck in

- Data in goes to DKAN

Analyst sees data in DKAN

- If they see something new (relative to narratives, incidents listed in MISP) they add a new incident or narrative to MISP and flag as new
- Team starts analysis and looking for related artifacts, urls, narratives etc

Documenting analysis

- We have DKAN and MISP, but also useful to have a google folder for each incident for other things that don't fit into those, like research notes
- Classifications: if it's openly available online, then it's okay to put through e.g. Tableau; if it's come though internal routes (e.g. SMS), then keep it off public internet (don't share).

Who communicate to

- Report when something significant happens - e.g. see this main effort for this new line
- Report on time period… if big, a daily report; if smaller a weekly report
- No report goes out without at least 2 people beyond the editor going over it
- End users are also watching the MISP

Who makes decisions

- Depends on decisions
- Need a board - vote via slack; person calling for vote does @channel to board, or emails them
- Who can add an incident? Anyone can start an incident.
- Who can release a report -
- Who can talk to customer/ victim? Needs to be agreed on
- Any transfer of funds in either direction needs board approval

Incident Endpoints

What we want to do with an incident is disrupt it as much as possible. If we can stop it completely, that's a big win, but generally, we're after disruption. CogSecCollab has a long-list (here: https://github.com/cogsec-collaborative/amitt_counters/blob/master/tactic_counts.md) of the things we can do to disrupt incidents at different stages of the disinformation killchain (https://github.com/cogsec-collaborative/amitt_framework - that, and DFRlab's object labels https://github.com/DFRLab/Dichotomies-of-Disinformation are what we're using in the MISP reporting), but frankly it's still messy so at this stage it's better to put our hacker hats on and think "which artefacts (observable objects) do we have in this incident, and what can we do to make them less effective?"

Examples: are there URLs pushing out covid5g disinfo? Are there social media accounts and groups pushing out covid5g disinfo? If we gather evidence on these, we can get that to the social media companies. Are there botnets involved (yes, yes, I said the b word, but they're part of this too)? Can report those too. Etc etc (and I suspect many of you have etcs CogSecCollab didn't think of when they created that counters repo).

Narrative dataflows

Narrative: Narratives are part of incidents - each incident might have multiple narratives involved, or just one, but there's usually an identifiable narrative somewhere in there, that you can use to see if there are related incidents already tracked or dealt with etc.

But there are a lot of them. Hence the mindmap, which starts to group narratives into hierarchies, making them easier to read and manage.

The other thing about narratives is that they, like incidents, have lifetimes. Some narratives appear as a result of a world or local event (or upcoming or anticipated event), and are only useful whilst that event is in peoples' minds. Example: using the Stafford Act to make everyone stay indoors was a narrative we tracked a month ago, before the stay-at-home orders started and it was a lot clearer about what states could, couldn't, would and wouldn't do.

Other narratives appear for a while, go dormant, then reemerge in different forms. Example: 5G, which was originally part of the radiation-of-all-forms-will-do-bad-things-to-you narratives, and has now come back in a mixup with covid19.

So what we need is a way to log all the narratives that we know (or care) about, whilst keeping a smaller list handy of "currently alive" narratives that we can check incoming disinformation against.