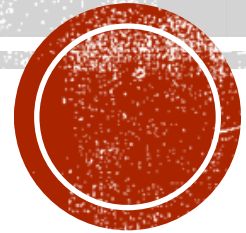
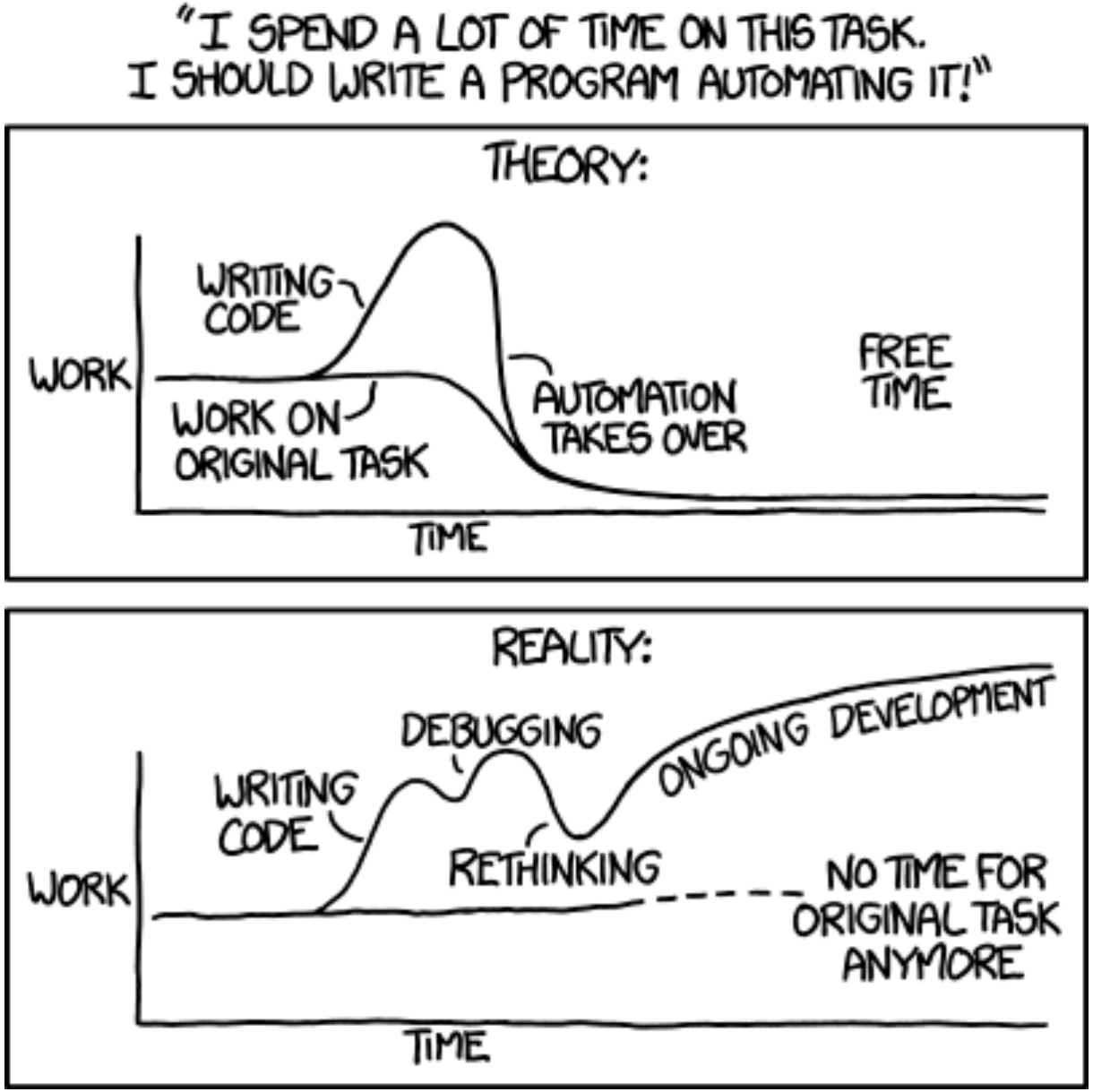
LISTING THE 1337



