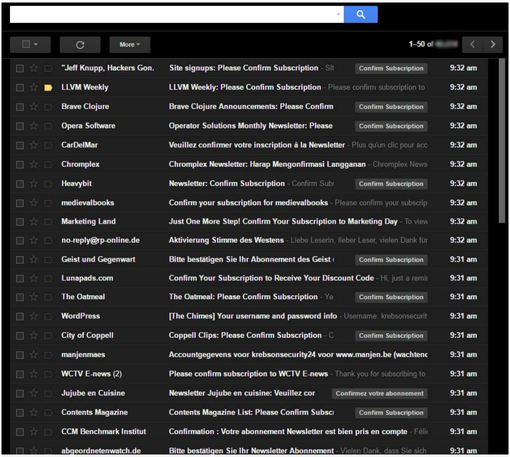
Doppel
Detect and disrupt social engineering attacks
AI-native Digital Risk Protection, Human Risk Management, and Email Security on one platform
LEARN MORE

Massive Email Bombs Target .Gov Addresses

August 18, 2016 35 Comments

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.



"Jeff Knupp, Hackers Gon.	Site signups: Please Confirm Subscription - Sit	Confirm Subscription	9:32 am
LLVM Weekly	LLVM Weekly: Please Confirm Subscription - Please confirm subscription to		9:32 am
Brave Clojure	Brave Clojure Announcements: Please Confirm	Confirm Subscription	9:32 am
Opera Software	Operator Solutions Monthly Newsletter: Please	Confirm Subscription	9:32 am
CarDelMar	Veuillez confirmer votre inscription à la Newsletter - Plus qu'un clic pour acc		9:32 am
Chromplex	Chromplex Newsletter: Harap Mengonfirmasi Langganan - Chromplex News		9:32 am
Heavybit	Newsletter: Confirm Subscription - Confirm Sub	Confirm Subscription	9:32 am
medievalbooks	Confirm your subscription for medievalbooks - Please confirm your subscrip		9:32 am
Marketing Land	Just One More Step! Confirm Your Subscription to Marketing Day - To view		9:32 am
no-reply@rp-online.de	Aktivierung Stimme des Westens - Liebe Leserin, lieber Leser, vielen Dank für		9:32 am
Geist und Gegenwart	Bitte bestätigen Sie Ihr Abonnement des Geist	Confirm Subscription	9:31 am
Lunapads.com	Confirm Your Subscription to Receive Your Discount Code - Hi, just a remir		9:31 am
The Oatmeal	The Oatmeal: Please Confirm Subscription - Ye	Confirm Subscription	9:31 am
WordPress	[The Chimes] Your username and password info - Username: krebsonsecurit		9:31 am
City of Coppell	Coppell Clips: Please Confirm Subscription - C	Confirm Subscription	9:31 am
manjenmaes	Accountgegevens voor krebsonsecurity24 voor www.manjen.be (wachtenc		9:31 am
WCTV E-news (2)	Please confirm subscription to WCTV E-news - Thank you for subscribing to		9:31 am
Jujube en Cuisine	Newsletter Jujube en cuisine: Veuillez cor	Confirmez votre abonnement	9:31 am
Contents Magazine	Contents Magazine List: Please Confirm Subsc	Confirm Subscription	9:31 am
CCM Benchmark Institut	Confirmation : Votre abonnement Newsletter est bien pris en compte - Féli		9:31 am
abgeordnetenwatch.de	Bitte bestätigen Sie Ihr Newsletter Abonnement - Vielen Dank, dass Sie sich		9:31 am

Doppel
Detect and disrupt social engineering attacks
AI-native Digital Risk Protection, Human Risk Management, and Email Security on one platform
LEARN MORE

Mailing List

Subscribe here

Search KrebsOnSecurity

SEARCH

Recent Posts

Data Broker Radaris Loses Domains in Privacy Fight

Microsoft Plugs Nearly 1,000 Security Holes

FBI Probes Service Selling 153M+ Drivers Licenses

Two Alleged 'TeamPCP' Hackers Arrested in Australia

Who's Tracking You? Use This New Service to Find Out

Story Categories

A Little Sunshine

All About Skimmers

Ashley Madison breach

Breadcrumbs

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!

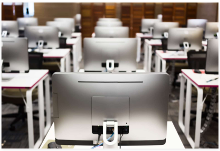
Make that 101 targets, apparently. At approximately 9:00 a.m. ET on Saturday, KrebsOnSecurity's inbox began filling up with new newsletter subscriptions. The emails came in at a rate of about one new message every 2-3 seconds. By the time I'd finished deleting and unsubscribing from the first page of 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

- Data Breaches
- DDoS-for-Hire
- DOGE
- Employment Fraud
- How to Break Into Security
- Internet of Things (IoT)
- Latest Warnings
- Ne'er-Do-Well News
- Other
- Pharma Wars
- Ransomware
- Russia's War on Ukraine
- Security Tools
- SIM Swapping
- Spam Nation
- Target: Small Businesses
- Tax Refund Fraud
- The Coming Storm
- Time to Patch
- Web Fraud 2.0

Why So Many Top Hackers Hail from Russia



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."

