MALWARE INCIDENTS

1) DaVita (Healthcare) — Ransomware Breach (August 2025)

On **August 21, 2025**, dialysis provider **DaVita** disclosed a **ransomware** incident impacting approximately **2.7 million people** (as listed on the U.S. Health Dept. breach portal). Portions of the network were encrypted and sensitive data may have been exposed.

Attack method:

- Likely **ransomware** intrusion leveraging initial access via exposed services, phishing, or third-party footholds (specific initial vector not yet public).
- **Encryption** of on-prem resources and data exfiltration are typical of double-extortion playbooks.

Resolution:

- **Incident response activated:** affected systems isolated, some IT services taken offline; forensics and third-party IR engaged.
- **Regulatory steps:** notifications to HHS and affected individuals; law enforcement informed.
- **Recovery:** phased restoration from clean backups; credential resets and hardening measures.
- **Hardening recommendations for peers:** rapid patching, network segmentation, MFA everywhere (especially for remote access and privileged accounts), EDR with ransomware canary detection, immutable/offline backups, tabletop exercises.

2) Anatsa (Mobile) — Android Banking Trojan via Fake PDF/Utility Apps (July 2025)

In **July 2025**, researchers observed a new **Anatsa** campaign in **North America**, with malicious apps (posing as **PDF readers or utility tools**) on **Google Play** amassing **~90,000 installs** before takedown.

Attack method:

- **Dropper apps** delivered the Anatsa banking **trojan**, which uses **overlay attacks** to steal credentials from banking apps, abuses **Accessibility Services** to intercept OTPs and control UI, and supports **ATS (Automated Transfer System)** for fraudulent transactions.
- Additional capabilities include keylogging and device info exfiltration.

Resolution:

- **App store action:** Google removed flagged apps; Play Protect updates pushed.
- **User remediation:** uninstall rogue apps; run mobile AV; rotate banking credentials; disable Accessibility for unknown apps; check statements and enable bank alerts.
- **Enterprise controls:** enforce **mobile device management** (block unknown stores, require Play Protect), restrict Accessibility abuse, and monitor for overlay permissions.

3) Colt Technology Services (Telecom) — Warlock Ransomware via SharePoint CVEs (August 2025)

On **August 12, 2025**, UK telecom **Colt Technology Services** took multiple systems offline (incl. customer portal/API) following a **cyberattack** linked to the **Warlock** ransomware group. Data theft claims (hundreds of GB) were posted on a Tor forum.

Attack method:

- **Exploitation of Microsoft SharePoint vulnerabilities** to achieve **remote code execution** and credential/key theft on **unpatched servers** (public reporting references **CVE-2025-53770** among others).
- Post-exploitation: data staging/exfiltration and disruptive encryption (ransomware).

Resolution:

- **Containment:** affected systems isolated; internet-facing services temporarily disabled; customer communications moved to alternative channels.
- **Eradication & recovery:** patching SharePoint to vendor guidance; key/cert rotation; credential resets; rebuild of compromised hosts; staged service restoration.
- **Risk reduction:** enforce rapid **patch management**, restrict management interfaces, harden SharePoint (least privilege, service isolation), deploy **EDR** and **NDR**, implement **exfiltration controls** (DLP/egress monitoring), and maintain **tested offline backups**.