Adventures in Curating HackerTwitter's Institutional Knowledge

hex waxwing @hexwaxwing

daniel gallagher @DanielGallagher



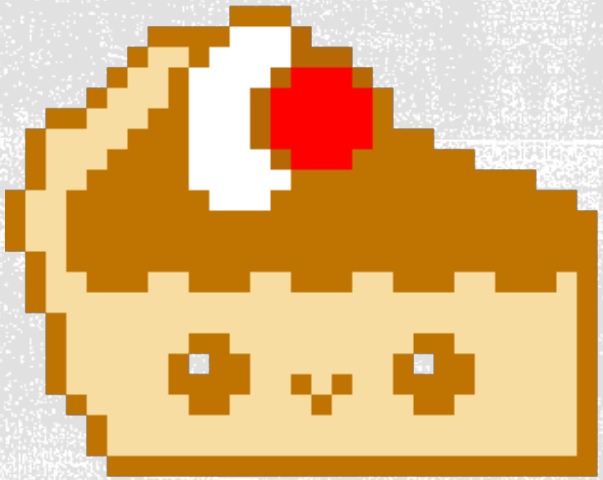
WHO TF ARE YOU?

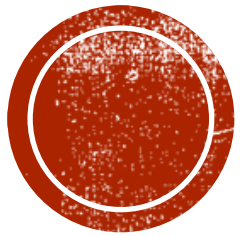
@DanielGallagher

- Medsec
- Splunk fanboy
- Ransomware Hunting team

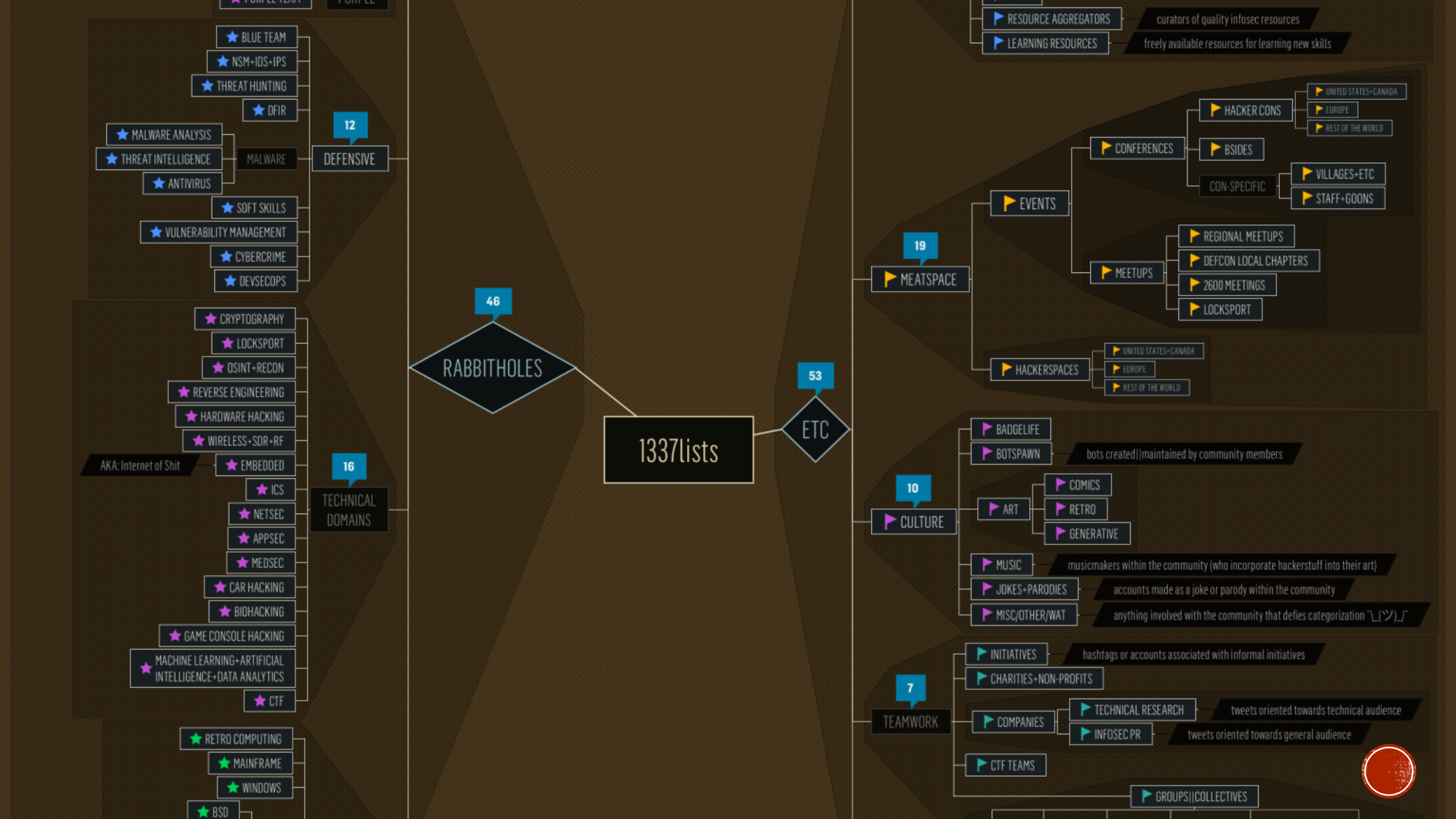
@hexwaxwing

- lateral transplant from neuroscience, anthropology, the arts, and other interdisciplinary hooha
- intensely thaasophobic
- infosec newbie





WHAT IS 1337LIST?


1337lists
RABBITHOLES
46
ETC
53
DEFENSIVE
12
BLUE TEAM
NSM+IDS+IPS
THREAT HUNTING
DFIR
MALWARE
MALWARE ANALYSIS
THREAT INTELLIGENCE
ANTIVIRUS
SOFT SKILLS
VULNERABILITY MANAGEMENT
CYBERCRIME
DEVSECOPS
TECHNICAL DOMAINS
16
CRYPTOGRAPHY
LOCKSPORT
OSINT+RECON
REVERSE ENGINEERING
HARDWARE HACKING
WIRELESS+SDR+RF
EMBEDDED
AKA: Internet of Shit
ICS
NETSEC
APPSEC
MEDSEC
CAR HACKING
BIOHACKING
GAME CONSOLE HACKING
MACHINE LEARNING+ARTIFICIAL INTELLIGENCE+DATA ANALYTICS
CTF
RETRO COMPUTING
MAINFRAME
WINDOWS
BSD
RESOURCE AGGREGATORS
curators of quality infosec resources
LEARNING RESOURCES
freely available resources for learning new skills
MEATSPACE
19
EVENTS
CONFERENCES
