# stop badware

## Best Practices for Web Hosting Providers
**Responding to Badware Reports**

---

### Background

Badware poses a serious threat to the open Internet, and a large and growing share of badware is distributed via websites. Malicious actors may settle on unsuspecting web hosting companies, set up websites with a veneer of legitimacy, and lace their site content with badware or links to badware. These actors may use automated utilities to scan the Web for websites vulnerable to compromise by badware code. This code, once injected, transforms legitimate sites into badware distribution points. In both cases, badware puts the computers and data of site visitors at the mercy of criminals—and when owners of legitimate but compromised sites find their websites compromised, they are subjected to the burdensome and often expensive task of cleaning their sites as well. In addition to the cost of cleaning their sites, such site owners may also suffer a loss of reputation and site traffic due to warnings from search engines and web browsers indicating that such sites are infected. In many cases, neither the site owners nor the users visiting compromised websites have the technical skill to counter such tactics.

Web hosting providers are integral links in the chain of trust that binds the Internet together. They are also uniquely placed to lend assistance to their customers and resellers when badware compromises occur on systems under their control. Typically, they have the necessary control over the network infrastructure, IP address space, physical servers, and software; they have expertise in systems management and an awareness of the importance of computer security; and they are partners in important financial and contractual relationships with their customers.

Nevertheless, it can be difficult for web hosting providers to know how to act as good Internet citizens when forced to confront malicious or compromised websites hosted on their networks. Corporate security experts, independent anti-malware organizations (like StopBadware), security research firms, law enforcement personnel, national CERTs/CSIRTs, and concerned members of the public frequently gather information about these sites and report them to the providers. How web hosting providers respond to these reports makes a meaningful difference in the overall health of the Web and the degree of trust users place in the websites they visit.

# Purpose and Scope

These best practices are designed to provide a best-of-breed framework that web hosting providers can use to respond to badware reports. They are designed to prescribe an overall strategy for receiving and processing the reports, rather than to specify highly specific tactics for providers to employ. They are tailored, as much as possible, to avoid burdening providers unnecessarily while still emphasizing the special responsibility inherent in hosting providers' unique position in the architecture of the Web. Responsible hosting providers of every size, type, and capability can—and should—strive to meet these guidelines.

The practices do not include discussion of proactive—and desirable—measures web hosting providers may take to combat web-based badware, including participation in ongoing badware education campaigns, use of proactive threat monitoring software, and the like. Nor do the practices seek to specify the form reporters should use to report web-based badware to hosting providers. (Note: this may be addressed in a subsequent best practices document.) Instead, the focus is entirely on the actions providers should take in response to badware reports.

StopBadware has included a graphical model of the practices, as well as sample communications providers may use to implement the practices, as appendices to this document. These appendices are intended to be tools, and do not replace the text of the practices themselves. StopBadware has made supplemental materials related to these best practices available on its website at
[http://www.stopbadware.org/home/webhost](http://www.stopbadware.org/home/webhost).

# Definitions

**Badware** is any software that fundamentally disregards users' choices about how their computers or network connections are used.

A **provider** manages or controls infrastructure used to host websites or web applications for third parties. 'Managing or controlling infrastructure' includes such activities as:
- owning and/or operating the autonomous system (AS) on which the site is hosted;
- managing the IP address space used by the server(s) hosting the site, whether by direct allocation or sublease;
- owning and/or operating the physical or virtual server(s) hosting the site;
- controlling and/or maintaining the backend software on server(s) hosting the site, including, as applicable, operating systems, web server software, databases, etc.;
- deploying and/or maintaining public-facing web applications, including content management systems, blogging platforms, etc., for site owners.

A provider's **zone of control** includes all hardware, software, IP address space, and data within the provider's managed infrastructure. Often, contracts or other agreements may empower another

party to manage or control some parts of the infrastructure used to host websites. These parties are **downstream providers**, and providers in their own right. Such downstream providers are often referred to as resellers. From the perspective of such a provider, the empowering party is an **upstream provider.**

A **reporter** is any person or entity making a badware report (hereinafter a '**report**'). At a minimum, a report includes three elements:

1. a URL;
2. a statement or indication that the URL is a report of badware; and
3. a means of contacting the reporter for follow-up.

