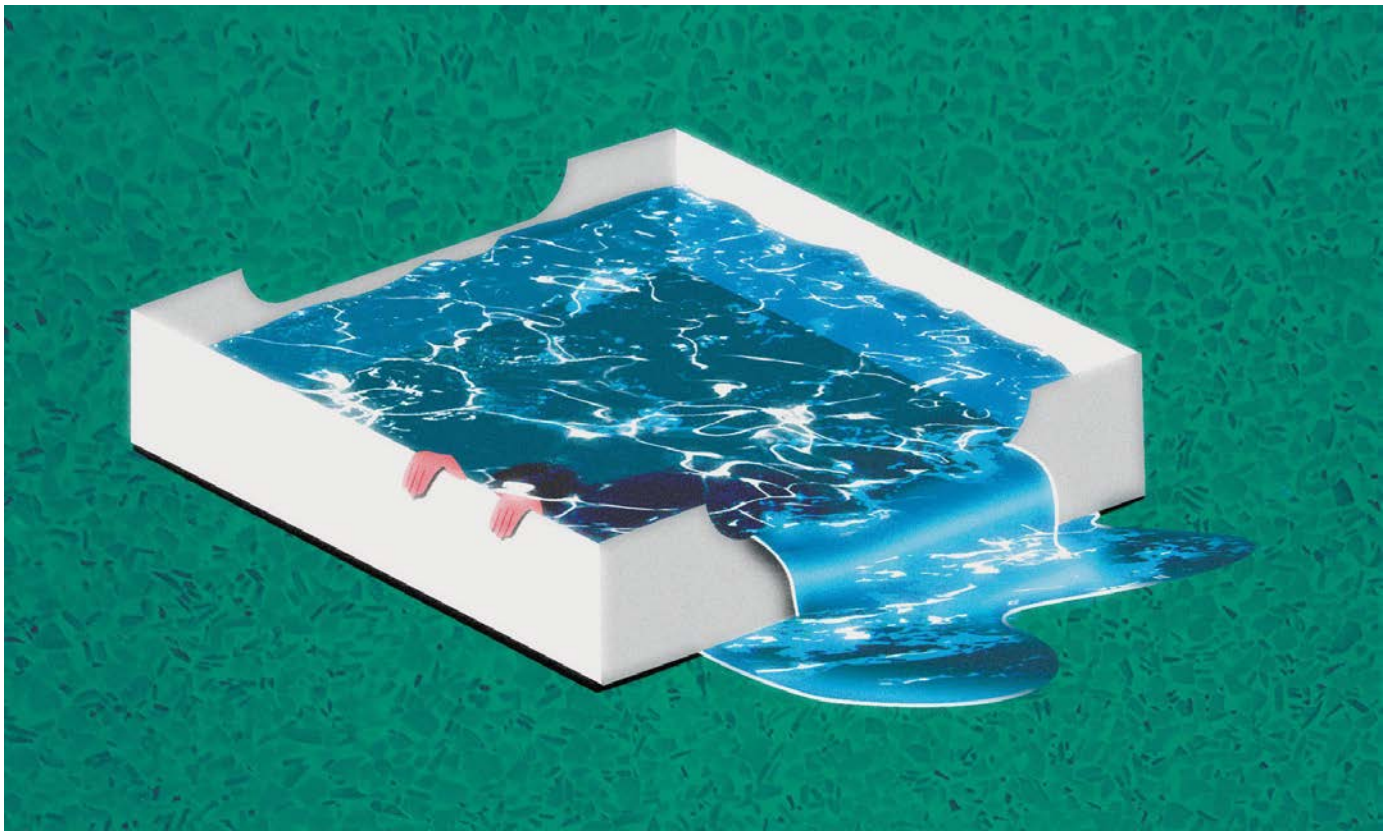
https://www.wired.com/story/how-journalists-fought-back-against-crippling-email-bombs/

HOW JOURNALISTS FOUGHT BACK AGAINST CRIPPLING EMAIL BOMBS

h



A flood of emails sent by bots shut down the servers of ProPublica, the investigative journalism nonprofit. MARK PERNICE FOR WIRED

IT WAS 10 am on a hot, humid Tuesday in August when I decided I could finally relax. After a frantic weekend of finishing a big story—and typing so much that my forearms tingled—I needed to decompress.

I placed my phone on do not disturb, turned on my air conditioner, and blissfully spent an hour contorting myself into various poses on the yoga mat next to my bed.

Precisely at 11 am, my yoga routine finished, I turned my phone back on to see a text message from my colleague Lauren Kirchner: "I am under some kind of email attack."

