Detection Strategy for Spearphishing Voice across OS platforms, Detection Strategy DET0245

Archived: 2026-04-05 17:33:27 UTC

AN0683

Monitor call log records from corporate devices for unusual or unauthorized numbers, especially repeated calls to/from known malicious phone numbers. Correlate with subsequent system events (e.g., browser navigation, remote management tool execution).

Log Sources

Mutable Elements

Field	Description
PhoneNumberBlocklist	List of known malicious or suspicious phone numbers; must be tuned per environment
TimeWindow	Threshold for correlating call events with subsequent suspicious system activity

AN0684

Audit VoIP/SIP logs for suspicious outbound calls or call setup messages to unusual endpoints. Correlate with user activity such as browser execution or package installation following the call.

Log Sources

Mutable Elements

Field	Description
CallDestinationPatterns	Regular expressions or rules for spotting abnormal call destinations
UserContext	Expected users who initiate VoIP traffic vs. anomalous accounts

AN0685

Monitor Facetime, iMessage, or SIP client logs for anomalous voice call attempts. Link to subsequent user execution events (downloads, RMM installs) triggered post-call.

Log Sources

Mutable Elements

Field	Description
CallerIDPatterns	Patterns of spoofed caller IDs that must be tuned based on region and telecom provider
PayloadCorrelation	Define what follow-on events (browser downloads, execution) to correlate with call logs

AN0686

Correlate MFA push fatigue or unusual consent grant attempts with call activity where adversaries may have socially engineered the user over voice.

Log Sources

Data Component	Name	Channel
Application Log Content (DC0038)	m365:unified	Unusual MFA requests or OAuth consent events temporally aligned with user-reported vishing call

Mutable Elements

Field	Description
MFARequestThreshold	Number of MFA push requests within a timeframe aligned to a suspicious call
ConsentGrantPatterns	Unusual OAuth consent URLs or delegated scopes

---