2020-05 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 and sat 4pm PST/ 7pm EST /OMG elsewhere
- Format
    - 30 mins team coordination
    - 30 mins team training
- 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]
- Process: in team README
- How-tos: in Big Book of Disinformation Response
- Tech: HIVE, MISP, DKAN, Googledrive, Python, github, bots

Log

2020-05-02 Team Meeting

Status Update

- Alerts: arbeitmachtfrei, may 1st
- Incident analysis:
- Process: cleaning up processes, continuing the BigBook, added kanbans
- Tech: more MISP, started HIVE integration
- Shout outs: [Name Redacted] for HIVE!

Training requests

- Sources
- Narrative detection
- How to best determine between Fact (or fake fact) and opinion (which may be protected speech)
- Sections from the BigBook
- Tracking foreign vs domestic disinformation
- Keeping it safe and segregated from work stuff
- HIVE as used by the Disinfo team

Ongoing work and help requests

- Alerts: as they come in…
- Incident analysis: MMS, adding China disinformation
- Process: handling narratives, adding tasks lists to the BigBook
- Tech: HIVE setup, more MISP bots, chase people to get github and hive accounts
- Also: inviting people to participate; diversity, equity & inclusion

2020-05-03

Process:

- Rewrote disinformation section of CTI League handbook, and team readme.
- Rewriting process sections of BigBook, ready for use in Hive.

2020-05-05

Process:

- Wrote Hive template for incident
- Started Disinfo book club - [Name Redacted] is leading it; first reading is https://medium.com/dfrlab/facebook-shut-down-commercial-disinformation-network-based-in-myanmar-and-vietnam-d8c07c518c04

2020-05-06

Process:

- Training on disinformation
- Narratives: need to edit master list https://docs.google.com/spreadsheets/d/1yoiHNNSkNq5HoNEFiSrYTAE3nuFnp9wMBMcsh-TRx_w/edit#gid=398450894

2020-05-06 Team Meeting

Status Update

- Alerts: SpanishFlu, MilesGuo, Fauci, film-based
- Incident analysis: minimal whilst we ran up the new tech. Hive is now in place.
- Process: Can now create incidents in Hive. Adding links to MISP etc
- Tech: adding more bots
- Shout outs: [Name Redacted] getting the twitter bot working, [Name Redacted] starting reading group!

Training requests

- Next: writing the bots
- Next next: End to end tech use
- Sources - where to find alerts, fill gaps, other efforts etc
- Narrative detection
- Sections from the BigBook
- Tracking foreign vs domestic disinformation
- Keeping it safe and segregated from work stuff
- Countermeasures

Ongoing work and help requests

- Alerts: as they come in…
- Incident analysis: see Hive
- Process: handling narratives, keyword lists ([Name Redacted]?), WeMe?
- Tech: see operational Kanban, tech Kanban in team README
- Also: inviting people to participate; diversity, equity & inclusion

2020-05-11

Process
- Cleaned up the team github, so we can start loading code into it

2020-05-13 Team Meeting: planning how we work

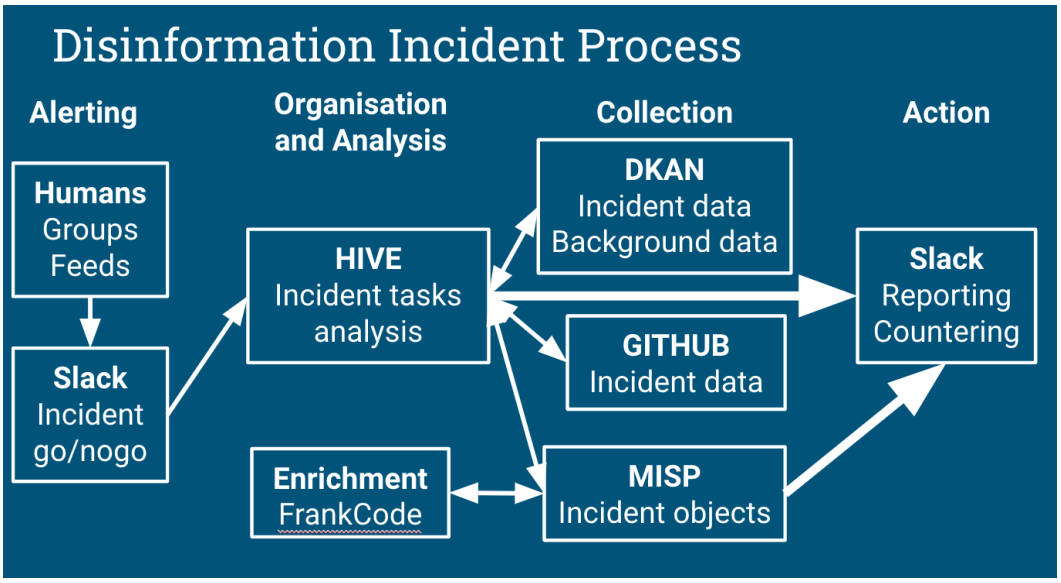
Status Update:
- Alerts:
- Incident analysis:
- Process:
- Tech:
- Shout outs:

