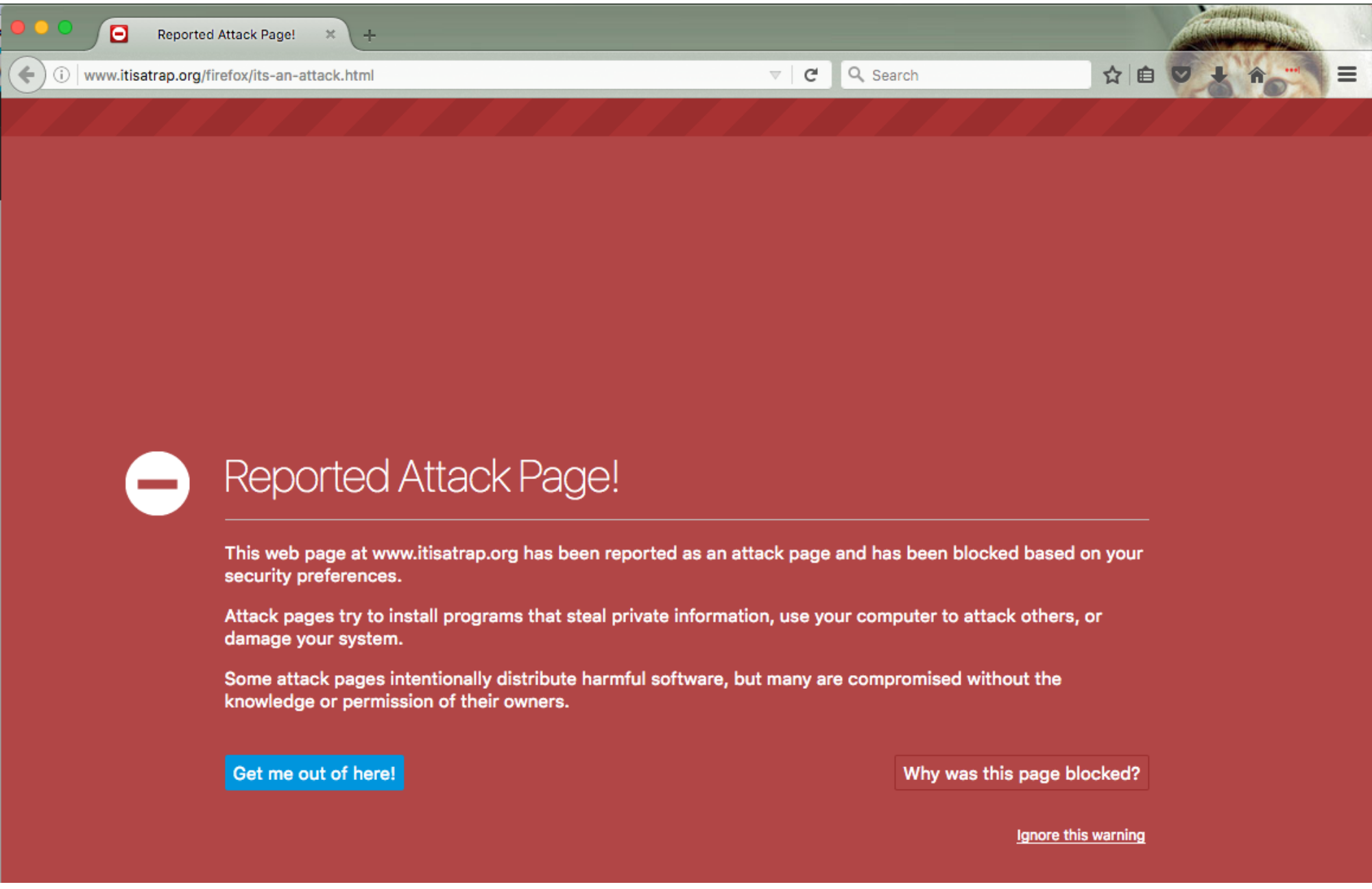
Measuring the Impact of Sharing Abuse Data with Web Hosting Providers

Marie Vasek, Matthew Weeden, and Tyler Moore

University of Tulsa

WISCS
24 October 2016


Reported Attack Page!
www.itisatrap.org/firefox/its-an-attack.html
Search
Reported Attack Page!
This web page at www.itisatrap.org has been reported as an attack page and has been blocked based on your security preferences.
Attack pages try to install programs that steal private information, use your computer to attack others, or damage your system.
Some attack pages intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.
Get me out of here!
Why was this page blocked?
Ignore this warning

StopBadware

- Founded in 2006 by Harvard's Berkman Klein Center for Internet and Society
- Now housed at the University of Tulsa
- Provides independent reviews of websites appearing on 3 malware blacklists

Review Requests for Individual URLs

Review Requests for Bulk URLs

Research Questions

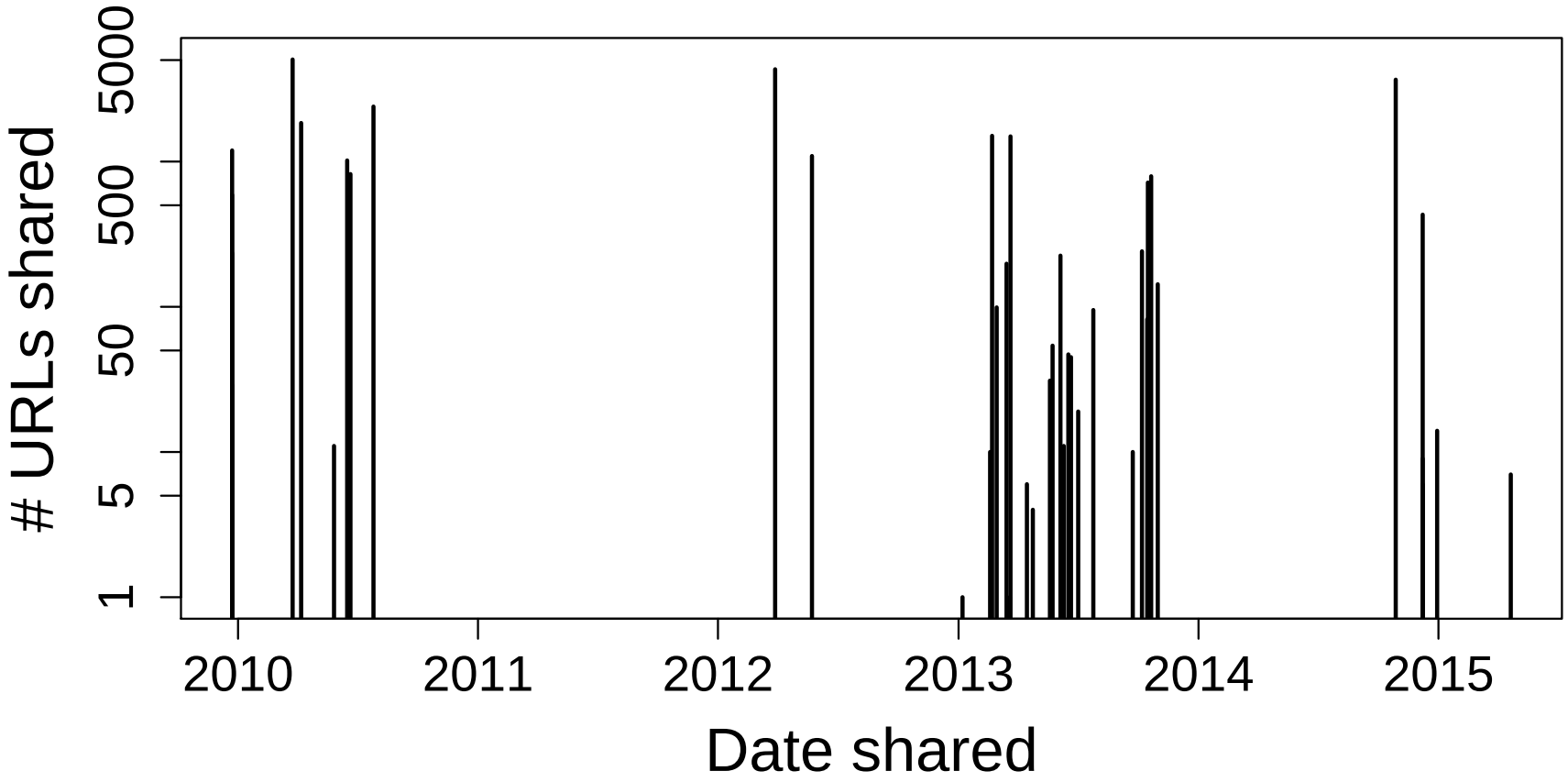
Does sending bulk reports help?

