Phishing → Ransomware: Kill Chain + MITRE ATT&CK — One-Page Detection Cheat-Sheet

Scenario: Malicious 'Invoice' .docm sent via phishing. User enables macros → dropper pulls payload → C2 → encryption.

Kill Chain Stage	Attack Example	MITRE IDs
Reconnaissance	Collect staff emails & org details for believable lures.	T1591, T1598
Weaponization	Craft malicious .docm with embedded VBA macro / dropper.	T1587.001
Delivery	Send phishing email with 'Invoice' attachment to targets.	T1566.001
Execution	User opens file & enables macros; script executes.	T1204.002, T1059.001
Installation / Persistence	Dropper fetches payload; sets autoruns / tasks / services.	T1547.001, T1053.005, T1543.001
C2 (Command & Control)	Beacon to remote server over encrypted web/TCP	T1573, T1071.001
Impact	Encrypt files; delete shadow copies; drop ransom r	T1486, T1490

Detection Checklist

Email / Perimeter

- Flag newly registered or look-alike domains; extra scrutiny for 'invoice' themes.
- Block or quarantine macro-enabled attachments from external senders by default.
- Secure Email Gateway rules for T1566.001; detonate suspicious docs in sandbox.

Network

- Detect rare outbound hosts, unusual SNI/JA3, and off-hours beacon patterns.
- Alert on first-seen domains with high egress; correlate proxy & DNS logs.

Host / EDR

- Alert when Office apps spawn scripts: WINWORD → powershell/mshta/wscript.
- Enable PowerShell Script Block Logging (4104) & AMSI; watch for obfuscated commands.
- Monitor autoruns (Run/RunOnce), new services, Scheduled Tasks; Sysmon EIDs 1, 13.

Impact / Recovery

- Alert on vssadmin delete shadows / wbadmin / bcdedit usage.
- Detect mass file changes/renames & ransom-note creation bursts.
- Maintain immutable backups; test restores regularly.

Muhammad Elladan — Aspiring SOC 1 Analyst