Analyzing 24 Years of CVD

Allen Householder

adh@cert.org

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM18-0268

Agenda

Process & data overview

Cases & messages over time

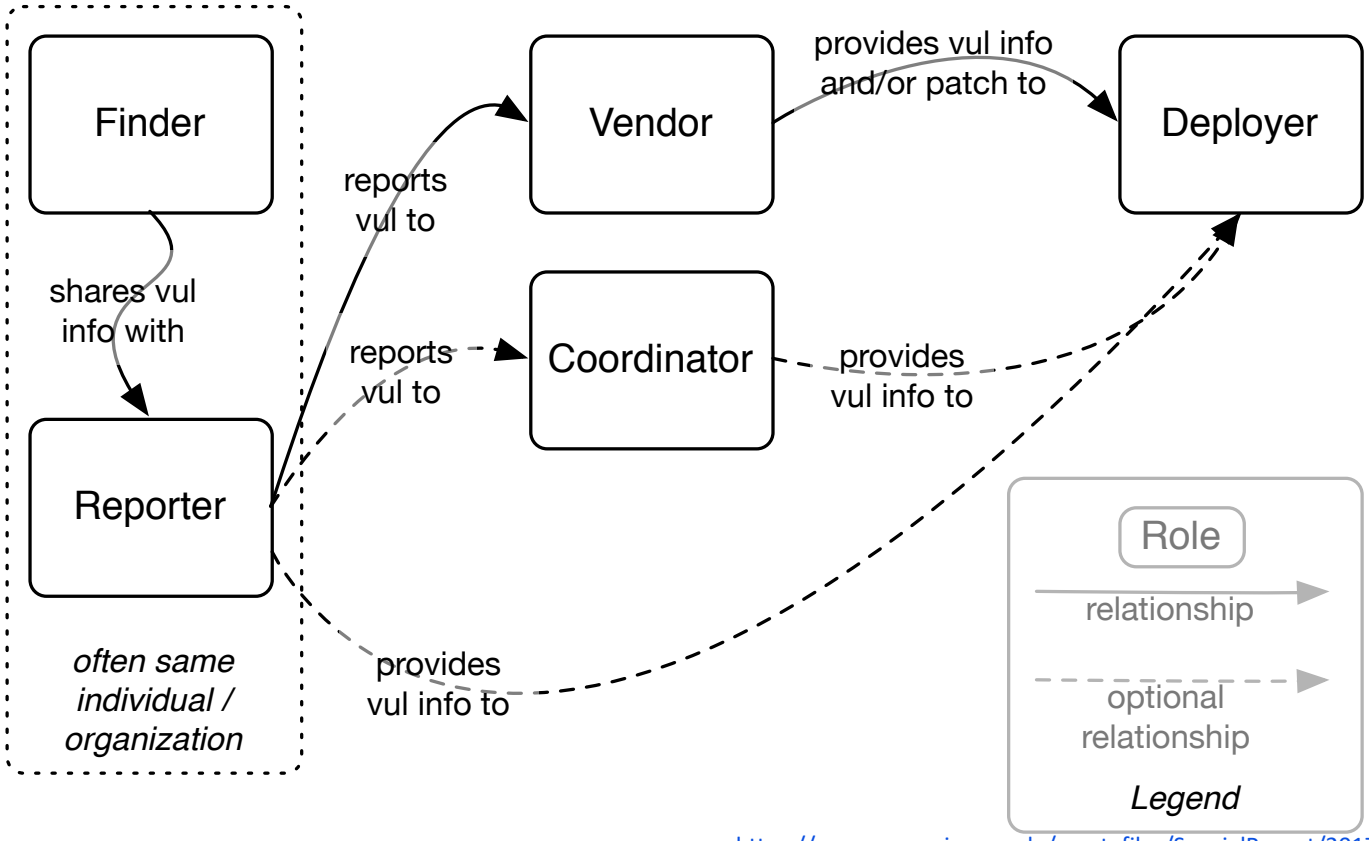
Case duration distribution

Case size distribution

When does the work happen?

Observations on Case Complexity

The CVD Process



https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf

The Data

This is work in progress, all results are preliminary.

CERT/CC has been coordinating vulnerability disclosures since 1988.

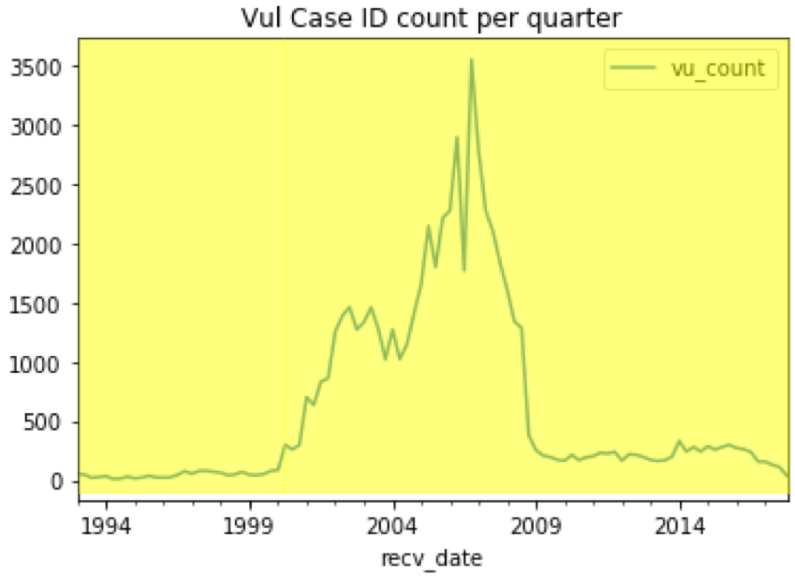
- Email-centered process, “hub and spoke” communication pattern
- Messages sent/received as proxy measure of coordination effort

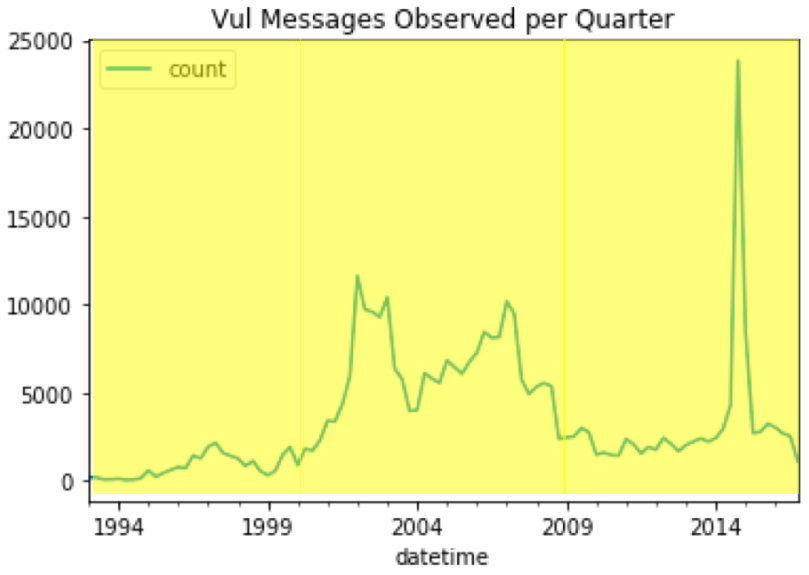
Database log of email sent/received by cert@cert.org about VU#nnnn and VR-nnn cases

