HC3: Sector Alert

March 12, 2024 TLP:CLEAR Report: 202403121700

Defense and Mitigations from E-mail Bombing

Overview

E-mail bombing, also known as mail bomb or letter bomb attacks, occur when a botnet (a single actor or group of actors) flood an e-mail address or server with hundreds to thousands of e-mail messages. They are a type of Denial of Service (DoS) attack that allows attackers to bury legitimate transaction and security messages in an unsuspecting inbox by rendering the victim's mailbox useless. By overloading a victim's inbox, attackers hope that a victim will miss important e-mails like account sign-in attempts, updates to contact information, financial transaction details, or online order confirmations.

This type of attack is of particular importance to the Healthcare and Public Health (HPH) sector. In 2016, unknown assailants launched a massive cyber attack aimed at flooding thousands of targeted "dot-gov" (.gov) e-mail inboxes with subscription requests, rendering many unusable for days. E-mail bombs are not only an inconvenience to the victim, but to everyone using that particular server. When an e-mail server is impacted by a DDoS, it can downgrade network performance and potentially lead to direct business downtime. This Sector Alert provides an overview of types of e-mail bomb techniques, as well as defenses and mitigations for targets of this type of attack.

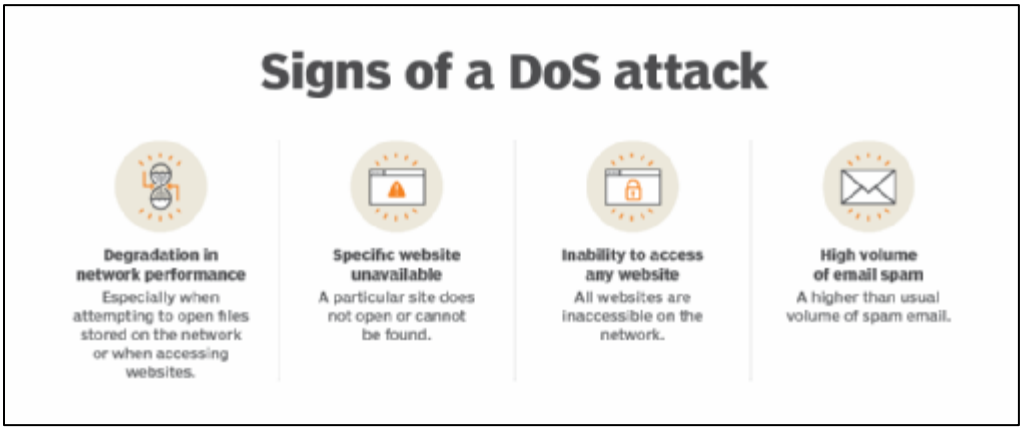

Figure 1: Signs of a bot-driven Denial-of-Service attack. *(Source: TechTarget)*

Types of E-mail Bombs

Registration Bombs: While e-mail bombing attack methods vary, most attacks use legitimate newsletter sign-ups from normal websites. The e-mail utilizes automated bots, which crawl the web, searching for newsletter sign-up pages or forms that do not require a form of live-user authentication. Attackers maintain lists of these vulnerable sites, and some will even advertise how often they update their attack lists.

Once the e-mail bomb order is placed, scheduled, and begins, the bots will sign an unlucky recipient up for all of these newsletters at once. This generates thousands of e-mails arriving to the victim immediately. Beside the immediate impact, victims receive an annoying, steady flow of unwanted e-mails that will keep arriving years after the initial attack. To add further frustration, the victim is added to additional spam, phishing, and malware lists by malicious actors. Since the bombs originate from numerous sources, this type is a Distributed Denial of Service attack (DDoS).

Attachment: An attachment attack occurs when multiple e-mails with large attachments are sent. They are designed to overload server storage space quickly and render it unresponsive.

Link Listing: A list linking attack is a tactic used by threat actors to sign up targeted e-mails to multiple e-mail subscription services. The goal is to flood e-mail addresses indirectly with subscribed content. This is possible because many subscription services do not require verification. If they did, the verification e-mails could be used as a list linking mail bomb attack. It is difficult to defend against list linking attacks because the traffic originates from legitimate sources.

Mass Mailing: Mass mailing is a type of mail bomb that is not always intentional. For example, instead of clicking on one e-mail address, a user may accidentally select all and mistakenly send the e-mail to hundreds or thousands of targeted e-mail addresses. Intentional mass mail bombs are often initiated by using botnets or malicious scripts. For example, threat actors can automate the filling of online forms with the target e-mail address as the requesting/return address.

