CYBERFORCE

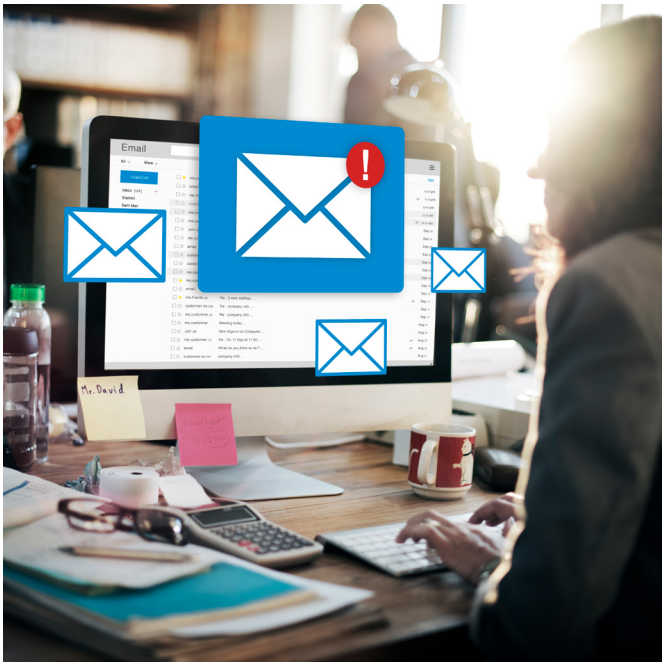
THREAT BULLETIN

DECEMBER 2025

THE RISING THREAT OF EMAIL BOMBING ATTACKS

OVERVIEW

A surge in email bombing attacks has been observed targeting enterprise and consumer email accounts. This technique involves sending an overwhelming number of emails, often thousands within minutes to a single inbox. The goal is to disrupt normal email usage, obscure legitimate security alerts, and create opportunities for secondary attacks such as account takeover or fraud. Unlike typical spam campaigns, email bombing is not primarily about phishing; it's about volume-based disruption. Attackers exploit automated subscription forms, compromised mailing lists, and botnets to flood inboxes, making it difficult for victims to identify critical messages.



KEY OBSERVATIONS & FACTS:

Attack Pattern

Victims receive thousands of emails in rapid succession, often from legitimate services (newsletters, sign-up confirmations).

Purpose

> Conceal important notifications (e.g., password reset alerts).

> Exhaust user attention and overwhelm email security systems.

Common Exploits

> Abuse of open subscription forms and newsletter APIs.

> Use of botnets to automate mass sign-ups.

> Targeting during account compromise attempts to hide alerts from financial institutions or cloud services.

Impact

> Inbox flooding leads to missed security warnings.

> Increased risk of fraudulent transactions or credential theft.

> Creation of fake helpdesk chats in Microsoft Teams: After the inbox flood, attackers impersonate IT support in Teams or other collaboration tools, tricking users into granting remote access or installing malicious software.

EXPLANATION:

01

MECHANICS OF EMAIL BOMBING

Attackers leverage automated scripts or botnets to subscribe the victim's email address to thousands of legitimate mailing lists. Each subscription triggers a confirmation or welcome email, resulting in a flood of messages.

02

WHY IT WORKS

> Most email providers treat these messages as legitimate because they originate from trusted domains.

> Victims often ignore inbox activity during the attack, allowing attackers to perform unauthorized actions unnoticed.

03

SECONDARY ATTACK VECTOR

Email bombing is frequently paired with account takeover attempts and fake IT support chats. While the inbox is flooded, attackers initiate password resets or fraudulent transactions, then follow up with Teams messages posing as helpdesk staff, requesting remote access via tools like Quick Assist.

MITIGATION & GUIDANCE:

Email Filtering & Rate Limiting

> Implement rate-based detection to identify abnormal email volume spikes.

> Use rules to quarantine bulk subscription emails during suspected attacks.

> Set an hourly limit for received emails (e.g., max 50 emails per hour) to prevent inbox flooding and trigger alerts when thresholds are exceeded.

User Awareness & Response

> Train users to recognize email bombing as a potential precursor to account compromise.

> Warn users about fake IT support chats following email floods. Verify all IT requests through official channels.

> Advise immediate password changes and multi-factor authentication (MFA) if bombing occurs.

Technical Controls

> Deploy behavioral anomaly detection on email gateways.

> Block or throttle traffic from known subscription abuse sources.

> Consider temporary inbox lockdown or auto-archiving rules during active attacks.

Third-Party Service Hardening

> Encourage vendors to implement CAPTCHA and rate limits on subscription forms.

> Monitor for API abuse by attackers leveraging automated sign-ups.

CLOSING THOUGHTS

Email bombing attacks represent a growing and increasingly effective tactic for disrupting users and concealing more serious malicious activity. By overwhelming inboxes with legitimate-looking messages, attackers are able to obscure critical security alerts and create opportunities for account compromise, fraud, and social engineering through secondary channels like collaboration tools. As these attacks continue to evolve, organizations must treat sudden spikes in email volume as a potential security incident, not a nuisance. Proactive monitoring, user awareness, and layered technical controls are essential to detecting email bombing early and limiting its effectiveness. Preparedness and coordinated response remain the strongest defenses against this volume-based threat.

How CyberForceQ Can Help

For 30 years, CyberForceQ has been a trusted name in advancing cybersecurity programs. Our expertise lies in designing and executing measurable cybersecurity strategies tailored to organizations of all sizes. With a track record of proven results, we offer services such as customized security assessments, robust security operations centers, and comprehensive strategic guidance. Let us assist your organization in prioritizing its goals, elevating your cybersecurity capabilities, and providing meaningful measurements of progress. Our participants are innovative leaders who share optimal strategies to implement and advance a proven cybersecurity program. CyberForceQ, in collaboration with our participants, is protecting the cyber realm.

CONNECT WITH US

www.cyberforceq.com 248.837.1400 solutions@cyberforceq.com