2020-08 CTI Disinfo Team Log

Sticky

These are running notes on the CTI disinfo team. They're a log of what we're trying to do, as we're trying to do it. They're also a log of our team meetups.

Disinformation Meetups

- Every weds 5pm PST/ 8pm EST /OMG elsewhere
- Recorded
- See Training folder in Googledrive
- See Team README for meeting link

Hi Newbies!

The disinformation team finds coordinated inauthentic activities ("disinformation campaigns"), and the objects and people attached to them, and uses known ways (some of which we have to invent ourselves) to expose, disrupt or stop their operations.

- Team: in Slack #4-Disinformation
- Leads: [Name Redacted], [Name Redacted], [Name Redacted], [Name Redacted], [Name Redacted], [Name Redacted], [Name Redacted]
- Process: in team README
- How-tos: in Big Book of Disinformation Response
- Tech: HIVE, MISP, DKAN, Googledrive, Python, github, bots

Log

2020-08-12

Agenda:

- tech; [Name Redacted] still working on a bot for the jupyter hub and slack integration, looking for notebooks to start with.
- tech/infra: [Name Redacted] kicked out of (or just his invite expired for?) github
- infra: moving unclassified stuff over to CogSec so a) more teams can access, b) less friction getting team to see it, c) less to protect in here
- Process: bigbook editing continues; new sections, doing lift from training and presentations into the book being hosted in CSC - DM to get edit access
- general: Wired article on this team definitely going ahead after about 10-15 hours of interviews; will be out in print edition in September
    - Press contact? Secure email?
- general: first week of swapping the CTI team and RedTeam meetings. Expect confusion. Also first week of external expert guests in RedTeam. Should be fun. Anyone got a pet project for this week?
- infra: want to clean up the github repo - split out the stored incident datasets from the codebase.
- outreach: some outreach towards Twitter going on. Did outreach this week with CS-ISAO's new director, and with ProjectDomino (covid disinfo team linked to Defcon AI Village)
    - Intro to Graphika… spinning up a DS team soon… [Name Redacted] doing this!
    - [Name Redacted] and [Name Redacted] are on [Name Redacted] podcast on the 20th… Covid, election, disinfo etc.
- Incidents: starting incidents is still scrappy. Where did we get to with the D3PO commands?
    - Need to follow up on this… was ready to go with default commands, so can create incident, assign subtasks and individuals… do we want custom stuff?
    - Let's start with the vanilla version. Socialise how to start incidents with the team.
- Tech (D3po, misp, hive etc) shouldn't be getting in our way. What are ideal workflows for people digging through disinfo all day long… what are personal workflows, before putting into MISP etc. Pay attention to this.
    - Document templates - back to spreadsheets? We have googledoc and CSV templates already. (we have googledocs to MISP code in the git repo)
    - Action: use the D3PO ticketing system
    - Action: use document templates
    - Still use MISP. Drop HIVE, unless we have automation capabilities.
- Trainings: video on text representations up this week: video, slides… [Name Redacted] around to discuss
    - Good: breaking down complex things into easy parts, funny… in sessions, pull out a 2-3 minute

2020-08-19 Incidents Check

In Hive

- Closed Hive 52 million unmasked march
- Closed Hive 57 Fake CDC anti-mask brochure

2020-08-19 Team Meeting

Agenda

- Outreach
  - Wired! Yay!
  - Bloomberg as well!
- Tech
  -
- Process
  - Big Book editing
- Incidents
  - [Name Redacted] is out for a while, so we need help on Incidents management
  - [Name Redacted] is helping out on that front with Process
  - [Name Redacted] is help with Incidents list
  - Building to alert system for Disinfo
    - Alerting Law Enforcement /lenew
    - rather than relying on the Hive
    - Folks not starting incidents in MISP and Hive
    - Folks end up putting things in threads and get lost in channels
    - [Name Redacted] interested in incident response
    - Disinformation D3PO Commands (there's a closed Google doc with these)
    - We've written a book which includes descriptions of how to do all of these things
- Outreach