Detection Notes

▨ Status	Done

Attack	Tactic	Technique ID	Detection Note	Scoring
Phishing Link	Initial Access	T1566.002	Detect emails containing suspicious URLs, especially shortened links or mismatched domains; use secure email gateway logs.	5 (Critical)
Credential Harvesting (Fake Login)	Credential Access	T1056.003	Monitor web proxy logs for requests to suspicious domains hosting login	3 (Medium)

Attack	Tactic	Technique ID	Detection Note	Scoring
			pages; detect multiple credential submissions from same IP.	
Domain & Hosting Infra	Resource Development	T1583.001 / T1583.003	Detect lookalike or recently registered domains via threat intel feeds; monitor for free hosting services tied to malicious activity.	4 (High)
SSH Brute Force	Credential Access	T1110.001	Alert on repeated failed SSH login attempts from same IP within 5 minutes using SIEM correlation.	4 (High)
Port Scanning	Reconnaissance	T1046	Monitor network flow logs for a single source IP connecting to many different destination ports in a short time.	3 (Medium)