- Short term:
  - Do reported URLs get cleaned up?
  - Which URLs are more likely to get cleaned up?
- Long term:
  - Do ASes get better at cleaning URLs after receiving bulk reports?

Overview

- Brief overview of study
- Define metrics
- Direct impact of sharing abuse data
- Indirect impact of sharing abuse data
- Conclusions

Bulk Requests over Time



Summary Statistics

- Google Safebrowsing Data used exclusively
- 6 year time frame (2010 - 2015)
- 69 stakeholders requested reports
- 41 web hosting providers in our study
  - Responsible for entire AS
  - Sent Google Safebrowsing Data
  - Had at least a month of data before/after
- 28 548 URLs reported

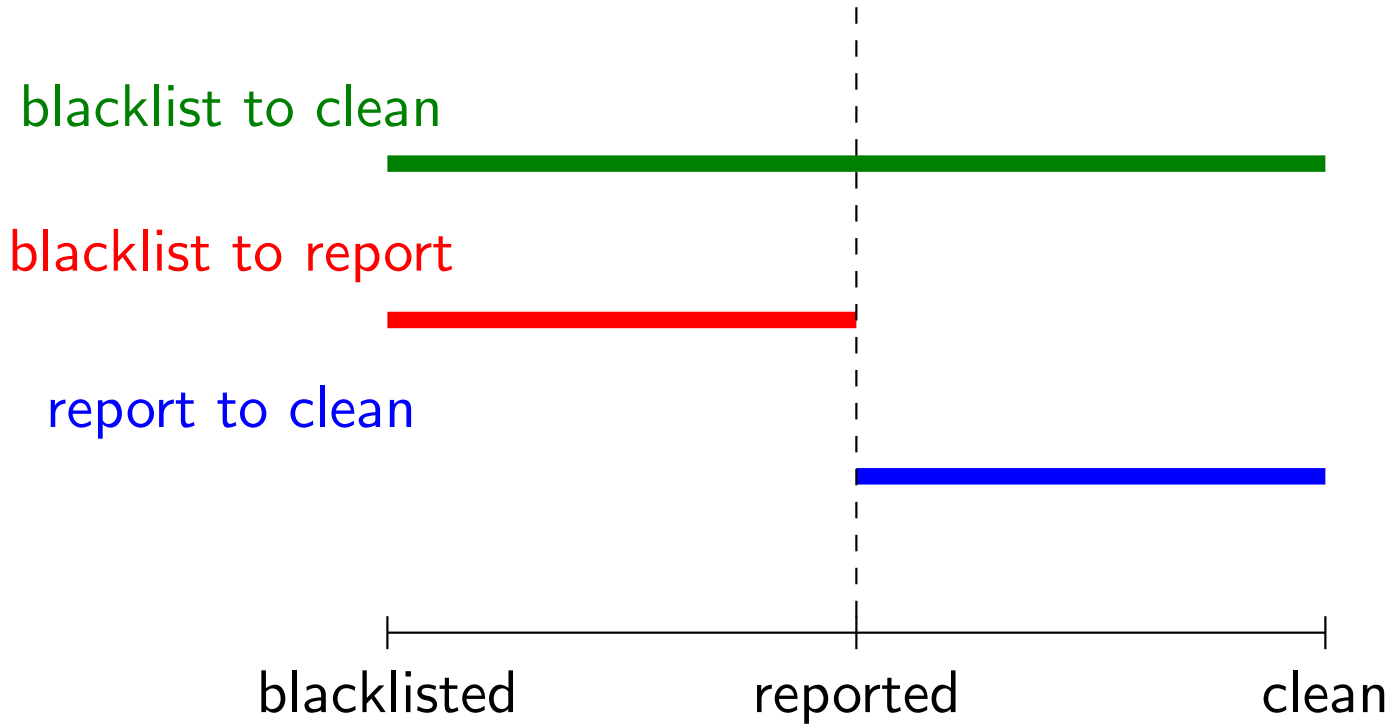
Malware Cleanup Metrics

- **Clean**
  - Off the blacklist
  - Stays off for 3 weeks
- **Recompromise**
  - A previously blacklisted URL is clean and then is reblacklisted