- Spans 1993-2017 (24 years)
- 350k+ CVD-related email messages observed
- 46k+ CVD cases observed
- 2,300+ years of CVD embargo*

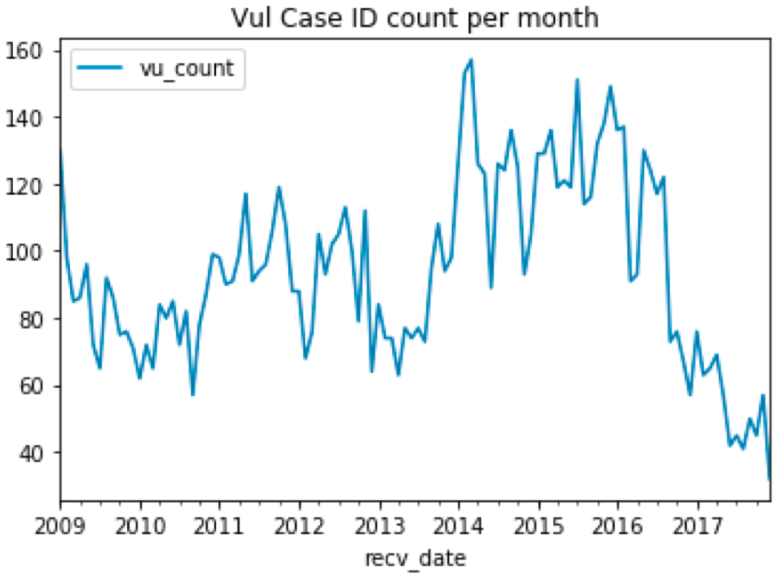
*sum across all domain-level participants

