Messaging, Malware and Mobile Anti-Abuse Working Group

M^{3}AAWG Companion Document: Calendar operator practices — Guidelines to protect against calendar abuse

Version: 1.0

October 2018

The direct URL to this paper is: www.m3aawg.org/dns-crypto-recipes

This document is intended to accompany and complement the companion document, "M^3 AAWG Tutorial on Third Party Recursive Resolvers and Encrypting DNS Stub Resolver-to-Recursive Resolver Traffic" (www.m3aawg.org/dns-crypto-tutorial).

This document was produced by the M^3 AAWG Data and Identity Protection Committee.

Table of Contents

Warning for Drafts

This document is not an M3AAWG Standard. It is distributed for review and comment, and is subject to change without notice and may not be referred to as a Standard. Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Messaging, Malware and Mobile Anti-Abuse Working Group

781 Beach Street, Suite 302
San Francisco
California 94109
United States of America

www.m3aawg.org

Foreword

The Calendaring and Scheduling Consortium ("CalConnect") is global non-profit organization with the aim of facilitating interoperability of technologies across user-centric systems and applications.

CalConnect works closely with liaison partners including international organizations such as ISO, OASIS and M3AAWG.

The procedures used to develop this document and those intended for its further maintenance are described in the CalConnect Directives, and in this case, also aligned with the procedures used at M3AAWG.

In particular the different approval criteria needed for the different types of CalConnect documents should be noted. This document was drafted in accordance with the editorial rules of the CalConnect Directives.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CalConnect shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the CalConnect list of patent declarations received (see www.calconnect.com/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

This document was prepared by Technical Committee *CalConnect TC CALSPAM*.

Authors:

Thomas Schäfer, 1&1 Mail&Media Development and Technology GmbH

Jesse Thompson, University of Wisconsin-Madison

Introduction

Rise of calendar spam

"Calendar spam" — unsolicited, or otherwise unwanted, calendar events and meeting invitations — is a recently exploited channel for abuse aimed at users of calendaring & scheduling systems.

It is a new form of application-specific spam which takes advantage of the application layer across multiple technologies that spans scheduling, calendaring and messaging systems.

As is the case with email spam, calendar spam is not only used to deliver unwanted information, but can also be used for malicious purposes such as phishing attempts and delivering dangerous payloads.

Because calendar events and meeting invitations are often (but not exclusively) transported and delivered via email, combatting calendar spam requires awareness, intervention and integration with email systems and services.

Impact of calendar spam

Calendar spam is unique in a number of ways:

a) Calendar spam, unlike email, can be placed chronologically anywhere in calendars, in the past or the future, not just the present, making it difficult for the end-user to detect at the time of delivery.

b) Spam meeting invitations, may automatically see these unwanted invitations added to their calendar without their consent, with notifications sent to all their devices. These invitations are not only difficult to find, but in some cases there is no way for the user to remove these events short of deleting the entire calendar.

c) Calendar events and meeting invitations do not yet carry the rich provenance which today accompanies email (detailed header information), making it difficult to ascertain where and when events originated and were delivered.

d) Calendar events often contain notifications/alarms which are propagated across a user's desktop and mobile calendaring clients. It is common for users to have multiple calendaring clients which exacerbates the abuse.

e) Calendar events can include recurrence meaning that one event can show up in the user's calendar multiple times with multiple notifications/alarms being triggered over time.

Acknowledgements

The editor of this document wishes to thank the experts of CalConnect — the Calendaring and Scheduling Consortium and attendees of the M3AAWG conference sessions about the topic, as well as the following individuals who have participated in the drafting, review, and discussion of this document:

Arne Allisat, Bron Gondwana, Andrew Laurence, Andrey Maevsky, Gary Schwartz, Dave Thewlis and Ronald Tse

1. Scope

This document specifies guidelines for calendar and mail system operators to:

- detect the occurrence of calendar abuse;
- consider processes and procedures to mitigate calendar abuse; and
- suggest acceptable (non-abusive) practices with calendar usage.

2. Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IETF RFC 6047, *iCalendar Message-Based Interoperability Protocol (iMIP)*

IETF RFC 5546, *iCalendar Transport-Independent Interoperability Protocol (iTIP)*

3. Terms, definitions and abbreviated terms

For the purposes of this document, the following terms and definitions apply.