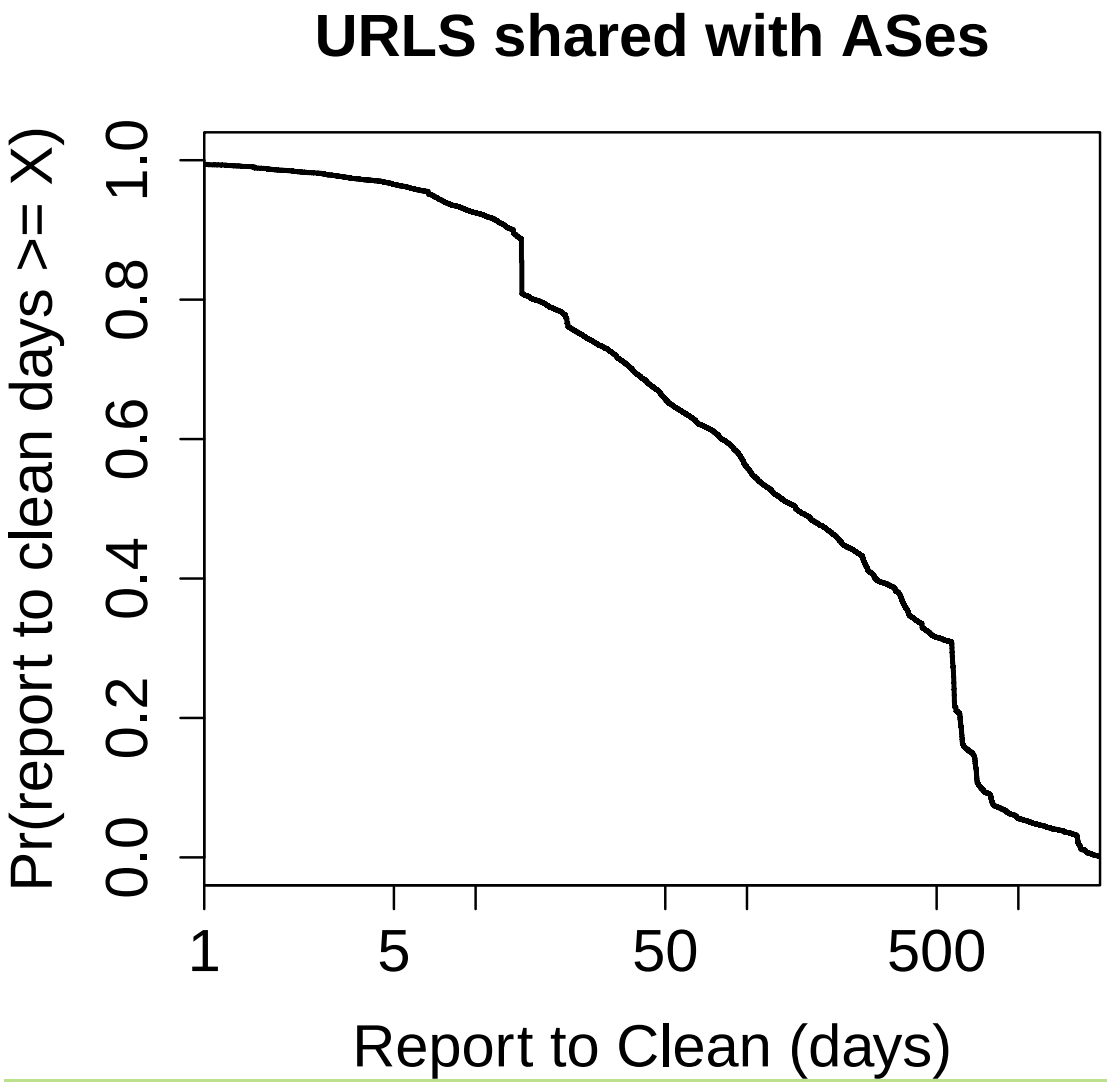
Measuring Direct and Indirect Impact of Reporting

- **Direct Impact**
  - Are the URLs we shared cleaned up?
- **Indirect Impact**
  - Are networks "better" after receiving a bulk review from StopBadware?
    - Do they clean malware URLs faster?
    - Do they clean malware URLs more effectively?