The term **site** refers to the website that is referenced by the reported URL. The **site owner** is directly responsible for managing the content of the site, and leases or has been otherwise granted the ability to do so by a provider.

# Best Practices

## 1. Acknowledge receipt of reports.

A provider may receive a report via e-mail, a form the provider makes available for receiving abuse notifications, or another communications channel (for example, a dedicated API). Once the provider has received the report, the provider should acknowledge that the report has been received. The provider's acknowledgment should include, at a minimum, the following elements:

a. Acknowledgment that the report has been received;
b. Acknowledgment that the report received is a badware report;
c. A way for the reporter to submit further information relevant to the report.

The acknowledgment need not warrant that the report is relevant to the provider's zone of control, is accurate, or that the provider will (or has a duty to) take any action on the basis of the received report.

In order to allow a reporter to submit further information, the provider may provide the reporter with: a unique report identification number for use in further communication; a specific e-mail address or other point of contact to use for follow-up correspondence; or another method for follow-up specific to the report.

A provider should acknowledge receipt of a badware report as soon as practicable, but no later than one business day following the report's receipt. A sample acknowledgment can be found in Appendix B.

## 2. Evaluate reports in a timely manner.

Once a provider has acknowledged receipt of a report, the provider should evaluate the report and assess what action, if any, the provider should take. A provider should evaluate the report in a timely manner, but no later than two business days following the report's receipt. This time frame does not necessarily include mitigation and/or resolution, as appropriate (see Best Practices 4 and 5).

The criteria used by a provider to determine the courses of action taken should include the following:

a. Does the report apply to the provider's Zone of Control?

   The provider should check each reported URL to determine whether it lives on a site within the provider's Zone of Control. If a provider determines that a URL does not live within its Zone of Control, it should immediately communicate that determination to the reporter. A sample communication can be found in Appendix B.

b. Is the report credible?

   The provider should examine the report to determine whether there is a reasonable chance the report is accurate. The provider should consider a range of criteria, which may include:
   - the form of the report (is it coherent? is it spam?);
   - the level of detail given (does it specify the type of badware observed, or when?);
   - the reputation of the reporter (does the report come from a trusted source?); and
   - whether the report corroborates other reports the provider has received.

   The provider need not take further action if a report is not credible. When a provider deems a report not credible, however, it should note the basis for that determination.

c. What is the appropriate role for the provider to play in resolving a credible reported issue?

   The provider should investigate credible reports to determine what steps the provider may take to resolve the reported badware problem. These roles might include any of the following:
   - identifying and resolving the issue through technical means;
   - providing technical assistance to a downstream provider or site owner so they can resolve the issue;
   - reporting the issue to the downstream provider or site owner; or
   - suspending or cancelling the account of the downstream provider or site owner.

The provider should consider a range of criteria in determining steps it should take, such as:

- whether the issue has been caused by, or can only be resolved by changing, infrastructure under the provider's direct control;
- whether multiple site owners or downstream providers have been affected by the same issue;
- whether the provider possesses technical expertise that the downstream provider or site owner may lack;
- whether the downstream provider or site owner has installed custom code or applications on the provider's infrastructure that caused the issue, or may be affected by resolving the issue;
- how the contractual relationship between the provider and a downstream provider or site owner limits or affects the provider's ability to act;
- any relevant legal or regulatory requirements imposed on the provider;
- whether there is a pattern of non-responsiveness from the downstream provider or site owner; and
- whether there is clear evidence that the site owner or downstream provider is deliberately engaged in distributing or harboring badware (see Best Practices 3, 5 and 6).

To the extent practicable, providers should arrange their contractual relationships (e.g., customer agreements, terms of service) with downstream providers and/or site owners to allow mitigation and resolution of such issues; in no case should a provider be contractually unable to act in extreme cases of non-responsiveness or abuse.

d.  Can the provider temporarily mitigate the effects of the reported issue on site visitors and infrastructure until the issue can be resolved?