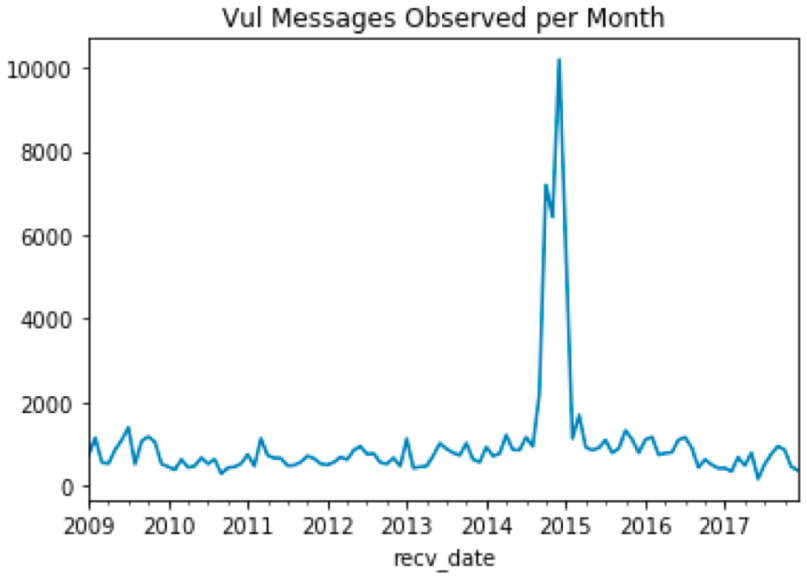
Cases, Messages per Quarter 1994-2017



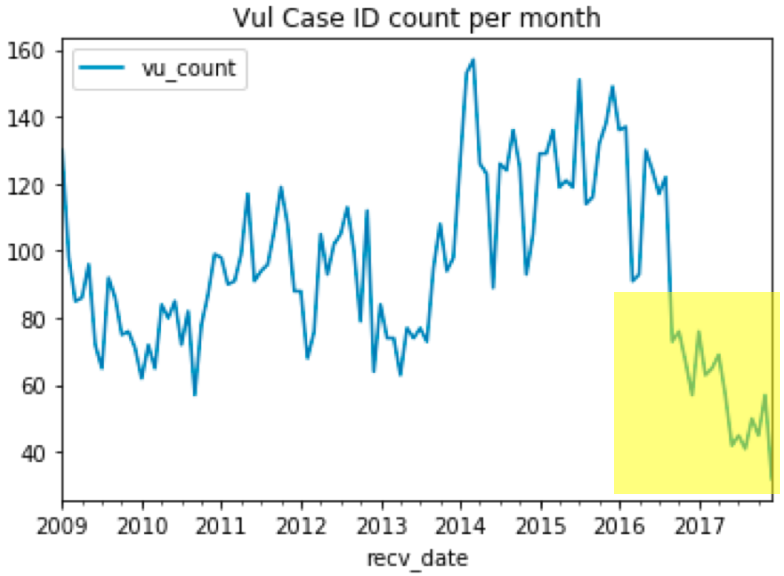


Cases, Messages per Month 2009-2017

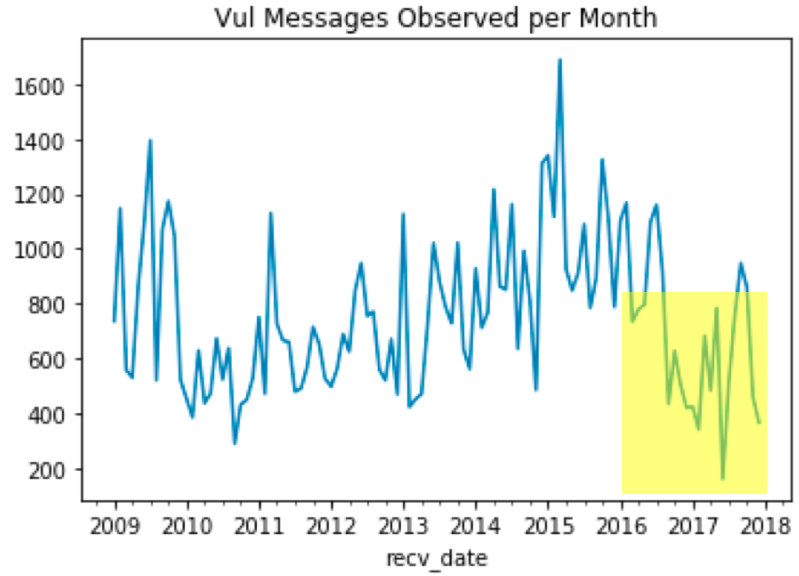




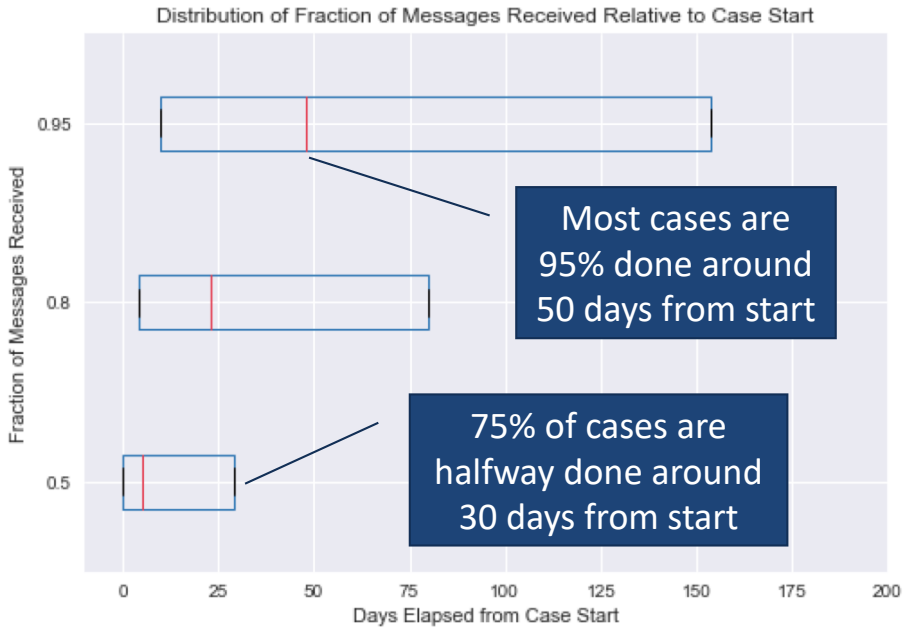
Cases, Messages per Month 2009-2017

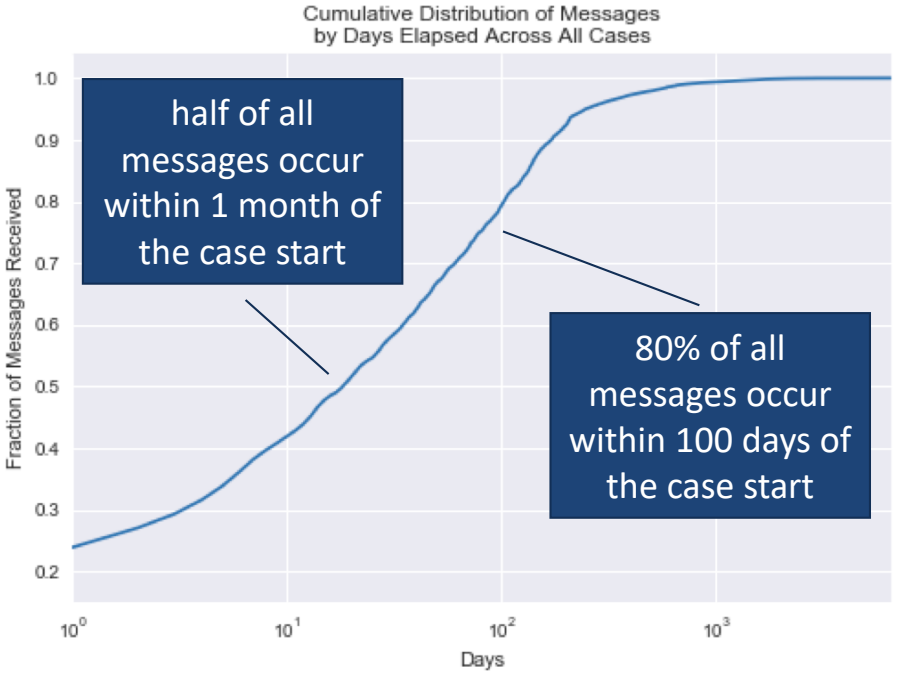


(Same chart, but remove VU#582497)



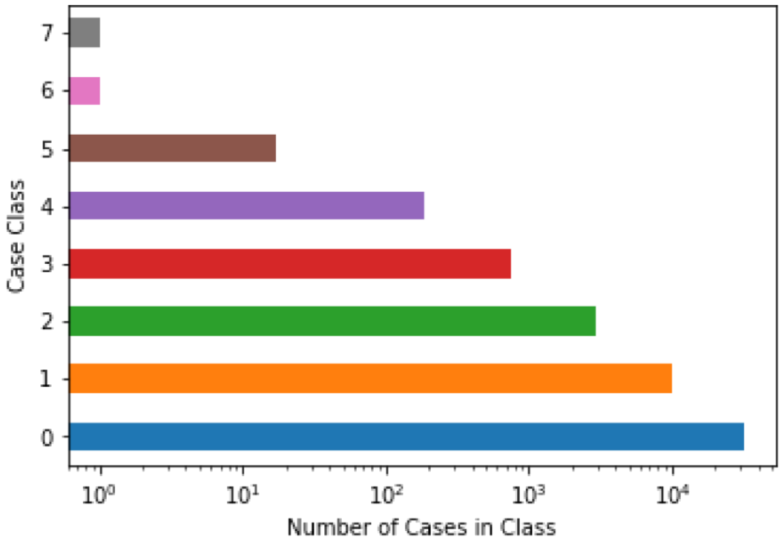
How long do cases last?