HACKER CONS
UNITED STATES+CANADA
EUROPE
REST OF THE WORLD
BSIDES
CON-SPECIFIC
VILLAGES+ETC
STAFF+GOONS
MEETUPS
REGIONAL MEETUPS
DEFCON LOCAL CHAPTERS
2600 MEETINGS
LOCKSPORT
HACKERSPACES
UNITED STATES+CANADA
EUROPE
REST OF THE WORLD
CULTURE
10
BADGELIFE
BOTSPAWN
bots created||maintained by community members
ART
COMICS
RETRO
GENERATIVE
MUSIC
musicmakers within the community (who incorporate hackerstuff into their art)
JOKES+PARODIES
accounts made as a joke or parody within the community
MISC/OTHER/WAT
anything involved with the community that defies categorization ¯_(ツ)_/¯
TEAMWORK
7
INITIATIVES
hashtags or accounts associated with informal initiatives
CHARITIES+NON-PROFITS
COMPANIES
TECHNICAL RESEARCH
tweets oriented towards technical audience
INFOSEC PR
tweets oriented towards general audience
CTF TEAMS
GROUPS||COLLECTIVES

IMPORTANT DISCLAIMER:

The current lists are…

- INCOMPLETE and require COMMUNITY VETTING & FEEDBACK before we can *confidently* say that it is an accurate representation of the community.
- Currently completely skewed towards accounts that are largely posting on-topic, relevant tweets.

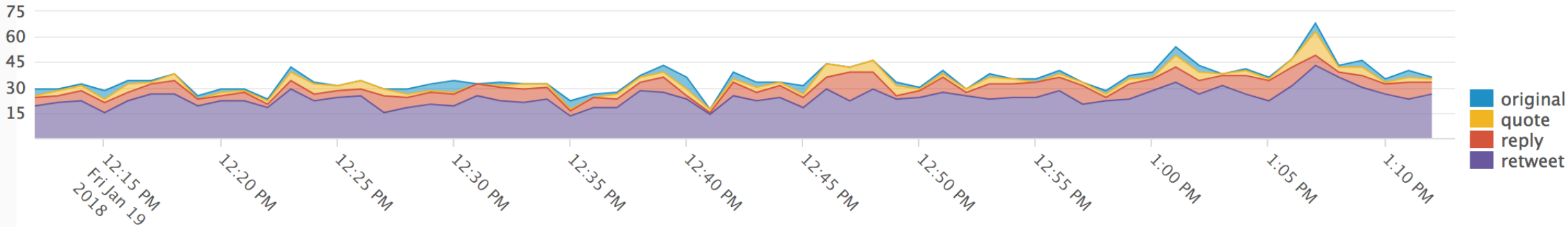
ULTIMATE OBJECTIVE:

