Do malware reports expedite cleanup? An experimental study

Marie Vasek and Tyler Moore
Southern Methodist University / Wellesley College

USENIX CSET

August 6, 2012

Hacked websites distribute malware to unsuspecting visitors

Hacked websites distribute malware to unsuspecting visitors

Voluntary infosec enforcement

- Law enforcement is usually not involved in the detection and cleanup of hacked websites distributing malware
- Instead, cleanup is coordinated and carried out by voluntary efforts
  - Security companies
  - Search engines
  - Non-profit organizations
  - Web hosts and site owners

- Malware cleanup process
  1. Detect a website distributing malware
  2. Notify the website owner and hosting provider of infection if compromised, or hosting provider and registrar if purely malicious
  3. Search engines might block results until malware is removed

StopBadware Best Practices for Reporting Badware URLs

- Developed Spring & Summer 2011 by StopBadware working group
  - Guide for malware reporters to send more effective malware reports
- What should be in every malware report:
  - Specific URL, date/time *bad*ness occurred, IP address, brief description of *bad*ness, list of report targets, your contact info
- Additional helpful information:
  - Specific *bad* code observed, more detailed information needed for malware delivery, scope of behavior, hash of executable, etc.
- Who to contact and how:
  - Hosting provider unless bulletproof
  - Site owner if compromised ; Domain Registrar if malicious
  - Escalate to AS owner, DNS provider, registry, CERT/CSIRT, police
  - Quick methods of contact: phone or email (fax? postcard?)

Example Badware URL Notification

To: abuse@wehateabuse.example.com
Subject: Badware URL notification – malicious-url .net

hxxp://malicious-url .net/evilscript.js appears to be a badware URL. This means it may be placing Internet users at risk. We believe that malicious-url.net is primarily used for malicious purposes. Please investigate and take appropriate action to resolve or mitigate the threat.

Badware description: Delivers malicious PDF and Flash files.

Date/time of detection:	15 July 2011 at 1048 EDT
IP address at time of detection:	192.10.20.30
Additional parties notified:	Friendly Registrar, Inc. (domain name registrar)

You are receiving this report because this email address is listed as the hosting provider contact in the WHOIS record for 192.10.20.30.

Caution: Opening badware URLs in your browser can infect your computer. For security reasons, URLs in this email have been modified by replacing http with hxxp and by adding a space before the last dot (.)

==========
ADDITIONAL INFORMATION
==========

Detailed badware description:
URL accessed: hxxp://malicious-url .net/evilscript.js
Bad Code: eval(function(p,a,c,k,e,r){e=function(c){return(c<a?'':e(parseInt(c/a)))+((c=c%a)
[truncated]
Behavior: Delivers malicious PDF and Flash files
Special conditions: Only delivers files when referred by a compromised site, such as hxxp://compromised.example .com.

Best practices for web hosting providers receiving reports like this:
http://www.stopbadware.org/best-practices/web-hosting-providers