Case Sizes

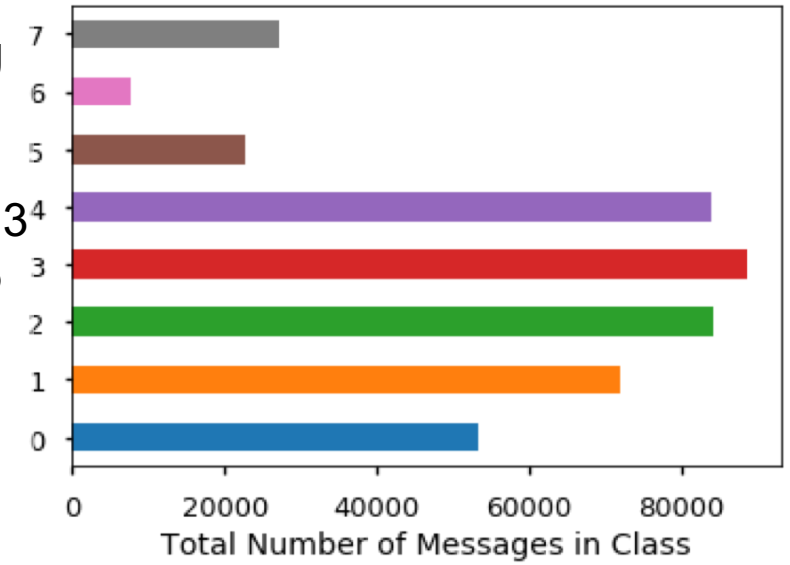
Case Counts by Class
(log count)



