
Best Practices for

# Reporting Badware URLs

# Background

Badware in its various forms—viruses, spyware, scareware, and so on—is a core component of cybercrime and threatens to undermine the trust necessary for the Internet to continue thriving as an open, generative platform. Because it is quick, easy, and inexpensive for malicious actors to create and disseminate new badware, the ecosystem faces a significant challenge: to keep up in its efforts to remove badware as it is discovered.

One way to address this challenge is to improve the communications between those who detect badware URLs and those best positioned to address the threat they pose. Today, there is no clear expectation of who should be notified of a badware URL, what information should be included in that notification, or how to escalate the issue if the URL remains malicious. Absent this common standard, some parties choose not to report badware at all, while others develop their own approaches to reporting. This duplicates effort and makes it more difficult for web hosting providers, individual site owners, and other recipients of badware reports to prioritize and act upon the information they receive.

# Purpose and Scope

This document establishes best practices for reporting badware URLs at each stage in the reporting process: targeting reports, identifying contact information, assembling report contents, and delivering reports. It also specifies procedures for escalating those reports when needed. The Practices are designed to promote reporting useful to report targets and to offer both guidance and flexibility to reporters who have voluntarily committed to reporting badware URLs. A complement to this document, StopBadware's *Best Practices for Web Hosting Providers*, can be found at http://www.stopbadware.org/best-practices/web-hosting-providers.

# Definitions

**Badware**: Software that fundamentally disregards users' choices about how their computers or network connections are used.

**Badware URL**: A URL referencing a resource that facilitates—or attempts to facilitate—the distribution or operation of badware, regardless of the awareness or intent of the URL owner.

**Report**: A communication describing a badware URL or a set of closely related badware URLs.

**Reporter**: An individual or organization initiating a report.

**Target**: An individual or organization to whom a report is communicated.

**Hosting provider**: An entity that manages or controls infrastructure used to host websites or web applications for third parties. (A more extensive definition may be found in StopBadware's *Best Practices for Hosting Providers: Responding to Badware Reports*.)

**URL owner**: An individual or organization that is directly responsible for managing the content or functionality of a resource referenced by a URL, by virtue of having leased or otherwise been granted access by a hosting provider.

# Stage 1: Determining report targets

When possible, reporters should determine whether the badware URL references a compromised domain or a domain that is used primarily for malicious activity. We recommend reports be targeted as follows:

| URL Type | Report target(s) |
|---|---|
| Domain name is ordinarily legitimate<br>*(e.g., a compromised website)* | Hosting provider<br>URL owner |
| Domain name is primarily malicious<br>*(e.g., associated with exclusively malicious content, uses false WHOIS data, is generated algorithmically)* | Hosting provider<br>Domain name registrar |
| Domain name type cannot be determined<br>*(e.g., URL was not manually investigated or investigation is inconclusive)* | Hosting provider |

**Additionally**, we recommend that reporters modify a report's target in the following special cases:

| URL Type | Report target(s) |
|---|---|
| References a malvertisement | Advertising network<br>URL owner |
| Domain name employs fast-flux DNS resolution | Domain name registrar<br>Hosting provider(s) at time of detection |
| References SEO content associated with badware | Hosting provider<br>URL owner<br>Search engine(s) exploited by SEO content |
| Hosted on a bulletproof hosting provider | URL owner (only if ordinarily legitimate)<br>Domain name registrar (only if malicious) |

A visual summary of these targeting recommendations can be found in Appendix A.

## Stage 2: Identifying contact information

Reporters should strive to respect the contact preferences of report targets whenever possible. When reporters possess verified contact information for a particular target, they should use it. However, if a reporter does not have pre-existing contact information, we recommend following the steps below to determine contact information for these standard targets:

| Report Target | Sources of contact information |
|---|---|
| URL owner | 1. Technical or general contact information available on the site the URL references<br>2. Technical or (if unavailable) other contact information in domain name WHOIS record<br>3. The **`webmaster@`** and **`abuse@`** email addresses for the URL's domain name. |
| Hosting provider | 1. Abuse or technical contact in WHOIS/RWHOIS record for IP address to which URL resolves<br>2. When hosting provider name can be determined, abuse or technical contact information available on provider website.<br>3. When hosting provider name can be determined, the **`abuse@`** email address for the hosting provider domain name. |
| Domain name registrar | 1. Contact information for registrar in domain name WHOIS record.<br>2. When registrar name can be determined, abuse contact information available on registrar website. |

Email is the most common reporting method; however, reporters may also contact targets by phone, web form, API, or other methods as needed.