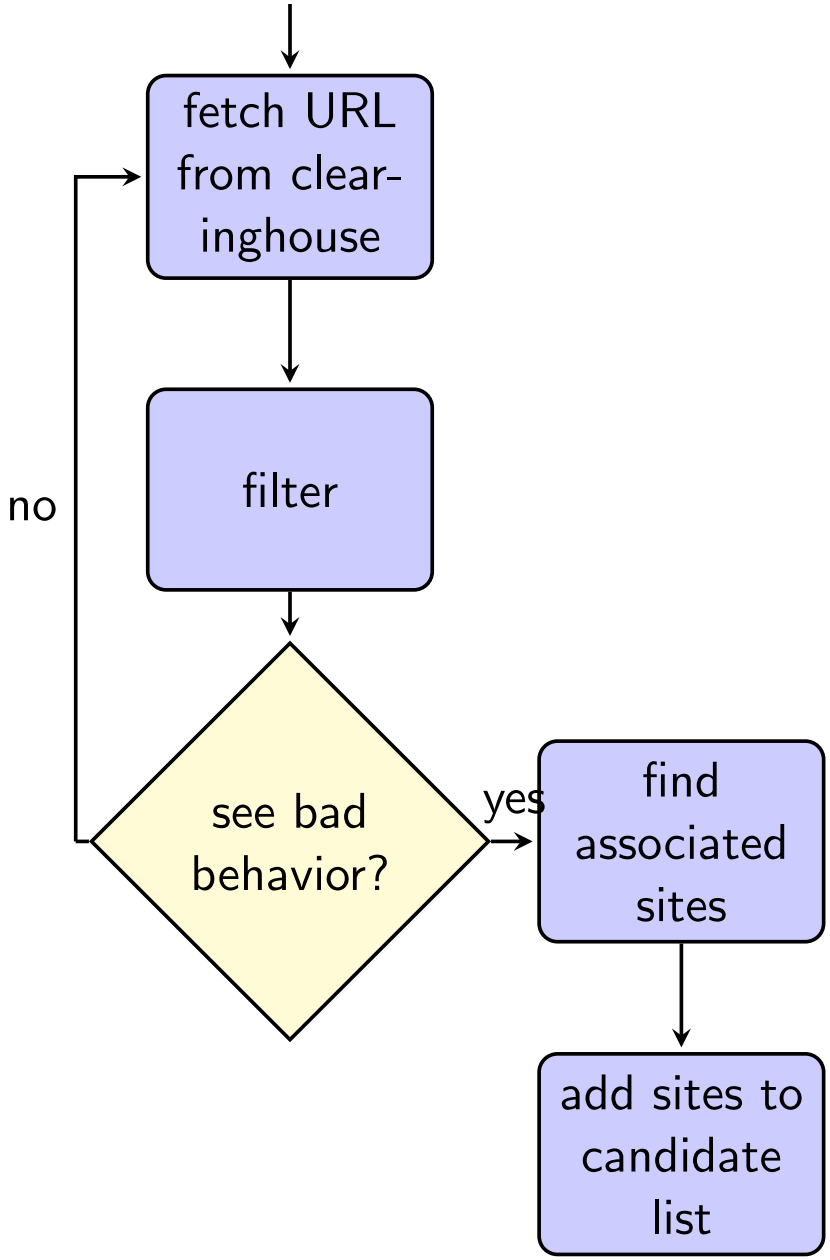
The Experiment

Hypothesis 1: Sending malware notices helps cleanup -- in particular, more sites will be cleaned and they will be cleaned more quickly

