New Registration Bomb Email Attack Distracts Victims of Financial Fraud

by Evan on March 1, 2022

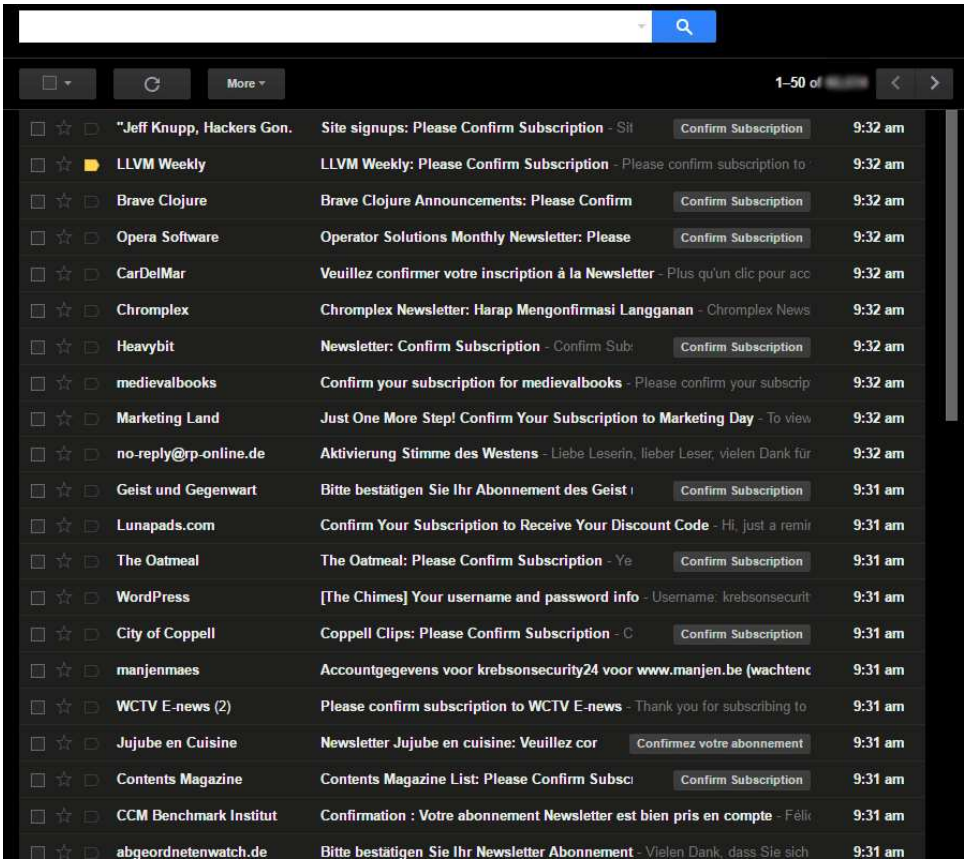
Email bombing attacks, in which bots flood an email address or server with hundreds to thousands of email messages, have been a significant thorn in the sides of CISOs and ordinary email users since the late 2000s. This nefarious act, which can achieve a similar outcome to that of a distributed denial of service (DDoS) attack, is also frequently deployed to distract and hide important emails.

One of the most notable email bombing campaigns came in 2016 when, according to Brian Krebs, "unknown assailants launched a massive cyber attack aimed at flooding targeted dot-gov (.gov) email

inboxes with subscription requests to thousands of email lists." The email server was so overwhelmed that many .gov email addresses remained unusable for days.

Walmart.com 'registration bomb' cloaks financial fraud with inbox overload

Overview: Over the past six months, BlackCloak analysts discovered a growing number of new and existing clients' whose inboxes were overwhelmed with registration confirmation emails from websites that they had never visited and had no affiliation with. Our investigation quickly revealed that these 'registration bombs' – the term we designated to differentiate these attacks from traditional email bombs – were being deployed to distract victims from recognizing that their Walmart.com account had been hacked and that financial fraud had occurred.



Inbox example of registration bomb courtesy of Krebs on Security

What happened: Our research found that attackers obtained an

Upcoming Webinars

Podcast

Futurum Security Boulevard PODCAST
Security B…
Always Liste… 32:33
OpenAI's Cy… 37:03
Is Your Rout… 35:01

Listen to all of our podcasts

Secure by Design »

unknown number of Walmart.com login credentials that were leaked onto the Dark Web, often from unrelated website data breaches. With usernames and passwords at their disposal, attackers were able to reuse these stolen credentials to log into active Walmart.com accounts, and make purchases using the valid credit card that remained on file. We quickly recognized that the majority of transactions were $250 or less. This is likely intentional so as to avoid triggering fraud alerts . Here's where the 'registration bombing' attack comes in: to distract from the financial fraud, the attackers would overload the victims' inbox with said registration emails, thereby pushing the Walmart.com purchase confirmation email completely out of sight. Astoundingly, some victims received more than 500 registration emails, pushing down the purchase receipt 5, 7 and even 10 pages deep. For many, the financial fraud went unnoticed for a long period of time.

