NEWS

Subscription Bombing: COI, CAPTCHA, and the Next Generation of Mail Bombs

by The Spamhaus Team

September 16, 2016

4 minutes reading time

Share

Threat intelligence | Deliverability | Website security

JUMP TO

Introduction

Internet harassment is becoming an increasingly ugly and widespread issue, and over the weekend of August 13-14 it spilled into territory we could do something about. After a few weeks of low level activity, over that weekend some unknown cyber criminals launched a targeted attack on over 100 government email addresses, using bots to create mailing list subscription requests at the rate of over 1000 per minute. Effectively, this was a denial of service attack, rendering the government mailboxes useless for considerable time. Over the next couple of months the targets expanded from government addresses to others, some of which were targeted and timed to be especially disruptive.

Examples of Recent Subscription Bombs

- 22K signups at a single ESP, targeting 3000 different domains, resulting in a volume of sometimes over 100 messages a minute to some addresses.
- One company saw nine specific addresses signed up over 9,000 times over the course of two weeks, creating 81,000 confirmation emails.
- Brian Krebs was targeted as well, receiving a new subscription confirmation message every two or three seconds.
- Word to the Wise was also attacked, after publishing several articles about the subject (links below).
- Ultimately, on August 19, Spamhaus itself was hit with a fairly small attack.

Spamhaus Response

The first attack we detected was on August 12. Over that weekend, we began to create listings of the IP addresses from the largest sources of list bomb mail in an attempt to mitigate the damage. This is not something we did happily, but it was necessary.

Bots were - and are - being used to sign up innocent email addresses through open or poorly secured web sign-up forms in high volumes. Some subscriptions were added at ESP interfaces, many more were introduced at diverse list-owner locations around the web. These signups were made possible by the fact that many web forms use Single Opt-In (SOI) and accept all subscriptions without any verification, though in this case even using Confirmed Opt-In (COI) didn't help much because the volume of confirmation emails alone was enough to cause a substantial problem. In fact, many of the lists that were victimised had already been using COI.

It is interesting and concerning that the attacks were not all composed of list subscription responses; half consisted of account sign ups at WordPress sites, so the emails were also seemingly legitimate, as they contained the new account credentials. This means the onus of stopping this kind of attack is not only on ESPs or mailing list owners. It is on everyone that has any sort of web-based signup that results in an email being sent: somebody clearly spent a great deal of time assembling URLs of mailing lists, and of account sign up pages, and has written a script to submit addresses to them at speed. We suspect that this was a test run for a tool that will will soon be offered for sale in the 'Underground Economy': Mail-bombing as a Service - MaaS.

ESP Response

Efforts are ongoing to help ESPs clean up, and there has been a significant community effort among the ESPs that we feel is eminently praiseworthy. Lists of email addresses used for sign-ups were compiled and shared, as were lists of IP addresses known to be doing the deed. A Slack channel was created by Word to the Wise to facilitate communication between the interested parties. The cleanup has been quick and efficient in most cases, and we are confident that these ESP's will be proactively pushing their customers to secure their various online sign up forms.

ESPs are aware that these attacks are on-going, and that measures to secure sign-up forms must continue to be implemented.

How Does One Protect Against This?

The single best thing that can be done to secure a form and avoid becoming an attack vector is to put a CAPTCHA on it. (Google's ReCAPTCHA is a free service and will foil most bots.) Even using COI in this situation is not sufficient, as the sheer volume of confirmation emails can be completely overwhelming. Use CAPTCHA plus COI to protect your mailing list subscription form!

Internet harassment is not going away. In fact, it is becoming a bigger and bigger problem; the fact that this first wave has died down should not be a reason to become complacent. This situation should be viewed as a call to arms by all senders, ESPs, and any businesses that utilise online sign up methods. They need to neutralise the attack vectors, educate their customers, tighten their policies and ensure they cannot be used as a conduit for personal or corporate harassment or DDoS attacks meant to disrupt online activities.

Additional Reading

Word to the Wise: Subscription bombing, ESPs and Spamhaus

Help and recommended content

See below for helpful articles and recommended content

How I'm fighting cybercrime with Spamhaus (and how you can too!)

Meet Jeroen Gui - student, founder of JustGuard, and a top contributor to Spamhaus' Threat Intel Community Portal. Passionate about making the internet a safer place, Jeroen submits thousands of malicious domains, URLs, and raw email sources every month. But what drives him to share his data, and how can you get involved too?

Threat intell... | Threat hunt...

Blog - February 26, 2025 - *Jeroen Gui*

Using OMI on Microsoft Azure? Here's an update you need to read

An easy-to-exploit security vulnerability that allows remote code execution (RCE) on virtual machines where Open Management Infrastructure (OMI) is installed has been observed. Users need to take action.

Threat intell... | Compromis...

News - September 28, 2021 - *The Spamhaus Team*

Suspicious network resurrections

***UPDATE** Dec 1st 2020: A big thank you to Telia Carrier, Hurricane Electric and GTT for taking swift and positive action in shutting down the related announcements.* We believe there is a serious issue relating to the equivalent of 56 "/20" networks, with a corresponding 230k IPv4 addresses. The total...

Threat intell... | BGP

News - November 25, 2020 - *The Spamhaus Team*