I was chagrined but not surprised. Lauren had been harassed all weekend, a result of an article we had coauthored about companies

This article was co-published with ProPublica, where author Julia Angwin is a senior reporter.

such as PayPal, Newsmax, and Amazon whose technologies enabled extremist websites to profit from their hateful views. Simply in the interest of journalistic fairness, Lauren had sought comment from about 70 websites designated as hateful by the Southern Poverty Law Center and the Anti-Defamation League.

In return, her voicemail and her email inbox were filled with threats and insults. Her Twitter mentions were filled with people criticizing her appearance. Several of the sites she contacted posted negative articles about her, calling her a “fascist” and a “troll.” Alarmed, she had asked the security guards in our building to not let anyone into the office who asked for her.

But then I looked at my inbox and realized that something troubling was happening to me too: 360 emails had poured in while I was pretzeling myself. Every single one was a confirmation of a newsletter subscription or account signup from a website I’d never heard of.

“Thanks for signing up, here is your coupon!” an email from the Nature Hills Nursery said. “Please Confirm Subscription” Fintirement said. “Account details for xvwgnagycdm 1992 at ami-forum.org are pending admin approval,” a Montessori organization in Australia said.

“I am under some kind of email attack as well. Jesus,” I texted Lauren. Then I messaged my colleague Jeff Larson, who had shared a byline with me and Lauren on the article. His inbox was flooded too. Fortunately the inbox of our part-time colleague Madeleine Varner, who also had a byline but whose email address is not published on our website, was quiet.

As a reporter who has covered technology for more than two decades, I am familiar with the usual forms of internet harassment —gangs that bring down a website, haters who post your home

address online, troll armies that hurl insults on a social network. But I'd never encountered this type of email onslaught before. I wasn't sure what to do. "Hey Twitter—any advice on what to do when somebody malevolent signs you up for a thousand email subscriptions, making your email unusable?" I tweeted.

At first it seemed like a funny prank, like ordering pizza delivered to an ex-boyfriend's house. "TBH [to be honest] it's kind of a clever attack," I tweeted again.

But as the emails continued to roll in, my sense of humor faded. By noon, the entire email system at our employer, ProPublica, was overwhelmed. Most of my colleagues could not send or receive messages because of the backlog of emails to me, Jeff, and Lauren that were clogging the spam filters.

The tech team advised that it would likely have to block all incoming emails to our inboxes—bouncing them back to senders—to save the rest of the organization. A few hours later, when ProPublica pulled the plug on our email accounts, I realized that what our attackers did was no joking matter; they had cut off our most important avenue of communication with the world. "Preparing to say goodbye forever to my inbox," I tweeted. "It does seem like killing a reporter's email account is the definition of a chilling effect, no?"

Email senders are not in the business of making it harder for people to receive their missives. MARK PERNICE FOR WIRED

LATER I LEARNED that the type of attack aimed at me and my colleagues is often called "email bombing" or "subscription bombing." It's clever jujitsu that turns one of the hallmarks of spam

prevention—the confirmation email—into a spam generator. It works like this: The attacker uses an automated program to scan the web for any signup form that asks for an email address, from a newsletter subscription to an account registration. It then inserts the target's email address into each of the forms, flooding the victim with confirmation emails.

It's laughably easy to launch an email bomb. Anyone with decent technical skills can set up an automated program to enter email addresses across the web. Or they can buy a service that will automate the attack for $5 per 1,000 emails sent to an address, according to ads on online hacker forums.

Despite its limited sophistication, email bombing is extremely difficult to defend against. Stopping it would either require every single website with an email entry form to take steps to identify and block automated entries, or some kind of network of email surveillance that would notice huge numbers of email signups and block the sending of confirmation emails. But neither approach is foolproof, and the latter could potentially erode the privacy of web users.

In other words, email bombing is a perfect parable for 2017, a time in which we appear to be collectively losing faith in the promise of the internet. For the first 20 years of this new communications medium, it seemed to hold out the promise of fostering democracy and shifting the balance of power from the powerful to the masses. In recent years, though, a depressing realization has taken hold: The internet is fragile and easily exploited by hackers, trolls, criminals, creepy corporations, and oppressive governments.

Social media in particular has become a battleground, filled with disinformation, hoaxes, and conspiracies—some pushed by Russian trolls, we have learned, and some by our own homegrown harassers.

Most disturbing is the rise of hateful, inflammatory speech. At its

worst, it veers into the territory of what researcher Susan Benesch calls dangerous speech—the type of propaganda that has historically been used in places like Rwanda and Hitler's Germany to convince people to commit violence.