- Blank because we need to talk about this

Training requests
- Countermeasures
- Next next: End to end tech use
- Sources - where to find alerts, fill gaps, other efforts etc
- Narrative detection
- Sections from the BigBook
- Tracking foreign vs domestic disinformation
- Keeping it safe and segregated from work stuff

Ongoing work and help requests
- Alerts: as they come in…
- Incident analysis: see Hive
- Process: organise active team
- Tech: see Kanbans in team README
- Also:

Planning how we work



1. We're looking for, and trying to reduce, harms.
2. To do that, we need to get from alerts to actions

Strategic Level Work

- Create a response system and knowledge base capable of making a difference in a high-volume, multi-actor, multi-motivation cognitive security environment
- Create a body of knowledge to support the above, for use both in Covid19 and in reuse in later events
- Create a network of professional to find, fix, track, attribute, and engage narratives

Operational Level work

- Train and place people who can build out a network of cognitive security defences from existing infosec defence
- Maintain an operational understanding of campaigns across verticals.
- Update body of knowledge based on changing situational realities.
- Engage with the various communities to enable greater cognitive and system resilience and response.

Tactical Level work

Create the team, processes and toolset that we need to quickly

- Alert on new incidents
- Make incident data available for analysts and other teams
- Analyse data and find trends, pressure points etc
- Mitigate and counter disinformation incidents as they happen both proactively and reactively

- Recommend proactive defenses prior to incidents
- Educate the masses

What we learn is also useful to many other teams (this is the prototype for large organisations, countries etc)

Execution level work

- Use our placement within CTI and other teams to spot disinformation incidents whilst we can still do something about them
- Gather the data needed to:
    - Track the source of an incident, if possible
    - Understand the mechanics of an incident
    - Find weak points in an incident, that could be countered
- Analyse data and trends, to produce enough information for:
    - Connected organisations to start investigation/ action, as appropriate
    - Us to deploy appropriate counters
    - Find connections to previous events
- Counter and mitigate
- Learn

Team

- People
    - 500 people in #4-disinformation
    - 20 active?
- Making that work better
    - Team structure and responsibilities
    - Skill tree?
    - Who manages what - what other skills do we need

Team Tasks

We've got the kanbans… but we have streams of work…

- Tech builds, tests, documentation
- Process design, test, documentation (BigBook)
- Onboarding, training, buddying, team management
- Integration into other teams
- Team logging, tracking, coordination etc
- Across-incident management (e.g. prioritisation of incidents);
- Incident management;
    - Alerting, collection, analysis, mitigation
    - Cleanup

Can we train people fast enough to do what we need? Do we slow down instead? What are we missing (e.g. a list of alerts?)

2020-05-17

Looking at the other datasets we'll need

- Persistent threats
    - Groups: antivax, reopen, far-right etc
    - Artefacts: facebook groups, hashtags, command accounts etc.

Scraping facebook groups:

- Data needed from a group page:
    - Group name
    - Person who started group
    - Admins?
    - Group size?
    - Date started,
    - Dates modified, older names etc?
    - Related groups?
    - About text
    - Related websites?
- Scrape lists of groups related to a topic?

2020-05-18

Cleaned up the googledrive.
Asked about contact in Reddit. Need to chase that up.
Added to tech: [Name Redacted]

2020-05-20

Action: need to change weekly announcements from "training" to 'team checkin"
Discussion about references - how to keep a team "library" going.

