Ransomware Incident Analysis

Example report

Kit Baroness | Security analysis example

Assessment and source basis

My Incident Handler's Journal examines a ransomware incident affecting a small health care clinic. The supplied account describes employees opening malicious email attachments, malware installation, encryption of critical files, and disruption to patient records and business applications.

The work organized the incident into who, what, when, where, and why, then connected the impact to investigation and recovery priorities. No cybersecurity tools were directly used in the analysis. Email logs, endpoint records, malware analysis, and backup checks were identified as potential investigation sources, rather than completed tests.

Findings and reasoning

The references below identify sections of my journal, not independently collected system artifacts.

Source reference	Observation in the supplied account	Assessment
J-S1: incident description	Malicious attachments preceded malware installation and encryption.	Phishing is the reported entry path; confirm the message, attachment, and endpoint sequence before treating the full cause as independently established.
J-S2: discovery and impact	Staff could not access files and saw ransom notes at approximately 9 a.m. on a Tuesday.	The account supports an availability incident. The exact event date, time zone, affected asset count, and outage duration remain unverified.
J-S3: affected environment	Employee computers, patient records, and business systems were involved.	Recovery priorities must account for patient-care workflows and dependencies between systems.
J-S4: response notes	Affected systems were shut down and technical assistance was sought.	The account describes response activity; effective isolation, clean restoration, and return-to-service results require evidence.

The journal attributes the attack to a group targeting health care and transportation. That attribution is part of the supplied scenario; supporting threat-intelligence or forensic evidence was not included. It is not necessary to resolve attribution before protecting affected services.

Business effect

Loss of access to patient records can interrupt care and administrative work. The record also raises a confidentiality concern because affected systems hold sensitive information. Encryption alone does not establish whether information was copied or disclosed; investigation should preserve that distinction.

Proposed response and validation

Work item	Proposed accountable role	Completion evidence
Establish affected systems and preserve investigation records.	Incident lead	Asset scope, event timeline, evidence references, and recorded gaps.
Verify containment and remove the cause of compromise.	Security operations owner	Documented isolation, reviewed endpoint findings, and checks against continued activity.
Validate recovery of priority services.	Service owner	Backup integrity, clean restoration, application checks, and business-owner acceptance.
Improve prevention and readiness.	Operations owner	Reviewed email controls, endpoint protection, training, and a demonstrated recovery process.

These roles and checks are proposed follow-through. The journal does not establish that the checks were performed or that recovery was completed.

Closure and reference method

Closure requires verified service restoration, a decision on remaining exposure, and assigned improvement actions. This reporting structure uses current NIST SP 800-61 Rev. 3 and Cybersecurity Framework 2.0 to organize analysis, response, recovery, and improvement.

https://doi.org/10.6028/NIST.SP.800-61r3