## Stage 3: Assembling Report Contents

A report should, at a **minimum**, include:

1. The badware URL(s)
2. The date and time at which you last observed the badware URL(s)
3. The IP address(es) to which the badware URL(s) resolved when last observed
4. A brief description of the nature of badware behavior observed at the URL(s)
5. A list of targets to which you are reporting the badware URL(s) (see stage 1)
6. Contact information that the targets can use to follow up with the reporter

**Additionally**, we recommend that reporters include supplementary information to assist targets in investigating the report. This may include:

- Specific conditions necessary to reproduce the observed/detected behavior (e.g., some drive-by downloads only occur if accessed with a specific HTTP referrer)
- The scope of the behavior (e.g., if you report `http://www.example.com`, are you reporting a problem with the home page or with the entire domain?)
- Data or observations that place the detected/observed behavior in a larger context (e.g., "thousands of websites using this same JavaScript code deliver drive-by downloads")
- Specific malicious code detected at the badware URL(s)
- Additional information about specific malicious executables (e.g., hash, VirusTotal report link)
- Other related URLs, such as those in a redirect chain including the reported URL
- Specific end user applications or operating systems exploited

We recommend that reporters employ the following safeguards when formatting their reports (where applicable):

1. Sanitize badware URLs in the body of each report to reduce the risk that targets will accidentally access them as links.
2. Send all report emails in plain text to reduce the risk of target email clients rendering malicious code excerpts.
3. Do not include attachments when emailing targets for the first time to reduce the risk that the report email will be discarded.

A visual summary of these report content recommendations can be found in Appendix A. Sample reports corresponding to these recommendations can be found in Appendix B.

**Note:** Some reporters may wish to deliver their reports anonymously. Even in these cases, however, reporters must include some form of contact information. The targets can use this information to acknowledge receipt of the report, gauge the report's credibility, ask questions, or follow up after the issue has been addressed.

# Stage 4: Delivery and Follow-Up

Reports should be delivered to all of the initial targets as quickly as possible, ideally as soon as the necessary information is collected. Reporters should keep a record of the date, time, URL(s), and target(s) of each report, as this information will be helpful for escalation (see below), for tracking effectiveness of the reports, and for identifying patterns in both the badware itself and the responsiveness of specific targets.

We recommend that reporters observe the following practices when following up with targets:

1. If using the contact information for a particular target results in a technical error (e.g., undeliverable message), select the next available contact method (see stage 2).
2. If a target indicates that action has been taken in response to a report, verify that the reported badware behavior has been addressed. If the behavior has not been addressed satisfactorily, respond with appropriate evidence of the badware behavior, including network capture logs, screenshots, or other documentary evidence.

If report targets fail to take appropriate action in response to a report within a reasonable time (in the reporter's judgment), it may be appropriate to escalate the report to other targets. We recommend the following escalation targets **(all escalation circumstances assume that the hosting provider has failed to respond satisfactorily)**:

| Escalation Target | Circumstances |
|---|---|
| AS owner<br>for IP address(es) to which URL(s) resolve | • Hosting provider and AS owner are not identical |
| DNS provider<br>for domain name in URL(s) | • Domain name is primarily malicious<br>• Hosting provider and DNS provider are not identical |
| Domain name registry<br>for domain name in URL(s) | • Domain name is primarily malicious<br>• Domain name registrar fails to respond satisfactorily |
| CERT/CSIRT<br>with relevant jurisdiction | • Report reflects a broader pattern of connected attacks<br>• Report is especially serious |
| Law enforcement or regulators<br>with relevant jurisdiction | • Report reflects a broader pattern of connected attacks<br>• Report is especially serious |

Escalation reports should include information from the original report (see stage 3), the date and time the original report was delivered to its targets, and a reason for escalation.

## Conclusion

Effective communication is key to reducing the threat that badware poses to Internet users and to users' trust in the Internet itself. By following these practices, badware reporters maximize the value of their efforts and increase the likelihood that action will be taken quickly. Over time, accurate tracking of reports and their outcomes will help the ecosystem to better evaluate the responsiveness of hosting providers, registrars, and other key players in addressing badware threats. Coupled with other efforts to prevent and react to malicious activity on the Web, adherence to these guidelines will help advance the common goal of protecting the integrity of the Internet for all its users.

## Acknowledgments

These Practices were developed in collaboration with a volunteer working group. Final decisions on the contents of the document and related materials were made by StopBadware. Membership in the working group does **not** imply that the individuals, or their associated organizations, endorse the Practices.