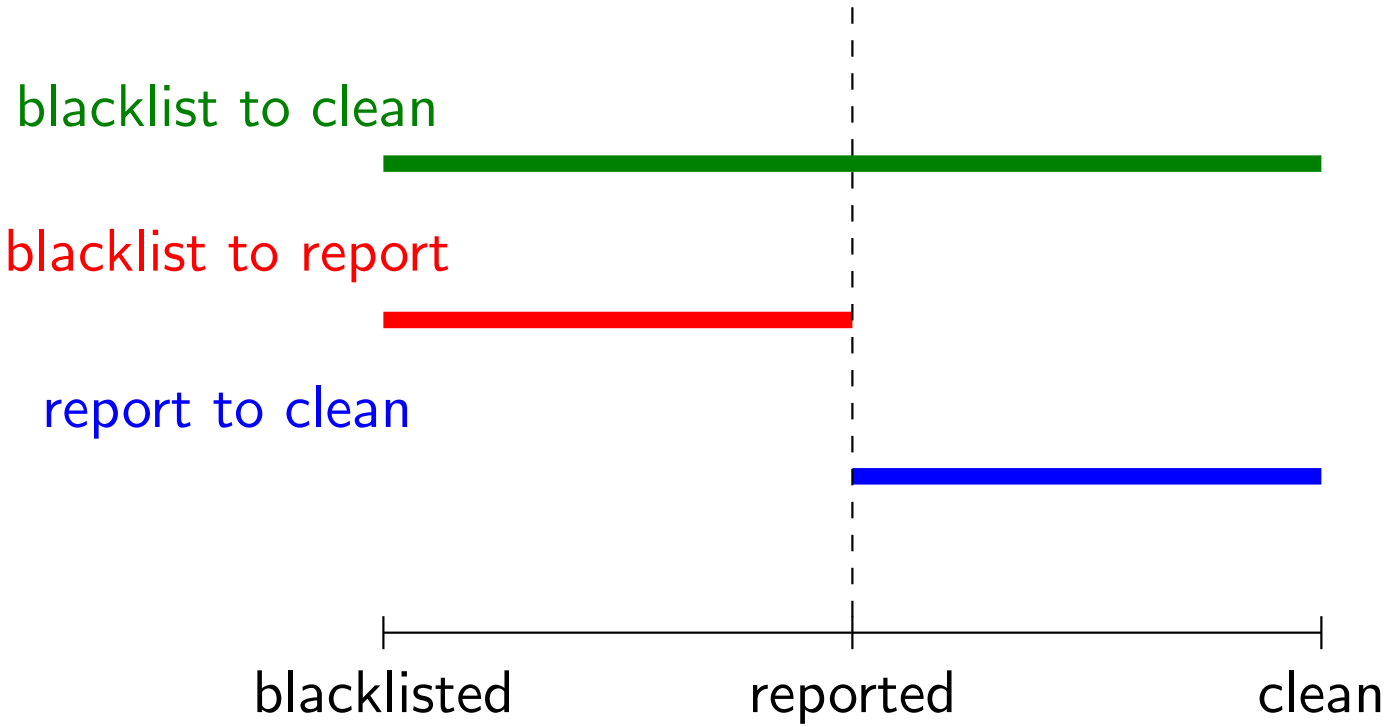
Measurement Timeline



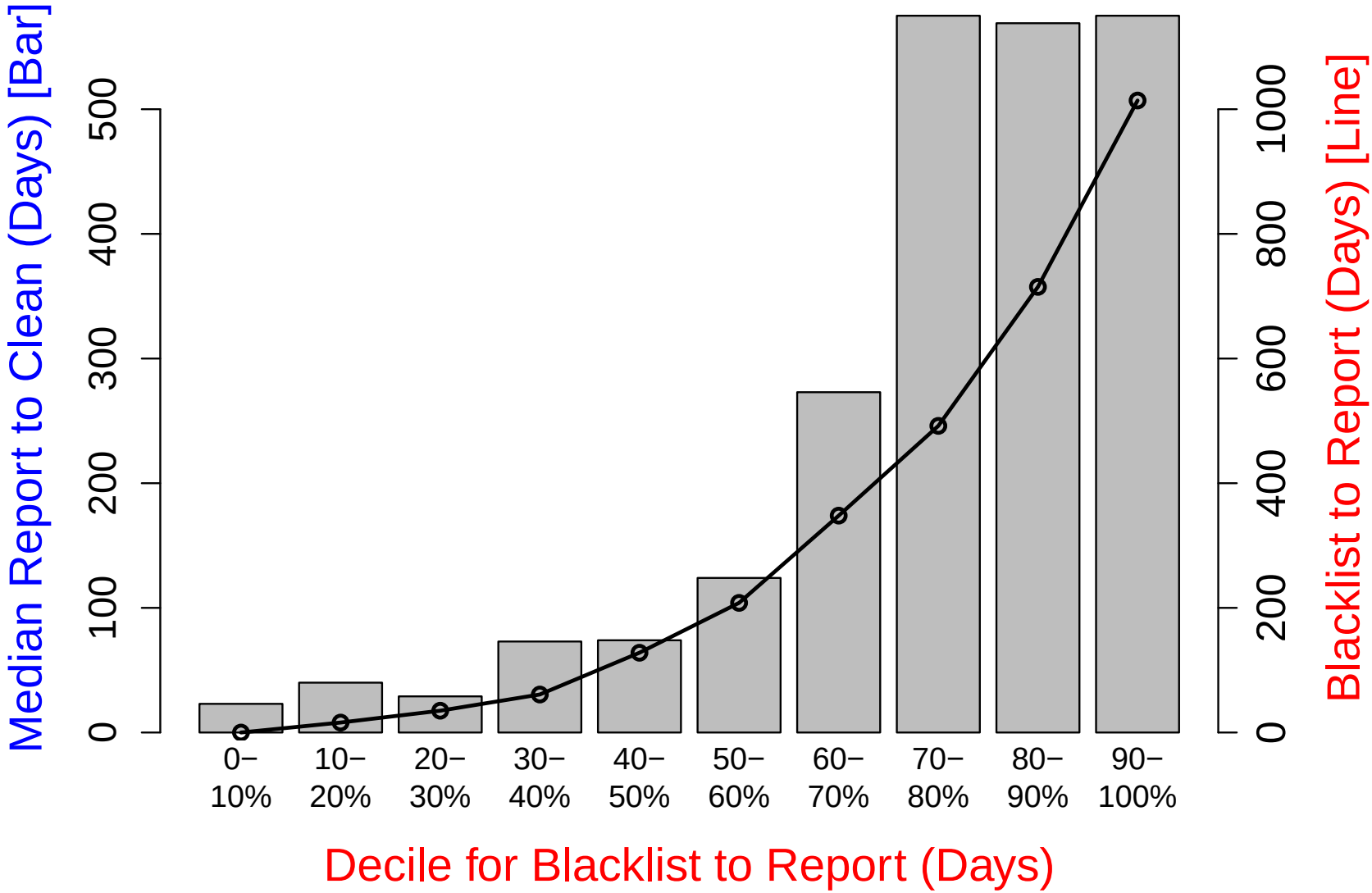
Cleanup of URLs Shared with ASes



