Calendar Spam

Thomas Schäfer @ CalConnect XLIII Conference Karlsruhe

09/26/2018

wsdwl

CalConnect & M3AAWG & calendar spam

Nov 2016	Jan 2017	June 2017	Oct 2017	Feb 2018	April 2018	June 2018
recent re-occurrence	Definition @CalConnect	first panel discussion @ M3AAWG 40	Guest @ M3AAWG 41	joined work in TC CALSPAM started	official liaison announced	first draft of BCP

TC CALSPAM

- Goal:

  The goal of this TC is to better protect users from receiving undesired information delivered through calendar systems, which currently range from spam to phishing attacks.

- Deliverable:

  Provide best common practice for mail and calendar service providers

- Charter:

  https://github.com/CalConnect/public/blob/master/charter/charter-TC-CALSPAM.md

Who is engaged?

- Chair and main editor:
    - Thomas Schäfer (1&1/CalConnect)

- Active participation:
    - Jesse Thompson (UW Madison/M3AAWG)
    - Arne Allisat (1&1/M3AAWG)
    - Andrey Maevsky (Cyren/M3AAWG)
    - Andrew Laurence (UC Irvine/CalConnect)
    - Bron Gondwana (FastMail/M3AAWG/CalConnect)

calendar spam is different

- Events are often automatically inserted in calendar for convenience reasons

- Events can be placed in the future

- Hard to tell, where and when events originated and were delivered

- Contain or trigger notifications/alarms in clients

- Can include recurrence -> multiply the annoyance

Some numbers

Definition	UW Madison (MS 360)		Cyren	
	May 18	Sept 18	May 18	Sept 18
Ratio clean calendar/mail	0,2 %	0,2 %	0,12 %	0,09 %
Ratio calendar spam/clean	0,7 %	0,07 %	11 %	5 %
Ratio mail spam/clean	25,0 %	14,8 %	35,3 %	13,5 %

Explanation:
- UW: end-user / traffic varies depending on time of the year
- Cyren: traffic mainly within big provider (as suspected calendaring systems used for sending calendar spam to the same system for reputation reasons but also because of being a bigger target group)

Based on 1 week traffic analysis at UW and cyren in May and September 2018.

No chance to be a hero

It's all about prevention and dirt work

inspect and adapt

pixabay

Current status

- Draft of BCP document has been created and feedback from CalConnect and M3AAWG received and integrated

- We would like to go to last call directly after the conference and if the publishing process has been moved forward

- This is how it looks at the moment:

https://goo.gl/bMbjXT or direct at

https://github.com/CalConnect/TC-CALSPAM/tree/master/BP_workingdraft

Decisions made

- Publish best practice document as CalConnect document (M3AAWG will cross-reference it)

- Two interesting topics identified to be followed up at CalConnect:

  - Event origin

  - Generic calendar spam client/server interaction

  -> both discussed in Abuse audit draft discussion yesterday

Feedback from Abuse audit session

- Event origin
  - Divide into channels
  - Create: user, Timestamp (TS), IP, client (HTTP header?)
  - Email: sender email, TS, message id
  - Subscription: URL, TS
  - Import: TS, (file name?)
  - iTIP: TS
  - Other: TS
- Abuse audit draft
  - Delete status (GOOD, WARNING, BAD) as included in score
  - Client -> server: PROPPATCH calls

Next steps

- Finalize CalConnect document process

- Move on to last call on document

- Interested in engaging yourself?
    Contact chair of TC:
    Thomas Schäfer at thomas.schaefer@1und1.de

Open for discussion!