*Working group members:*

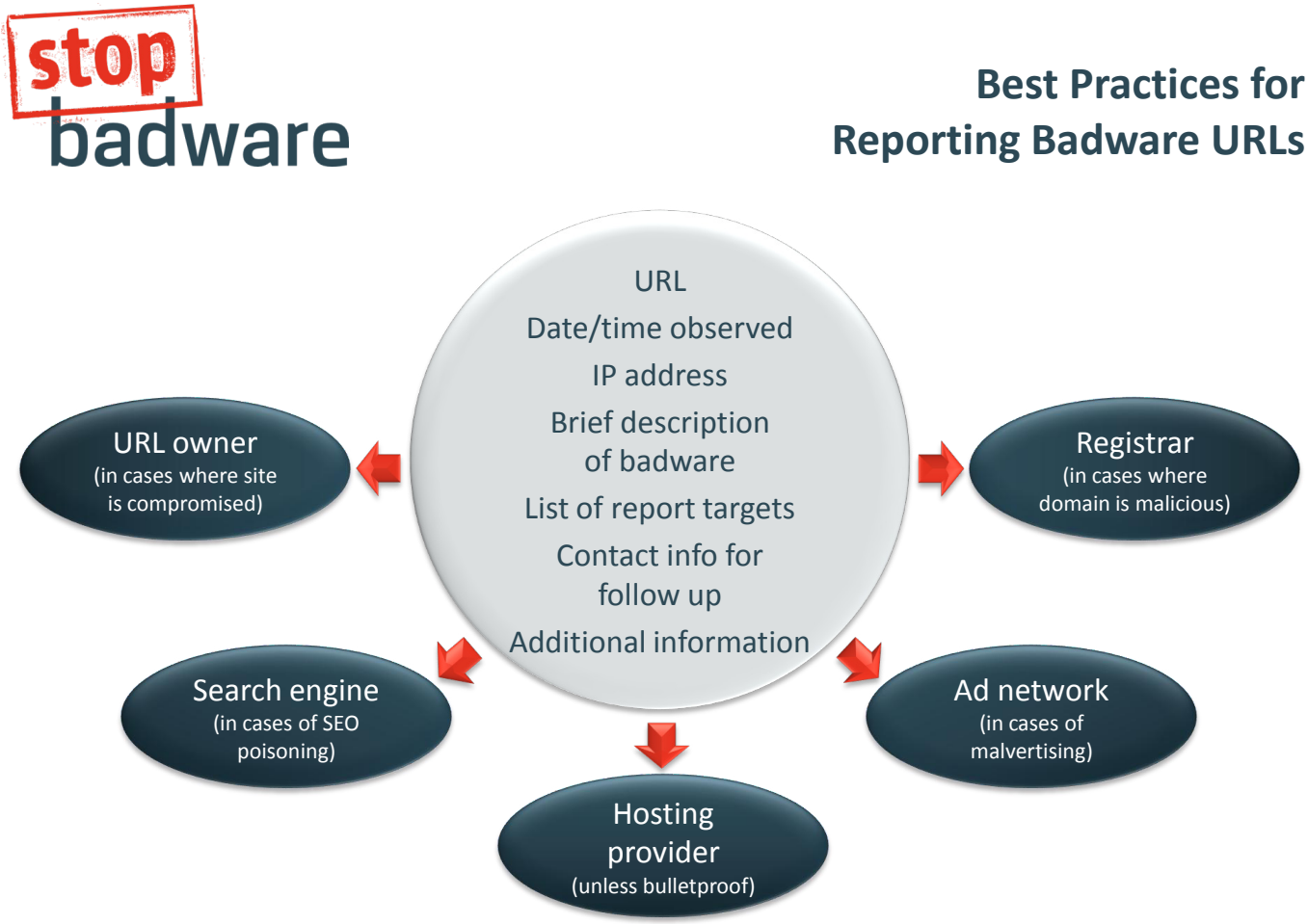
Saeed Abu-Nimeh, Damballa
Jessica Anthony, Network Solutions
Bill Barns, Verizon
Stephan Chenette, Websense
Andre' M. DiMino
Fraser Howard, Sophos
Eric Howes, GFI
Paul Kincaid-Smith, SendGrid
Garrick Lau, Tucows
Ramses Martinez, Yahoo
Brett McDowell, PayPal
Jong Purisima, GFI
Thomas Raef, WeWatchYourWebsite
John Roberts, CloudFlare
William Salusky, AOL
Steve Santorelli, Team Cymru
Jim Schuyler, CyberSpark
Foy Shiver, APWG
Maria Tillero, Verio
Oscar Veras, Verio

*Other contributors:*

Marnie King, Peer1
Joe St Sauver, University of Oregon and Internet2

StopBadware is grateful to the working group members and the other individuals who contributed to the best practices as they evolved into their current form.

# Appendix A: Illustration of Best Practices



# Appendix B: Sample Reports

*Example 1*

**URL**: `http://compromised.example.org/`.
**Badware type**: Injected script that redirects site visitors to `http://malicious.example.net/evilscript.js`. This JavaScript delivers a drive-by download.
**Report targets:** Site owner and hosting provider (`compromised.example.org` appears to be a compromised, legitimate site).
**Contact information:** No contact information is given on the site. A WHOIS lookup of `example.org` yields a technical contact of John Doe, `webmaster@example.org`. The domain name resolves to 10.1.2.3, and a WHOIS lookup yields a hosting provider SAMPLEHOST with abuse contact `abuse@samplehost.example.com`.