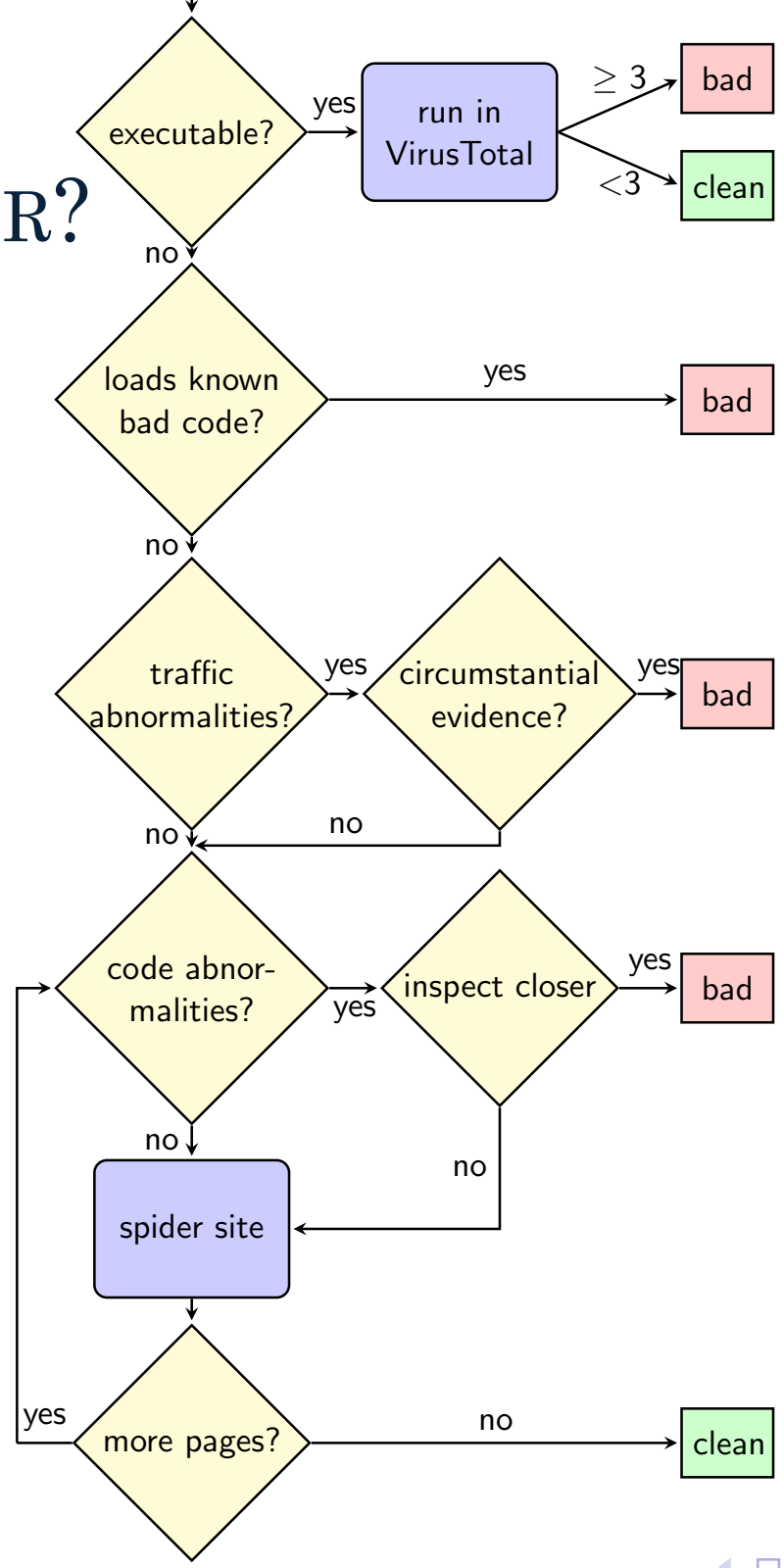
Hypothesis 2: More details help expedite cleanup

1. Process potential malware URLs
   - Reported to StopBadware by Internet users
   - Find the *bad* ones
2. Send out badware reports
   - Find contact information
   - Randomly assign to group (control, minimal, full)
   - Email reports to contacts
3. Follow-up on malware URLs
   - 1, 2, 4, 8, 16 days after initial report
   - Evaluate if site is still *bad*