This entry was posted on Thursday 18th of August 2016 04:07 PM

OTHER

EMAIL BOMB EMAIL SERVICE PROVIDERS ESPS LAURA ATKINS SPAM SPAMHAUS WORDTOTHEWISE.COM

← SSA: Ixnay on txt msg reqmnt 4 e-acct, sry

Malware Infected All Eddie Bauer Stores in U.S., Canada →

35 thoughts on "Massive Email Bombs Target .Gov Addresses"

Rev Barbara LS MacLennan

August 18, 2016

Thank you for the ‘head’s up’ and the ‘self-care’ information.

Regina

August 18, 2016

Nice article. Good information. Thank you.

Lucas Cooper

August 18, 2016

Brian, you made a point about “email newsletters that don’t take the basic step of validating new signup requests”. However, it seems the email newsletters are attempting to do just that. You’re getting bombed by validation emails.

- John Fix

-

August 18, 2016

A single validation email is what he is looking for, not the repeated validation emails he describes that some lists send out. A proper listserver should send one email that says “Someone (possibly you) signed up for this list. Click here to validate. If you didn’t sign up for this list do nothing and you will not be added”.

Lucas Cooper

-

August 19, 2016

From the screenshot, that looks exactly what had happened, though they were running around a bunch of lists that all sent validation emails. He wasn’t subscribed, just got hit by a ton of validations from different lists at once.

Brad Knowles

August 18, 2016

Lucas is right — almost all of these are confirmation requests, not actual direct subscriptions.

That doesn’t mean that it’s not still a lot of work to clean up, but at least you’re not being directly subscribed to each of these lists without confirming that is what you want.

Mike

August 18, 2016

I agree with Lucas and Brad, they were actually validating new signup requests. The problem is they were not using something like Google reCAPTCHA:
https://www.google.com/recaptcha/intro/index.html

Teddy Robinson

August 18, 2016

Not that you’d run just any script in your gmail, but the concept of this script seems to work (h t t p://w w w .labnol.org/internet/gmail-unsubscribe/28806/). Custom scripting is a good option to your likings. I’ve tested it out and it “seems” to do the trick but I didn’t use it on a live, personal mailbox.

Graham Cluley

August 18, 2016

Add me to the list of victims.

The rate at which the emails came in was astonishing and, of course, because it wasn’t technically spam nothing was stopping them.

The basic filtering options on Gmail don’t look inside the full headers of emails, which makes it a challenge to stop the messages. However, I ended up using the content compliance features of Google Apps for Business to search for indicators in the email headers that the messages were newsletter-related. That killed off most of them.

Getting one message for each newsletter (asking you to verify your email address) is a pain, but manageable. When those newsletters then persistently ask you if you forgot to verify that's a pain.

But worst of all, have been the newsletters which don't bother to verify with double opt-in at all. This includes some very well known names.

Anyway, with the filters in place things are much better now, and email is usable again.

But a real REAL pain.

Hayton

-

August 18, 2016

@Graham, @Brian : so as well as the dot-gov addresses whoever is behind this is apparently targetting security researchers. Do you know of any others in your field who were also targetted? And is this just malice or is it because of some recent story you both covered?

Anon

August 18, 2016

Chuckling (kind of). I worked on e-mail filtering and DLP for years. Old trick from back in the day and was more commonly used with smut sites and signing up individuals where somebody was mad at someone else or were playing a prank. I'd never heard of this occurring on a "large" scale until now. Wait until someone thinks it's funny to do this with the millions upon millions of e-mail addresses compromised across the many breaches over the years. Sheer volume alone could be expensive in the form of lost productivity and potentially sluggish or crashing e-mail servers/filled inboxes – even if it's only subscription confirms mostly. All depends on configuration at the recipient end. Slack is better. E-mail is meh and has often been cast as a counterproductive communication method. Interested to see if this event starts to occur more frequently.

timeless

-

August 19, 2016

I've been hit by that variation repeatedly over the years. I'm not sure if there's someone maliciously signing up my account to every imaginable dating-like service or if a lot of people with email addresses vaguely similar to mine don't actually know how to spell their own email addresses.

