


**Paperwork Reduction Act**

The public reporting burden to complete this information collection is estimated at 1 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and the completing and reviewing the collected information. The collection of information is voluntary. An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a currently valid OMB control number and expiration date. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to DHS/NPPD/CS&C/NCCIC/US-CERT, 245 Murray Lane, SW, Mail Stop 0640, Arlington, VA 20598-0640 ATTN: PRA [OMB Control No. 1670-NEW].

**Malware Analysis Submission Form**

<https://www.malware.us-cert.gov/MalwareSubmission/pages/submission.jsf>

Browser window showing the US-CERT AMAC Malware Analysis Submissions page. The address bar displays <https://mal...> and the page title is "US-CERT AMAC Malware A...".



# US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

## US-CERT AMAC Malware Analysis Submissions

**Web Disclaimer**

By submitting malware artifacts to the Department of Homeland Security's (DHS) United States Computer Emergency Readiness Team (US-CERT), submitter agrees to the following:

Submitter requests that DHS provide analysis and warnings of threats to and vulnerabilities of its systems, as well as mitigation strategies as appropriate.

Submitter has obtained the data, including any electronic communications, and is disclosing it to DHS consistent with all applicable laws and regulations.

Submitter acknowledges that DHS's analysis is for the purpose of identifying a limited range of threats and vulnerabilities. Submitter understands that DHS makes no warranty that information provided by DHS will detect or mitigate any particular threat or vulnerability.

Submitter agrees that the U.S. Government, its officers, contractors, and employees are not liable or otherwise responsible for any damage resulting from the implementation of any guidance provided.

Submitter understands that DHS may retain data submitted to it and use it, alone or in combination with other data, to increase its situational awareness and understanding of cybersecurity threats; that DHS may share data submitted to it with other cybersecurity centers in the US Government; that DHS may, from time to time, derive from submitted data certain indicators of malicious activity related to cybersecurity, including but not limited to Internet Protocol (IP) addresses, domain names, file names and hash/digest values; and that DHS may issue warnings to the public about the malicious nature of such indicators, in a way that is not attributable to submitter.

Submitter agrees to the terms above

(All fields are optional)

First Name

Last Name

Organization

Open Incident ID

Phone Number

Email Address

Select file

Comments

**Privacy Act Statement:**

**Authority:** 5 U.S.C. § 301 and 44 U.S.C § 3101 authorize the collection of this information.

**Purpose:** The primary purpose for the collection of this information is to allow the Department of Homeland Security to contact you regarding your request.

**Routine Uses:** The information collected may be disclosed as generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act of 1974, as amended. This includes using the information as necessary and authorized by the routine uses published in DHS/ALL-002 - Department of Homeland Security (DHS) Mailing and Other Lists System November 25, 2008, 73 FR 71659.

**Disclosure:** Providing this information is voluntary, however, failure to provide this information will prevent DHS from contacting you in the event there are questions regarding your request.

[Privacy Policy](#)