Email Hunting and Detection Cheat Sheet

Version 1.0
Mehmet Ergene @Cyb3rMonk

Attribute	Technique	What to look for
Sender IP	Calculate email count by SenderIP-SenderDomain and order by SenderDomain. If possible, calculate email count per SenderIP for each SenderDomain.	If there are more than 1 IP for the same SenderDomain and the email count is small for one of the IPs, it may indicate domain spoofing or phishing. Exclude known email service provider domains like Gmail, Hotmail, Yahoo, etc. Focus on corporate domains.
Sender Domain	Get a list of most used brands in phishing attacks (vade secure provides top 25). Generate lookalike domains of these domains by using dnstwist or any other tool.	Search emails that come from these lookalike domains. Apply the same technique for your own domain(s).
	Detect sender domains that are seen for the first time in the environment.	Check the domain age. Newly registered domains may be malicious.
Sender Address	Calculate email count per SenderAddress-RecipientAddress and RecipientAddress-SenderAddress for the same SenderAddress, RecipientAddress (bidirectional traffic).	A high number of inbound and outbound emails might indicate C2 over email. A high number of outbound emails between the same sender and recipient might indicate data exfiltration.
From Address	Calculate dcount(SenderIP) by FromAddress.	2 different IPs for the same FromAddress may indicate phishing. Whitelist secondary IPs if the domain and IP are known.
Recipient Address	Calculate email count per SenderAddress-RecipientAddress and RecipientAddress-SenderAddress for the same SenderAddress, RecipientAddress (bidirectional traffic).	A high number of inbound and outbound emails might indicate C2 over email. A high number of outbound emails between the same sender and recipient might indicate data exfiltration.
Recipient Domain	Calculate the sum of email size per RecipientDomain for outbound emails.	Higher values may indicate data exfiltration.
URL Info	Calculate URL and/or URL Domain count for the last 24h.	Small values may indicate a spear phishing URL. High values may be a phishing or marketing/spam.
	Correlate URL info with other logs. The guide can be found here.	Follow the guide
Attachment Info	Attachment info requires pivoting and correlation. The related guide is here.	Follow the guide
Size	Calculate the sum of email size per RecipientAddress or SenderAddress for outbound emails for the last 24h or longer.	Higher values may indicate data exfiltration.
Forwarding Rules	Periodically check forwarding rules in mailboxes and gateways.	Look for suspicious email addresses. May indicate data exfiltration.