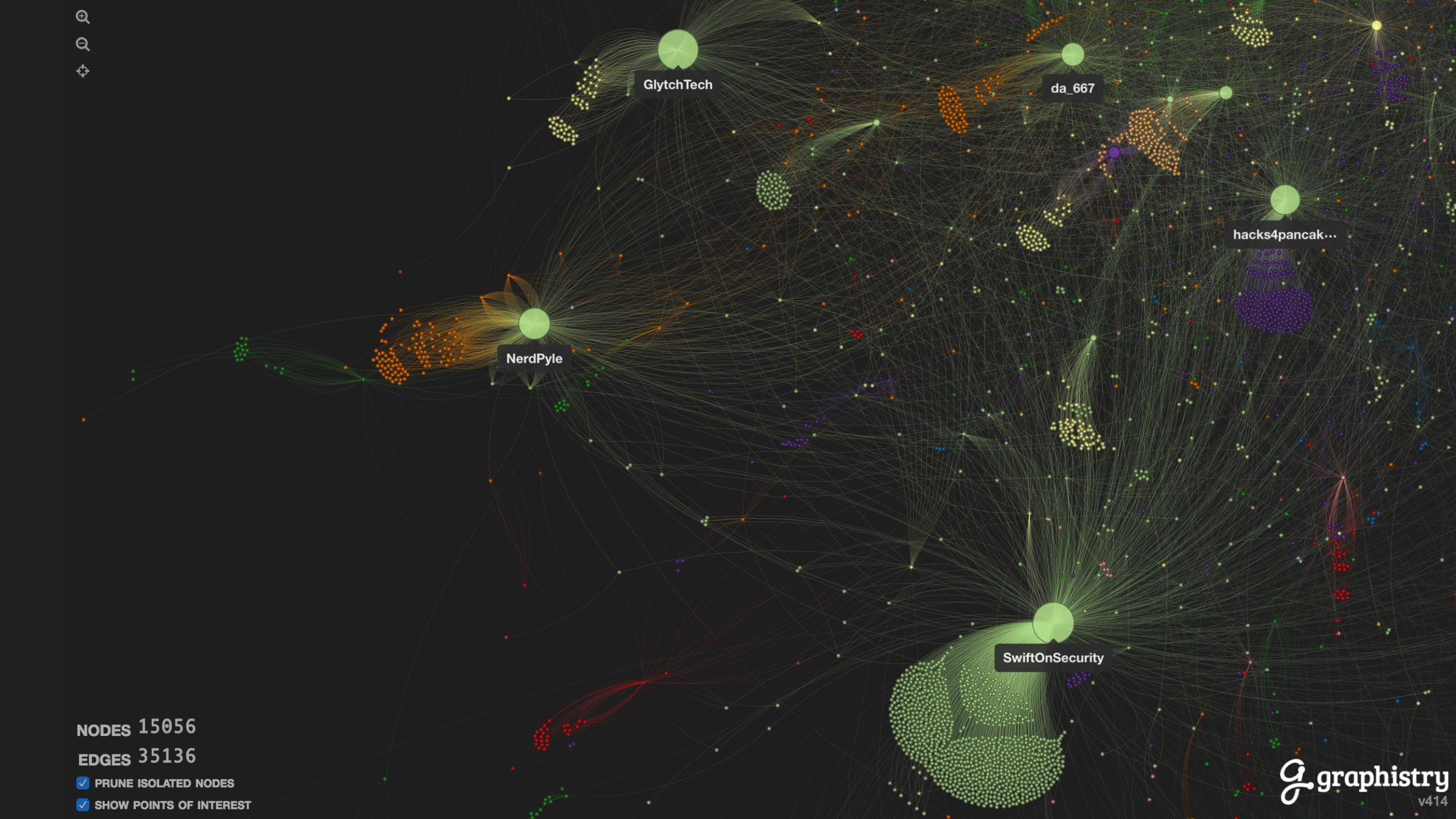
- include *everybody* within the community! :D
- …but have all content be reliably autocategorized, so feeds can be fine-tuned according to use-case