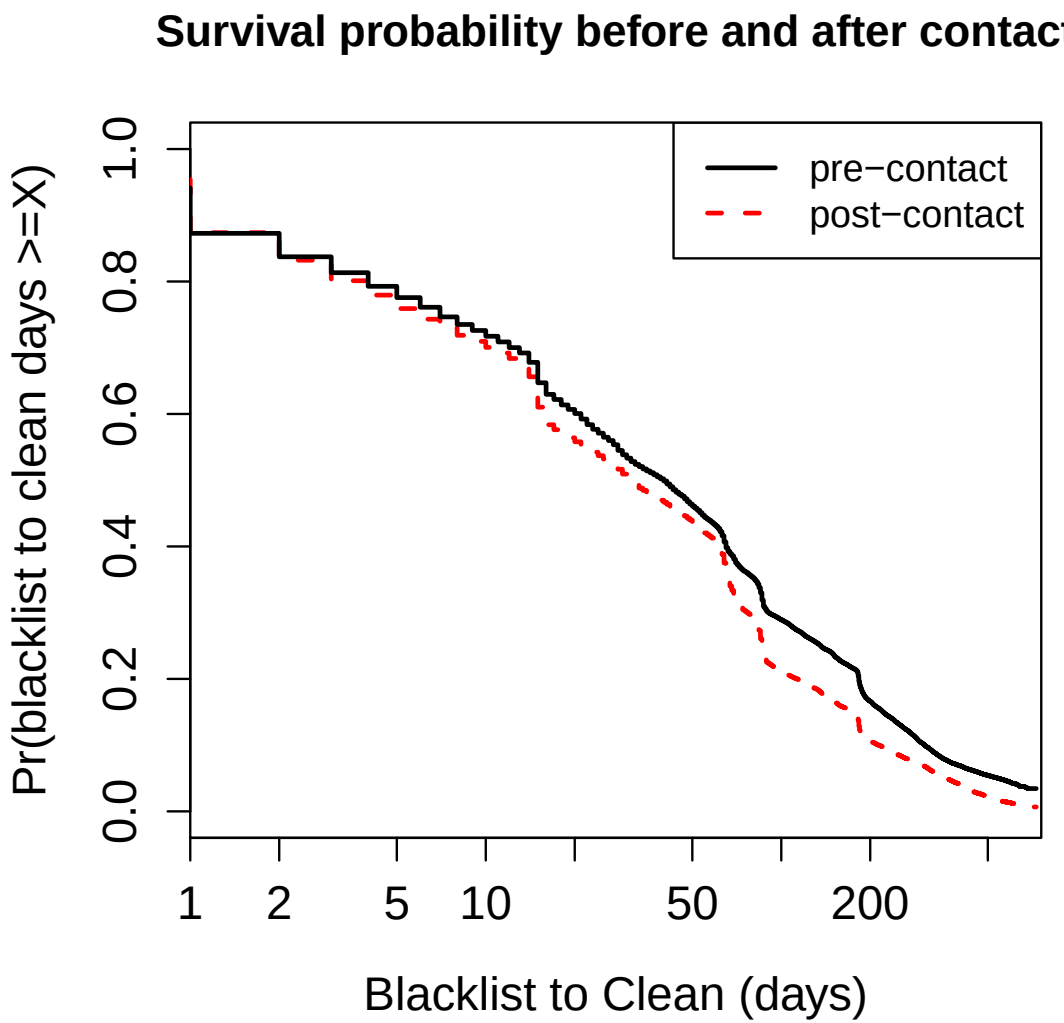
Measurement Timeline



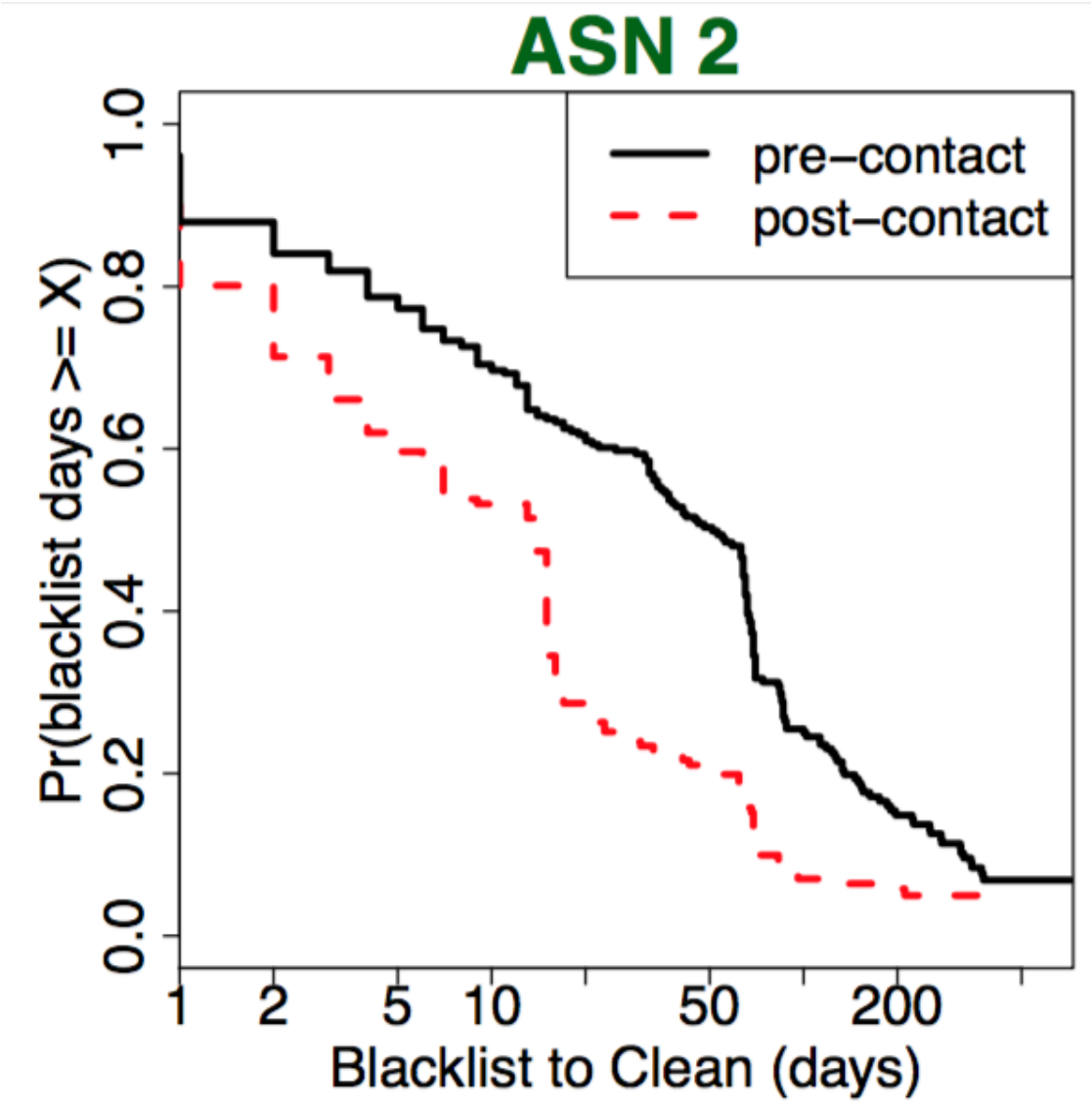
Long Lived Malware Takes Longer to Clean



