

FIRST WORKING DRAFT
FOR PUBLIC COMMENT

StopBadware's Best Practices for Web Hosting Providers:
Responding to Malware Reports

Introduction

Malware poses a serious threat to the open Internet; a large and growing share of malware is distributed via websites. Sometimes malicious actors settle on unsuspecting web hosting companies, set up websites with a veneer of legitimacy, and lace their site content with malware or links to malware. Sometimes these actors use automated utilities to scan the Web for websites vulnerable to compromise by malware code. This code, once injected, transforms legitimate sites into malware distribution points. In both cases, malware puts the computers and data of site visitors at the mercy of criminals; and when legitimate site owners find their websites compromised, they are subjected to the burdensome and often expensive task of cleaning their sites as well. 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 well placed to lend assistance to their customers and resellers when malware 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, 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 help of the Web and the degree of trust users place in the websites they visit.

These best practices are designed to provide a best-of-breed framework that web hosting providers can use to respond to malware 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. We believe that they set goalposts that hosting providers of every size, type, and capability can—and should—strive to meet.

The practices exclude discussion of proactive measures web hosting providers may take to combat web-based malware, including participation in ongoing malware education campaigns,

FIRST WORKING DRAFT FOR PUBLIC COMMENT

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 malware 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 malware reports.

Definitions

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.

A **reporter** is any person or entity making a malware report (hereinafter a ‘**report**’). At a minimum, a report includes two elements:

1. a URL, and
2. a statement or indication that the URL is a report of malware.

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.

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:

FIRST WORKING DRAFT
FOR PUBLIC COMMENT

- a. Acknowledgment that the report has been received;
- b. Acknowledgment that the report received is a malware 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.

2. Evaluate reports in a timely fashion.

Once a provider has acknowledged receipt of a report, the provider should assess the report and what action, if any, the provider should take. The criteria used by a provider to determine the courses of action taken should include the following:

1. 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. A provider need not take further action if the report does not apply to its Zone of Control.

2. 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 malware observed, or when?)
- the reputation of the reporter (does the report come from a trusted source?)
- 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. (See Best Practice 6 below for further discussion.)

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

FIRST WORKING DRAFT
FOR PUBLIC COMMENT

The provider should investigate credible reports to determine what steps the provider may take to resolve the reported malware problem. These roles might include any of the following:

- 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;
- whether there is a pattern of deliberate abuse and/or a pattern of non-responsiveness from the downstream provider or site owner.

To the extent practicable, providers should not arrange their contractual relationships with downstream providers and/or site owners to preclude resolution of such issues; in no case should a provider be contractually unable to act in extreme cases of abuse or non-responsiveness.

4. 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 malware infections by taking interim steps to prevent the distribution of malware 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, malware 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.

FIRST WORKING DRAFT
FOR PUBLIC COMMENT

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 malware 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 malware infection
- whether temporary mitigation might interfere with resolution (e.g., would quarantining content prevent the site owner from removing the content manually?)
- how the contractual relationship between the provider and a downstream provider or site owner limits or affects the provider's ability to temporarily mitigate malware

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. 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.

Reports passed on by a provider should contain as much information available about the reported issue as possible. At a minimum, a provider should always include the provider's name and the URL(s) related to the reported issue; 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 malware's behavior, 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

FIRST WORKING DRAFT
FOR PUBLIC COMMENT

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
- requesting removal of the owner's site from relevant blacklists

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

A provider engaging in mitigation after evaluating a malware report (see Best Practice 2) should take steps to prevent the reported malware 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 malware 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.

Providers should also make a review process available to site owners and/or downstream providers. 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.

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

A provider engaged in resolution of a malware infection may employ a variety of techniques to eliminate malware 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;
- requesting removal of the site from malware blacklists, such as Google's Safe Browsing blacklist;
- patching or altering systems or processes that allowed the malware to affect the site or server(s) hosting it;
- implementing new systems or rules to detect or prevent similar events in the future;
- suspending some or all of the site owner's or downstream provider's access privileges, if

FIRST WORKING DRAFT
FOR PUBLIC COMMENT

the party displays manifest bad faith or gross non-responsiveness.

Complete resolution may be time consuming and require assistance and cooperation from multiple parties. 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 that enables providers to be responsive to perceived errors or collateral damage caused by the resolution process.

6. Track the disposition of credible malware reports.

Providers should track the handling of credible malware 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 malware, 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 7 below.

When feasible, providers should independently verify resolution by downstream providers or site owners and track successful incident responses.

7. Notify reporters and/or upstream providers of the disposition of malware 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 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 be a generic invitation to contact the provider's abuse team or other responsible party.

8. Review malware reports to improve effectiveness when processing future reports.

Providers should periodically review previously tracked reports (see Best Practice 6 above). This provides an opportunity to identify patterns of infection and operational lessons that may

FIRST WORKING DRAFT
FOR PUBLIC COMMENT

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 malware.

Conclusion

The above Best Practices are intended to help underscore how the malware threat, and how web hosting providers cope with it, is a collaborative and interconnected issue. The practices, especially combined with provider efforts to proactively detect and prevent malware 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 malware 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.