1 week ago | Chris Blask

The Willow Doesn't Restore From Backup

2 weeks ago | Chris Blask

The Braid: Rethinking Trust, Continuity and Human-AI Systems

3 weeks ago | Chris Blask

The Architecture of Liberty

4 weeks ago | Chris Blask

AI Governance Without Surveillance: The Missing Evidentiary Layer

1 month ago | Chris Blask

The AI Didn't Go Rogue. The Boundary Did.

Press Releases

Attacker tool used to initiate attack courtesy of GitHub

What to do: It is unknown how many Walmart.com customers have been impacted by this 'registration bombing' campaign. What is clear however is that this is a concerted attempt by attackers to cover up the account compromise and financial fraud by drowning victims in email after email. Being that Walmart.com has suffered several data breaches in the past several years, it's wise for all patrons to update their password immediately. The best passwords are at least 12 characters in length, randomly generated and are not used on any other website. In addition, Walmart.com shoppers should enable two-factor authentication and check their credit card statements for the past 6 months, reporting any anomalous activity to both the retailer and the credit card company.

Reducing risk of email bombing attacks

It is easy to understand why 'registration bombing' is a successful tactic and a reasonable evolution of the email bomb. It's easy to deploy and time-consuming to resolve. Moving forward, everyone should be extra cognizant of unsolicited emails, especially those in mass quantity that are requesting an action be taken.

BlackCloak members who think they might have been impacted by the Walmart.com 'registration bombing' attack, or suspect an email bombing attack in the future should contact the Concierge Support Team immediately for investigation, analysis and the appropriate response. And of course, don't forget to deploy multi-factor authentication on Walmart.com and on any other e-commerce accounts that offer it.

The post New Registration Bomb Email Attack Distracts Victims of Financial Fraud appeared first on BlackCloak | Protect Your Digital Life™.

Cyber Threats, Prevent Hacks

Zama Raises $73M in Series A Lead by Multicoin Capital and Protocol Labs to Commercialize Fully Homomorphic Encryption

Most Read on the Boulevard

Iran, Yemeni Cell Used Claude in Developing Weapons, Threats: Anthropic

PaperCut Flaw Compromise Illustrates the Maturing Use of AI By

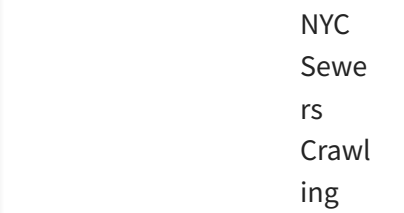
← Bigger Organizations Have Multiple Attack Surfaces

Don’t rely on your Storage & Backup Vendors for Security →

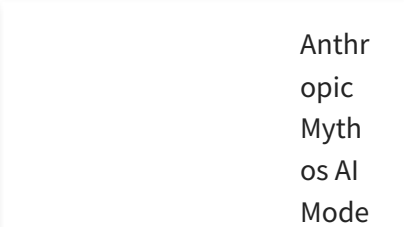
Attackers

Microsoft Teams IT Support Calling? Not So Fast, Hackers are Exploiting Trust in Spring Ring

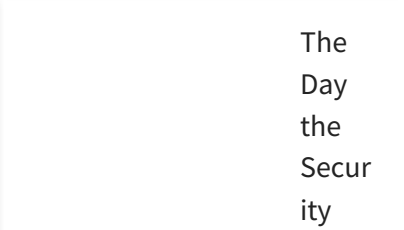
Industry Spotlight »



NYC Sewers Crawling With Rats and Potential Bad Actors

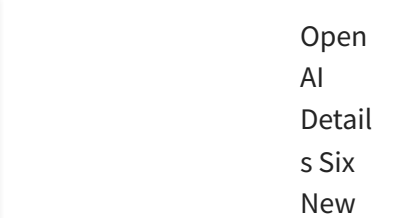


Anthropic Mythos AI Model Strikes Fear in Trump Administration, U.S. Banks



The Day the Security Music Died

Top Stories »



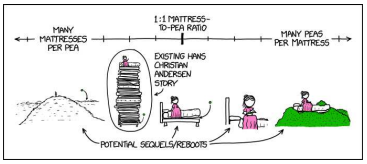
Open AI Details Six New Instances of ‘Concerning’ AI Agent Behavior

Roblox Games, Piracy

Platforms Fertile Ground for Terrorist Grooming

Attackers Target Vite Servers in Scanning Campaign to Steal AWS, Azure Info

Security Humor »



Randall Munroe's XKCD 'The Princess and the Pea'

Download Free eBook

[su_panel border="0px solid #ddd" radius="0" text_align="center" padding-top="0px" padding-bottom="0px"]

[/su_panel]

Join the Community

Add your blog to Security Creators Network

Write for Security Boulevard

Bloggers Meetup and Awards

Ask a Question

Email: info@securityboulevard.com

Useful Links

About

Media Kit

Sponsor Info

Copyright

TOS

DMCA Compliance Statement

Privacy Policy

Related Sites

Techstrong Group

Cloud Native Now

DevOps.com

Digital CxO

Techstrong Research

Techstrong TV

Techstrong.tv Podcast

DevOps Chat

DevOps Dozen

DevOps TV