N_msg

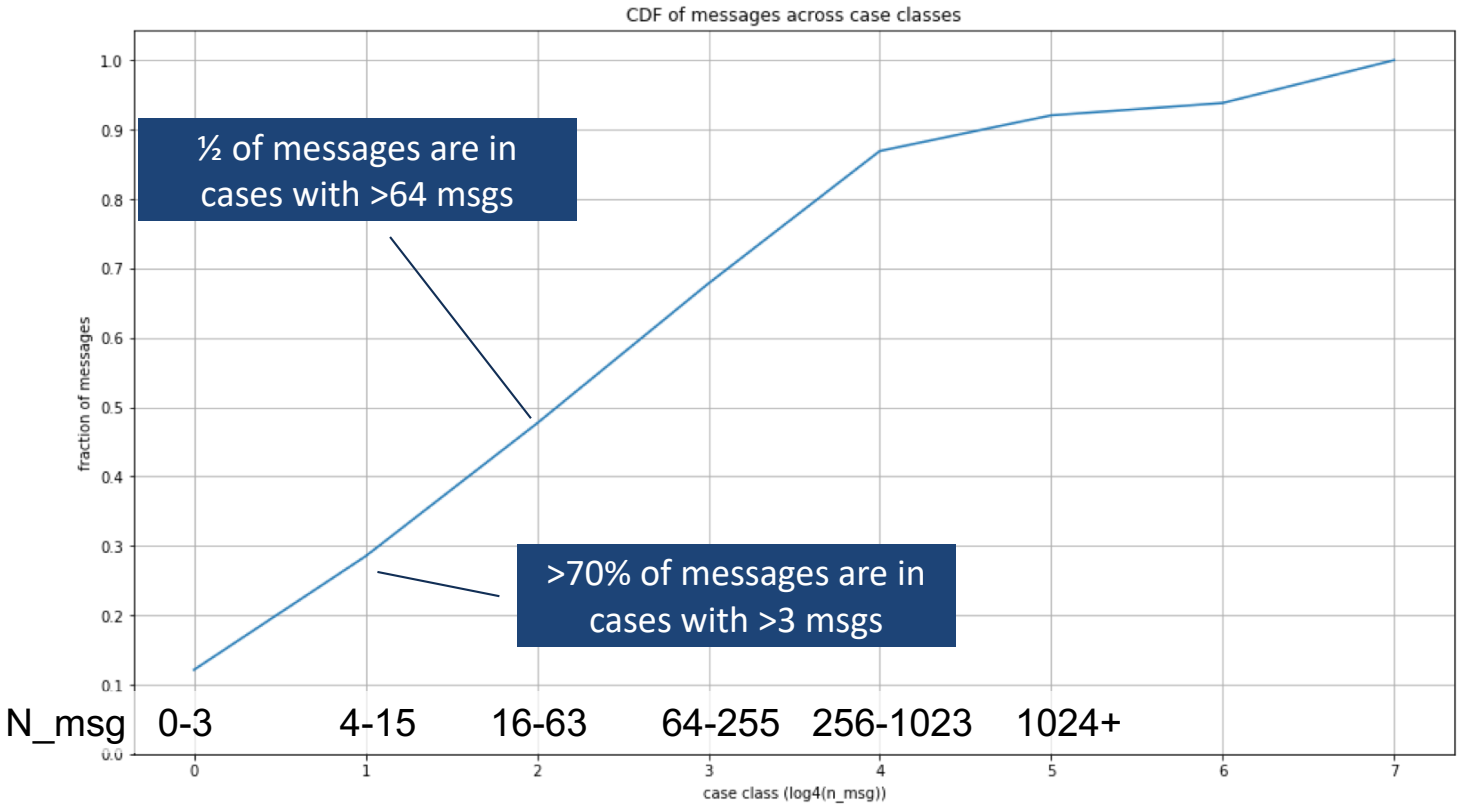
1024+
256-1023
64-255
16-63
4-15
0-3

Message Counts by Class

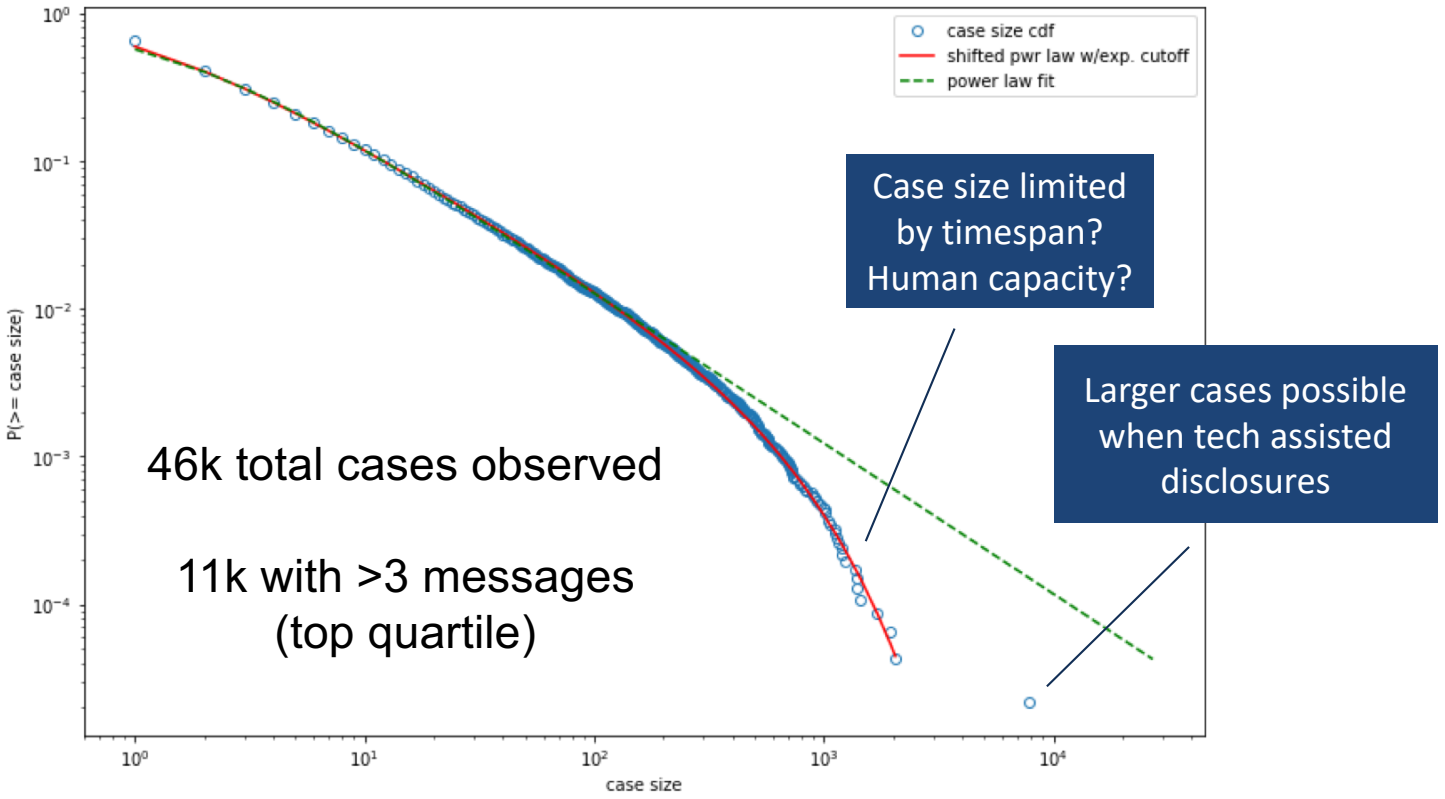


"Case class" = $\log_4$(n_messages)