**Sample report to URL owner**:

```
To: webmaster@example.org
Subject: Badware URL notification - compromised.example .org

hxxp://compromised.example .org/ is currently being abused to spread badware. It's likely
the domain was infected by a third party without your knowledge. Please take action
to clean up the URL as quickly as possible. For more information about identifying,
removing, and preventing badware, please see http://www.stopbadware.org/home/webmasters.

Description: Embedded JavaScript loads a malicious exploit script from another domain.

Date/time of detection:            15 July 2011 at 1048 EDT
IP address at time of detection:   10.1.2.3
Additional parties notified:       SAMPLEHOST (hosting provider)

You are receiving this report because this was listed as the technical contact email
in the WHOIS record for example .org. If you believe you have received this report in
error, or for more information, please contact us at this address: reporter@organization.
example.

Caution: Opening badware URLs in your browser can infect your computer. For security rea-
sons, 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://compromised.example .org/
Bad Code: <script src="http://malicious.example .com/evilscript.js">
Behavior: Delivers malicious PDF and Flash files
Special conditions: Only redirects when referrer string is set to google.com or another
popular search engine.

Tips for cleaning & securing a compromised website:
http://www.stopbadware.org/home/security
```

# Appendix B: Sample Reports

**Sample report to hosting provider**:

```
To: abuse@samplehost.example.com
Subject: Badware URL notification - compromised.example .org

hxxp://compromised.example .org/ appears to be a badware URL. This means it may be plac-
ing Internet users at risk. Please investigate and take appropriate action to resolve or
mitigate the threat.

Description: Embedded JavaScript loads a malicious exploit script from another domain.

Date/time of detection:            15 July 2011 at 1048 EDT
IP address at time of detection:   10.1.2.3
Additional parties notified:       webmaster@example.org (site owner)

You are receiving this report because this was listed as the hosting provider contact in
the WHOIS record for 10.1.2.3. If you believe you have received this report in error, or
for more information, please contact us at this address: reporter@organization.example.

Caution: Opening badware URLs in your browser can infect your computer. For security rea-
sons, 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://compromised.example .org/
Bad Code: <script src=”http://malicious.example .com/evilscript.js”>
Behavior: Delivers malicious PDF and Flash files
Special conditions: Only redirects when referrer string is set to google.com or another
popular search engine.

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

Contact us about this badware URL report: reporter@organization.example
```

# Appendix B: Sample Reports

*Example 2*

**URL**: `http://malicious.example.net`.
**Badware type**: `http://malicious.example.net/evilscript.js` delivers malicious PDF and Flash files.
**Report targets**: Hosting provider and domain registrar (`malicious.example.net` appears to be a primarily malicious site).
**Contact information**: `malicious.example.net` resolves to 192.168.10.20. A WHOIS lookup of that IP address yields hosting provider WEHATEABUSE, with abuse contact `abuse@wehateabuse.example.com`. A WHOIS lookup of `malicious.example.net` shows that the registrar is Friendly Registrar, Inc. A search for "friendly registrar abuse" finds the email address `abuse@friendlyreg.example.org`.

**Sample report to hosting provider**:

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

hxxp://malicious.example .net/evilscript.js appears to be a badware URL. This means it
may be placing Internet users at risk. We believe that malicious.example.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 pro-
vider contact in the WHOIS record for 192.10.20.30. If you believe you have received this
report in error, or for more information, please contact us at this address: reporter@
organization.example.

Caution: Opening badware URLs in your browser can infect your computer. For security rea-
sons, 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.example .net/evilscript.js
Bad Code: [obfuscated]
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
```

# Appendix B: Sample Reports

**Sample report to domain name registrar**:

```
To: abuse@friendlyreg.example.org
Subject: Badware URL notification – malicious.example .net

hxxp://malicious.example .net/evilscript.js appears to be a badware URL. This means it
may be placing Internet users at risk. We believe that malicious.example.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:       WEHATEABUSE (hosting provider)

You are receiving this report because Friendly Registrar, Inc., is listed as the domain
registrar in the WHOIS record for malicious.example. net, and this email address is list-
ed as the abuse contact for Friendly Registrar, Inc., at http://friendlyreg.example.org/
contact.html. If you believe you have received this report in error, or for more informa-
tion, please contact us at this address: reporter@organization.example.

Caution: Opening badware URLs in your browser can infect your computer. For security rea-
sons, 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.example .net/evilscript.js
Bad Code: [obfuscated]
Behavior: Delivers malicious PDF and Flash files
Special conditions: Only delivers files when referred by a compromised site, such as
hxxp://compromised.example .com.
```