Some providers have the technical ability to mitigate the effects of badware infections by taking interim steps to prevent the distribution of badware from sites hosted on their infrastructure. These strategies, in increasing order of intrusiveness, may include:

- filtering outbound network traffic capable of causing direct distribution of, or redirection to, badware code;
- temporarily disabling access to specific pages, files, or services hosted on the provider's infrastructure; and
- temporarily quarantining sites or the servers hosting them.

The provider should consider a variety of factors that may affect a decision to mitigate the effects of the reported infection. These may include:

- the degree of technical access and resources required to mitigate the effect of the badware infection—particularly whether a downstream provider and/or site owner is willing and able to mitigate the effects less intrusively;
- how long the issue will take to resolve;
- the risk of negatively affecting legitimate site content and traffic, balanced with the risk of propagating further badware infection;
- whether temporary mitigation might interfere with resolution (e.g., would quarantining content prevent the site owner from removing the content manually?); and
- how the contractual relationship between the provider and a downstream provider or site owner limits or affects the provider's ability to temporarily mitigate badware.

Providers should maintain a responsive process that allows downstream providers and site owners to request reversal of mitigation measures when the issue has been resolved, if the issue turns out to be a false positive, or if the mitigation causes unintended consequences.

## 3.  Report issues to affected downstream providers or site owners in a timely manner.

After evaluating a report, a provider should transmit the report to the next downstream provider or, if no downstream provider exists, the site owner. Under typical circumstances, site owners should receive reports only from providers that have direct contractual relationships with them.

Reports should be passed on to downstream providers or site owners, as appropriate, in a timely manner, but no later than two business days following receipt of a report. A provider may elect to pass on reports after undertaking initial mitigation or resolution efforts. A provider may bundle reports received separately that affect a particular downstream provider or site owner. A sample report can be found in Appendix B.

Reports passed on by a provider should contain as much information about the reported issue as possible; however, a provider should not reveal the identity of a reporter unless the reporter explicitly requests so. At a minimum, a provider should always include the provider's name, the URL(s) related to the reported issue, and a timestamp of when the report was received; it should also include supplementary information, including:
- any reported or otherwise available information about the nature of the issue (e.g., detected code, any exploits that appear to be in use, details of the badware's behavior, timestamp of when malicious activity was observed, etc.);
- any actions the provider has already taken or intends to take to mitigate or resolve the issue;
- what the downstream provider or site owner is expected to do to address the issue; and
- what resources are available to the downstream provider or site owner to assist them in taking the expected action.

When a provider passes on a report to a downstream provider, that downstream provider should follow these Best Practices to address the situation. When a provider passes on a report to a site owner, the courses of action that a provider suggests may include:
   • resolving the issue;
   • upgrading or patching code;
   • changing passwords or site settings;
   • waiting for further information; and
   • requesting removal of the owner's site from relevant blacklists.

If a provider has reason to suspect that the reported badware infection is a result of the deliberate conduct of a site owner or downstream provider, it should state so explicitly.

**4.  Mitigate, if appropriate, in a narrowly tailored and reversible manner.**

A provider engaging in mitigation after evaluating a badware report (see Best Practice 2) should take steps to prevent the reported badware from affecting Internet users or other systems. For example, a provider may prevent certain code on a site from being served to site visitors, or may disable access to a file that causes site visitors to be redirected to a badware distribution site. Mitigation may not be necessary if the issue can be permanently resolved more quickly than mitigation measures can be put into place.

A provider engaging in mitigation should act in as narrowly tailored a fashion as possible. For example, a provider should only disable access to files containing malicious code, and, if feasible, continue to serve such files but excise the malicious code itself. A provider should communicate the mitigation steps it takes to downstream providers or site owners, as appropriate, as soon as is practicable.

Providers should also make a review process available to site owners and/or downstream providers affected by mitigation actions a provider takes. The process should allow providers to respond quickly and appropriately in case of error, or in the event that mitigation measures cause collateral damage to the site. Providers should ensure that their contractual relationships with downstream providers and/or customers, including Terms of Service, do not prevent mitigation measures that providers deem appropriate.

