

# Malware Infection Analysis Worksheet

## Incident Details

Date/Time of Detection

Analyst Name

Case / Incident ID

## System Information

Hostname

IP Address

Operating System & Version

Location / Department

## Malware Details

Malware Name (if known)

Type/Category

Indicators of Compromise (IOC)

Infection Vector (how malware entered system)

Behavior Observed / Symptoms

Analysis Summary

Tools/Methods Used

Files / Processes Involved

File/Process	Path	Hash	Status

Network Indicators / Traffic Analysis

Persistence Mechanisms

Remediation

Actions Taken / Recommendations

Follow-up / Monitoring Steps