Task 5

Research three recent malware incidents, describe their attack methods, and explain how each was mitigated or resolved.

1. "GreedyBear" Firefox wallet extensions (August 2025).

- Situation: Over 150 fake crypto wallet extensions slipped into Mozilla's add-ons store and launched clean to pass reviews, collected good ratings and pushed malicious updates to siphon seed phrases and drain crypto wallets - at least a million dollars were stolen.
- Method: Wallet extensions that become malicious after approval, siphoning crypto via extension hollowing.
- Solution: Mozilla pulled the extensions. Users still had to manually remove them, rotate their wallet keys/seed phrases, and reset credentials. Organisations were advised to enforce extension allow-lists via browser policy and monitor for IOC domains/Ips.

2. Anatsa Android banking trojan on Google Play (July 2025)

- Situation: A Document Viewer - File Reader app turned into a dropper after it accumulated over 50K installs. Then it used overlay phishing, fake "scheduled maintenance" screens, keylogging, and automated transactions that targeted North American banking apps.
- Method: A Trojan dropper app from Google Play Store that overlays fake banking screens, logs keystrokes, and automates fraud.
- Solution: Google removed the app and Play Protect was updated so that it started flagging it. The affected users were asked to

uninstall, run Play Protect scans, and reset banking credentials and also reset 2FA. The banks also tightened overlay protections and device-integrity checks for further security.

3. Raspberry Pi ATM jackpotting (August 2025)

- Situation: Threat group UNC2891 planted Raspberry Pi devices inside ATMs, interfacing with internal components to issue illicit dispense commands. In this method physical intrusion was combined along with modern day scripting to get the cash out easily.
- Method: Hidden Raspberry Pi implants inside ATMs issuing direct cash dispense commands.
- Solution: Banks started fleet-wide hardware inspections, added tamper-evident seals and sensors, reviewed firmware, and segmented internal ATM buses. The cases escalated to law enforcement and information sharing groups.