Reply All: When a user responds by clicking 'Reply All' to an extensive list of e-mail addresses instead of just the original sender, inboxes are flooded with e-mails. Automated replies, such as out-of-office messages, often compound these e-mails. Often, reply-all mail bombs are accidental rather than an e-mail bomb attack. However, threat actors can spoof e-mail addresses and related automatic replies, and direct them to spoofed addresses.

Zip Bomb: A zip bomb, also known as a decompression bomb or zip of death attack, is a large and compressed archive file sent to an e-mail address that, when decompressed, consumes available server resources and impacts server performance.

Dark Web Attacks for Hire: There are many sellers and marketplaces on the dark web catering to anyone wishing to e-mail bomb someone. These sellers will request the e-mail address and desired starting time for the e-mail bomb. Pricing structures vary for e-mail bombs, however, one of the most "reputable" sellers that has been around the longest charges approximately $15 per 5,000 messages. Like any enterprising model, they offer price breaks for higher quantities - $30 for 20,000 messages and so on. This group's bomb is based on length of time instead of quantity of messages sent.

Mitigations After an E-mail Bomb Attack

Steps that victims that can take if they are e-mail bombed include:

- **Do not respond to an attacker:** Educate users to avoid engaging with the attacker to prevent escalation. Engaging with the attacker could increase e-mail bombardment, worsening the situation. Refraining from clicking on links or opening attachments within suspicious e-mails is crucial to avoid potential malware infections.

- **Alert your IT or cybersecurity team:** Report the situation and provide any available details about the attack. They are equipped to assist and can take measures to mitigate the attack, such as implementing additional security measures.

- **Review your account information:** It may take some time, but review your accounts for suspicious transactions. You may need to check bank, credit card, investment, loyalty program, and other

account statements. Some websites, like e-commerce platforms, will allow transactions to be archived. It is important to check recent and archived transactions, or review all transactions after sorting by date.

- **Contact your financial institution:** If you find suspicious transactions, report them immediately to your financial institution. You should also let them know what happened, as they may be able to identify any additional suspicious activities. In addition, victims should enable two-factor authentication and check their credit card statements for the past six months. Report any anomalous activity to both the retailer and the credit card company.

- **Change your passwords:** The attacker may have accessed one or more of your accounts. Change your passwords and review your account settings, including any recovery contact information, such as phone numbers. Set better passwords using a combination of letters, characters, and numbers. Regularly update your passwords, but do not resuse them.

- **Contact your e-mail provider**: Most e-mail bomb attacks subside after a day or two. Your system administrator or e-mail provider might be able to help you sort and delete the hundreds or thousands of junk e-mails you have received.

Defending Against Potential E-mail Bomb Attacks

To defend against or prevent e-mail bombs, organizations should implement security policies that address both user behavior and technical processes.

Spot the Beginning of an Attack

E-mail bombs can have the following characteristics that users can look for:

- **Lack of Coherence:** The content refers to websites or products of which you are not a subscriber or a client.
- Duplicates of the same e-mail with minor changes.
- **Unknown E-mail Senders:** Attackers frequently employ tactics to conceal their identity, using unfamiliar or spoofed sender e-mail addresses.

Addressing User Behavior: Many people have never heard of e-mail bomb attacks. Businesses are encouraged to raise awareness among colleagues. Users should also avoid using work e-mail addresses to subscribe to non-work related services. Additionally, users should limit their online exposure to direct e-mail addresses by using contact firms that do not expose e-mail addresses.

Confirmed Opt-In: A confirmed opt-in process sends an e-mail with a unique link to new signups. Once they have clicked the link, you can verify that they are a real user who owns the address that they have signed up with, and at that point, you can begin sending them a welcome email. E-mail bombers will not be able to verify that address, and will be prevented from causing damage.

Implement a reCAPTCHA: reCAPTCHA utilizes technology to determine if a human is using your platform. It can require entering a series of numbers or checking a specific box to prove that the person signing up is a real person. E-mail bombing bots are generally unable to bypass a reCAPTCHA, which would prevent them from signing up.

