

Disinfo team vision

2020-08-05

Who do we want to be, what change do we want to make in the world?

-

Tactical

- Reduce scope. Start preparing for and pushing on antivax disinfo (maybe add anti-mask).
- Direct everything else to the CSC incubator.
- Flash report formats: sort these ([Name Redacted] will create a sample of MISP exports for us to augment)
- Run counters.
- Reports: Jinja2 template and python script to process markdown formatted reports. So we write intel reports in markdown.
- Should extend MISP so we have 1-2 templates for what a report should look like; can select objects to add to the report, export it, load into googledocs and flesh it out. Okay. So we can output PDF reports, put them on a website etc.
- Reports: <https://www.fireeye.com/blog/threat-research/2020/07/ghostwriter-influence-campaign.html>

This week

- Last week's meeting notes: https://docs.google.com/document/d/17rJmQ78ySt1p9olct3Kbcin-LodF-A0r_evqcqj_gs/edit
- Did we lose the fight on Covid disinfo? Is there anything we can actively do?
- Volunteers are coming in because they want to make a difference - not the academic toolbuilding we're doing. The US is hard to respond in. Disinfo-random is more active than the covid channels - shift focus there? Direct people to the CSC incubator slack if they're wanting to work on non-CTI disinfo.
- Students - need to spec a process for data entry; [Name Redacted] has students who can do this.

Today's team meeting topics: going to edit this list to reflect any comments on it (including things y'all want to add):

- * Team meeting and training times: can we move the Saturday meeting to a weekday (e.g. Mondays) please? Is there a better time for people in Europe/East Coast/with

kids/etc? Now meeting on Wednesdays only. 4PST/7EST = RedTeam, 5PST/8EST = CTI meeting. [Name Redacted] to add these to the calendar...

- * Training videos: have started to record 15-20 minute short training videos with examples to match (e.g. jupyter notebooks) - also collecting links to build an "Open Source Disinfo Response Training Course" similar to the "Open Source Data Science" online course list of good videos and trainings to watch to get the skills people need for response.
- * BigBookOfDisinfoResponse: we've been hard at work moving this into two documents: 1) a gitbook that can be shared with other teams who need a how-to on disinformation response (elections are coming up etc); and 2) CTI Disinfo specific instructions like what goes where and how to use tools specific to here. If you wrote sections of the BigBook, they don't get shared without your permission; there's also an authors section at the start of it to add you all too unless you want to stay anonymous.
- * Incidents: family matters meant we slacked off a bit in July, but we're back and ready to roll again in August. First order of business is starting to create "flash reports" for anything we think should be an incident, whether we end up building it out in detail or not.
- * Persistent threats: time to start talking datastores (ELK etc) and how to get feeds out to partner teams - e.g. the medical sector and LE channels.

Notes

- CogSec still waiting for IRS - holding up funding etc. CSC has a slack, CSC-incubator, for all non-CTI deployments and interests - anyone can dm us and join.
- BigBook is now in a gitbook...
- Training: [Name Redacted] doing training for darkweb. Need to put out simple training, quick demo content.
- [Name Redacted]: red team/ pen testing... looking for work streams... yes, uplevel skills with training...
- Elk stack: elastic mappings for the social media platforms: need help with this, also if it doesn't exist for the platforms, need to create and socialise the standards. Twitter and Reddit have mappings already. Nothing for Facebook yet? Not sure what else we want. Pushshift already does a lot of that - could copy their work (they had e.g. Gab, Telegram, other messaging apps). Need a clear plan of what's important.
 - Action: discuss important platforms. Look at 2019 reports for countries, areas, demographics we're interested in.
 - Action: flesh out the antivax feed lists
 - Discord channels? Reading the right-wing channels?
 - Action: go look for antivax in the discord channels.
-