A hallmark of dangerous speech is called accusation in a mirror—in which the inciter asserts that the listeners are in severe danger from the target group, thus allowing them to commit or condone violent action. A classic example are the lynchings of African Americans that became commonplace after the Civil War. Often the lynchings were incited by false accusations of rape—allowing the murderers to profess that they were acting in defense of themselves and their families.

On a much smaller scale, the assault on our inboxes may have been unleashed by similar assertions of victimhood. The websites that we had written about claimed to be under attack by Lauren—because she had emailed them fact-checking questions—allowing their followers to justify a tsunami of hateful attacks on us at ProPublica. One of Lauren's email correspondents called her an "ugly swine" and hoped she would be raped by a Muslim refugee who threw acid in her face.

PROPUBLICA IS A nonprofit newsroom dedicated to investigative journalism. We spend a lot of time and effort thinking about how to protect reporters, sources, and readers. We were one of the first major news outlets to launch a secure whistle-blower submission system, and the first to publish our site on the dark web so that readers could browse our stories anonymously.

And we have run our own email server so that we haven't had to rely on the big providers such as Google and Microsoft. Unlike telecommunications companies, which are prohibited by law from listening to their customers' phone calls, there is no restriction against email providers reading their customers' communications.

In fact, Google has long monitored the inboxes of its users to determine what type of ads to show them. (Google recently said it plans to stop scanning Gmail inboxes for ad purposes).

Our system was designed to fight the last war—to defend against a traditional spam attack, in which an identical email is sent to multiple recipients. Its design didn't take into account the inverse strategy adopted by our harassers: thousands of unique emails sent to the same recipient. When our systems were overwhelmed, we didn't have the advantage of a major internet provider with massive capacity in its spam filter.

Life without our work email accounts was a little strange. ProPublica gave us temporary accounts with different user names, but since no one knew these new email addresses and we were afraid to publicize them, our inboxes were eerily silent.

I couldn't shake the worry that I was missing out on some important email that was being sent to my old address. Lauren had similar concerns. On the other hand, she says, "I was intensely relieved that it had finally stopped. I could breathe."

Jeff was determined to find out who launched the attack. He noticed that many of the confirmation emails came from websites using Wordpress, a popular open source blogging software. For nearly a decade, Wordpress users have requested that Wordpress implement a feature that would make it harder for automated bots to complete registrations. But the programmers who contribute to the open source software project have not chosen to include features to block automated email signups.

Wordpress also has a commercial arm, Automattic, which offers paid services, including hosting. Automattic spokesman Mark Armstrong says the company only identified 312 emails to ProPublica that were likely part of the attack, and that the rest probably came from sites running Wordpress that aren't hosted by Automattic. "We do not own, control, or have access to every single

WordPress site in the world," he says.

Jeff wrote a program to automatically email the owners of nearly 500 of the Wordpress websites that had been hijacked to send us email. These emails had been sent automatically to confirm that we'd signed up for an account, usually for the purpose of being able to post a comment on a blog. "I'm a reporter with ProPublica, a nonprofit news organization," Jeff wrote. "Earlier this week, we started receiving thousands [of] emails in our inboxes. After investigating them, we found that someone was signing us up for new accounts on sites like yours." He asked them to send him any information for the accounts created under our names.

Only a handful of sites responded. One website owner, Raul Silva from Chicago, said he was shocked that his nearly abandoned blog —he only posted once, in 2012—was being used by bots. "Holy crap! There are 2,800 registered users," Silva wrote to Jeff. "Must be bots using the site as a launch board for spamming and scamming."

A small web hosting company, Alterhosting, provided server logs that showed the IP address of the person who registered for an email account at ABetterFitYou.com under Jeff's name. We hoped the server logs would help us find out who had attacked us, but the IP address was a dead end. It led to a Tor exit node in Luxembourg that calls itself HelpCensoredOnes. It's not unusual for bad actors to mask their activities behind Tor, a web browsing technology designed to conceal the identity of its users.

"Even though Tor is a force for good, it sometimes is used by evil people," says Shari Steele, executive director of the Tor Project. "The same tool that empowers activists in hostile regimes, journalists using off-the-record sources, and individuals trying to take back their privacy can also be used to launch email subscription bombs and do other nefarious deeds."

No sooner had ProPublica cleaned up from the attack than it was hit again.
MARK PERNICE FOR WIRED

THE DAY AFTER we were attacked, ProPublica was email bombed again, this time in response to a colleague's article about pro-Russian Twitter bots supporting white supremacists and their violent rally in Charlottesville, Virginia. ProPublica immediately blocked all incoming email to his address, preventing the spam filter from clogging.

