Recent Malware Incidents

Kido Nursery Schools — Radiant Data Theft & Extortion (September 2025)

Incident Summary

In late September 2025, UK-based Kido nurseries (with branches worldwide) were targeted by a cybercriminal group calling itself Radiant. The attackers stole highly sensitive data including children's photos, staff records, and family information. They posted ransom demands of £600,000 on the dark web and threatened to leak the stolen data unless paid. The group claimed to have deleted the data after widespread media coverage and law enforcement involvement, though experts warned this cannot be trusted.

Attack Method

- Likely initial access through phishing or weak credentials in remote systems
- Attackers exfiltrated data instead of encrypting systems
- Psychological extortion by highlighting sensitive children's data

Mitigation & Resolution

- Kido refused ransom and worked with UK law enforcement
- Immediate family and regulator notifications under GDPR
- Plans for stronger access control and encryption for sensitive data

Lessons Learned

- Extortion-only ransomware is becoming common
- Schools/childcare must enforce strict data minimization and access policies
- Transparent communication is critical in sensitive cases

Collins Aerospace — Ransomware on Muse Check-in Platform (September 2025)

Incident Summary

Between 19–24 September 2025, a ransomware attack crippled the Muse passenger check-in and boarding system, provided by Collins Aerospace. This disruption cascaded into major delays at European airports, including Heathrow, Brussels, and Berlin, forcing airlines to process check-ins manually. ENISA confirmed ransomware as the cause, and police later announced the arrest of one suspect.

Aparna Prasad
Amal Jyothi College of Engineering

Attack Method

- Attackers targeted a third-party service provider
- Ransomware payload encrypted core Muse servers
- Outages spread internationally, showing dependency risks

Mitigation & Resolution

- Airports reverted to manual processes temporarily
- Collins Aerospace worked with ENISA and law enforcement
- Full service restored within 5 days with system patches applied

Lessons Learned

- Critical systems need resilient fallback mechanisms
- Vendors require strict cybersecurity audits
- Law enforcement collaboration is essential for supply chain ransomware cases

Oracle E-Business Suite — Cl0p Extortion Campaign (October 2025)

Incident Summary

In early October 2025, Oracle issued a security advisory warning of a mass extortion campaign linked to the Cl0p ransomware group. Attackers exploited unpatched Oracle E-Business Suite vulnerabilities to compromise systems and sent threatening emails demanding payment. This continued Cl0p's pattern of exploiting enterprise software flaws.

Attack Method

- Attackers scanned the internet for vulnerable Oracle E-Business Suite servers
- Exploited unpatched vulnerabilities and misconfigurations
- Sent extortion emails threatening to leak financial/HR data

Mitigation & Resolution

- Oracle urged customers to apply latest security patches
- Network segmentation and WAFs to protect ERP applications
- Audit logs and enable MFA to detect and block attacks

Lessons Learned

- Patch management is critical
- Legacy ERP systems pose long-term risks
- Extortion tactics mix technical exploitation with social engineering