Malware Incident Report Updated

Summary:

A ransomware variant was executed via a phishing email attachment.
Critical data was encrypted and access was denied until a ransom was paid..

Identify:

Unusual file extensions and high disk usage triggered alerts.
Endpoint detection systems identified the malware's source..

Protect:

Devices were isolated.
Email filtering was updated.
Endpoint protections and user permissions were hardened..

Detect:

Logs showed encryption processes.
Security software confirmed malware signatures..

Respond:

Affected systems were removed from the network.
Forensic analysis was conducted and staff alerted..

Recover:

Systems restored from offline backups.
Reimaged endpoints.
Conducted user training..

Reflections/Notes::

Revealed gaps in phishing awareness and backup validation.
Offline backups were critical..