Weekly I get to complain to companies like Apple (customer bought a phone in a store), AT&T (and T-Mobile and a number of other carriers), BlackBerry (ironic as I think I was employed by then at the time, but I didn't want to use this persona for BlackBerry ID– someone else tried), Wallet Hub (this month), and Education.com that they didn't perform basic email address verification.

I'm especially annoyed at the bank and bank like services (hello Chase) who have gotten this wrong in the past (it took me years to fix that one, including flying in and walking into a branch to complain, which wasn't actually effective, I think the only thing that worked was a letter to a VP in some special office of the board or something).

Ernest

August 18, 2016

Thanks for the heads up and keeping all aware and up to date.

John Clark

August 18, 2016

Many years ago I worked for a federal agency. All the email I received at work was from other individuals in that agency. One day I and all my team mates started to get flooded with emails from a large number of different .com addresses. I quickly made an Outlook filter that deleted anything but the .gov domain. I reported the incident to the mail administrator and three days later they had the solution dealt with.

I communicated the temporary solution to my team mates but they liked using their work email for personal use so they felt they could not use my solution.

Daniel

-

August 22, 2016

You’ve got to love Federal employees and their deep-rooted understanding of email policy (assuming this took place during a time where you didn’t have to sign forms saying that this system was for official use only).

0XFF

August 18, 2016

The email spamming technique described in the article is often used to hide a legitimate email notification that would point to a malicious activity or to a compromised account.
Practical application would be for a malicious threat actor to compromise an account (e.g. Amazon), submit an order, and mail bomb the user legitimate email address to ensure Amazon email notification remains unnoticed.

Jamie

-

August 30, 2016

Yes! This happened to me the same day my eBay account was hacked and somebody ordered over $2500 worth of merchandise to an address in Palm Desert, CA. 21st century problems 🙁

JackofTins

-

September 9, 2016

Exactly! If you’re getting email bombed, then chances are that you’ve already been hacked.

Markus Jakobsson

August 18, 2016

Sadly, it does not matter whether the sites require subscribers to validate email addresses, since that request, too is an email.

Details at http://arxiv.org/abs/cs/0305042

- Filippo Menczer

-

August 19, 2016

Here is a shorter magazine version of the technical report describing the “email cluster bomb” attack:

- https://www.usenix.org/system/files/login/articles/1154-jacobsson.pdf

Larry St. Regis

August 18, 2016

I, too, got hit with this — about a month ago. Like you, Brian, my email account was basically useless for a couple of days while I systematically unsubscribed from each phony subscription.

Ron G

August 19, 2016

I wonder if it is only me who is thinking "What's the motivation here?"

Apparently, there were no ransom notes sent, and its pretty clear that this wasn't a personal vendetta or anything like that. Too many people and organizations were targeted. So what happened here?

I think I know.

Some programmer someplace was sitting at his keyboard one day when the 875th unrequested piece of commercial email blather this week came into his inbox, and it said "Click here if you DON'T want any more of this crap…" So, ya know, he/she musta just blown a gasket and cooked up this new little tool in his/her spare time. (It isn't as if this sort of thing would be all that difficult to construct.) Now, the programmer just wants to make sure a whole lotta people whose opinions might matter will share his/her angst about the sorry state of email on the Internet. So he/she sent "a message" to them all. The message was: "Things are totally f**ked in the world of email. Please DO SOMETHING about it."

Unfortunately, even this rather misguided attempt to make the connected and powerful suffer so that they will sit up and take notice isn't actually going to change anything in the end. This incident just proves that when it comes to the future of email, we're all doomed anyway.

Or maybe not.

We can all just put guards in front of our email boxes that will require each new sender who tries to email us to go through a manual confirmation process, you know, before that mail actually gets delivered. Some people have actually already been doing this for years, and it actually works terrfically well… *except* when it comes to joining mailing lists and/or receiving any other kind of automated email (e.g. the monthly gas bill). That's when this system breaks entirely. But if you are willing to manually maintain a list of places that you actually do want to receive automated emails from (e.g. the monthy gas bill) then it can work.

That's the future we're all headed to. There is no other option except to wait around until somebody takes a dislike to you and then listbombs your personal inbox out of existance.

Anonymous

-

August 19, 2016

The motivation is for LELZ and to annoying/waste time. Nothing more besides that.

NigerianGuy

August 19, 2016

Let me tell you the purpose of this. Its a fraud that's been going on for a while now but I think it doesn't affect .gov so maybe people didn't notice it. Anyway when there is an account takeover, most cc companies now send emails to let the owner know of 'change in address' or 'change in phone number'.

However when takeover an account and flood the email, the message from the bank get lost. You probably even delete it unknowingly while trying to clean your inbox plus unsubscribing. This gives time for COB (change of billing) to complete and a criminal would have spent enough money and even answered calls from bank for verification before you know. I am not sure why .gov is targeted but I feel some people use it in credit card profile details so go figure!

