Detection Strategy for Email Bombing, Detection Strategy DET0355

Archived: 2026-04-05 18:42:54 UTC

AN1008

Detect abnormally high volume of inbound email messages or repetitive attachments being delivered to a single mailbox within a short time window. Defenders should look for anomalous spikes in message counts and repetitive attachment file creation events correlated with targeted users.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Defines the aggregation interval (e.g., 5 minutes, 1 hour) for detecting spikes in inbound email traffic.
RecipientThreshold	Defines maximum number of acceptable messages per user before triggering anomaly.
AttachmentSizeThreshold	Defines the size threshold for repetitive attachments to be flagged.

AN1009

Monitor mail server logs (e.g., Postfix, Sendmail) for excessive connections or inbound message counts targeting a single recipient. Correlate with repetitive attachment storage in /var/mail or /var/spool/mail directories.

Log Sources

Mutable Elements

Field	Description
MailVolumeThreshold	Tunable value for the maximum acceptable emails per minute per user.
AttachmentPatternList	List of suspicious attachment extensions that may be abused for repetitive delivery.

AN1010

Detect abnormal use of email clients (e.g., Outlook, Thunderbird) showing mass arrival of messages or repetitive attachments being locally stored. Correlate message volume with file creation activity in mail cache directories.

Log Sources

Data Component	Name	Channel
Application Log Content (DC0038)	m365:exchange	MailDelivery: High-frequency delivery of messages or attachments to a single recipient

Mutable Elements

Field	Description
UserContext	Context for distinguishing between VIP or sensitive recipients and general users.

AN1011

Monitor unified logs and Mail.app activity for repetitive incoming messages with attachments. Defenders should look for large volumes of incoming mail stored under ~/Library/Mail with unusual timing or repetitive subjects.

Log Sources

Mutable Elements

Field	Description
FileCountThreshold	Threshold for repetitive attachment files created within a defined interval.
