2020-04 CTI disinfo deployment log

Sticky

These are running notes on the CTI disinfo deployment. 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
    - Hi newbies!
    - Status Update and planning
    - 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: MISP, DKAN, Googledrive, Python, github, (Hive, bots)

Log

2020-04-09

Looking at the channels we're in

- 5-osint-misp: folks managing the MISP we're feeding to.
    - [Name Redacted] is in here, team is adding the DFRlab taxonomy for us.
    - "BTW, if anyone wants access to the covid MISP instance - just click on the registration link at https://covid-19.iglocska.eu"
- Cti-bot-development: folks responsible for the bots we're going to need to push data to us.
    - Developers are in here looking for things to do. We have things to do, if only we know how to ask for them.
    - [Name Redacted] flagged that we're putting in a request soon "about how to utilize the phishing feed for the disinformation channel"
    - @[Name Redacted] offered to log the request if we write it up- will be free over the weekend
    - @[Name Redacted] has been working on MISP integration of the #2-phishing-attachments
    - Jarvis runs on Azure using Azure's bot service and framework
        - The way that Slack Development works is kinda interesting.
        - It has a notion of an 'App' which you can sort of think of as an authorization container of sorts, it has the various hooks and is the construct by which Slack API Permissions are granted to.
        - This 'App' logically lives inside of Slack and has OAuth Tokens and scopes. These scopes are what allows it to interact with channels/users etc.
        - When you perform a slash command, the "App" takes that input and just passes it blindly to whatever WebHook that has been associated with a given slash command.
        - Beyond simple slash commands, there is the business of the OAuth piece and thats where Jarvis's AzureBot Service backend comes into play... Like a regular old IRC bot, various chat interactions in channel or directed to Jarvis are sent to a service backend hosted in azure, and when those various keywords or triggers are met, they perform specific functions/processing actions. So while the slash commands can all vary and point to numerous different webhook endpoints/uris, The main brains

    - in Jarvis is centralized and capable of a far more extensible interactivity and processing.
    - [Name Redacted]: could utilize the analyzers [Cortex-Analyzers/analyzers at master · TheHive-Project/Cortex-Analyzers]() which are written in Python and available for most enrichment providers.
    - Web risk? https://cloud.google.com/web-risk
    - https://docs.microsoft.com/en-us/azure/bot-service/bot-service-overview-introduction?view=azure-bot-service-4.0
-

2020-04-11

[Name Redacted]: wrote draft readme for team. Working the “vaxxter.com” note through it to iron out wrinkles, set process etc.
Covid5g incident run-through:

- Added spreadsheet for incidents. Still trying to work out a process that’s lightweight enough not to get in our way, but also has enough structure so we don’t descend into chaos when we get hit with 30 things a day.
- Started with vaxxter.com, realised was tracking covid5g. Changed title on everything. Should add note somewhere that we can start something like thing, and spawn off other investigations (e.g. vaxxter) when they get big enough for their own.
- Also need to add pointers to “things we can do” - we don’t want to just be admiring the problem here.

2020-04-12

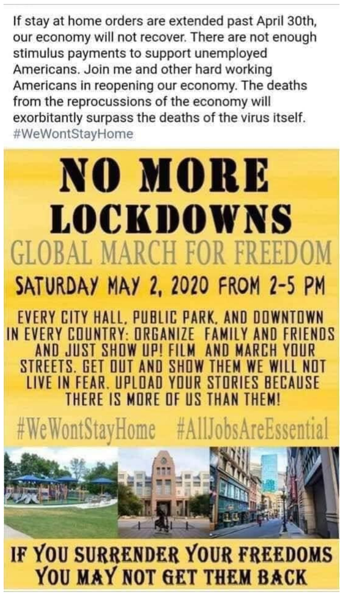
Still sorting out processes and tech in the background. Am mid-episode (bug has hit me hard) so team is handling this whilst I go back to do some more data science / stress testing the systems.

Covid5g - pulled tweets for related hashtags.

Working through data storage: notes gone into CTI League Disinfo Dataflows

- Adding feeds from messenger DMs to list.

And this appeared:



If stay at home orders are extended past April 30th, our economy will not recover. There are not enough stimulus payments to support unemployed Americans. Join me and other hard working Americans in reopening our economy. The deaths from the reprocussions of the economy will exorbitantly surpass the deaths of the virus itself. #WeWontStayHome

NO MORE LOCKDOWNS

GLOBAL MARCH FOR FREEDOM

SATURDAY MAY 2, 2020 FROM 2-5 PM

EVERY CITY HALL, PUBLIC PARK, AND DOWNTOWN IN EVERY COUNTRY: ORGANIZE FAMILY AND FRIENDS AND JUST SHOW UP! FILM AND MARCH YOUR STREETS. GET OUT AND SHOW THEM WE WILL NOT LIVE IN FEAR. UPLOAD YOUR STORIES BECAUSE THERE IS MORE OF US THAN THEM!