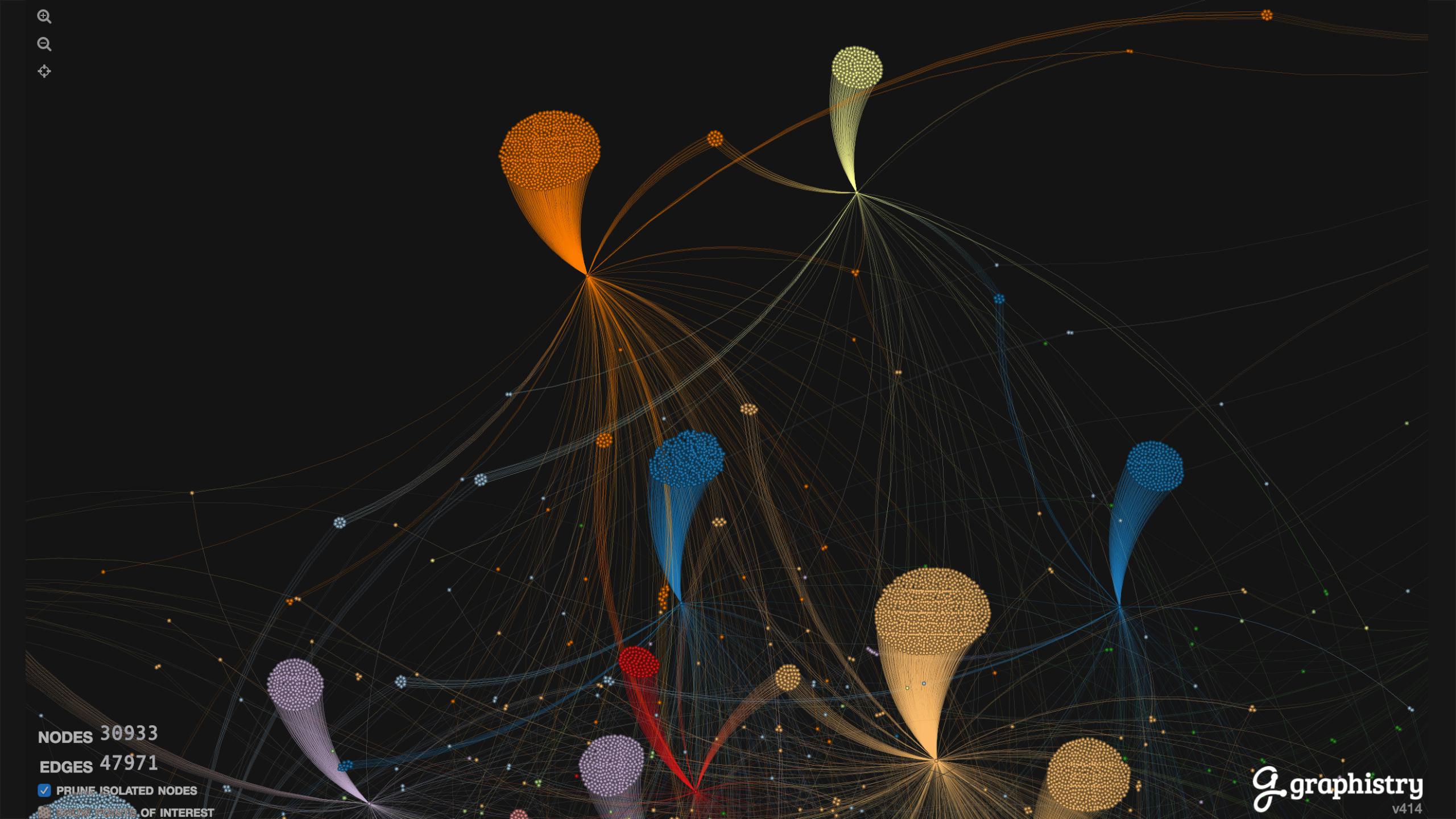
34
Tweet Count

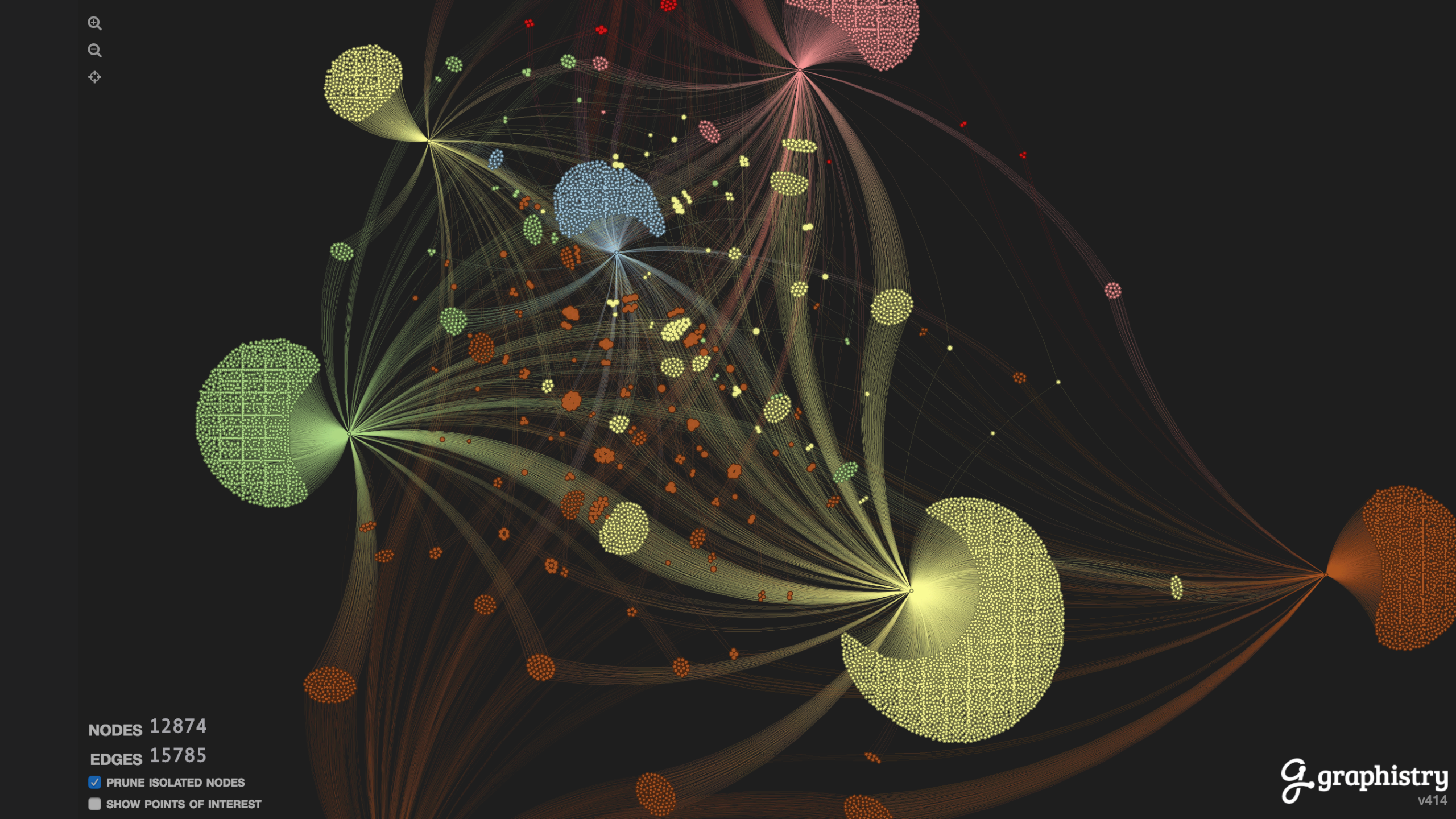
30
Total Users

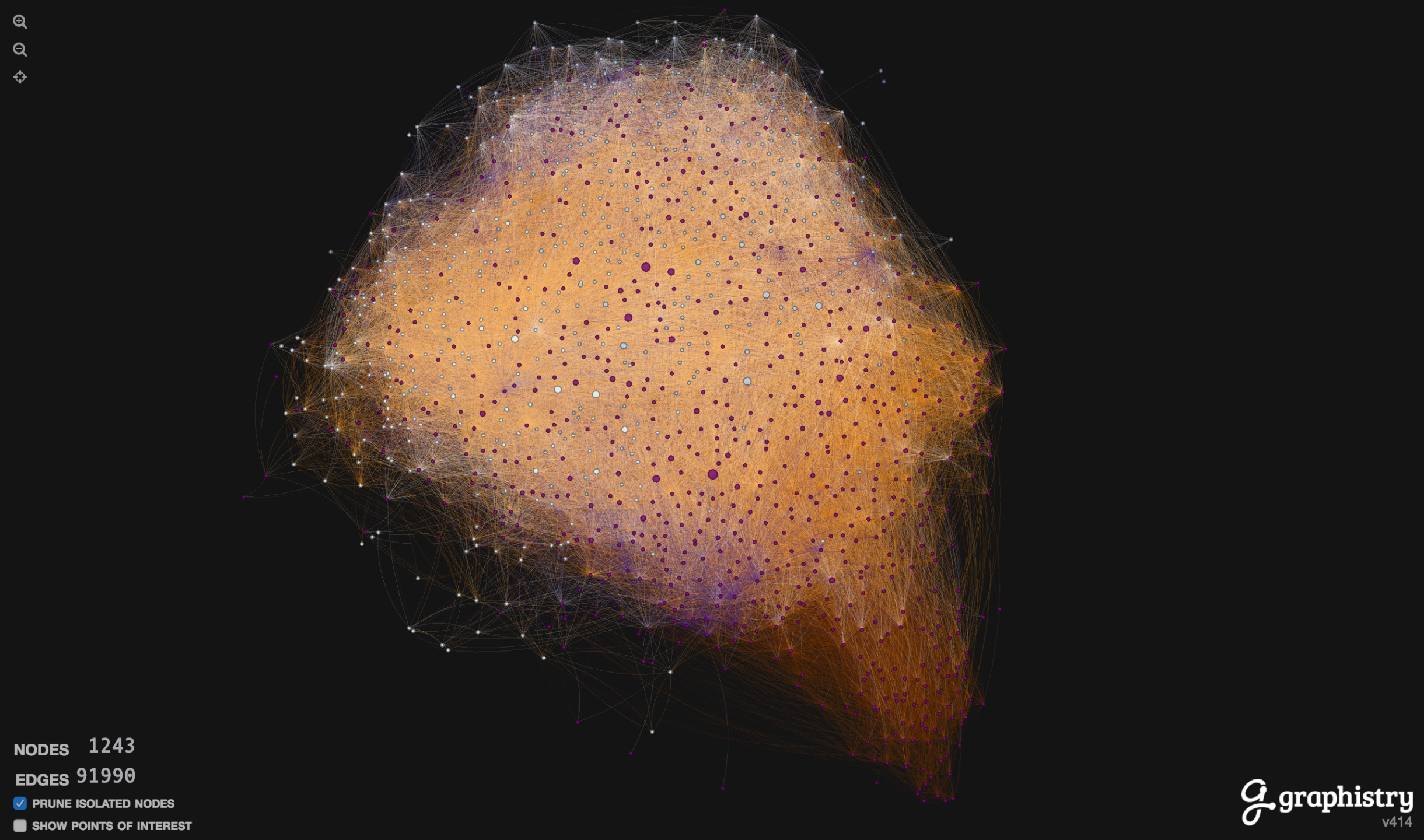
5
Unique List Members

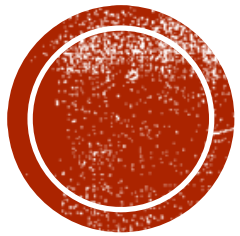



GlytchTech
da_667
hacks4pancak…
NerdPyle
SwiftOnSecurity
NODES 15056
EDGES 35136
PRUNE ISOLATED NODES
SHOW POINTS OF INTEREST
graphistry
v414


NODES 30933
EDGES 47971
PRUNE ISOLATED NODES
SHOW POINTS OF INTEREST
graphistry
v414


NODES 12874
EDGES 15785
PRUNE ISOLATED NODES
SHOW POINTS OF INTEREST
graphistry
v414


NODES 1243
EDGES 91990
PRUNE ISOLATED NODES
SHOW POINTS OF INTEREST
graphistry
v414



COOL PICS, BROSEPH

BUT WHAT CAN YOU ACTUALLY DO WITH IT?

BUT WHAT PROBLEMS CAN 1337LIST SOLVE?

(↓ open problems 1337list can be leveraged to resolve... ↓)

SIGNAL-TO-NOISE RATIO • VISIBILITY OF DOMAINS • ICYMI DIGESTS • EMERGENCY ALERTS • COMMUNITY RESOURCE CURATION


PARTY

SIGNAL-TO-NOISE RATIO

OPEN PROBLEM

- Firehose of information is a potential goldmine for institutional knowledge, but…
- …it's completely untapped.