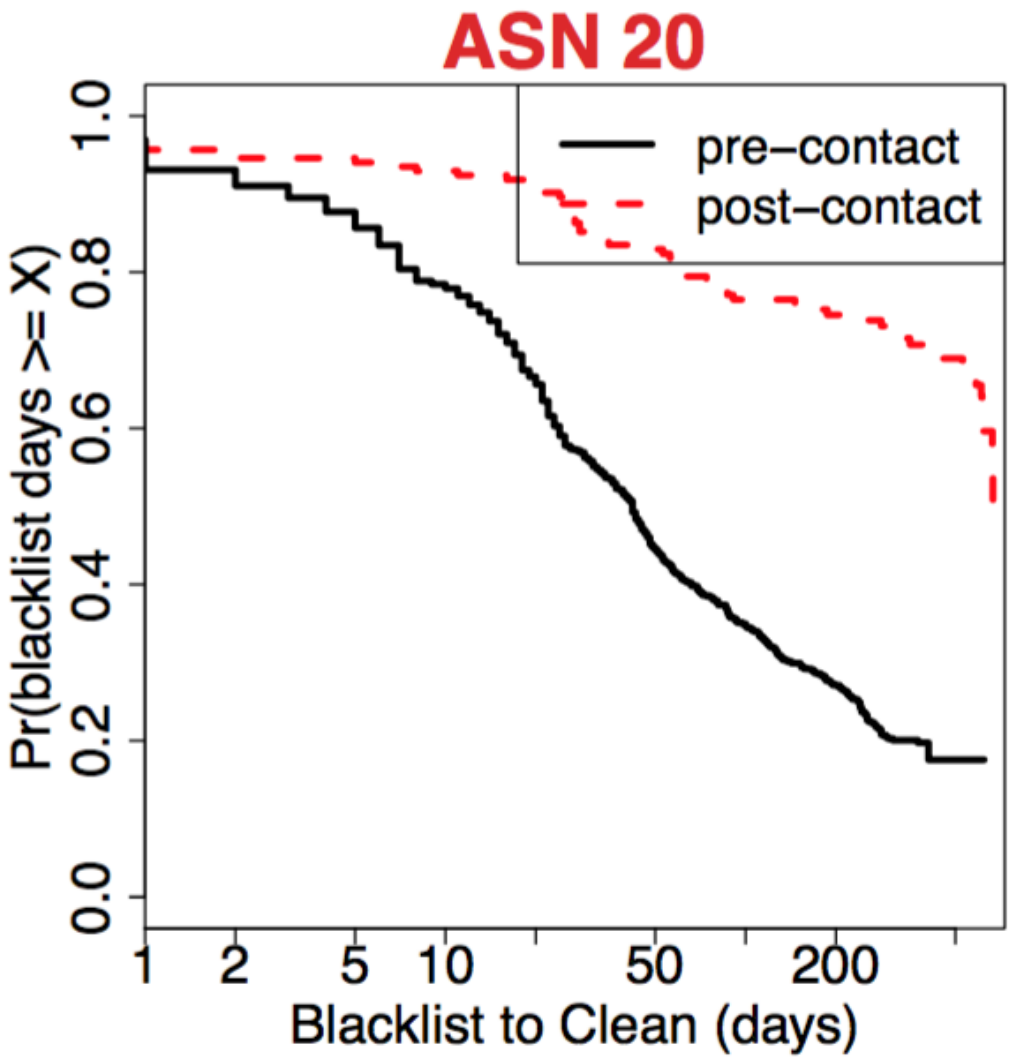
Pre- vs. Post-Contact Cleanup



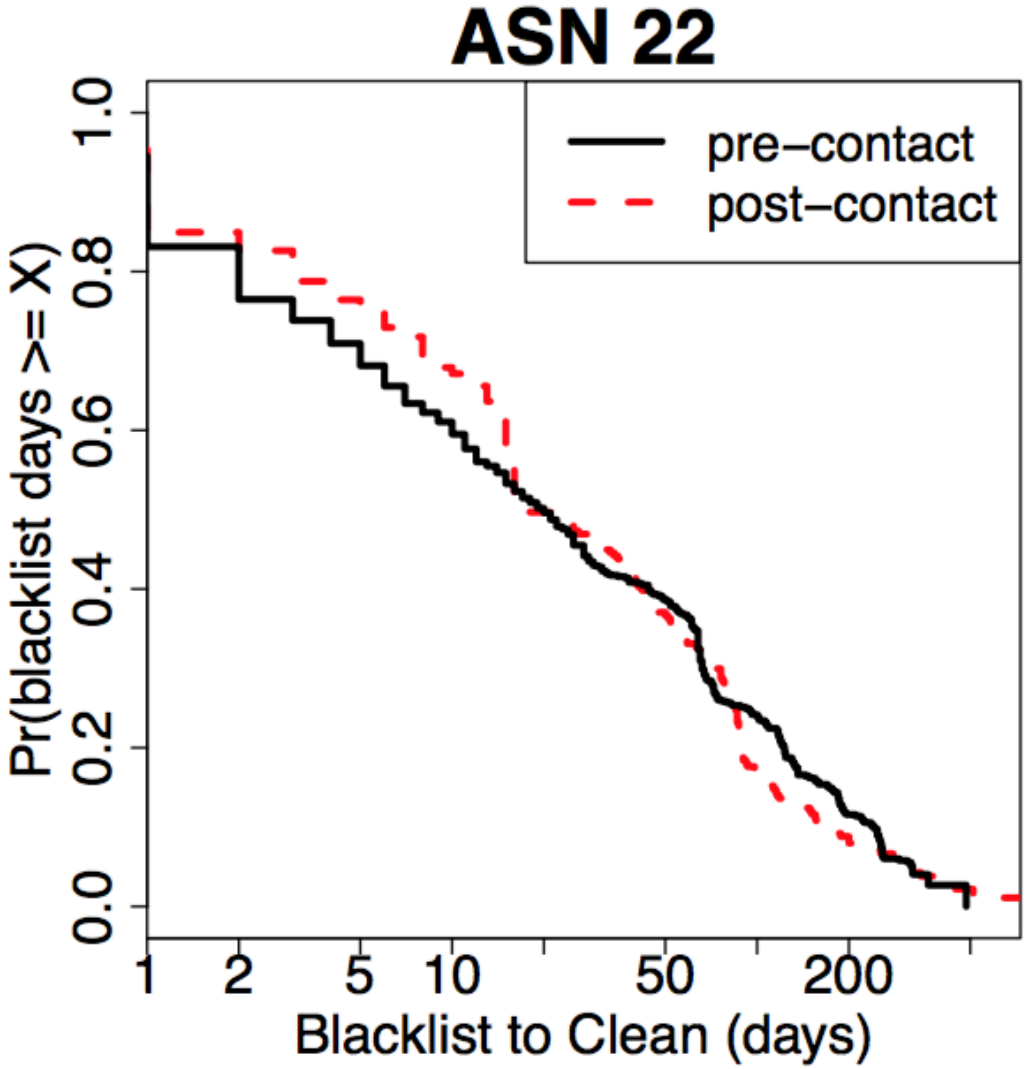
Pre- vs. Post-Contact Cleanup: Improved AS



Pre- vs. Post-Contact Cleanup: Worsened AS



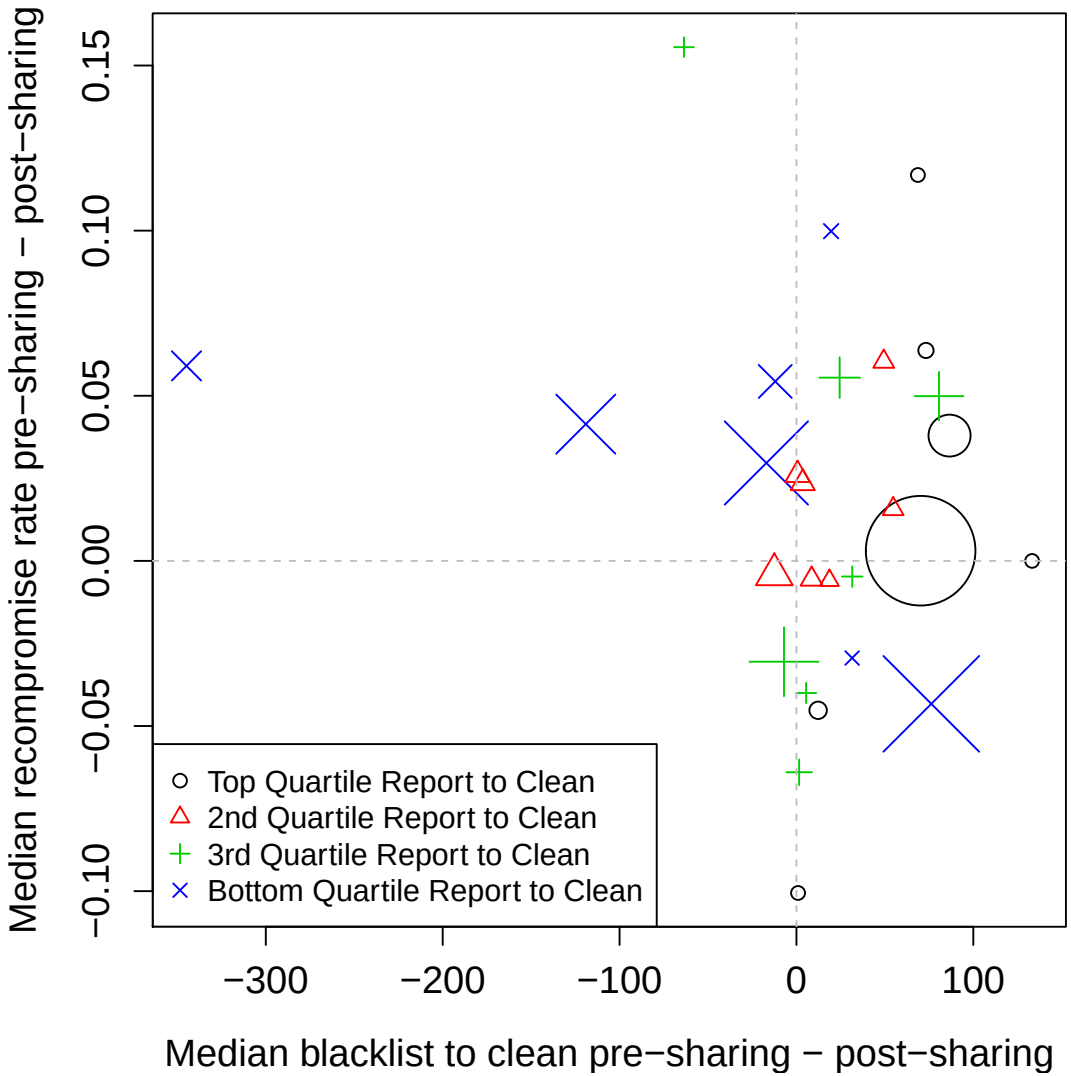
Pre- vs. Post-Contact Cleanup: Unclear effect AS