#WeWontStayHome #AllJobsAreEssential

IF YOU SURRENDER YOUR FREEDOMS YOU MAY NOT GET THEM BACK

2020-04-14

Events:

- Moving from Googledrive to github team https://github.com/orgs/COVID-19-CTI-LEAGUE/teams/cti-disinformation - need to reset processes to go with this, but the issues list and wiki should come in useful for keeping track of artefacts, things we need to do etc
- Got this link from [Name Redacted] for downloading video from youtube: https://jdownloader.org/
- And this is slack to MISP bot; can modify to add artefacts (twitter etc) to MISP https://github.com/IRATEAU/sam-bot/blob/master/SAMbot.py
- And [Name Redacted] is creating a new slack channel for disinformation inputs!

2020-04-24

Going back to a daily log, so we can post what happened yesterday / what's coming up today at the start of each day.

Yesterday:

- Alerts:
  - spanish language disinfo under #covidfake
  - Ourgovernoristryingtokillusga - counterprotest to operationgridlock, with counterprotesters taking to their cars too(!)
  - Coronavirus phishing sms with text that looked worth checking online

- Analysis:
  - incident “governorkill”: Looked into ourgovernoristryingtokillusga - appears to be local protest
  - Shortinvestigation 2020-04-23_govus_email: Investigated coronavirus alert SMS - text and url. Is phishing; domains appears to be squished already.
- Process:
  - Added lists of data feeds to the BigBook of Disinformation Response https://docs.google.com/document/d/1eeXoFtQpqthhVSBm91wer0uhS346lt3SEhU04ojQaPs/edit#
  - Added suggested reading list to the BigBook (needs more)
  - Started new notes category: shortinvestigation - for things that need checking but aren’t big enough to be incidents
  - Rewrote artefacts sheet for incident operationgridlock to match feed needed for MISP https://docs.google.com/spreadsheets/d/1pmEqn1rgGjzSIynpVupPySdnBOdqUbOaWJpH6yKFBrI/edit#gid=1251310592
- Tech:
  - [Name Redacted] demo of TheHive (was recorded)
  - We’re going to migrate to TheHive for handling incident logs and artefacts - it’s already integrated into Cortex (which we have here now) and MISP (which we already use)
  - Next steps on Hive:
    - Deploy Hive - [Name Redacted]
    - Training on Hive analysers
    - Make list of Hive analysers we need
    - Create custom data types
    - Create tasks (steps for each case; e.g. write instructions for how to do things)

2020-04-25

Yesterday (2020-04-24) in disinformation team:

- Alerts:
  - Alerts from team on fakenurses, mmscures, takeover of #inittogether - Qanon Japan community?
  - Alert from team on new narrative: “dont take the covid-19 test. Its intentionally 80% false positive”
  - ACTION: Alert from [Name Redacted] on America/China split narratives. Will start a new ongoing campaign and incident to cover this.
- Analysis

    - Incident inittogether - Qanon takeover of hashtag #inittogether on twitter. Appears to be Qanon check-in/coordination, not medically related. Did checks on data, closed down.
    - Incident mmscures - live
- Process
    - Asked to answer 4 questions - working on this (includes data governance, which we do need to think about).
        - Detailed description of what platform is being used to gain information related to disinformation campaigns,
        - How that information is being gathered,
        - Type of information being gathered, e.g. PII, the intent behind gathering the information, and
        - How the information will be used and stored.
    - Added section to the BigBook on incidents: starting, running and acting on them
- Tech
    - [Name Redacted] twitter scanner results

Today:

- Alerts
    - Quiet
- Analysis
    - Continuing incident mmscures
    - Planning to look at US/China disinfo
- Process
    - Adding to BigBook
- Tech
    - Bots coming out?

2020-04-29

Process: Starting meetup/ training sessions for team, with MISP training

- Set overall meeting format as 1-hour trainings with
    - 5 min on welcome to newbies, where we are etc
    - 5 min on framing
    - 30 min on training
    - 20 min on discussion of where we want to go next / things we're stuck on etc

2020-04-29 Team Meeting

Status Update:

- Alerts: expecting US reopen activity around May 1st. extendthelockdown?

- Incident analysis: continuing MMScures; jobscam analysis; waiting on process and tech before pushing larger incidents
- Process: continuing the BigBook, started meetup/training sessions
- Tech: finishing MISP integrations/ data push from incident spreadsheets
- Shout outs: BigBook editing! Jobscam analysis. MISP bot

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, May 1st Reopen, adding China disinformation
- Process: handling narratives, adding to the BigBook
- Tech: more MISP bots
- Also: inviting people to participate; diversity, equity & inclusion
- HIVE = incident project management…

2020-04-30

Alerts:

- More coming in on May 1st (tomorrow) - expecting mass protests across the USA. Not sure how much is homegrown / how much target of opportunity from outside.

Analysis:

-

Process: Got the master narratives list up

- Tagged and cleaned CMU list: 120+ narratives, many very similar
- Created master Covid19 list of about 23 narratives from that
- Master list needs looking over, discussion, adding new narratives (e.g. lockdown ones)

Tech:

- MISP: used https://github.com/COVID-19-CTI-LEAGUE/PRIVATE_BOT_DEVELOPMENT_LOOKUPS/blob/master/misp-twitter/app/misp_objects.py to push tweets to incident using pymisp; adapting that to push incident spreadsheet contents up