M3AAWG | MESSAGING MALWARE MOBILE ANTI-ABUSE WORKING GROUP

Messaging, Malware and Mobile Anti-Abuse Working Group

M^{3}AAWG Recommendation on Web Form Signup Attacks

October 2017 – URL to reference this document: www.m3aawg.org/WebFormAttacks

Problem Description

Since late in 2015, web forms for mailing lists and other services have been exploited for the purpose of denying attack victims effective use of their email inbox. The effect is to create a DDoS (Distributed Denial of Service) attack against an individual mailbox.

Many organizations have web forms that provoke an email confirmation to the email address provided in the form. Malicious entities do bulk form submissions with forged addresses, resulting in mail floods to the holders of those addresses. When a victim receives a flood of various email confirmation messages like this, they are very likely to miss critical security notices amid the onslaught.

Earlier instances of this attack generally targeted specific individuals as a means to settle grudges or feuds but they are now being used by criminals as a way to defeat security processes. Since email accounts are increasingly used as the focal point for important communications in banking, online shopping, public services, and other amenities, denying access or usability to these communications can increase the timeframe in which criminal activities, for example money transfers or account takeovers, remain unknown by their victims.

With the first waves of these attacks, the highest profile subscription lists implemented anti-bot measures to limit the exploitation of their systems for this purpose but the malicious actors have simply moved on in successive waves of attacks to less well-defended systems. The internet is filled with many poorly protected or out-of-date systems so it is unlikely that relying on the owners or operators of these systems will be effective in stopping this avenue of abuse.

Response

Recognizing that this problem goes beyond the abilities of individual senders, hosting companies and receivers to address this threat, M^{3}AAWG members have worked in collaboration across the industry to propose an initial step that hosting and sending companies can implement in order to signal to receivers that a particular email message was triggered by a web form sign up. Details of the specification have been published by the IETF (Internet Engineering Task Force) at https://tools.ietf.org/html/draft-levine-mailbomb-header-00. The header allows receivers to identify floods of mail coming from sign-up forms that are bombarding victim mailboxes.

Initial Results (circa October 2017)

As of the M^{3}AAWG General Meeting in October 2017, a variety of companies have started using this new header and some receivers have incorporated it into their protection efforts. Wider adoption of this header will increase the value of the signal to protect victims from these denial of service attacks.

Call to Action

M^{3}AAWG highly recommends that all providers who generate mail in response to web form submissions should implement this straightforward signaling mechanism. All web forms which are publicly exposed should also be protected from bulk/automated submission attacks through standard measures that are available to distinguish manual from automated access, i.e., CAPTCHA systems of various types. M^{3}AAWG is also in the process of writing a more detailed paper regarding this abuse pattern and how providers can improve detection for exposed web forms and exploitation of those forms.

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