Workload Distribution By Case Size

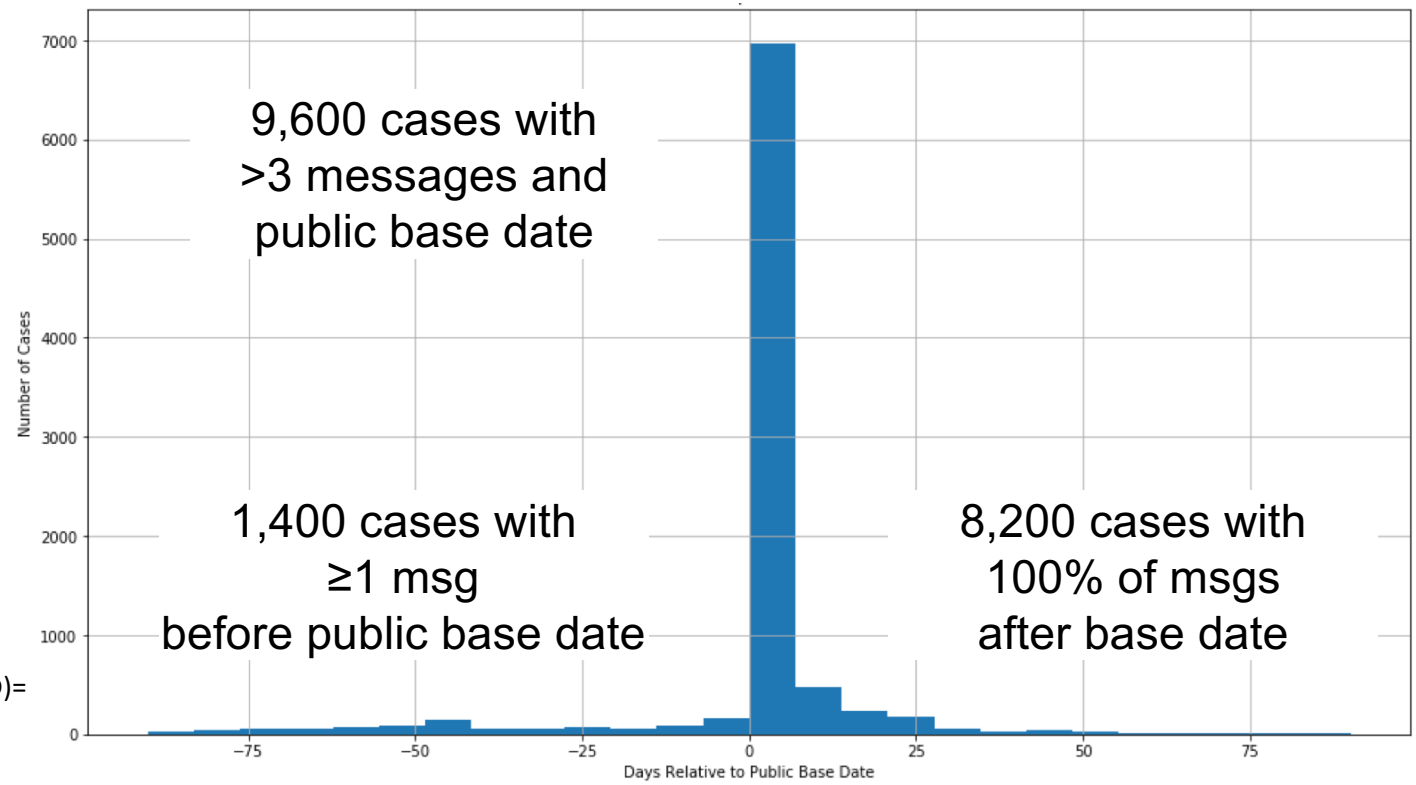


Case Size-Frequency



Case Start Relative to Date Public

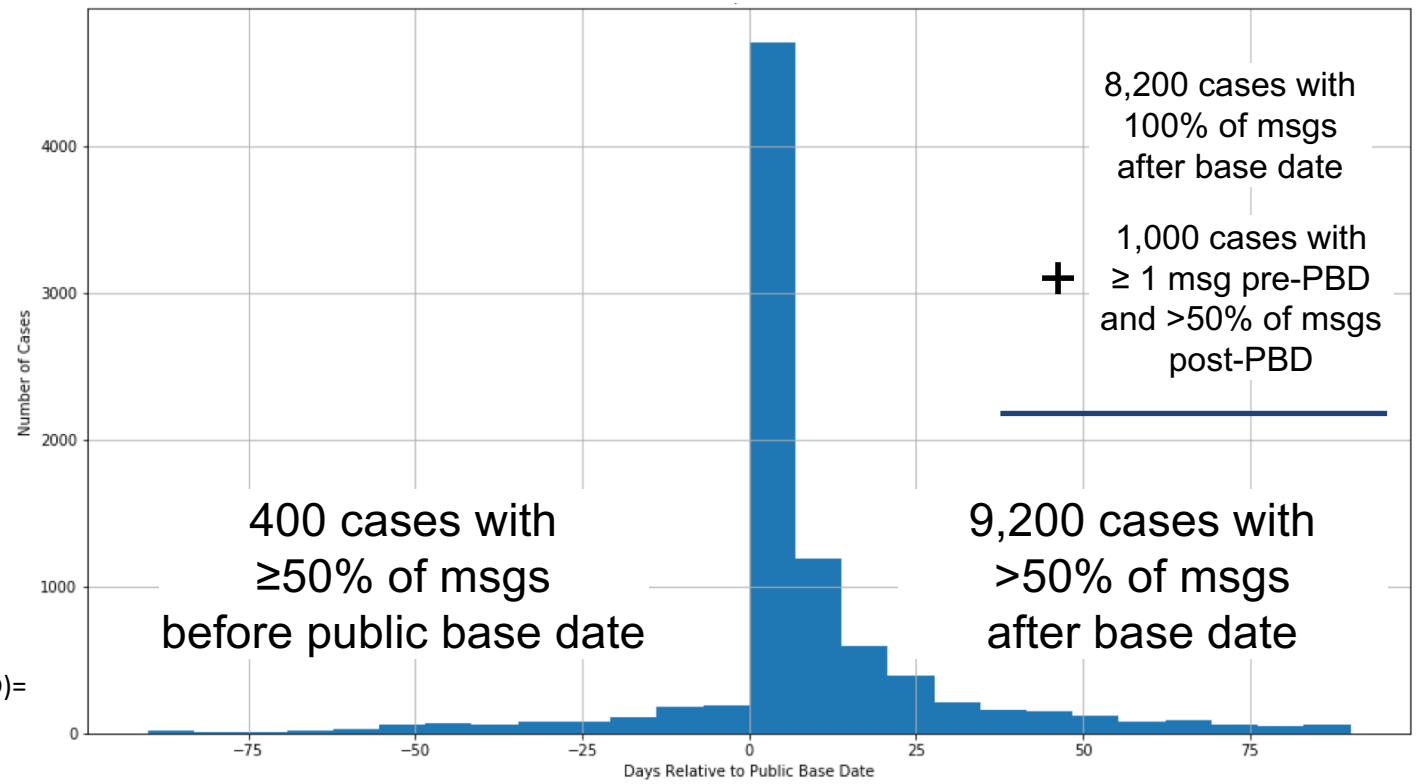
Relative date of first message observed



Public Base Date (PBD)= min(date_public, date_first_published)

Case Midpoint Relative to Date Public

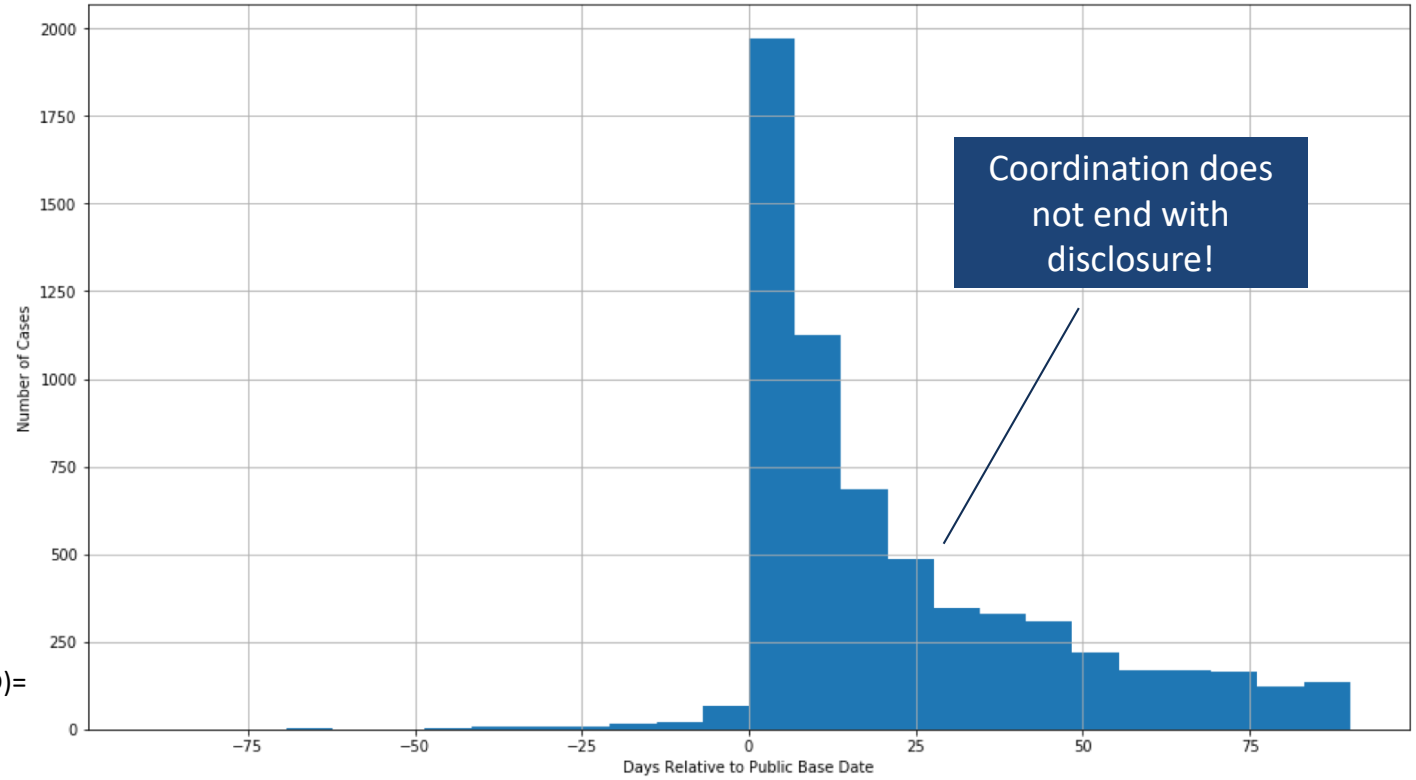
Relative date on which cases reached 50% of their total messages



Public Base Date (PBD)= min(date_public, date_first_published)