3.1. Terms and definitions

3.1.1.

calendar spam
calendar events and meeting invitations containing *spam* (Clause 3.1.3) delivered through *calendar systems* (Clause 3.1.5)

3.1.2.

calendar abuse
malicious usage of a *calendar system* (Clause 3.1.5), possibly leading to an *attack* (ISO/IEC 27000:2018, Clause 3.2) on the receiving user

3.1.3.

spam
unsolicited or unwanted information

3.1.4.

attack
attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset

[ISO/IEC 27000:2018]

3.1.5.

calendar system
information system that provides calendar and scheduling functionality for user accounts

3.1.6.

mail system
information system that provides electronic mail functionality

3.1.7.

user system
information system that provides authentication and authorization functionality

3.2. Abbreviated terms

ARF	Abuse Reporting Format
DNSBL	Domain Name System-based Blackhole List
iMIP	iCalendar Message-Based Interoperability Protocol (see IETF RFC 6047)
iTIP	iCalendar Transport-Independent Interoperability Protocol (see IETF RFC 5546)

SMTP	Simple Mail Transfer Protocol (see IETF RFC 2821)
URIBL	Realtime URI Blacklist

4. Calendar spam and its delivery path

4.1. General

Calendar spam and calendar abuse originates at the OSI application layer but also travels across multiple application layer technologies through networked hosts.

Best practices used at the various checkpoints that a calendar spam instance encounters within its delivery path are described in clauses that follow.

4.2. Information systems involved in calendar abuse

4.2.1. Calendar system

The calendar system plays a crucial role in calendar abuse, where it allows creating, editing and deleting events as well as scheduling events between different user accounts, including user accounts from other calendaring systems.

The calendar system should apply state-of-the-art methods to prevent calendar spam being sent from and received by user accounts on their system.

NOTE: The term “calendar system” in this document specifically refers to calendaring systems that fulfill the requirements of calendaring standards.

4.2.2. Email system

The email system is an important factor in calendar abuse as a delivery mechanism.

In calendar systems, the most common method to send calendar invitations to user recipients is iMIP (IETF RFC 6047), a way of exchanging iTIP (IETF RFC 5546) messages through email.

iTIP (and iTIP) are mechanisms that allow users of different calendar systems to communicate with one another, by delivering calendar event information through email.

EXAMPLE User A on a calendar system can invite another user B that does not belong to the same calendar system, to a calendar event, where the invitation information is sent through email to user B, either by user A or user A’s calendar system.

Email systems are also used to transport information relevant to the calendar event from organizers to attendees of events.

The email system should apply state-of-the-art methods to prevent calendar spam being sent by and received from user accounts on their system.

4.2.3. Related systems

Calendar and email systems are often connected with, and rely on, other information systems, such as identity management systems for authentication and authorization.

When a system depended on by the calendar system is compromised, such as through the creation of malicious user accounts, the dependent calendar (and perhaps email) systems are also affected. For example, the malicious user accounts may be used to send out calendar abuse.

These related systems should implement security best practices to protect systems that are dependent on them, such as, the calendar system.

EXAMPLE An identity management system should protect its user accounts from malicious actors; prevent registration of fake, bot or spam user accounts; and adopt strong authentication methods such as two-factor authentication.

5. Mitigating calendar abuse at source

5.1. General

Calendar spam may be produced by innocent calendar systems when:

- its users were compromised;
- it contains abusive users (such as a free-of-charge hosting provider).

In the latter case, approaches such as automation ("bots") can exacerbate the issue with the automated creation of free accounts.

Such user accounts can be readily used to create calendar spam events:

a) The malicious user account inserts spam content into a newly created calendar event;

b) The calendar system uses templating to send an email invitation with the calendar event attached;

c) The event content, which contains spam, will be inserted into body of the email.

The "source" calendar system provider should take steps to detect and mitigate such internal abuse, by placing detection mechanisms and automated responses at its calendar system and its email system associated with calendar event delivery.

5.2. Source calendar system

The source calendar system is where an calendar abuse instance originates from.