MITRE ATT&CK Techniques

The MITRE ATT&CK framework is a globally accessible knowledge base of adversary tactics and techniques designed for threat hunters, defenders, and red teams to help classify attacks, identify attack attribution and objectives, and assess an organization's risk. While not exclusive, below are some sample MITRE ATT&CK techniques that have been used by threat actors relevant to this problem set:

Compromise Accounts: E-mail Accounts
ID: T1586.002
Sub-Technique of T1586
Description
Adversaries may compromise e-mail accounts that can be used during targeting. Adversaries can use compromised e-mail accounts to further their operations, such as leveraging them to conduct phishing for information, phishing, or large-scale spam email campaigns. Utilizing an existing persona with a compromised e-mail account may engender a level of trust in a potential victim if they have a relationship with, or knowledge of, the compromised persona. Compromised e-mail accounts can also be used in the acquisition of infrastructure (ex: domains). A variety of methods exist for compromising e-mail accounts, such as gathering credentials via phishing for information, purchasing credentials from third-party sites, brute-forcing credentials (ex: password reuse from breach credential dumps), or paying employees, suppliers or business partners for access to credentials. Prior to compromising e-mail accounts, adversaries may conduct reconnaissance to inform decisions about which accounts to compromise to further their operation. Adversaries may target compromising well-known e-mail accounts or domains from which malicious spam or phishing e-mails may evade reputation-based e-mail filtering rules. Adversaries can use a compromised e-mail account to hijack existing email threads with targets of interest.

Phishing	
ID: T1566	
Sub-Techniques	
T1566.001	Spearphishing Attachment
T1566.002	Spearphishing Link
T1566.002	Spearphishing via Service
T1566.004	Spearphishing Voice
Description	
Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims e-mails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating e-mails or metadata/headers from	

compromised accounts being abused to send messages (e.g., e-mail hiding rules). Another way to accomplish this is by forging or spoofing the identity of the sender, which can be used to fool both the human recipient and automated security tools.

Victims may also receive phishing messages that instruct them to call a phone number, where they are then directed to visit a malicious URL, download malware, or install adversary-accessible remote management tools onto their computer (i.e., user execution).

The Way Forward

E-mail bombing, while not a novel attack method, can still adversely impact many users, including those in the HPH sector. Organizations and individuals are encouraged to implement protections, security policies, and address user behavior in order to prevent future attacks. Given the potential implications of such an attack on the HPH sector, especially concerning unresponsive e-mail addresses, downgraded network performance, and potential downtime for servers, this type of attack remains relevant to all users.

In addition to a HC3 Analyst Note on Healthcare Sector DDoS Guide on how to safeguard against ransomware/extortion attacks, some cybersecurity professionals advise that the healthcare industry acknowledge the ubiquitous threat of cyberwar against them, and recommend that their cybersecurity teams implement the following steps:

- Educate and train staff to reduce the risk of social engineering attacks via email and network access.
- Assess enterprise risk against all potential vulnerabilities, and prioritize implementing the security plan with the necessary budget, staff, and tools.
- Develop a cybersecurity roadmap that everyone in the healthcare organization understands.

At no cost, the Cybersecurity & Infrastructure Security Agency (CISA) also offers Cyber Hygiene Vulnerability Scanning services to federal, state, local, tribal and territorial governments, as well as public and private sector critical infrastructure organizations. This service helps organizations monitor and evaluate their external network posture.

The probability of cyber threat actors targeting the healthcare industry remains high. Prioritizing security by maintaining awareness of the threat landscape, assessing their situation, and providing staff with tools and resources necessary to prevent a cyberattack remains the best way forward for healthcare organizations.