Change in Metrics Pre- and Post- Sharing

	#	Δ days to clean	Δ recomp. rate
Improved	13	58	0.010
Worsened	3	-176	0.085
Unclear	17	13	0.008

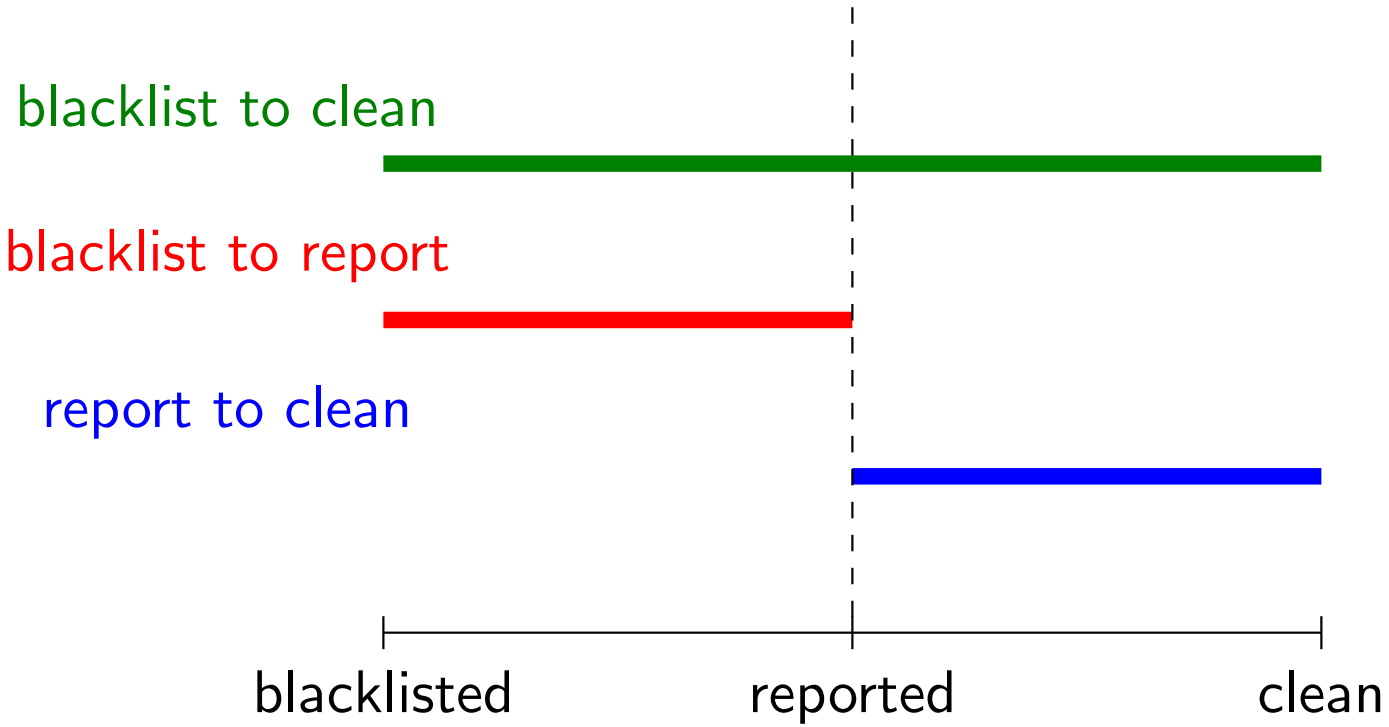
Comparing Change in Metrics by AS



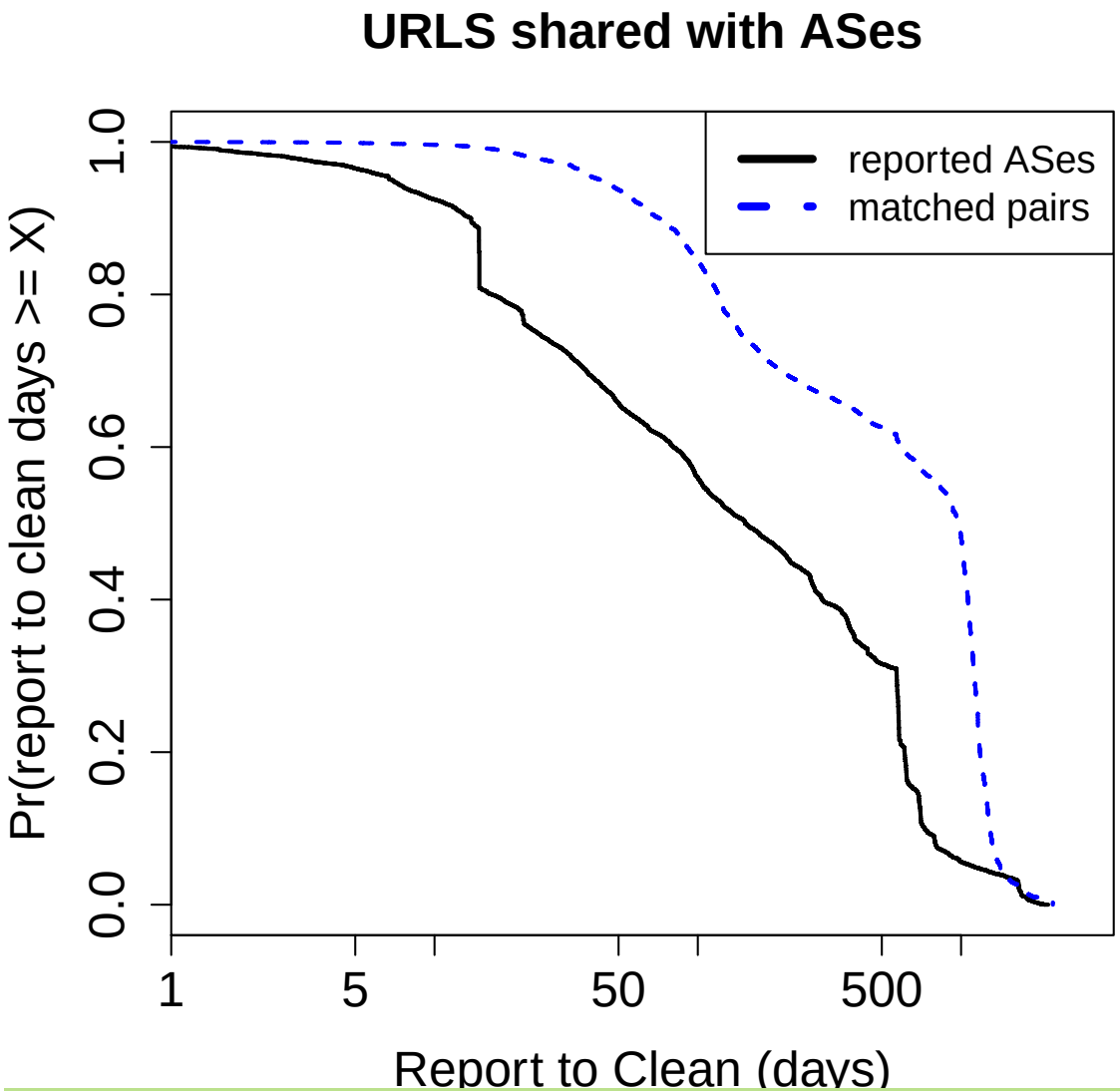
Matched Pair Analysis

- What would happen if StopBadware had not sent out reviews?
- Matched pairs between reported-to ASes and similar ASes
- Similar?
  - Same country
  - Similar level of badness
- Key Assumption: All else equal, ASes would exhibit similar patterns