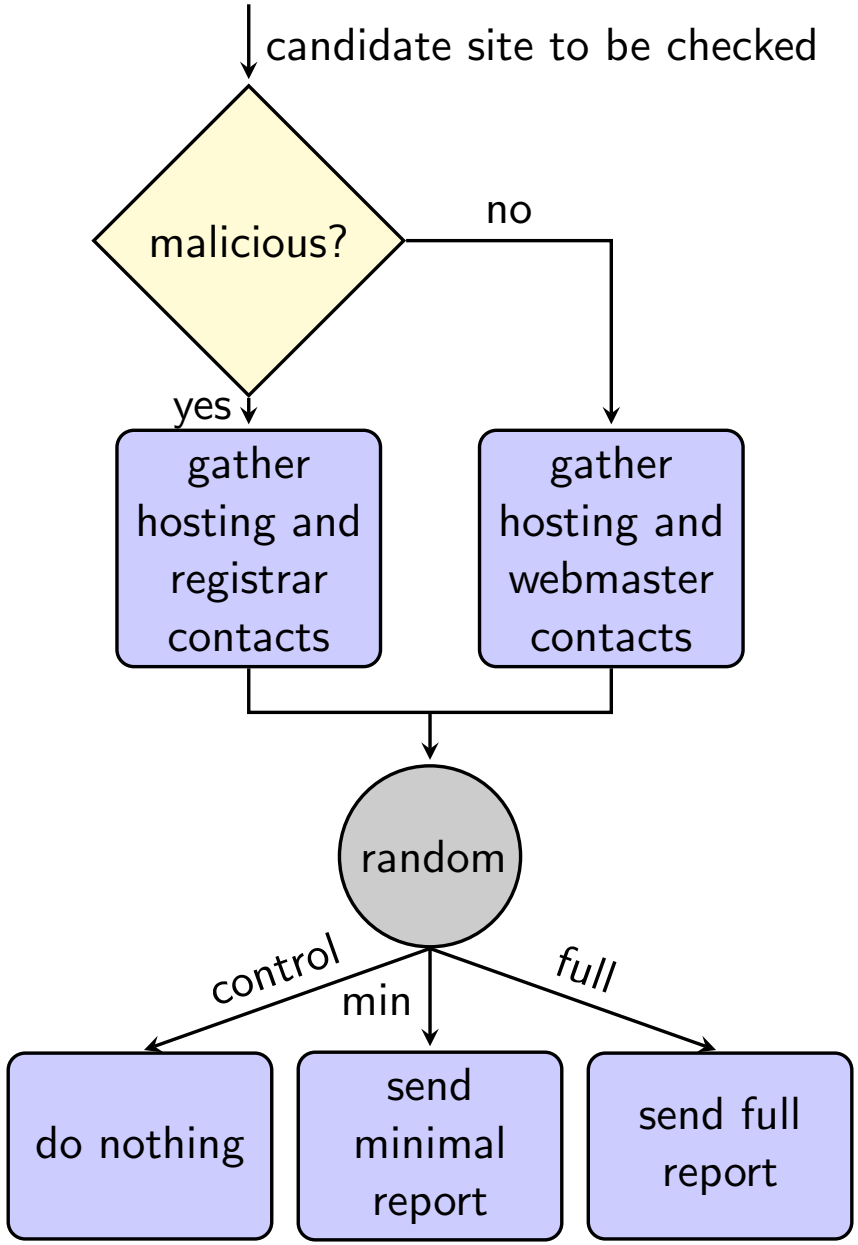
1. Process Potential Malware URLs



What is Bad Behavior?



2. Send Out Badware Reports



Example minimal notice

Subject: Badware URL notification - compromisedSite .com
To: support@good-host.com

hxxp://compromisedSite .com/ appears to be a badware URL. This means it may be placing Internet users at risk. Please investigate and take appropriate action to resolve or mitigate the threat.

Description: Contains malicious injected javascript

Date/time of detection: 2011-12-05 1303 EST
IP address at time of detection: 216.119.132.194
Additional parties notified: info@compromisedSite.com (site owner)

You are receiving this report because this e-mail address is listed as the technical or abuse contact address in the WHOIS record for 216.119.132.194. If you believe you have received this report in error, or for more information, please contact us at this address: reporting-beta@stopbadware.org.