The source calendar system can apply the following best practices:

a) abuse detection should be performed, through channels such as:

   1) user interface and input detection, such as user agent checks;

   2) network origination, such as network addresses and IPs; and

   3) user behavior such as click rate.

b) detection of malicious content for typical spam patterns, before event creation and the subsequent sending of email invitations, by checking event content, such as:

   1) subject;

   2) description;

   3) recurrence;

   4) number of attendees; and

   5) links.

A number of potential actions can be invoked once potential spam is detected, such as:

a) deny the sending of the calendar invite;

b) display of errors and feedback at the user interface;

c) alert the owner of the user account in case the user account has been hijacked;

d) application of rate limiting to prevent automated spamming;

e) implement automation detection measures, such as usage of a CAPTCHA prior to sending an invitation; and

f) blocking the user account altogether.

5.3. Electronic mail system (SMTP)

The source electronic mail system is where the calendar system delivers an event invitation to for its forwarding.

The following mitigation measures should be taken at the electronic mail system:

a) abuse detection for SMTP access should be performed based on input, such as:

    1) network patterns of the originator;

    2) DNSBL checks against the originating IP.

b) detection of spam content patterns of the email message, using standard email anti-spam scanning applications:

    1) scanning for malicious content;

    2) detection of blacklisted and/or known phishing URLs.

A number of potential actions can be invoked once potential spam is detected, such as:

a) bounce the email that contains suspected calendar spam;

b) silently discard the email with suspected calendar spam;

c) communicate with the upstream calendar provider to indicate potential abuse; and

d) communicate with downstream email providers who will be receive the potential spam.

6. Mitigating calendar abuse at destination

6.1. General

Calendar spam events are typically received by recipients in two ways:

a) via email from an external email system; or

b) directly from another account within the same calendar system the recipient resides on.

NOTE: The case of a same-system account abuse can apply when the calendar system contains compromised accounts.

Calendar spam events originating from a calendar system may be propagated back to its own accounts through different channels, depending on their method of integration, such as:

- from within the calendar system, where the event did not leave the calendar system; or
- delivered through email, where the event was sent by the calendar system to an internal email system, and re-routed back to the originating calendar system.

System providers at the receiving end should therefore take steps to detect and mitigate abuse originating from both external and internal calendar and mail systems.

6.2. Electronic mail system

The following best practices apply:

a) abuse detection for receiving email by analyzing input, such as:

   1) originating network addresses;

   2) content of the mail header and its structure.

b) analysis of email spam content patterns using standard email anti-spam scanning applications, such as through:

   1) checking of DNSBLs; and

   2) checking of URIBLs.

c) checking email header content against internal and external sources, such as:

   1) verification of sender address reputation using the `From:` address;

   2) detection of known malicious addresses from security advisories;

   3) determining whether the organizer has been whitelisted.

Actions to be taken when potential spam is detected are provided below:

a) bounce the message;

b) silently discard the message;

c) pick out the message into quarantaine;

d) moving the message into the spam folder.

When potential spam is detected, “interaction” (e.g. adding the event to the end-user’s calendar) between the recipient and the sender at the calendar system shall not proceed.

Certain mitigation actions, such as the silent discard of an email, do not provide any feedback to the originating calendar system. This means that there will be no method for the originator of the calendar event to learn of these events and handle them in the case of false positives.

Therefore, these actions should only be taken if the electronic mail system is very certain about the calendar invitation being an abuse instance or spam.

For some of the milder actions (e.g. putting in spam folder), the calendar system should provide options to the recipient user. For example, the recipient user can mark such emails as false positives, and are able to manually insert them into the user’s calendar.

7. Interactions between the calendar system and the mail system

Interaction between the electronic mail and calendar systems should follow these principles:

a) interaction between these systems should only be triggered for emails not already identified as spam, i.e. anti-abuse measures have already been applied on both systems independently;

b) calendar invitations should be analyzed and categorized by the calendar system to leverage its domain knowledge on calendar event information, which is necessary for a detailed analysis that takes into account calendar event data structures not understandable to electronic mail systems;

c) calendar event content should be checked for spam patterns in its text fields, such as the fields of subject, description, recurrence and links, to determine the likelihood of it being spam;

d) depending on the likelihood of being spam, spam handling options should be offered to the user directly, such as:

  - the automatic insertion of organizers on a whitelist or address book;
  - the state of this event in availability of calendar (e.g. free, conditional or blocked).