2020-05-20 Team Meeting: getting strategic

Agenda:

- Status updates
    - How disinformation fits into CTI
    - Team survey
- Team skills and structure
- AOB
    - <add more topics here>

Status Update:

- Alerts:
- Process:
    - Added "how disinformation fits into CTI" section in BigBook (1.4)
    - Added DKAN, mental health sections to BigBook
    - see Operational kanban
- Incident analysis:
    - 13 open cases in Hive
    - 11 events in MiSP https://covid-19.iglocska.eu/events/index/searchtag:2892
- Preparation:
    - added antivax sites case to Hive
- Tech:
    - see Development kanban
- Shout outs: [Name Redacted] for the team survey

Team skills and structure

- [Name Redacted] built the team survey. Kept back for a couple of days because the main team survey came out at about the same time.
- Need people to chase and report in on areas: idea is that lead is responsible for getting the thing done, not necessarily for doing it themself.
    - Leads - [Name Redacted]
        - Keeping all the people and pieces working well together
        - Team logging, tracking, coordination etc
        - Team: [Name Redacted]
    - People - [Name Redacted]
        - Onboarding, newbie training, buddying, team management, skills
    - Incident management - [Name Redacted]
        - Across-incident management (e.g. prioritisation of incidents);
        - Alerting, collection, analysis, mitigation, cleanup
        - Team: [Name Redacted]
    - Tech - [Name Redacted]
        - Tech builds, tests, documentation
        - Team:
    - Process and training - [Name Redacted]
        - Process design, test, documentation coverage (BigBook)
        - Training requests (see README: Training and Training requests)
        - Team: [Name Redacted], [Name Redacted] …
    - Outreach - [Name Redacted]
        - Alert and data sharing with other teams
        - Integration into other teams
        - Team: [Name Redacted]

Meeting notes:

- Team survey - waited til [Name Redacted] league survey went out, but clear to go now.
- Action: need an onboarding process, with an onboarding call instead of “ask these people for accounts”
    - New people go to a handy form… sends a ticket to e.g. [Name Redacted]... that person sends to training, signups etc (can we use D3PO?)
- Need strategic outreach plan, contacts, staffing needs for each area,
- Can we have someone from Twitter please?
- New format: weds all business, saturday the party
- Hive: can people send task requests to e.g. [Name Redacted] using Hive? Yes, and we can build templates for it too… e.g. “all the people who’ve used this hashtag lots”
    - Action: [Name Redacted] write up how to do this.
- Hive cases: want to go deep on a few cases, not wide… pull out all the tricks and skills we have on them.
    - If we have incidents, can merge them into high-level “buckets” based on narratives… work through tactic-by-tactic for AMITT techniques;
    - Get better at tagging in Hive?
- Action: need deeper dive into Amitt - taking an existing event, and working through it with AMITT
-

Next meeting:

- ACTION [Name Redacted]: Add a training session on non-USA disinformation happening now. Saturday will be a session on non-USA disinformation.
- [Name Redacted]: reading group is looking at other countries.

2020-05-21 Incidents update

UPDATE (Incident Management)
Today, I went been going through the HIVE incidents today, and created MISP events and DKAN folders for each incident. I also added the observables what we currently have when the incident was first started.
SO WHAT?
All of the incident initialization tasks have been completed (FINALLY) for the current incidents
NOW WHAT?
The fun part -- Investigation, collection, and analysis
WHO?
Who in this team (currently there are 644 of us) has time, expertise, or just wants to learn
HOW?

1. There are currently 10 open disinformation incidents that we need to run to ground and they are:

26 - Covid_Infringe,
27 - ru_west_bad_china_good,

30 - Spanish_Flu_1918_Nazi_Rise,
32 - plandemic,
33 - rxforliberty Jeff Barke,
35 - obamagate,
38 - Chinese Ambassador to Israel Sudden Death,
40 - persistent threat: antivax,
47 - persistent - qanon,
39 - corona2plus

2. Pick one that interests you, DM me and let me know which one you would like to work on, and dig in. ***If you have questions ASK, there are no dumb questions except the ones not asked. If you have a question, there is a very good likelihood that at least one of the other 643 team members has the same question, so ask for us too!