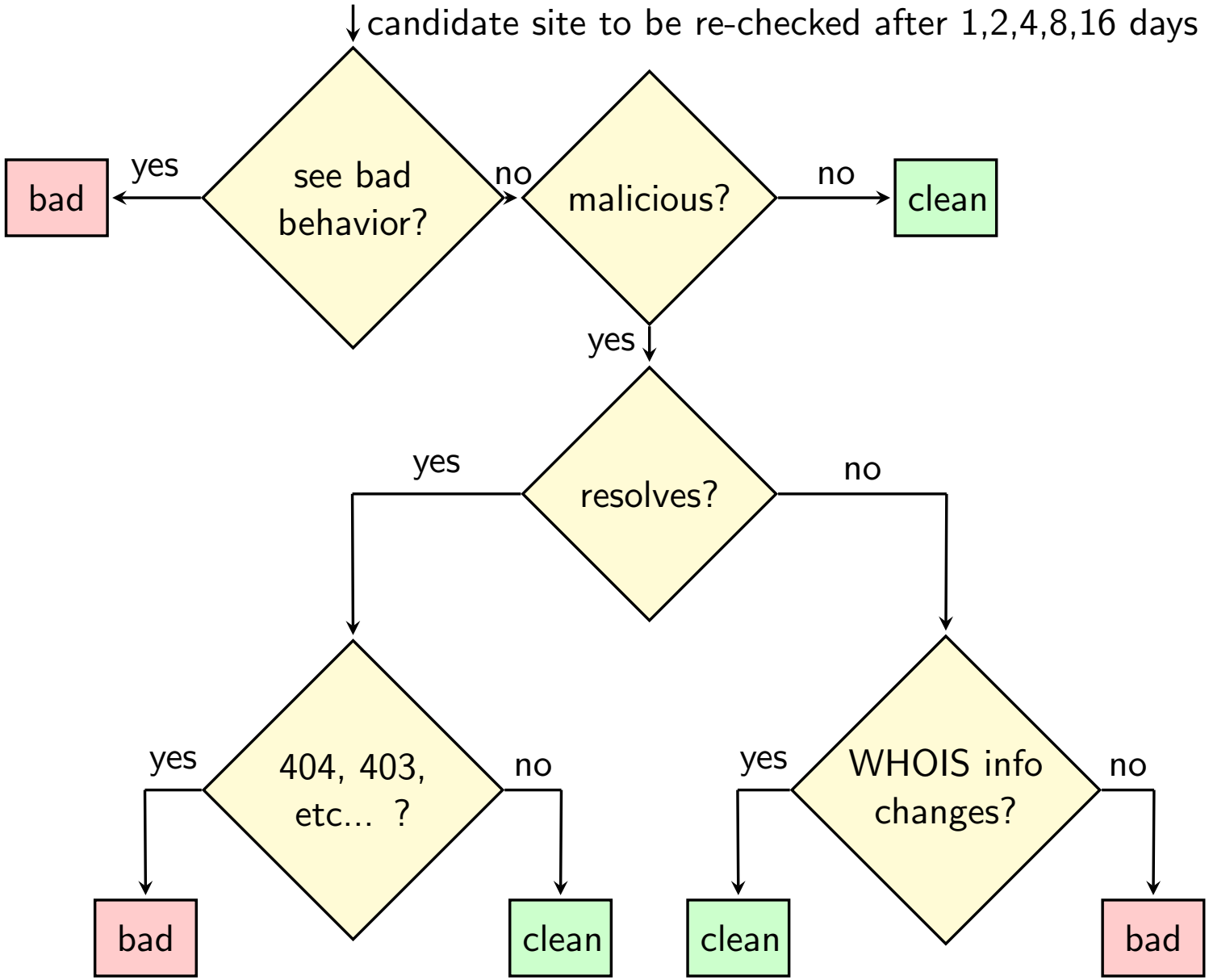
Caution: Opening badware URLs in your browser can infect your computer. For security reasons, URLs in this email have been modified by replacing http with hxxp and by adding a space before the last dot (.)

EXAMPLE DETAILED NOTICE

Everything in the minimal notice plus:

```
======================
ADDITIONAL INFORMATION
======================

Detailed badware description:
URL accessed: hxxp://compromisedSite .com/
Bad Code: <img heigth="1" width="1" border="0" src="hxxp://imgaaa
.net/t.php?id=9975084">
Behavior: Attempts to load malicious code from hxxp://imgaaa
.net/t.php?id=9975084.

URL accessed: hxxp://compromisedSite .com/.log/compromisedSite.com/xmlrpc.txt
Behavior: Is indication of further compromise of compromisedSite .com.

Special conditions: hxxp://compromisedSite .com/ only delivers malware when accessed
with a google.com HTTP referrer.

Best practices for web hosting providers receiving reports like this:
http://www.stopbadware.org/best-practices/web-hosting-providers
```

