Case Study: Exploitation in Personal Relationships

Scenario

Jane and John are a couple married for two years. Recently, John has become suspicious of Jane and suspects she might be having affairs. To confirm his suspicions, John decides to exploit Jane's phone. He avoids installing third-party applications, aiming to keep his activities hidden and less suspicious. Jane notices John's unusual behavior around her phone and consults a Security Analyst to determine if her device has been compromised.

Possible Exploitation Methods John Could Use

1. Call Forwarding Exploitation: John could secretly enable call forwarding on Jane's phone by dialing special network codes (e.g., *21*number#). This would redirect Jane's incoming calls to John's phone, allowing him to eavesdrop without installing apps.

2. Voicemail Manipulation: If Jane's voicemail PIN is weak, John could reset it and gain access to her voicemails remotely.

3. SIM Swap or SIM Cloning: John could attempt to duplicate Jane's SIM card, gaining access to calls and SMS messages without needing her physical device.

4. Exploiting Built-In Features: Instead of third-party apps, John might misuse default phone features such as conferencing, merging calls, or setting up silent call monitoring if supported by the carrier.

Security Analyst's Detection Steps

1. Check Call Forwarding Settings: Dial the carrier-specific code (e.g., *#21#) to verify whether any forwarding rules are active.

2. Review Voicemail Security: Ensure voicemail PINs are strong and check for suspicious login activity.

3. Inspect SIM Activity: Contact the carrier to confirm there are no SIM clones or duplicate SIMs registered.

4. Analyze Call Logs: Look for unusual three-way calls, merged calls, or repeated short call attempts that may indicate eavesdropping.

5. Check Permissions and Settings: Ensure no unauthorized accounts, paired devices, or changes in default communication settings exist.

Conclusion

This case study highlights how exploitation can occur without installing third-party software. By leveraging built-in carrier and device features, an attacker can discreetly

intercept communications. Security Analysts must focus on reviewing native settings such as call forwarding, voicemail security, and SIM activity to detect and mitigate such threats.