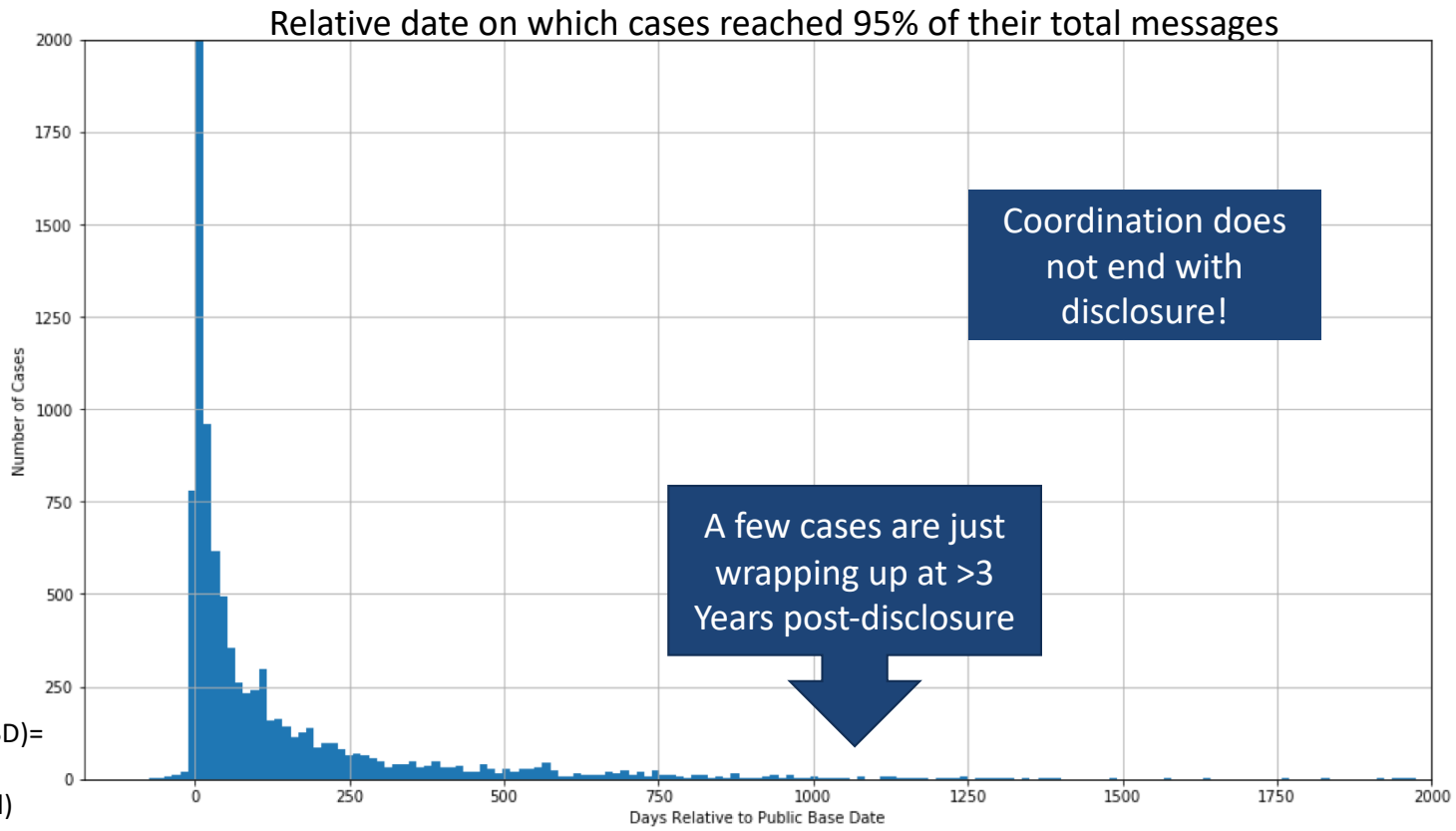
Case End (Effective) Relative to Date Public

Relative date on which cases reached 95% of their total messages



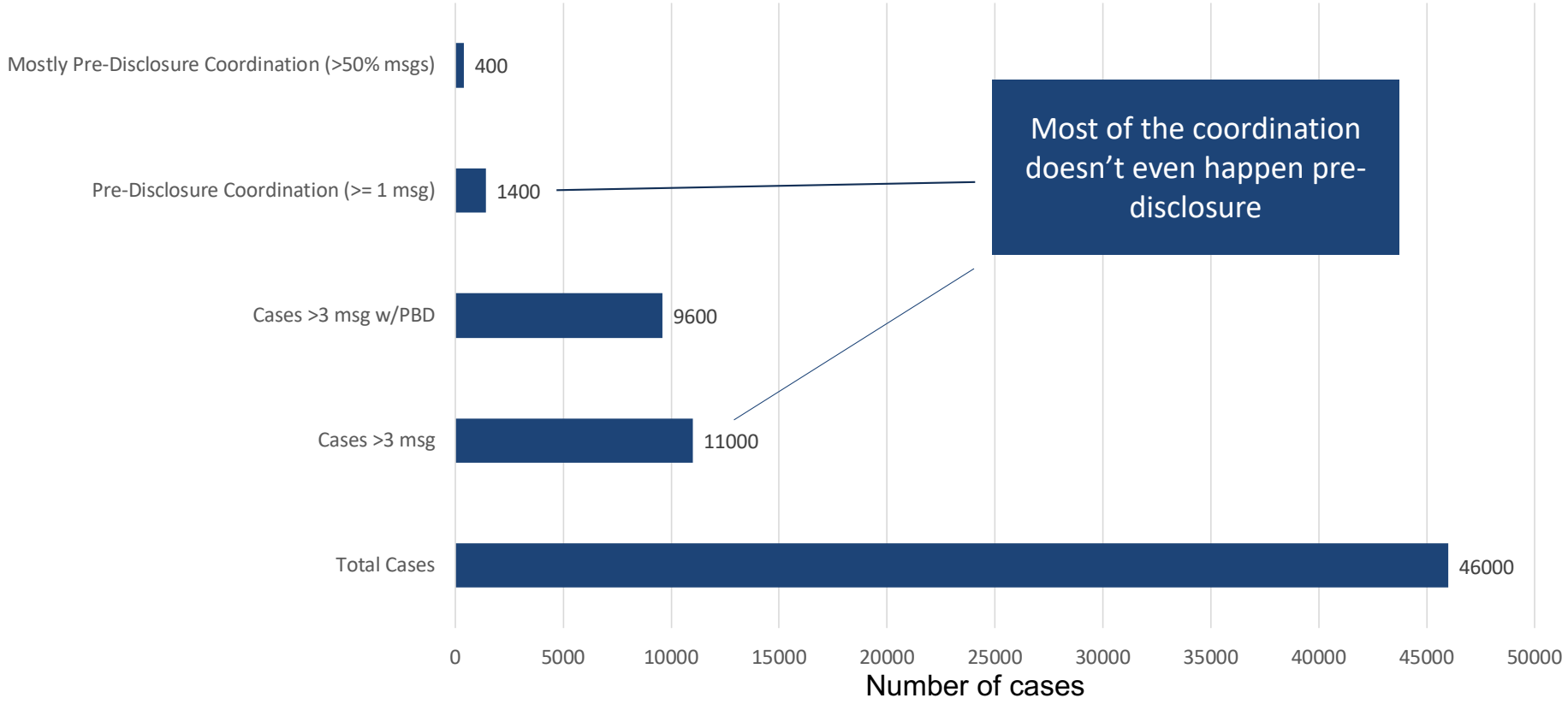
Public Base Date (PBD)= min(date_public, date_first_published)