When spam is detected during the interaction stage, a number of mitigation actions can be taken, such as:

a) do not automatically insert the calendar event into the user's calendar; or

b) deactivate calendar event notifications for this calendar event.

7.1. Calendar user application

The calendar user application, as part of the "calendar system", should offer the following functionality relating to calendar abuse:

a) allow the user to delete unwanted events (e.g. "Mark as spam"), without notifying the organizer as normally performed with calendar events;

b) submission of ARF reports to report calendar abuse;

c) store information on how a particular calendar event was inserted into the users calendar (e.g. by tracking the `Message-ID` attribute), to be able to inform the user such information and provide additional information to the originating calendar system on abuse.

In addition, further actions can be taken to detect calendar spam at the calendar user application, such as:

a) sending an email feedback loop if the original email that carried the calendar invitation and its `MailID` is still available.

8. Other ways calendar spam occur

8.1. Subscription to shared calendars

Malicious events can end up in user calendars through shared calendars.

Shared calendars are have a single origin and users are subscribed to its events, and therefore manipulation of the calendar source will impact all its subscribers.

Popular calendars, such as official calendars (e.g. public and bank holidays), schedules of shows and sports teams, are valuable targets for malicious actors.

Disturbingly, very often calendar applications do not allow deletion of such shared events if the subscription is set to “read-only”. This means that malicious events propagated through such calendars may not even be eligible for recipient removal, which adds salt to injury.

The only approach for users of these calendar applications are to unsubscribe the entire calendar, even though all previous events will be deleted from the user’s calendar when unsubscribed. More robust controls are certainly needed for calendar subscribers.

8.1.1. iTIP

Calendar systems using iTIP for direct communication between each other, e.g. within the same calendar system, should consider and implement anti-abuse best practices as described above.

9. Conclusion

Spam is a long-standing and well-known email problem. Because email is a commonly used transport for calendar (“meeting”) invitations and events, spammers are now using these calendar events and invitations as a spam vector. Consequently, knowledge of both domains is required to develop defenses against these attacks.

This document provides email and calendar system operators with an introduction to calendar spam, and highlights best practices for identifying and mitigating calendar spam. Implementation details will largely be system-specific.

The “war” against malware, including spam, is dynamic and ever-changing. As a result, email and calendar system experts will need to share their expertise and experiences with each other on an ongoing basis. CalConnect’s collaboration with M3AAWG represents the first formal collaboration in this area.

Appendix A
(informative)
Technical information

A.1. Structure of a best practice iMIP message containing an event

An email message should only contain a single iCalendar attachment (an iMIP file).

NOTE 1: Current practice allows attaching multiple iCalendar attachments to a single email.

The recommended MIME/`multipart` structure of an email that contains a calendar event invitation, optimized for interoperability, is provided as follows:

- a single `multipart/mixed` part, which contains:
  - a single `multipart/alternative` part, which contains:
    - a `text/plain` part; and
    - a `text/html` part;
  - a `text/calendar` part with `method=REQUEST`; and
  - an `application/ics` part, with a `content-disposition:attachment`, in `BASE64` encoding

This recommended structure was devised through interoperability testing with multiple existing implementations.

NOTE 2: A calendar system that conforms to calendaring standards produces an email structure similar to that above.

Guidelines on this structure:

- The filename of the `application/ics` part should end with the `.ics` file extension.
- Some calendar user applications will only see the part with the standard `text/calendar content-type` and the `method` header.
- Some calendar user applications are only able to see attached parts with `application/ics` (this is non-standard behavior).
- Some calendar systems automatically insert links within the HTML part, which can be used by email clients that are not calendar-aware to accept or decline an invitation without having to process the calendar parts. In this case, the server simply updates the `ORGANIZER's copy of the event based on the link clicked.
- The `text/plain` and `text/html` part of the message in the body will include information of the event, such as its subject and description.
- An email using the provide structure does not preclude spammers from inserting malicious content outside of the attached files—all parts of the email should still be parsed to detect malicious content.

Bibliography

[1] ISO/IEC 27000:2018, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

[2] IETF RFC 2821, *Simple Mail Transfer Protocol*

As with all M3AAWG documents that we publish, please check the M3AAWG website (www.m3aawg.org) for updates to this paper.