MS-ISAC®

MS-ISAC Security Primer

Email Bombs

February 2018, SP2018-0209

An email bomb is an attack against an email server designed to inhibit the server's normal function or render it unresponsive, preventing email communications, degrading network performance, or causing network downtime. An attack's intensity can range from an inconvenience to a complete interruption of service. Some email bombs are accidental or self-inflicted, such as when automatic replies sent to a distribution list cause a cascade of emails. Additionally, cybercriminals sometimes use email bomb attacks to mask other attacks and prevent users from receiving notices about account activity.

- *Mass mailing attacks* occur when actors intentionally or unintentionally send large quantities of email traffic to targeted email addresses.
- *List linking attacks* involve malicious actors signing targeted email addresses up to numerous email subscription services. Many of these services do not ask for verification or if they do, they send confirmation requests via email. This type of attack is difficult to prevent because the traffic originates from various legitimate sources.
- *ZIP bomb attacks* consist of malicious actors sending malicious archive files designed to decompress to very large sizes. When the email server decompresses the file, significant server resources are consumed, potentially causing the server to slow down or stop responding.
- *Attachment attacks* occur when malicious actors send multiple emails with large attachments, intending to overload the storage space on a server and cause the server to stop responding.
- *Reply-all email bombs* occur when dissemination list members reply to all members of the list instead of just the original sender. This inundates inboxes with a cascade of emails, which are compounded by automated replies, such as out-of-office messages. This type of attack also occurs when a malicious actor spoofs an email and the automatic replies are directed toward the spoofed address.

RECOMMENDATIONS:

Prevention

- Ensure email delivery software is up-to-date, patched, and includes anti-virus capabilities.
- Employ "tarpitting" to block or slow traffic from a sending IP address if the traffic from that address exceeds a predefined threshold (e.g. greater than ten emails per minute).
- Consider blocking file attachments used in email bomb attacks, such as .zip, .7zip, .exe, and .rar.
- Limit the maximum email attachment file size.
- Ensure out-of-office, bounce back, and other automatic messages are only sent once to prevent an endless loop of recurring automatic replies.
- Where possible, limit send permissions so that only internal and authorized users may send to distribution lists.
- Avoid posting plain text email addresses online as malicious actors are able to scrape webpages for email addresses allowing malicious actors to target them for spam campaigns.

During an attack

- If your inbox is overloaded, avoid mass deleting emails and instead using email rules to filter spam.
- Ensure critical inboxes use failover services and notification options to safeguard against deletion.

Avoid Unwitting Participation

- Implement CAPTCHA on user subscription forms to prevent bots from using your service.
- Send verification emails to newly subscribed users to prevent sending unwanted emails.

TLP: WHITE The MS-ISAC is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments. More information about this topic, as well as 24x7 cybersecurity assistance for SLTT governments, is available at 866-787-4722, SOC@cisecurity.org, or https://www.cisecurity.org/ms-isac/.