**5.  Resolve, if appropriate, by removing badware infections and, if applicable, fixing any vulnerabilities enabling those infections.**

A provider engaged in resolution of a badware infection may employ a variety of techniques to eliminate badware and its point of origin, including:

- removing malicious code from files, or malicious files, from the site or server(s) hosting it;
- reversing damage caused to the site or server(s) hosting it, including removal of security backdoors and replacement of modified or deleted files;
- patching or altering systems or processes that allowed the badware to affect the site or server(s) hosting it;
- determining root cause of the event and implementing new systems or rules to detect or prevent similar events in the future; and
- suspending some or all of the site owner's or downstream provider's access privileges, if the party displays manifest bad faith, gross non-responsiveness, or deliberate intent to distribute badware.

Complete resolution may be time consuming and require assistance and cooperation from multiple parties, including downstream providers and/or site owners. A provider should communicate the resolution steps it takes to downstream providers or site owners, as appropriate, as soon as is practicable. When a provider deems it appropriate for a downstream provider and/or site owner to take certain steps, the provider should indicate so explicitly. To the extent possible, steps taken by the provider during resolution should be reversible in case of error and narrowly tailored in scope; to that end, a review process should be available to site owners and downstream providers that enables providers to be responsive to perceived errors or collateral damage caused by the resolution process.

If a provider has determined through its investigation that the reported badware infection is a result of the deliberate conduct of a site owner or downstream provider, termination of the party's account(s) is generally the most appropriate remedy. Additionally, the provider should attempt, using whatever information is available to it, to determine if the malicious customer has other identifiable hosting accounts with the provider.

**6. Notify reporters and/or upstream providers of the disposition of badware reports.**

Providers should notify reporters and/or upstream providers of one or more of the following, as information becomes available:
- that the provider is taking steps to resolve the reported issue;
- that the provider has reported the issue to a downstream provider and/or site owner;
- that the reported issue has been resolved.

Reporters should be notified in a manner consistent with the provider's initial acknowledgment of the report per Best Practice 1 above. A sample notification can be found in Appendix B.

A provider's notification to a reporter or upstream provider should include a method for the reporter or upstream provider to contact the provider if there is reason to believe the reported issue has not been resolved completely or in a timely fashion. The method may be specific, referencing an

identifier similar to the one given to each report per Best Practice 1 above, or a generic invitation to contact the provider's abuse team or other responsible party.

If a provider terminates a site owner's or downstream provider's account due to deliberate abuse, the provider should inform upstream providers to assist in the prevention of future malicious activity. The provider may also consider notifying relevant law enforcement and/or security research organizations.

## 7.  Track the disposition of badware reports.

Providers should track the handling of badware reports, whether the provider engages in mitigation and/or resolution directly or passes on the report to a downstream provider or site owner. For example, a provider may track reports over time by customer, IP address, IP subnet, type of badware, and/or affected server. When providers pass on reports to downstream providers or site owners, providers should further request follow-up information from downstream providers or site owners and note their response(s) or lack thereof. Downstream providers should respond to a provider's request for follow-up per Best Practice 6 above.

When feasible, providers should independently verify resolution by downstream providers or site owners and track successful incident responses.
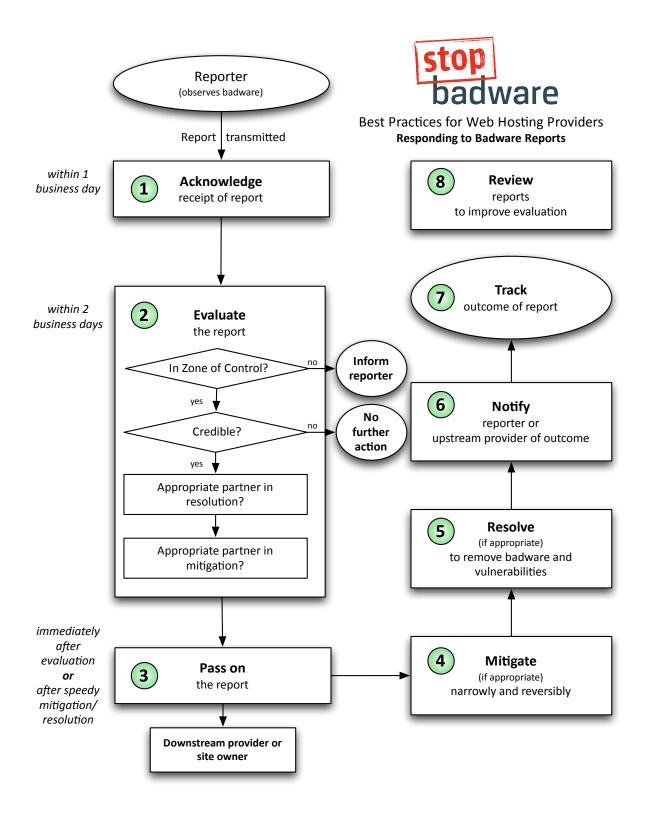
## 8.  Review badware reports to improve effectiveness when processing future reports.

Providers should periodically review previously tracked reports (see Best Practice 7 above). This provides an opportunity to identify patterns of infection and operational lessons that may not be obvious in the midst of addressing individual issues. For example, a specific site owner or downstream provider may repeatedly receive reports about the same site, indicating a failure to secure the site against reinfection. Or a provider may realize that it could save time and money by scanning its servers regularly for a common type of badware.

## Conclusion

The above Best Practices are intended to help underscore how the badware threat, and how web hosting providers cope with it, are collaborative and interconnected issues. The practices, especially combined with provider efforts to proactively detect and prevent badware and to educate their customers, help to create accountability and clarify responsibility within the web hosting ecosystem. Their emphasis on communication also performs a valuable educative function for site owners caught by surprise—and a customer base aware of the risk badware poses will be less likely to get compromised. We are confident that web hosting providers who choose to follow these Best Practices will improve the good order and health of their infrastructure and strengthen the chain of trust that underpins the open Internet.

## Appendix A: Illustration of Best Practices

**Reporter**
(observes badware)

Report transmitted

**stop**
**badware**

Best Practices for Web Hosting Providers
**Responding to Badware Reports**

*within 1 business day*

**1** **Acknowledge**
receipt of report

**8** **Review**
reports
to improve evaluation

*within 2 business days*

**2** **Evaluate**
the report

In Zone of Control? — no → **Inform reporter**

yes

Credible? — no → **No further action**

yes

Appropriate partner in resolution?

Appropriate partner in mitigation?

**7** **Track**
outcome of report

**6** **Notify**
reporter or
upstream provider of outcome

**5** **Resolve**
(if appropriate)
to remove badware and
vulnerabilities

*immediately after evaluation*
***or***
*after speedy mitigation/ resolution*

**3** **Pass on**
the report

**4** **Mitigate**
(if appropriate)
narrowly and reversibly

**Downstream provider or site owner**

# Appendix B: Sample Notifications

Below are four sample notification e-mails consistent with Best Practices 1, 2, 3, and 6, respectively. They are intended as a starting point, as StopBadware recognizes that each Provider will have its own business, legal, and communication needs. The samples are explicitly **not** intended to replace or serve as legal advice.

## Sample Acknowledgement of Report Receipt

Dear Badware Reporter:

We have received your report about possible badware on <URL(s) or "multiple URLs">. If you wish to provide us with additional information related to this report, please <send an email to xxx/reply to this email/include in the subject "Ticket #XXXX/etc.>.

Sincerely,
<Provider>

*<Provider> strives to follow StopBadware's Best Practices for responding to badware reports. <Provider>, however, assumes no liability or responsibility for the actions of any users or any content that such users may place on any website. This communication shall in no way be deemed an agreement, commitment, or promise in any way to take any action in response to your report.*

## Sample Response to Report About URL Not in Zone of Control

Dear Badware Reporter:

This is a response to your recent report about possible badware on <URL(s) or "multiple URLs">. We evaluated your report, and we did not find evidence that the URL(s) <is/are> hosted by <Provider> or within <Provider>'s network.