If it were 10s of thousands then I wouldn't know what to say but if it is 100s of emails, I think the criminals have built a profile already and are sure of the emails before sending those messages.

Mike

August 19, 2016

Too much dependency on the single largest attack vector (email) known to exist on the web. All for access to information that could just as easily be had without using email at all.

Iss Meftah

August 19, 2016

Great information. Thanks.

Bob Brown

August 19, 2016

I hope Spamhaus has finally blacklisted Mailchimp and Exacttarget. Neither requires validation, and I get nothing but spam from them.

In the mean time, instead of using "report spam and unsubscribe" you should use Gmail's "block" feature. That affects spammers' pocketbooks. The spammer will keep paying Mailchimp, or whoever, to send spam, but you'll never see it.

> JackofTins
>
> -
>
> September 9, 2016
>
> I have been using MailChimp for over 4 years for my makerbot newsletter and sign up confirmation has been in place since then. Unless you go the route of coding or connecting to their API, then they force sign up confirmations.

IA Eng

August 19, 2016

HA! Email bombs. It does not surprise me that these still exist. I can imagine companies hired some really smart people who followed the rules and procedures back in the day. They left over a period of time, and so did the basic overall understanding of all the IT functions that one was responsible for. Over time, much like software, passwords, dormant accounts and patches, these no longer on the front burner actions simply slipped away unnoticed.

usually one server can make life miserable. they contain thousands of possible email subscriptions, from animal care to zipper repair. Typically the server address can be pulled from the header information, and that can be passed to someone that might want to investigate the issue, and kindly ask the person in charge of the potential spam/email bomb servers to simply add a validation step, or a one step removal to all of the subscriptions they have to offer.

Back in the day, some email lists would tell you the time, date and IP of who signed you up. I do not know if that is still the case or not.

One way out is to purchase your own domain name hosting package. This typically has a domain name, a hosting service at that companies web server and a boatload of email addresses – too many for the average user.

I paid a little over 300 bucks for a www address, a hosting plan at the company's web server farm, and I think it was 1,000 email addresses. It was actually cheaper this way than trying to purchase say 10 or so email boxes per year. Check out Network Solutions or other large domain registering website for any specials.

That allows me to have as many email boxes that I wish to set up, and should one of them become wiped out by a email bomb, I can simply stand up another email box in order to replace the existing one, while the original is cleaned up. You can set up a ring of trust of say 3 or 4 email addresses, with a public facing one that is a catch all, a trusty subscriber list and then maybe a trusted/corporate/financial box.

Block all, report as spam. Carry on.

Andrew

August 19, 2016

Validation seems like a band-aid fix for this sort of problem. Would it not be easier, and wiser to include captcha on subscription forms?

Josh

August 22, 2016

Hey Brian,

I'm pretty sure that if you are using gmail or google apps, when marking those messages as spam google will attempt to automate the unsubscribing process. For those that fail to automatically unsubscribe they will be captured by Google's spam filter for your inbox.

Did you do the process of manually unsubscribing so that you could identify those that didn't honor it, perhaps?

Piere

August 22, 2016

Is okay. You will surely find way to blame Russia yet again.

Darron Wyke

August 31, 2016

Be careful. Some "legitimate" ESPs, like SendGrid, do absolutely nothing regarding spam. They give zero tosses about customers of theirs breaking the law.

Jerry Leichter

September 9, 2016

Several people have remarked that some lists send repeated confirmation requests. I personally have never encountered that – which doesn't mean it can't happen. However, someone causing an email bomb attack can easily *cause* it to happen, at least for some mail services. gmail in particular ignores periods in names, and also ignores everything after a "+" sign. So it's trivial to produce many variations of a gmail account name, all of which end up in the same mailbox.

These conventions are specific to gmail, though one or the other – or some other variation – may be implemented by other mail services. It's not reasonable to expect every subscription provider to keep track of the rules at every mail service so that it can filter requests that would be duplicated for that particular mail service. In fact, even just for gmail, it would be impossible, since gmail can be used as the back end to custom domains, a feature that's widely used. The gmail naming rules will apply to anything sent to those custom domains.

— Jerry

Dave

September 13, 2016

Great article, I had to really hunt for something on this topic.

I was also hit by this (or an identical) attack two or three weeks ago! My personal Hotmail account started getting flooded by several thousand subscription mails in the first 12 hours.

I had to use the Sweep and Junk filters in Hotmail to clean it up. The Sweep feature to delete all mail from a given sender and all future mail really helped a lot.

A couple of week since this started I am still getting ~10 new subscriptions a day.

I'd love to hear about what other strategies are available to recover from this seemingly pointless form of assault!

Comments are closed.