HC3: Sector Alert

March 12, 2024 TLP:CLEAR Report: 202403121700

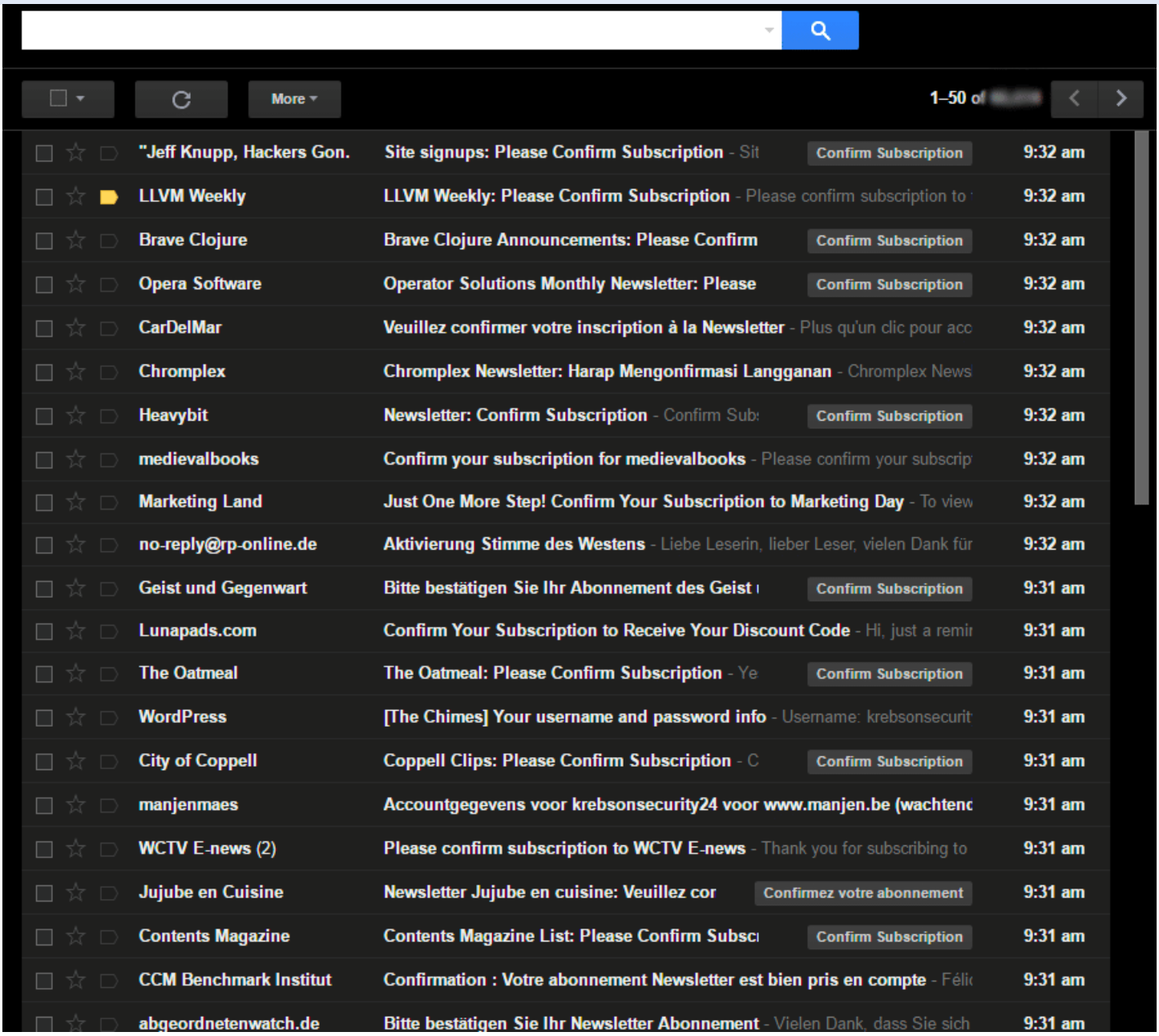

Figure 2: Inbox example of a registration bomb. *(Source: Black Cloak)*

HC3: Sector Alert

March 12, 2024 TLP:CLEAR Report: 202403121700

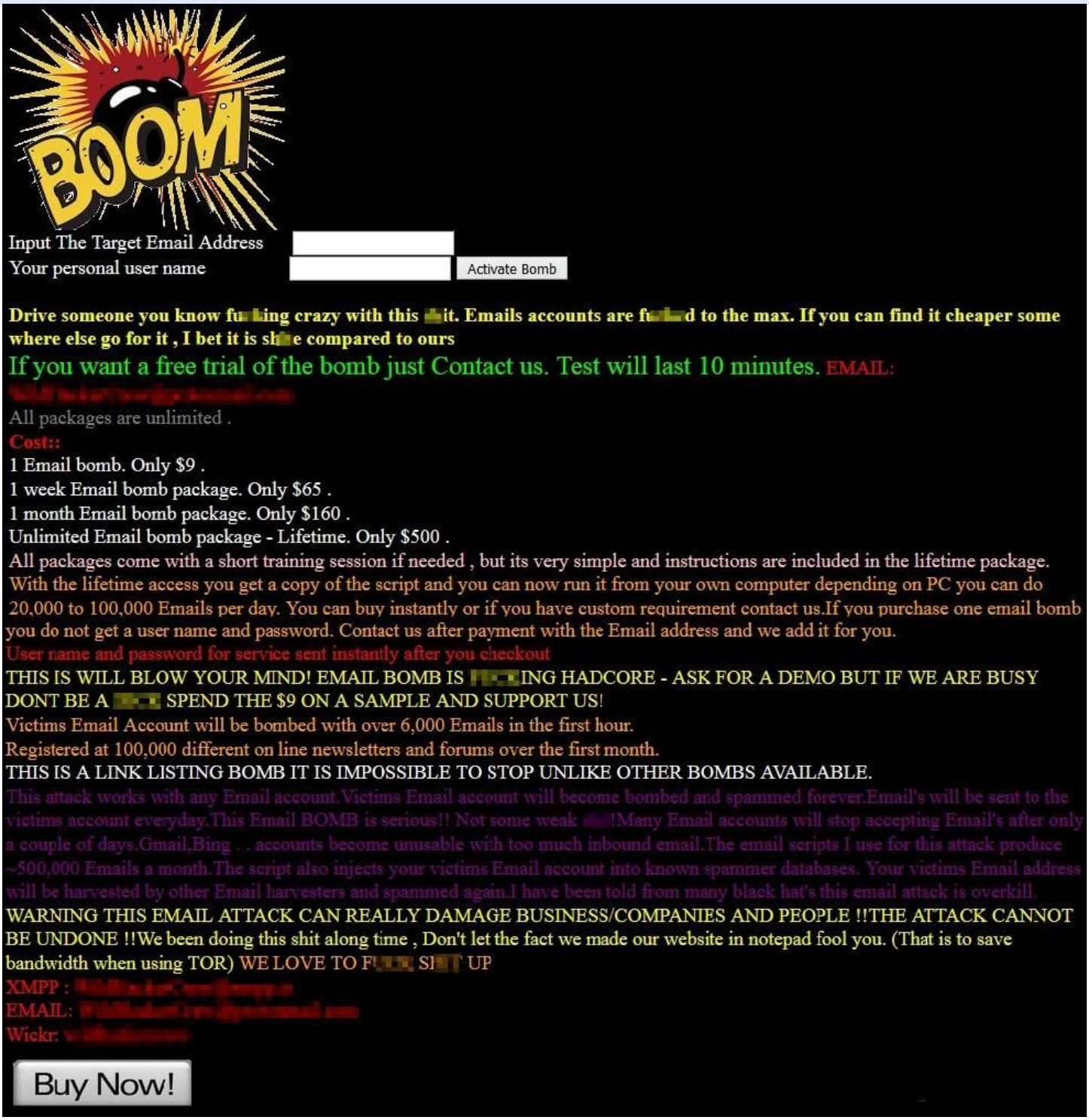

Figure 3: Sample e-mail bombing advertisement posted by a hacking group on the dark web. *(Source: AppRiver)*

Relevant HHS Reports

HC3: Analyst Note – Healthcare Sector DDoS Guide (February 13, 2023)

References

Floyd, Daniel. "New Registration Bomb Email Attack Distracts Victims of Financial Fraud." BlackCloak. Accessed March 11, 2024. https://blackcloak.io/new-registration-bomb-email-attack-distracts-victims-of-financial-fraud/

"Fraudster trick – Email spam attack." Ontario Securities Commission. Accessed March 11, 2024. https://www.getsmarteraboutmoney.ca/learning-path/types-of-fraud/fraudster-trick-email-spam-attack/

Haven, Simon. "Email Bomb Defense: 7 Essential Strategies to Protect Your Inbox." Mailfence. December 7, 2023. https://blog.mailfence.com/email-bomb-defense-7-essential-strategies-to-protect-your-inbox/

"MITRE ATT&CK Technique – Compromise Accounts: Email Accounts." MITRE ATT&CK. Accessed March 11, 2024. https://attack.mitre.org/techniques/T1586/002/

"MITRE ATT&CK Technique – Phishing." MITRE ATT&CK. Accessed March 11, 2024. https://attack.mitre.org/techniques/T1566/

Pickett, David. "Email Bombs Disguise Fraud – Distributed Spam Distraction." AppRiver. Accessed March 11, 2024. https://appriver.com/blog/email-bombs-disguise-fraudulent-activity

Southard, Scott. "How to protect yourself against email list bombing." Intercom. Accessed March 11, 2024. https://www.intercom.com/help/en/articles/3202277-how-to-protect-yourself-against-email-list-bombing

Zola, Andrew. "Mail Bomb." TechTarget. Accessed March 11, 2024. https://www.techtarget.com/searchsecurity/definition/mail-bomb

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback