Network Working Group
Internet-Draft
Updates: 6376 (if approved)
Intended status: Informational
Expires: 29 May 2020

J.R. Levine
Taughannock Networks

26 November 2019

A Message Header to Identify Subscription Form Mail
draft-levine-mailbomb-header-02

Abstract

Many organizations have web forms that provoke an e-mail confirmation to the e-mail address provided in the form. Malicious entities do bulk form submissions with forged addresses, resulting in mail floods to the holders of those addresses. This document defines a message header to identify mail sent in response to web forms, so that recipient mail systems can better recognize and mitigate the mail floods.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 29 May 2020.

Table of Contents

1. Introduction

Discussion Venue: For the time being, discussion about this draft is directed to the collaboration@mailman.m3aawg.org (mailto:collaboration@mailman.m3aawg.org) mailing list.

Many organizations have web forms that provoke an e-mail confirmation to the e-mail address provided in the form. Malicious entities submit multiple forms with forged addresses, resulting in mail floods to those addresses. We define a message header that identifies mail sent in response to web forms, so that recipient mail systems can better recognize and mitigate the mail floods.

Mail systems that recognize a mail flood may defer or reject the mail. We also define an SMTP enhanced status code that a mail system can use in a message rejection SMTP reponse to alert the sending system that the message was rejected due to being part of a mail flood.

2. Conventions

The terms Message Submission Agent (MSA) and Message Transfer Agent (MTA) are defined as in [RFC5598].

The ABNF [RFC5234] terms CRLF, FWS, and fields are imported from [RFC5322].

3. The Form-Sub header field

A MSA or an initial MTA adds a Form-Sub header field to indicate that the message was sent in response to a web form submission. The header consists of a semicolon-separated list of tag=value pairs. The first tag-value pair is "v=1" to indicate that the header uses the initial version of this specification. Receivers should ignore Form-Sub headers with a v= tag that indicates an unknown version. Subsequent tag-value pairs are optional, and receivers should ignore pairs with unknown tags.

The tags ip4 or ip6 contain the IPv4 or IPv6 address, respectively, from which the web form was submitted. The address may be partially redacted for privacy reasons, by replacing groups of digits with the letter "x", for example, 198.51.x.x or 2001:DB8::x or x::1234:abcd:5678:ef01. If the sender cannot determine the submitting IP address, it can include "ip=none". The goal of including the IP address is to help receiving mail systems recognize when a cluster of messages was provoked by the same submitter. Using "x" rather than a hash of the the address provides a redaction that cannot be reversed but still can be correlated among multiple messages.

```
ABNF:

fields =/ "Form-Sub:" FWS "v=1" *(FWS ";" FWS fsarg) CRLF

fsarg = "ip4=" ip4redacted
ip4redacted = IPv4 address with parts optionally replaced by "x"

fsarg =/ "ip6=" ip6redacted
ip6redacted = IPv6 address with parts optionally replaced by "x"

fsarg =/ "ip=none"

fsarg =/ x-fsarg

x-fsarg =/ ALPHA *(ALPHA / DIGIT) "=" tagdata
tagdata = string of VCHAR excluding quote and semicolon
```

The Form-Sub header should be included within the set of the headers signed by any DKIM [RFC6376] signature headers.

4. Mail flood enhanced status code

A mail receiver may choose to defer or reject mail that it recognizes as part of a mail flood. It can include the enhanced status code X.7.28 to indicate that the rejection is due to the message being part of a mail flood that includes Form-Sub headers.

A sender would typically interpret the code as a strong hint that their systems are being abused, so they should mitigate the abuse to stop the mail flood.

5. Security Considerations

IP addresses are sometimes considered to be personally identifable information. This specification allows partially redacted addresses as a compromise to avoid identifying individual persons, while still providing receivers a hint to recognize bulk submissions by the same party.

The Form-Sub header discloses information from a sender to a receiver, and the X.7.28 enhanced status code discloses information from a receiver to a sender that they would not otherwise have. If one party suspects the other is malicious, e.g., a receiver fears that a sender is probing to see what its mail volume limits are, it might not include the header or the status code for the possibly malicious other party.

6. IANA Considerations

IANA has updated registries as follows.

6.1. Provisional Message Header Registry

The following value has been added to the Provisional Message Header Registry

Header Field name	Template	Protocol	Status	Reference
Form-Sub	.	mail	.	(this document)

Table 1: Provisional Message Header Registry Added Value

6.2. Enhanced Status Codes

The following value has been added to the Enhanced Status Codes Enumerated Status Codes Registry

Code	Sample Text	Associated Basic Status Code	Description	Reference	Submitter	Change Controller
X.7.28	Mail flood detected	.	The message appears to be part of a mail flood of similar abusive messages.	[this document]	J. Levine standards@taugh.com	

Table 2: Enumerated Status Codes Registry Added Value

7. Acknowledgments

Kurt Andersen and the M3AAWG Collaboration Committee provided the good parts.

8. Normative References

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <https://www.rfc-editor.org/info/rfc5234>.

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, DOI 10.17487/RFC5322, October 2008, <https://www.rfc-editor.org/info/rfc5322>.

[RFC5598] Crocker, D., "Internet Mail Architecture", RFC 5598, DOI 10.17487/RFC5598, July 2009, <https://www.rfc-editor.org/info/rfc5598>.

[RFC6376] Crocker, D., Ed., Hansen, T., Ed., and M. Kucherawy, Ed., "DomainKeys Identified Mail (DKIM) Signatures", STD 76, RFC 6376, DOI 10.17487/RFC6376, September 2011, <https://www.rfc-editor.org/info/rfc6376>.

Appendix A. Change log

01 to 02 Convert to v3 xml

00 to 01 Fix ABNF to allow arbitrary tags. Fix typos.

Author's Address

John Levine
Taughannock Networks
PO Box 727
Trumansburg

Email: standards@taugh.com