3. Follow-up on URLs

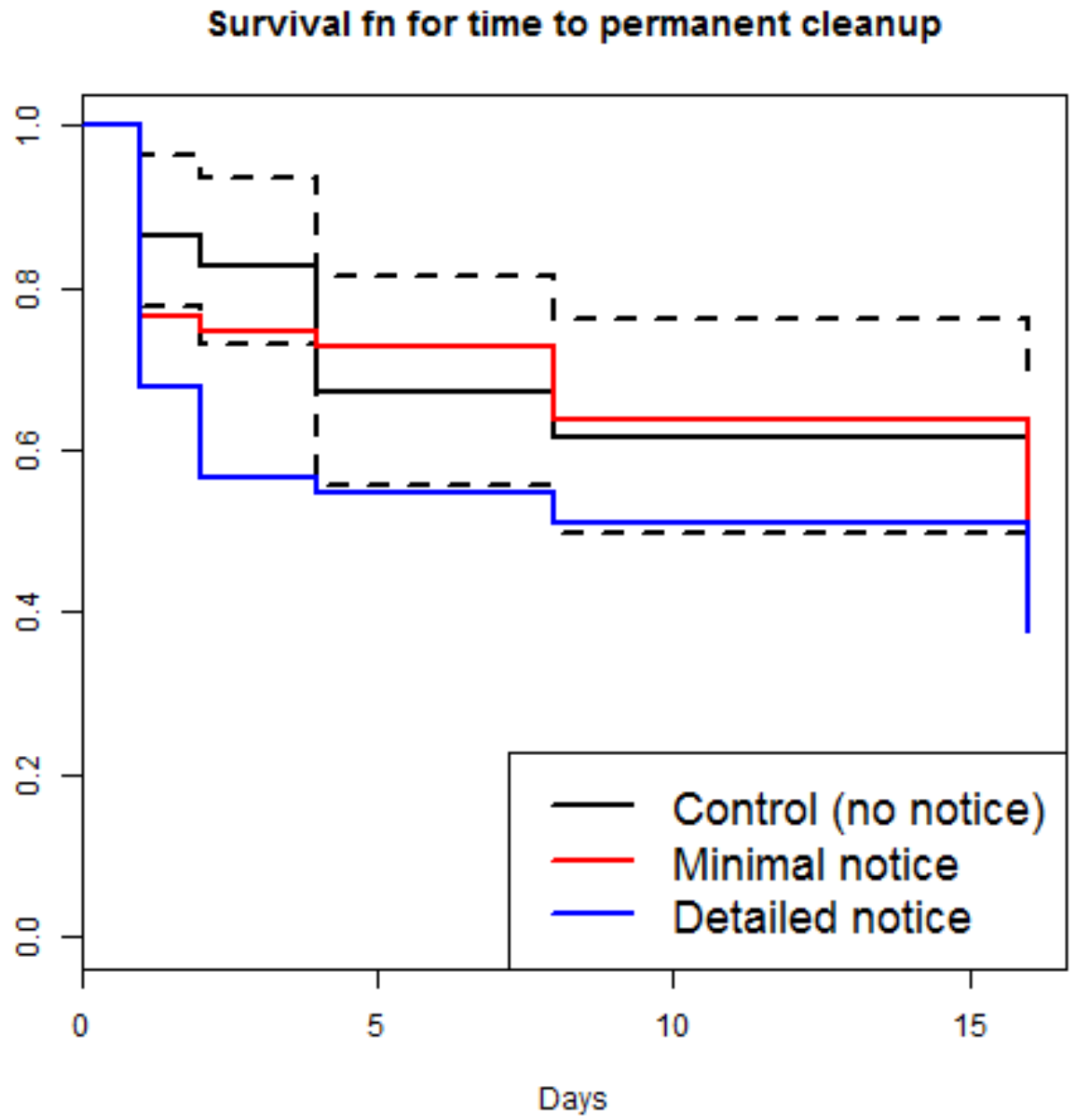


What We Found: Clean after 16 days

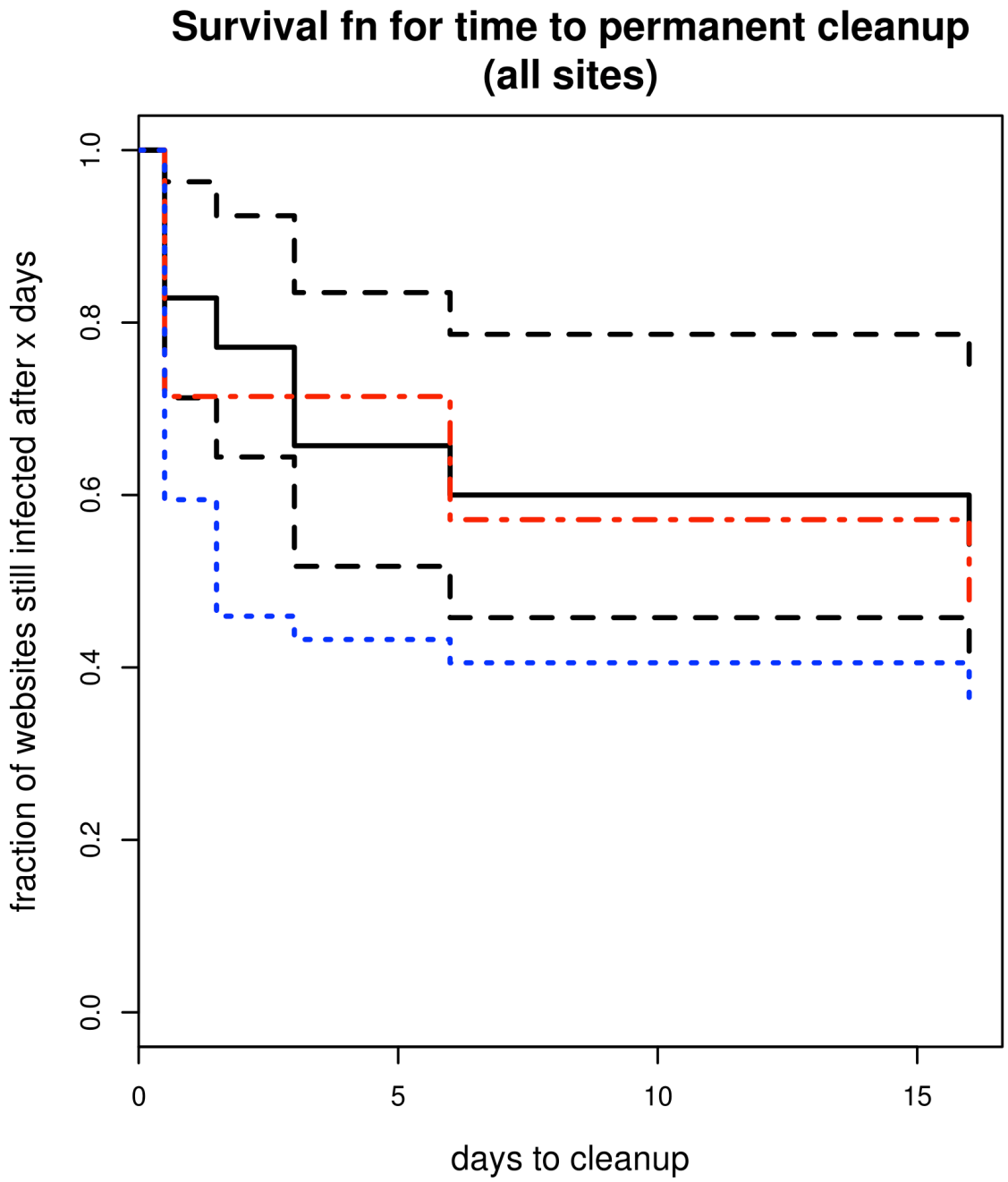
- 10 October – 5 December 2011
- 161 badware URLs (out of 960 reported to SBW)

	All Badware		Purely Malicious		Compromised	
Report Type	#	% Clean	#	% Clean	#	% Clean
Control	53	**45**	13	46	40	45
Minimal	55	49	17	53	38	47
Full	53	**62**	17	58	36	63