PROPOSED SOLUTION

- Define community
- Classify domains||categories within the community
- Identify patterns of activity or content that can be automatically detected
- Automate the stupid stuff so we can focus on the fun stuff

(↓ open problems 1337list can be leveraged to resolve… ↓)

SIGNAL-TO-NOISE RATIO • VISIBILITY OF DOMAINS • ICYMI DIGESTS • EMERGENCY ALERTS • COMMUNITY RESOURCE CURATION

IMPROVING VISIBILITY OF TECHNICAL DOMAINS

OPEN PROBLEM

- Education in infosec is a dumpsterfire
- Huge disconnect between book-learning and practical skills
- Hard to tell from outside actual what professions in infosec do
- Immersive learning environments are a critical component to learning

PROPOSED SOLUTION

- **This.**
- Classify different infosec domains to help newbies to get oriented
- Make it ~~easy~~ easier to stay up to speed
- Increase visibility between different niches

(↓ open problems 1337list can be leveraged to resolve... ↓)

SIGNAL-TO-NOISE RATIO • VISIBILITY OF DOMAINS • ICYMI DIGESTS • EMERGENCY ALERTS • COMMUNITY RESOURCE CURATION

ICYMI DIGESTS

OPEN PROBLEM

- Interesting things happen on Twitter all day…
- …but unless you're halving your attention between your actual work and Twitter, you end up missing a lot.

PROPOSED SOLUTION

- Generate daily|weekly digests of interesting threads & resources
- Allow users to generate a proper digest
- Configure ICYMI digests to target their specific areas of interest

(↓ open problems 1337list can be leveraged to resolve… ↓)

EMERGENCY ALERTS

OPEN PROBLEM

- When you're ignoring Twitter because you're concentrating on something else...
- ...sometimes Big Important Things happen!

PROPOSED SOLUTION

- Automated alerts for stereotypical patterns of activity
- EXAMPLE: major malware outbreaks
  - Distinctive interactions between members of the MALWARE_ANALYSIS, THREAT_INTELLIGENCE, and DFIR

(↓ open problems 1337list can be leveraged to resolve... ↓)

COMMUNITY RESOURCE CURATION

OPEN PROBLEM

- No systematic method for collecting and curating technical resources

PROPOSED SOLUTION

- An automatically-generated, dynamically-updated list of technical resources

(↓ open problems 1337list can be leveraged to resolve... ↓)

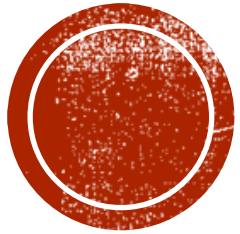
SIGNAL-TO-NOISE RATIO • VISIBILITY OF DOMAINS • ICYMI DIGESTS • EMERGENCY ALERTS • COMMUNITY RESOURCE CURATION

THIS PROBLEM ISN'T GOING AWAY

- The firehose of information isn't going away
- Who do WE want to be in charge of the algorithms that curate our content for us?
- Let's work on this problem in earnest before the platforms our communities thrive on force us to figure out the solution on short notice

(↓ open problems 1337list can be leveraged to resolve... ↓)

SIGNAL-TO-NOISE RATIO • VISIBILITY OF DOMAINS • ICYMI DIGESTS • EMERGENCY ALERTS • COMMUNITY RESOURCE CURATION



YEAH, SURE...OKAY.

BUT WHAT ARE WE *REALLY* GOING TO DO WITH THIS?

PLANNED IMPLEMENTATION OF PROPOSED LULZ BY END OF FISCAL YEAR

- 1337list Markov Bots
- 🎰PANDORA BOX MODE🎰: Instead of muting all the shitposting, muting all the signals.
- Live action pewpew map of the hackersphere!

PROJECT ROADMAP

- Complete building organizational infrastructure for keeping track of volunteers
- Integrate feedback from the vetting of the the initial 101 lists from folks with relevant experience
- Scrape all historical data from 1337list accounts, so we can examine patterns over a longer period of time and develop analytics based on a complete corpus of public interactions
- Then we can begin to build the technical resource repo.

WAYS TO CONTRIBUTE

Subject matter expert?

- Help vet the existing 1337lists
- Suggest additional accounts to include within the 1337lists
- Critique domain boundaries when I've gotten them wrong

Got skills?

- Assistance building the surrounding infrastructure and suggestions to make this possible
- Skills we're aware we need right now:
  - Splunk
  - BigQuery, maybe?
  - Neo4j
  - Frontend devs
  - Help building scrapers
  - **Foreseeable icebergs to avoid? LET US KNOW.**

Everybody else?

- Tune the "alpha" 1337lists feeds by indicating when off-topic tweets upset the signal-to-noise ratio within a particular 1337list's domain

GET INVOLVED!

- **GITHUB:** github.com/1337list
- **WIKI:** wiki.1337list.com
- **DISCORD CHAT:** discord.gg/qzh7Tad
- **VOLUNTEER SIGN-UP FORM:** volunteer.1337list.com