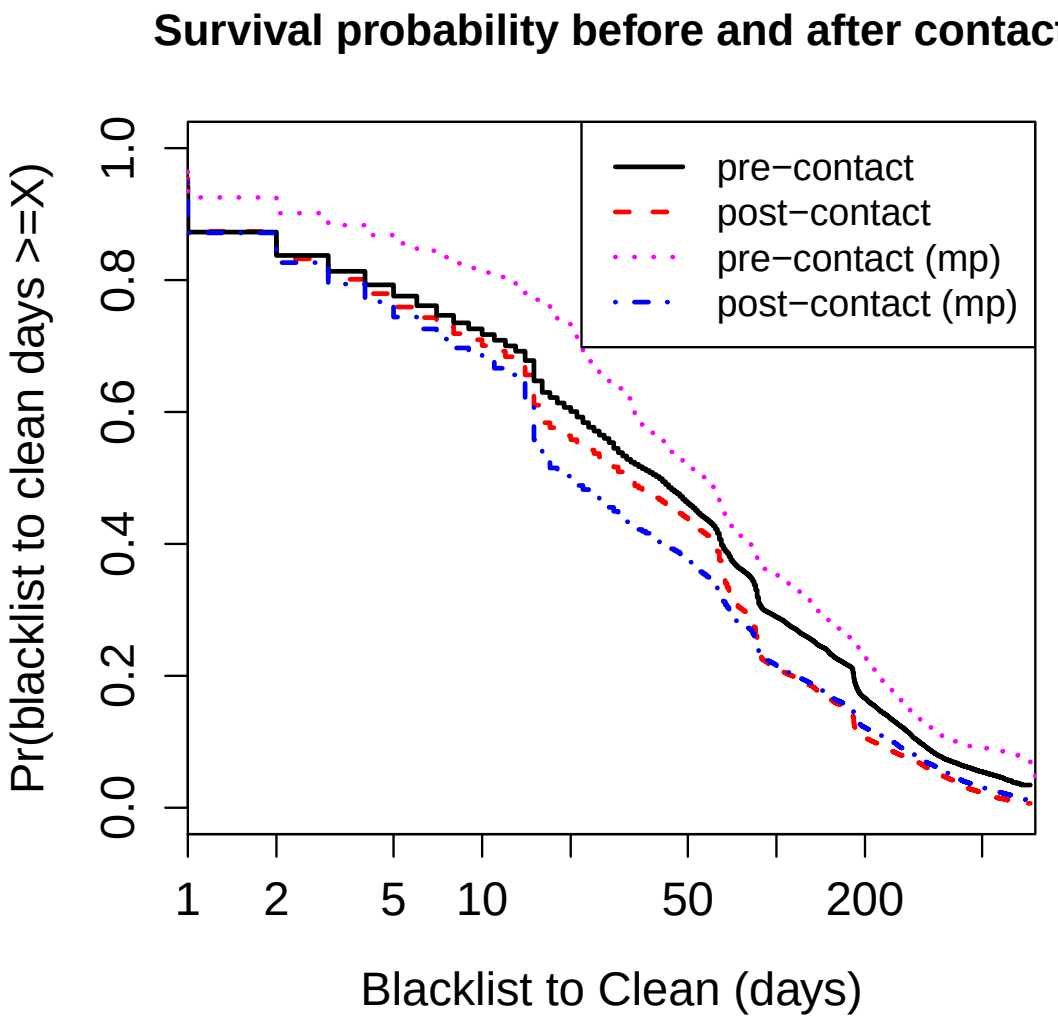
Measurement Timeline



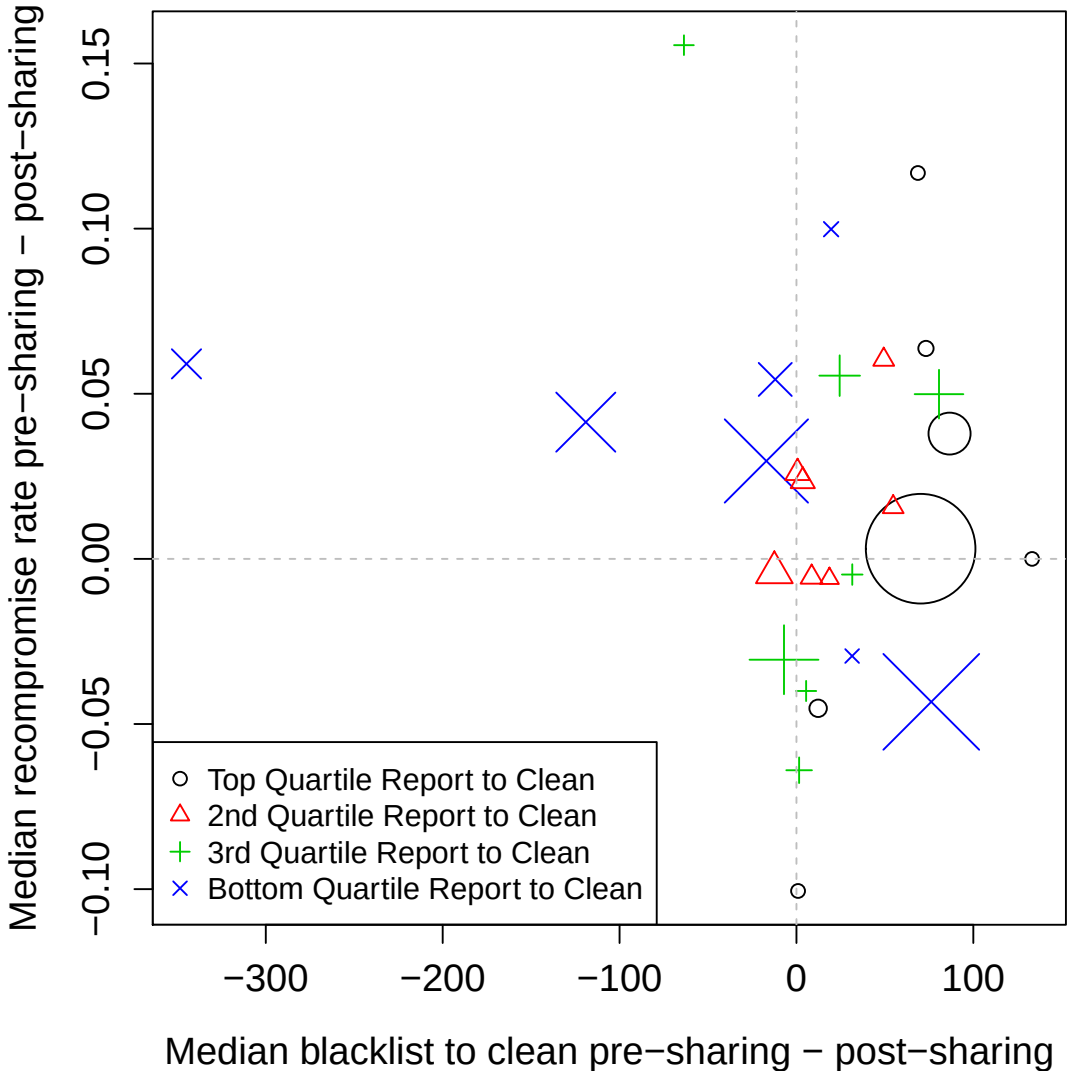
Matched Pair: Cleanup of URLs Shared with ASes



Matched Pair: Pre- vs. Post-Contact Cleanup



Responsive ASes Improve Long Term after Report



Conclusions

- Directly sharing URLs helps clean up those URLs
  - Consistent with prior work on individual reports
  - This work finds it to be true for **bulk** reporting
- No evidence for long term change overall
  - Improvements on individual providers
- Long lived malware a scourge
  - Lots of efforts concentrating on newly infected websites
  - Lurking infections continue to harm, perhaps compounding
  - Current efforts not sufficient for stopping this "immortal" malware