That same day, Jeff noticed something strange: One of his tweets about the email barrage against us—containing an image of his overflowing inbox—had been retweeted 1,200 times. Then Lauren realized that one of her tweets—alerting people that her email was down and they should reach her by other means—had also been retweeted 1,200 times. Each of us had gained 500 new Twitter followers overnight.

Clearly someone had unleashed some Twitter bots on us. But it was confusing: What was the point of making us seem more popular than we really were? Jeff speculated that maybe they were hoping we had turned on Twitter notifications and were being deluged with them. Or perhaps they wanted to tout their success at shutting down ProPublica's emails.

It also wasn't clear whether the Twitter accounts swarming us were entirely automated or just humans following instructions. But the results were the same: They tweeted in formation, like synchronized swimmers. Twitter user @kirstenkellogg_ tweeted at us: "ProPublica is alt-left #HateGroup and #FakeNews site funded by Soros." Her tweet was retweeted more than 23,000 times. Twitter user @yoiyakujimin tweeted that we were "presstitutes." That message was retweeted more than 20,000 times. (Investor George Soros is a funder of ProPublica, providing less than 3

percent of its revenues, through his Open Society Foundation.)

Jeff started to wonder how hard it was to actually launch a bot attack on Twitter. So he set up two fake Twitter accounts —@FauxPublica and @fauxpublicaru in the Russian language. He tweeted from each account: "This is a tweet to show how many retweets we can buy."

Then he went shopping for retweets. Turns out there are plenty of companies that openly sell Twitter followers—even though it's against Twitter's terms of service. But not all of them were willing to take our business, particularly for the fake Russian account. RedSocial, which describes itself as offering "social media promotion services starting from $1," turned us down. "Please take your business elsewhere," RedSocial wrote on our order for 5,000 Twitter retweets on the FauxPublicaRU account. It didn't explain why, but perhaps there is some honor even in the netherworld of social media.

A company called Followers and Likes had no such scruples. It sold us 10,000 retweets for the Russian FauxPublica account for $45, and 5,000 retweets for the English language FauxPublica account for $28. And we bought more expensive retweets from Devumi, which charged $29 for 1,000, promising that its retweets will "look 100 percent real."

For just about $100, we had mustered an impressive bot army. Soon our test posts had thousands of retweets.

Twitter declined to comment about our experience. It directed us to its policies that prohibit buying and selling Twitter accounts.

Within two days, we were discovered—but not by Twitter. Journalist Brian Krebs spotted our Russian language tweet and called it out on Twitter. Krebs, journalist and author of the noted cybersecurity blog Krebs on Security, was struggling with his own Twitter account. A week earlier, he had been followed by 12,000

Twitter bots and he was worried that they were malevolent. Then some of his bots retweeted us, suggesting that his attacker had used the same paid services that we used.

I called Krebs and explained to him that we were just doing a test. But I also had a question for him: What was the harm of these bots? It all seemed kind of innocuous to me. Not at all, he said: Being followed by too many bots could cause Twitter to kick you off the platform—which had happened to another journalist, Joseph Cox, who had his account suspended temporarily after being followed by bots.

But after Krebs wrote about the bot surges aimed at us and him, our new followers evaporated. And the bot harassment declined, perhaps scared away by the glare of public scrutiny.

Nowadays all that's left of the bots are two tweets that I get every morning—one directed at just me, and one at me and my colleagues. Every day they come in from a new account so that it is difficult to block them in advance:

"@JuliaAngwin Why are all leftist bitches ugly?"

and

"From Russia with love: FUCK YOU! @lkirchner @JuliaAngwin @thejefflarson @iarnsdorf"

ITÕS NOT SURPRISING that Krebs was the one who spotted our bot shopping. Because his work takes him into the cyber underworld, Krebs is under constant attack and constantly alert to new forms of information warfare.

He jokes that he is the Alderaan of the internet, a dark-humored reference to the planet that Darth Vader blows up in Star Wars to test the Death Star's destructive capabilities. When cybercriminals want to test a new technique, they often try it on Krebs.

His website is often fending off distributed denial of service attacks in which thousands of computers try to connect to his site in the hopes of overwhelming it until it shuts down.

Krebs was the first person I knew to get "swatted." Swatting is when an attacker uses a spoofed phone number—using shady techniques to make it seem as if a phone call is coming from a different number—to call 911 purportedly from the victim's house. The attacker tells a scary story of kidnapping or home invasion, which prompts the police to dispatch a SWAT team—hence the term "swatted"—to the scene of the supposed crime.

