Three Recent Malware Incidents (2025) — Methods & Mitigations

1) Interlock Ransomware at Kettering Health (Ohio, USA) — May–June 2025

What happened: Kettering Health, which operates 14 medical centers in Ohio, confirmed a systemwide outage beginning May 20, 2025 was the result of an Interlock ransomware attack. Normal operations for key services—including core components of its Epic EHR—were restored by June 2, 2025.

Attack method: Interlock is a RaaS operation that uses double extortion and has recently adopted new delivery techniques (e.g., malvertising, social engineering, and PowerShell-based initial access).

Mitigation / resolution: Kettering isolated affected systems, engaged law enforcement and incident response, restored EHR/Epic components and resumed clinical operations in phases. Sector guidance recommends layered defenses: user training against social engineering, domain filtering, network segmentation, strong backups, MFA, and timely patching.

2) Anatsa Android Banking Trojan via Google Play — June–July 2025 (North America)

What happened: ThreatFabric observed Anatsa (a device-takeover Android banking trojan) targeting U.S. and Canadian users via a Google Play dropper app that amassed 50,000+ downloads before removal.

Attack method: The dropper app is initially legitimate; a later update adds code that pulls down Anatsa. Once installed, Anatsa uses overlay attacks, keylogging, and remote-control capabilities to steal credentials and execute fraudulent transactions.

Mitigation / resolution: Google removed the malicious app from the Play Store. Impacted users should uninstall the app, revoke Accessibility permissions, run mobile AV/EDR, reset device if needed, and contact banks to monitor and reset accounts.

3) PS1Bot Multi-Stage Malware via Malvertising/SEO Poisoning — Ongoing in 2025

What happened: Cisco Talos detailed a widespread malvertising and SEO poisoning campaign leading to a modular framework dubbed PS1Bot (PowerShell + C#). Active throughout early–mid 2025, it delivers modules for info-stealing, keylogging, screenshot capture, wallet seed phrase harvesting, and persistence.

Attack method: Users are lured to download a ZIP archive. Inside is a JavaScript downloader that retrieves a JScript scriptlet, which then writes and runs a PowerShell script that beacons to the C2 and fetches further modules.

Mitigation / resolution: Block malvertising with DNS/web filters; prefer direct vendor downloads. Enforce application control on script interpreters (PowerShell, wscript/cscript), constrain PowerShell with logging, and monitor suspicious execution paths. Use EDR rules for JS/VBS + PowerShell chains and inspect network egress with IoCs from Talos.

References

- Kettering Health — Cybersecurity Incident FAQ & updates (May–June 2025): https://ketteringhealth.org/cybersecurity-incident-faq/
- Kettering Health — System-wide technology outage update (June 5, 2025): https://ketteringhealth.org/system-wide-technology-outage/
- The Record — "Kettering Health confirms attack by Interlock ransomware group…" (June 6, 2025): https://therecord.media/kettering-health-ohio-interlock-ransomware
- HIPAA Journal — "Kettering Health Resumes Normal Operations…" (June 2025): https://www.hipaajournal.com/kettering-health-ransomware-attack/
- HIPAA Journal — "Feds Issue Interlock Ransomware Warning…" (late July 2025): https://www.hipaajournal.com/interlock-ransomware-alert-2025/
- ThreatFabric — "Anatsa Targets North America…" (July 8, 2025): https://www.threatfabric.com/blogs/anatsa-targets-north-america-uses-proven-mobile-campaign-process
- The Hacker News — "Anatsa Android Banking Trojan Hits 90,000 Users…" (July 2025): https://thehackernews.com/2025/07/anatsa-android-banking-trojan-hits.html
- SC Media — "North American banks targeted by Anatsa…" (July 9, 2025): https://www.scworld.com/brief/north-american-banks-targeted-by-anatsa-banking-trojan
- Cisco Talos Blog — "Malvertising campaign leads to PS1Bot…" (Aug 12, 2025): https://blog.talosintelligence.com/ps1bot-malvertising-campaign/
- TechRadar Pro — Coverage of PS1Bot (Aug 2025): https://www.techradar.com/pro/security/this-new-malware-really-goes-the-extra-mile-when-it-comes-to-infecting-your-devices