### **Malware Incidents**

**1. City of Columbus Ransomware Attack (July 2024)**

* **What Happened:**
  + Rhysida ransomware group attacked the city’s systems.
  + Around 6.5 TB of sensitive data was stolen.
  + When the city refused to pay ransom , 3.1 TB of data was leaked online , affecting nearly 500000 residents.
* **Attack Method:**
  + Hackers made someone download a malicious file that deployed ransomware.
  + Used a ready made ransomware service to carry out the attack.
* **Mitigation and Resolution:**
  + Shut down infected systems quickly.
  + Coordinated with FBI and federal agencies.
  + Notified affected residents and provided credit monitoring.
  + Recovery costs totaled about $7 million.
  + Legal action against a security researcher was later dropped.

**2. Synnovis (London Hospitals) Ransomware Attack (June 2024)**

* **What Happened:**
  + Qilin ransomware gang targeted Synnovis, a key NHS pathology provider.
  + Critical systems were encrypted, blocking access to test results and disrupting diagnostics.
* **Attack Method:**
  + Ransomware disabled IT infrastructure, preventing hospitals from accessing essential medical data.
* **Mitigation and Resolution:**
  + NHS declared a critical incident and brought in cyber response teams.
  + Staff switched to manual processes to maintain urgent services.
  + IT systems were gradually restored over summer and autumn 2024.
  + Legal steps including injunctions , protected patient data from misuse.

**3. AnyDesk Supply Chain Compromise (Early 2024)**

* **What Happened:**
  + Attackers breached AnyDesk’s production environment.
  + Source code and code-signing certificates were stolen.
  + No malware was found in official software.
* **Attack Method:**
  + Exploited misconfigurations in production systems.
  + Created a supply chain risk but did not affect end user software directly.
* **Mitigation and Resolution:**
  + Revoked compromised code signing certificates.
  + Reset web service passwords.
  + Worked with CrowdStrike and law enforcement to contain the breach.
  + Released secure software updates and advised users to upgrade immediately.