The victim first finds out about it when a SWAT team storms into the house in military gear. If he or she doesn't answer the door fast enough, SWAT teams may break it down with a battering ram and throw flashbang grenades inside. It is often difficult for the victim to explain, during the heat of the raid, that the call was not real.

Krebs tried to warn his local police that he was a likely swatting target, but that didn't stop them from dispatching a team to his house in 2013 after he had exposed a criminal underground forum selling Social Security numbers and credit reports. "This is kind of the real problem with cybercrime in general—the costs for launching these attacks are so low and the costs of defending or blocking or recovering can be just extraordinary," Krebs says.

In August 2016, a year before the email bombing of ProPublica, Krebs woke up on a Saturday morning to discover that his Gmail inbox was overflowing with newsletter subscriptions. Upon investigation, he learned that the attackers had also flooded the inboxes of more than 100 government email addresses around the world. When Krebs wrote about this attack, the companies that specialize in sending bulk email took notice. Email bombs had surfaced occasionally in the past, but the scale of the attack and the publicity on Krebs's blog prompted a new reckoning.

A widely respected antispam

RELATED STORIES

YULIA JAMES
When Russian Trolls Attack

BRIAN BARRETT
MIT's Teaching AI How to Help Stop Cyberattacks

GREG NOJEIM
Letting Cyberattack Victims Hack Back Is a Very Unwise Idea

service, Spamhaus, notified several email providers whose services were used in the attack that they needed to stop the abuse. Spamhaus recommended that the "single best thing that can be done" would be for email lists to include a test known as a CAPTCHA to distinguish between human and automated signups. Most internet users know CAPTCHAs as the squiggly words or sequence of photos that they are asked to identify.

Few companies adopted Spamhaus' recommendation. Email senders are not in the business of making it harder for people to receive their missives, especially when the people harmed by the sham signups are not their clients. And many individuals hosting email forms on their websites are not likely to install a bot detection system unless it's drop-dead simple. My personal website, for instance, uses Wordpress for an email signup form. As we learned from the email bombing, Wordpress is not designed for installing a CAPTCHA by default.

Instead, at the email industry's get-together in June, M3AAWG, the Messaging Malware Mobile Anti-Abuse Working Group, came up with an email surveillance strategy. Their solution, which is voluntary for companies to adopt, would identify subscription confirmation emails with a special technical header. That would allow email services to filter and block confirmation emails during a subscription attack. The header would include the location of the

computer that signed up for the subscription, exposing a new detail of personal information.

The system also would make it easier for email inbox providers—like Gmail—to alert email senders to a possible subscription bomb attack.

Severin Walker, chairman of the messaging group, told me that some of the biggest email systems have already introduced the new practice. “While we may never get to 100 percent adoption, some fairly critical systems are adopting it,” he says.

MailChimp, one of the leading email sending services, said it has already introduced the technical header to help prevent subscription attacks. But at the same time, it has just announced it is dropping its practice of requiring confirmation emails before signing people up for newsletters (except in the European Union, which has strict privacy laws).

Without that double confirmation, even more of the newsletters that I was unwittingly signed up for during the subscription attack would be sending me regular updates.

Piotr Mathea, director of anti-abuse at a Polish email sender called GetResponse, says he is implementing the new header. “I think it should help to weed out at least part of mail bombing,” he says.

Mathea says that noticed the attack on ProPublica, and to blocked the sending of additional confirmation emails from his service. But clearly it wasn’t enough to stop the full attack on us.

I felt a bit leery about the prospect of the email subscription industry adding location monitoring. After all, I wrote a book about the harms of pervasive surveillance. But now, in a world of global information warfare, I had to admit that the idea of a small organization like ProPublica mounting a solo defense against all attackers was becoming increasingly unrealistic.

In the two months since the email bombing, our jobs have largely returned to normal. Lauren, Jeff, and I got our email accounts restored (minus a week's worth of messages), and Twitter deleted most of the accounts that badgered us. Still, we learned a sobering lesson about how easy—and inexpensive—it is for haters to disrupt our work. And it's likely only a matter of time before we will be attacked again. Information warfare—as a tactic designed to silence and intimidate—remains on the rise, and my colleagues and I don't plan to stop writing about online hate or any other controversial topic.

The next time it happens, we plan on having stronger fortifications against attack. As Piotr told me: "You cannot change the cannon, but you can always hide yourself behind higher and thicker walls."

RELATED VIDEO

CULTURE

How To Battle Trolling Ad Hominem Attacks Online

An internet troll's favorite way to argue? Ad hominem, of course! This is your guide to spotting bad arguments on the internet and how to fight them.