If you have evidence placing the reported URL(s) within our network, please let us know by <contact method>. Otherwise, please contact the relevant hosting provider(s).

Sincerely,
<Provider>

*<Provider> strives to follow StopBadware's Best Practices for responding to badware reports. <Provider>, however, assumes no liability or responsibility for the actions of any users or any content that such users may place on any website. This communication shall in no way be deemed an agreement, commitment, or promise in any way to take any action in response to your report.*

# Sample Notification to Site Owner

Dear <Provider> customer:

This is an important notification about badware-related activity reported at the following URL(s):

<URL(s)>

<Provider> has received a credible report from a third party that badware activity has been detected at <this/these> URL(s). Even if you did not upload badware yourself, your site(s) may have been compromised without your knowledge. In accordance with <Provider>'s Customer Agreement, you are responsible for keeping your website(s) free of badware. Please read this notice in its entirety for additional information.

Information provided by third-party reporter:

<relevant info, such as type of badware, sample code, description>

What <Provider> has done or plans to do:

Action 1 (e.g., removed malicious code from filename)
Action 2
Etc.

Some things you [can/should*] do:

Action 1 (e.g., update any third-party software in use on your site)
Action 2
Etc.

Resources to help you:

Resource 1 (e.g., StopBadware's Tips for Cleaning & Securing Your Website)
Resource 2 (e.g., <Provider>'s support department)
Etc.

Sincerely,
<Provider>

*<Provider> does not guarantee the accuracy of the report referenced, and assumes no liability or responsibility for the actions of any users or any content that such users may place on any website. This communication shall in no way be deemed an agreement, commitment, or promise in any way to take any action in response to this report.*

*Providers are encouraged to discuss with their attorneys whether they want to mandate specific remedies or simply offer recommended actions.

## Sample Follow-Up Notification to Reporter

Dear Badware Reporter:

Thank you for your recent report of possible badware on <URL(s) or "multiple sites">. After evaluating the report, we <have taken/are taking> the following action(s)  <one or more of following>:

- Passed along the information you provided to the affected <Provider> customer(s).
- Instituted measures to reduce the impact of the reported badware on Internet users.
- Removed badware content from the affected site(s).
- Terminated the affected site(s) or account(s).
- Instituted measures to reduce the risk of similar badware incidents in the future.

<This step/these steps> represent a good faith effort to protect our customers and the Internet public from badware. <Provider>, however, assumes no liability or responsibility for the actions of any users or any content that such users may place on any website. This communication shall in no way be deemed an agreement, commitment, or promise in any way to take any action in response to your report.

If you have further information about the reported site(s)/URL(s), please <contact instructions>.

Sincerely,
<Provider>

# Acknowledgements

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:

Dre Armeda, Sucuri
Anirban Banerjee, StopTheHacker
Ryan Carter, SoftLayer
Neil Daswani, Dasient
Paul Diaz, Network Solutions
André DiMino, The Shadowserver Foundation
Scott Gerlach, Go Daddy
Cecil Goldstein, Team Cymru
Joshua Gruenspecht, Center for Democracy and Technology
Wayne Huang, Armorize
Jack Johnson, Online Trust Alliance
Michael Kaiser, Natl. Cyber Security Alliance
Paul Kincaid-Smith, Verio
Dody Lira, SoftLayer
Brett McDowell, PayPal
Tyler Moore, Center for Research on Computation & Society, Harvard University
John Morris, Center for Democracy and Technology
Nico Popp, Symantec (formerly VeriSign)
Todd Redfoot, Go Daddy
Steve Santorelli, Team Cymru
Jai Saxena, Symantec (formerly VeriSign)
Denis Sinegubko, Unmask Parasites
Craig Spiezle, Online Trust Alliance
Michael Su, Armorize
Maria Tillero, Verio
Alan Wallace, Trend Micro
Jamz Yaneza, Trend Micro
Fyodor Yarochkin, Armorize

StopBadware is grateful to the working group members, to Tucows for its support during the Practices' development, and to the many other individuals that provided feedback as the Practices evolved into their current form.