Three Recent Malware Incidents (2025)

Report prepared by Sneha K

1) DaVita — Ransomware Attack (April 2025)

What happened:
About **2.7 million patients** were affected after attackers accessed DaVita's laboratory database. Critical dialysis services stayed online, but sensitive patient data was exposed.

Attack method:
Unauthorized access followed by **ransomware encryption**. Attackers used data exposure as leverage.

Mitigation / resolution:

- DaVita isolated affected systems.
- Engaged third-party cybersecurity experts.
- Notified patients and provided **credit monitoring**.
- Absorbed ~$13.5M in Q2 2025 costs.

---

2) Inotiv — Qilin Ransomware (August 2025)

What happened:
On **August 8, 2025**, Inotiv detected ransomware in its systems. The **Qilin** group claimed theft of ~176 GB of data (~162,000 files).

Attack method:
Double-extortion ransomware — data exfiltration followed by encryption.

Mitigation / resolution:

- Shut down parts of IT infrastructure.
- Brought in external experts and notified authorities.
- Forensic analysis and offline recovery initiated.
- Temporary disruption to operations.

---

3) City of St. Paul, Minnesota — Interlock Ransomware (July–August 2025)

What happened:
On **July 25, 2025**, ransomware crippled city infrastructure (payments, Wi-Fi, internal networks). A **state of emergency** was declared, with the **National Guard** mobilized. The **Interlock** gang claimed responsibility and leaked ~43 GB of stolen data after ransom was refused.

Attack method:
Ransomware targeting **critical infrastructure** with theft + disruption.

Mitigation / resolution:

- Refused ransom demand.
- Shut down networks and reset all accounts manually.
- Partnered with FBI and launched **Operation Secure St. Paul** for hardening and recovery.

Comparison Table:

Incident	Malware Type	Impact	Mitigation
DaVita	Ransomware	2.7M patients' data exposed	Isolation, patient notifications, credit monitoring
Inotiv	Qilin Ransomware	176 GB stolen; operations disrupted	Shutdown, experts engaged, forensic recovery
St. Paul City	Interlock	City services offline; data leaked	Emergency response, FBI help, password resets