All –

Here is a blog post by security researcher Brian Krebs of Krebs on Security summarizing the issues:

Massive Email Bombs Target .Gov Addresses
http://krebsonsecurity.com/2016/08/massive-email-bombs-target-gov-addresses/

Over the weekend, unknown assailants launched a massive cyber attack aimed at flooding targeted dot-gov (.gov) email inboxes with subscription requests to thousands of email lists. According to experts, the attack — designed to render the targeted inboxes useless for a period of time — was successful largely thanks to the staggering number of email newsletters that don't take the basic step of validating new signup requests.

These attacks apparently have been going on at a low level for weeks, but they intensified tremendously over this past weekend. This most recent assault reportedly involved more than 100 government email addresses belonging to various countries that were subscribed to large numbers of lists in a short space of time by the attacker(s). That's according to Spamhaus, an entity that keeps a running list of known spamming operations to which many of the world's largest Internet service providers (ISPs) subscribe.

What my inbox looked like on Saturday, Aug. 13. Yours Truly and apparently at least 100 .gov email addresses got hit with an email bombing attack.
What my inbox looked like on Saturday, Aug. 13. Yours Truly and apparently at least 100 .gov email addresses got hit with an email bombing attack.

When Spamhaus lists a swath of Internet address space as a source of junk email, ISPs usually stop routing email for organizations within those chunks of addresses. On Sunday, Spamhaus started telling ISPs to block email coming from some of the largest email service providers (ESPs) — companies that help some of the world's biggest brands reach customers via email. On Monday, those ESPs soon began hearing from their clients who were having trouble getting their marketing emails delivered.

In two different posts published at wordtothewise.com, Spamhaus explained its reasoning for the listings, noting that a great many of the organizations operating the lists that were spammed in the attack did not bother to validate new signups by asking recipients to click a confirmation link in an email. In effect, Spamhaus reasoned, their lack of email validation caused them to behave in a spammy fashion.

“The issue is the badly-run ‘open’ lists which happily subscribed every address without any consent verification and which now continue as participants in the list-bombing of government addresses,” wrote Spamhaus CEO Steve Linford. It remains unclear whether hacked accounts at ESPs also played a role.

Also writing for wordtothewise.com, Laura Atkins likened email subscription bombs like this to “distributed denial of service” (DDoS) attacks on individuals.

“They get so much mail from different places they are unable to use their mailbox for real mail,” she wrote. “The hostile traffic can’t be blocked because the mail is coming from so many different sources.”

Atkins said over 100 addresses were added to mailing lists, many from Internet addresses outside the United States.

“The volumes I’m hearing here are significantly high that people cannot use their mailboxes. One sender identified fewer than 10 addresses each signed up to almost 10,000 of their customer lists during a 2 week period,” Atkins wrote. “Other senders have identified addresses that look to be part of the harassment campaign and are working to block mail to those addresses and get them off their lists.”

I WAS ON THE LIST, TOO!

Make that 101 targets, apparently. At approximately 9:00 a.m. ET on Saturday, KrebsOnSecurity’s inbox began filling up with new newsletter

subscriptions. The emails came in at a rate of about one new message every 2-3 seconds. By the time I'd finished deleting and unsubscribing from the first page of requests, there would be another page or two of new newsletter-related emails. For most of the weekend until I got things under semi-control, my Gmail account was basically useless.

Some of the lists I was signed up for did require confirmation, but the trouble is if you don't validate the request within a certain time they still send you additional emails reminding you to complete the signup process.

But those that required validation were in the minority, at least in the emails that I saw. I was aghast at how many of these email lists and newsletters did not require me to click a link to verify my subscription. I used Gmail's "mark as spam and unsubscribe" option to report all of those subscriptions. It's taken me almost a day's worth of effort so far to clean up, and I'm still getting one or two new junk newsletters per minute.

Atkins said many ESPs are now asking their customers to tighten signup requirements to include verification, and to comb through their lists for any recent signups that match certain fingerprints associated with this attack.

I have no idea why I'd be on a list of targets, and no one has contacted me about the attack thus far. But this isn't the first time that KrebsOnSecurity has been the target of an email bombing attack. A very similar deluge was launched specifically at my inbox in July 2012. I later traced that inbox flooding service back to a guy in Ukraine who was intimately involved in selling credit and debit cards stolen in the 2013 breach at Target.

I don't know who's responsible for this latest attack, and I'm not suggesting a connection between it and the 2012 attacks I just mentioned. But I do marvel at how little seems to have changed since 2012 in terms of how organizations run their newsletters. It's also mind-boggling to ponder how many of these time-wasting attacks are the result of organizations that fail to secure or properly configure their software, technology and services.

In the past week alone, for example, KrebsOnSecurity.com has been the

target of more than a half-dozen DDoS attacks aimed at knocking this site offline. These attacks are increasing in both frequency and intensity because the criminals behind them have access to virtually limitless firepower — millions of poorly-configured systems that can be leveraged to flood the target with so much junk traffic that it is rendered unreachable to legitimate visitors.

Let's hope the ESPs of the world step up and insist that customers using their email infrastructure take a bit more care to ensure they're part of the solution and not part of the problem. Atkins captures my thoughts on this subject precisely in the conclusion of her writeup on the attacks.

"Internet harassment seems to be a bigger and bigger issue," she wrote. "I don't know if it's because people are being more open about harassment or if it's actually more common. In either case, it is the responsibility of networks to minimize the harassment. If your network is a conduit for harassment, you need to do something to stop it."

+ + +

Best regards,

Reed