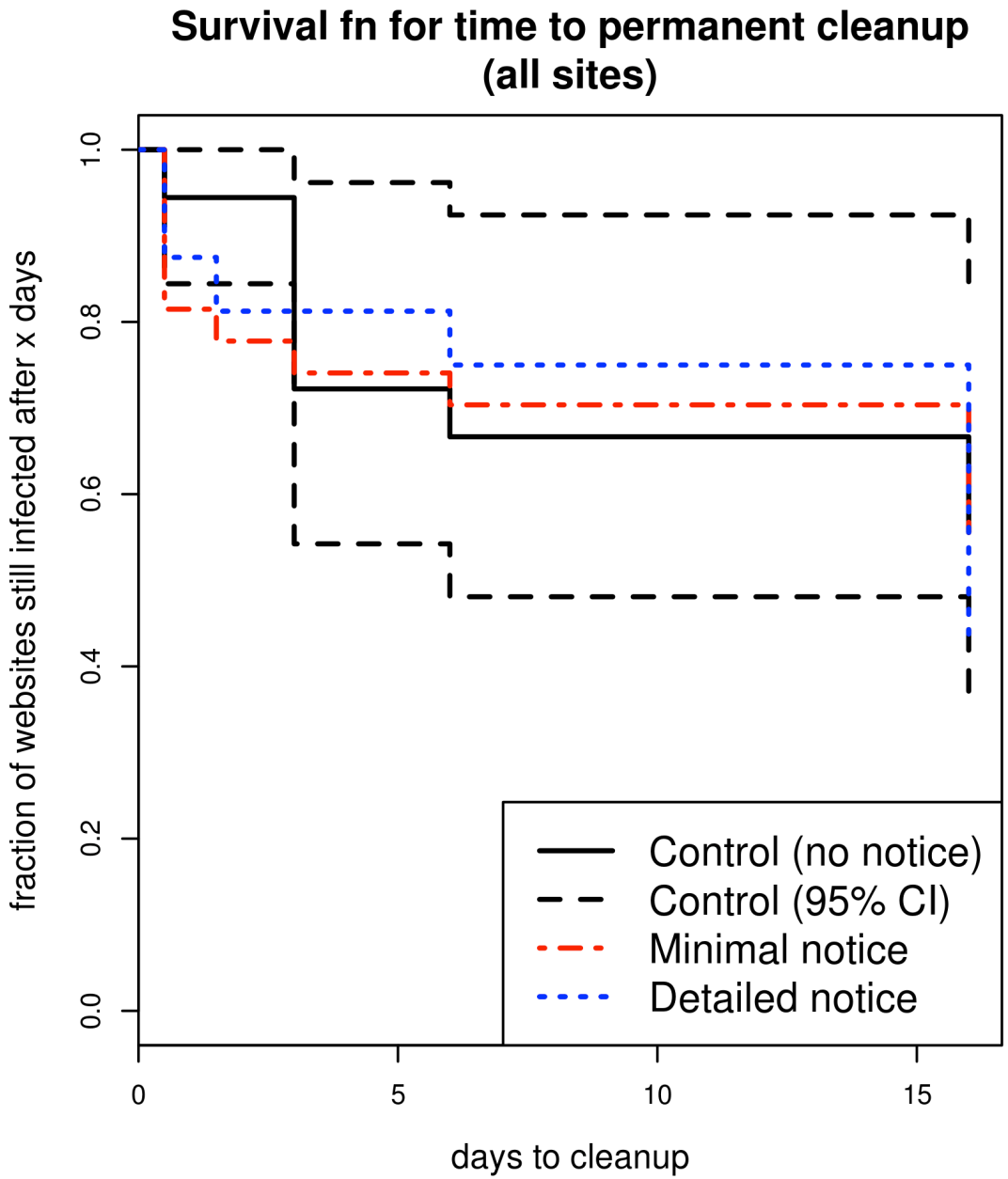
Tracking Cleanup Over Time (161 URLs)



What happens if Google hasn't already sent a notice? (100 / 161 URLs)



On Google's Blacklist (61 / 161 URLs)



Conclusion

- Reporting works
  - 40% cleaned up 1 day after receiving full report, vs. 18% w/o notice
- Fuller reports better than concise reports
  - But only the first report matters
  - Concise reports a waste of time
- Methodology for evaluating malware notices
- Limitations and future work
  - Small sample size
  - Mostly manual
  - Automated assessment of malware could enable larger scale studies