Case End (Effective) Relative to Date Public

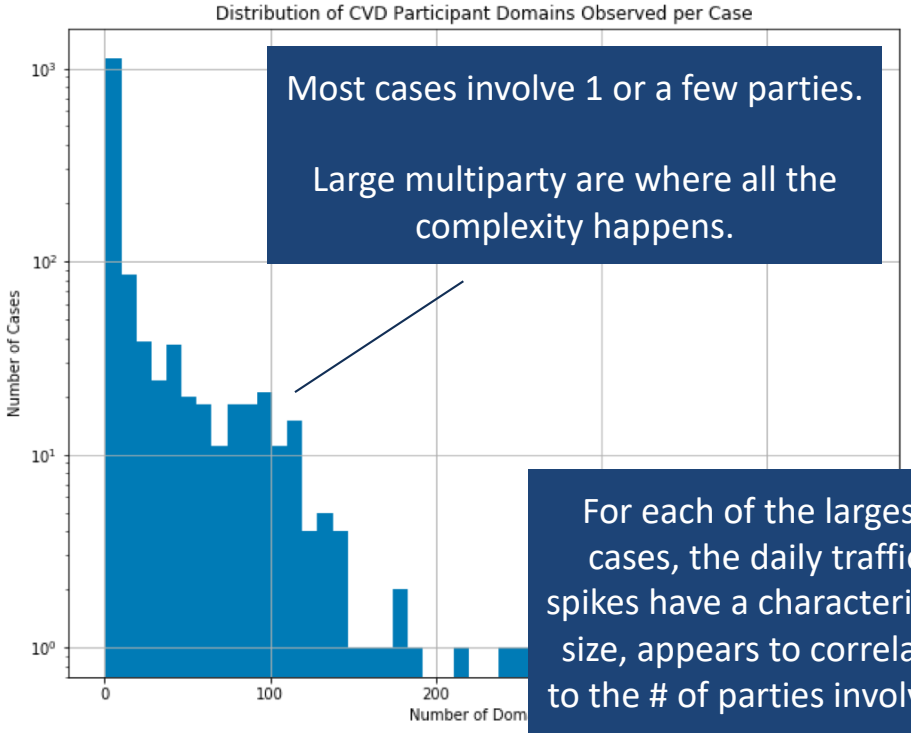


Public Base Date (PBD)= min(date_public, date_first_published)

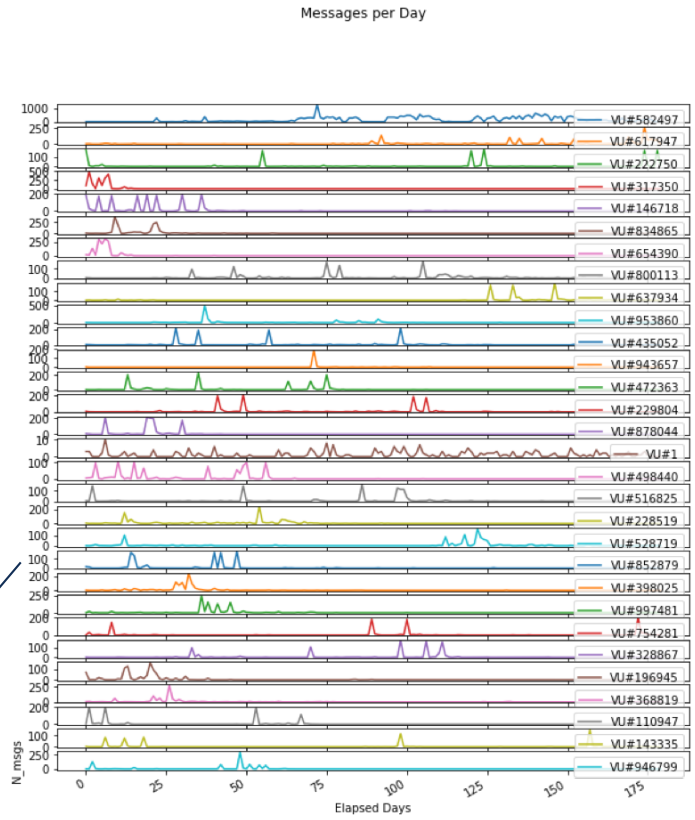
Case Breakdown



Underlying Mechanism for Case Size: Multiparty



For each of the largest cases, the daily traffic spikes have a characteristic size, appears to correlate to the # of parties involved



Limiting Factors for Case Size

Factor	Potential causes of limit
Timespan	• Vendor responsiveness to creating patches *(This is a good thing!)* • Attention span of orgs before other work takes precedent • Reporters sometimes under inflexible timelines
Identifying affected vendors	• What products contains libfoo? • What vendors are affected by a vul in libfoo? • What vendors implemented this protocol?
Number of vendors involved	• Contact management (acquisition & maintenance) • Communication channel efficiency (hub & spoke, tools) • How many people can keep a secret for how long?

These are all about *efficiency* and *efficacy* of vulnerability response processes, driven by information *availability* and *utility*.

Parting Thoughts

CVD doesn't end with public disclosure.

- Most of the coordination work actually happens *after* public disclosure

"Average case" is not a useful concept for capacity planning

- Large cases are rare, but dominate the day-to-day work

Case complexity is driven by the number of participants involved

Case sizes appear to be limited by organizational factors

- There might be an upper limit to how big a coordination can be before it's better to just go public

Got Data?

- This is ongoing research work at CERT
- We are looking for CVD metadata from other orgs
- Minimum required: *(Case ID, Message Timestamp)*
- Contact us if you have data you can share.

Contact Info

Allen Householder

Team Lead, Threat Ecosystem Analysis

CERT Division

Email: adh@cert.org

Twitter: @__adh__