Digital Forensics Investigation – Insider Threat & Data Exfiltration Analysis

Environment: Corporate Workstation (Disk Image Analysis using Autopsy)

Overview

This investigation analyzed a compromised workstation belonging to an internal user suspected of unauthorized access to confidential company data. A forensic disk image was examined using Autopsy to identify evidence of data misuse, policy violations, and potential data exfiltration activity.

The objective was to determine whether sensitive company information had been accessed, manipulated, or prepared for unauthorized distribution.

Objective

- Identify unauthorized access to confidential files
- Recover deleted artifacts and analyze user activity
- Determine intent behind suspicious behavior
- Assess risk of data exfiltration and policy violations

Methodology

The investigation was conducted using Autopsy to analyze a forensic disk image and extract relevant digital artifacts.

Key steps included:

- Loaded and processed disk image containing user data
- Indexed file system artifacts, including documents and images
- Analyzed file metadata (ownership, timestamps, access history)
- Investigated deleted files for potential evidence concealment
- Reviewed user activity and browsing behavior

Key Findings

Unauthorized Access to Confidential Data

- Multiple proprietary files were accessed without authorization
- Documents included:
    - Business_Strategy.pdf
    - Drilling Methodology.pdf
- Metadata confirmed files belonged to another user, not the suspect

Deleted Files Indicating Evidence Concealment

- A total of 12 deleted files were recovered during analysis
- Deleted files contained sensitive company data
- Deletion suggests an attempt to remove evidence of unauthorized activity

Exposure of Proprietary Company Information

- Recovered files included confidential schematics and internal documents
- Example artifacts:
    - Proprietary oil company configuration images
    - Internal strategy and operational documents

Suspicious Activity Related to Cryptocurrency

- User conducted searches related to:
    - Bitcoin transactions
    - Cryptocurrency laundering
    - Anonymous financial transfers

This behavior strongly suggests intent to:

- Sell or transfer stolen data anonymously

Analysis & Interpretation

The combination of:

- Unauthorized file access
- Recovery of deleted confidential documents
- Research into anonymous financial transactions

indicates a high likelihood of intentional data exfiltration.
User activity was consistent with:

- Insider threat behavior
- Attempted concealment of evidence
- Preparation for unauthorized data transfer

Security Impact

This incident represents a critical security breach with potential consequences including:

- Exposure of proprietary company data
- Financial and reputational damage

- Violation of internal security policies
- Potential legal implications

SOC / Incident Response Relevance

This investigation demonstrates practical experience in:

- Digital forensic analysis and evidence recovery
- Identifying insider threats and suspicious user behavior
- Correlating artifacts to establish intent
- Investigating deleted files and data concealment techniques

In a SOC environment, this directly applies to:

- Investigating endpoint alerts
- Analyzing suspicious user activity
- Supporting incident response and escalation

Tools & Technologies

- Autopsy (Digital Forensics Platform)
- Disk Image Analysis
- File System & Metadata Analysis