Detection of Email Addresses, Detection Strategy DET0814

Archived: 2026-04-02 11:09:43 UTC

Technique Detected: Email Addresses | T1589.002

ID: DET0814

Domains: Enterprise

Analytics: AN1946

Version: 1.0

Created: 21 October 2025

Last Modified: 21 October 2025

Version Permalink

Live Version

Analytics

- PRE

AN1946

Monitor for suspicious network traffic that could be indicative of probing for email addresses and/or usernames, such as large/iterative quantities of authentication requests originating from a single source (especially if the source is known to be associated with an adversary/botnet). Analyzing web metadata may also reveal artifacts that can be attributed to potentially malicious activity, such as referer or user-agent string HTTP/S fields.

Log Sources

Data Component	Name	Channel
Network Traffic Content (DC0085)	Network Traffic	None