We are all volunteers, and we are still building out the tools, capabilities, and teams, but this is a great time to see how your skills can help solve the problem set of Cognitive Security (Mis/Disinformation), learn new skills, and learn about skills you didn't know you had.
Thank you all in advance and we are all glad you are here:partyparrot: (edited)

2020-05-25

Mapping between MISP and Hive objects added to BigBook - [Name Redacted] working on code to push from Hive to Misp

2020-05-26

Cleaning up slack pinned items

- https://github.com/COVID-19-CTI-LEAGUE/PRIVATE_BOT_DEVELOPMENT_LOOKUPS/tree/master/misp-twitter
- Action: start that list of disinformation sites
- Added persistent_threats note on canaries

Created new misp objects:

- Facebook-post
-

2020-05-27 Team Meeting

Agenda:

- Status updates
    - Alerts:
    - Incident analysis:
    - Process:

    - Tech:
    - Shout outs: [Name Redacted] for MISP object training,
- [Name Redacted] training on Data Science
    - <add more topics here

Status Update:

- Status updates
    - People:
        - First people coming through new onboarding process - fill out the survey form please!
    - Alerts:
        - Trump tweet labelled by twitter
        - “Coronavirus uses same strategy as HIV to dodge immune response, Chinese study finds”
    - Incident analysis:
        - Restarted Miles Guo analysis (48 - #MilesGuo)
        - Coronavirus uses same strategy as HIV to dodge immune response, Chinese study finds
    - Process:
        - [Name Redacted] and [Name Redacted] reading through BigBook, adding comments and items to the operational kanban
        - Cleaned up pins in Slack Channel (thanks [Name Redacted] and [Name Redacted])
        - Building out training calendar moving forward
        - BigBook is now comment-only for anyone outside triage
    - Tech:
        - Added facebook-post to MISP objects
        - Signing up for Hypothesis group: CTI Annotations Group
    - Outreach
        - Connected with darknet team
        - [Name Redacted] signed us up to researchgate.
        - Are there vendors we’d like to approach?
        - New google for groups account for this? [Name Redacted] looking into for CogSec
    - Shout outs: [Name Redacted] for MISP object training,
- [Name Redacted] training on Data Science
    - <add more topics here>

Notes:

- Outreach to twitter, facebook etc? Facebook has an academic data feed we can apply to - we should.
- Action: [Name Redacted], [Name Redacted] look into getting ResearchGate set up.

Training/ knowledge sharing

- Where we get data from and how we get it
- [Name Redacted] tidying up the BB
- Lots of people all over the world working on these
- Easy for one person to type into a Google doc or folder
- How do you take the work a single data scientist does and bring it to scale
- Incident workflows
    - Incident diagram doesn't really talk about what's happening behind that process
    - That's the data science process

Data science process

- 1. Frame the problem
- 2. Collect raw data
- 3. Process the data
- 4. Explore the data
- 5. Perform In-Depth Analysis
- 6. Communicate results

- Giving people the tools, process data and insight they need to make sense of the world and to make decision in that world
- Start with those question and needs
- Machine learning is about getting machines to do part of that sense-making process
    - Limited: are there patterns and anomalies?
    - What's unusual in here?
    - Use it when there aren't humans to do it (or they're not good at it)
    - The dull and the overwhelmed
- 1. Frame the problem
    - What are we starting with?
        - Initial artifact, theme, narrative, lead
    - What's our "research question"?
        - What do and don't we care about here?
        - What's more and less important to us (if we have limited resources)?
    - What are we trying to produce and for whom?
        - Enough evidence that we can identify who to pass it to, and give them enough to either act or start their own investigation
        - Enough evidence and information to take action ourselves
- 2. Collect raw data
    - Finding the direct data and data proxies that tell you what's going on
    - Identify all available datasets
    - Existing collections: check the list in the BigBook
    - NB their collection isn't your collection: be aware of biases, data gaps etc
    - Social media feeds: searches, APIs, and spreadsheets
    - Extract data into usable format
        - A spreadsheet entry isn't a MISP object…

- 3. Process the data
    - Input data: alerts and canaries
        - Typical alerts:
            - New narrative
            - local or world event
            - Anomalous or significant-sized online activity
            - Command signals from known disinformation groups (e.g. qanon)
        - Typical starting artefacts:
            - Image
            - Message, e.g. tweet, facebook post, SMS
            - URL
        - “Canaries” = known producers or early adopters of many disinformation campaigns.
            - E.g. known conspiracy / extremist / target etc groups
        -
- 4. Explore the data
    - Look at what you’ve got
    - Use Gephi on twitter relational outputs
    - Find the patterns visually before you start modeling
- 5. Perform In-Depth Analysis
- 6. Communicate results
    - We can also take actions like takedowns
- Most time spent collecting and cleaning up data, shovel work
- Data science is detective work