Malware Outbreak Simulation – Clue Sheet

Clue 1:

"Several computers are suddenly running very slowly, and some files on the system appear to be locked or inaccessible."

Clue 2:

"A pop-up message has appeared on the screen:

'Your files are encrypted! Pay $500 in Bitcoin to get them back! You have 72 hours.'"

Clue 3:

"There is a noticeable increase in network traffic originating from an unknown IP address: 192.168.1.103."

Clue 4:

"A teacher’s sensitive files (containing personal student data) have been accessed without permission and are now missing."

Clue 5:

"Antivirus software on some of the computers is disabled, and users cannot run a scan or install updates."

Clue 6:

"Emails are being sent from school email accounts without the owners' knowledge."

Network Traffic Log for Analysis

Network Log 1

Timestamp: 10:01:12

Source IP: 192.168.1.25

Destination IP: 192.168.1.1

Traffic Volume (MB): 1.2

Activity: Normal Internal Access

Notes: Routine login from workstation

Network Log 2

Timestamp: 10:02:45

Source IP: 192.168.1.103

Destination IP: 192.168.1.25

Traffic Volume (MB): 3.5

Activity: Suspicious External Connection

Notes: Unknown IP attempting to access sensitive files

Network Log 3

Timestamp: 10:05:18

Source IP: 192.168.1.103

Destination IP: 192.168.1.12

Traffic Volume (MB): 5.2

Activity: Data Transfer

Notes: Large data transfer detected to an unknown destination

Network Log 4

Timestamp: 10:07:33

Source IP: 192.168.1.1

Destination IP: 192.168.1.25

Traffic Volume (MB): 0.5

Activity: Normal Internal Access

Notes: Routine communication between server and workstation

Network Log 5

Timestamp: 10:09:45

Source IP: 192.168.1.25

Destination IP: 192.168.1.103

Traffic Volume (MB): 8.7

Activity: Suspicious Activity

Notes: Possible unauthorised download attempt

Incident Response Report Template

Incident Response Report

Incident Details

Type of Malware Detected: _____

Time of Attack: _____

Source of Attack (IP or Method): _____

Systems Affected: _____

Damage Caused: _____

Response Actions

Steps Taken to Contain the Attack:

_____

_____

Tools Used (e.g., antivirus, backup systems):

_____

_____

Analysis

What caused the attack?

_____

_____

Could the attack have been prevented?

Recommendations for Future Prevention

Fake Email Alert

Subject: Urgent: Action Required to Restore Access

Message:

Dear User,

Our system has detected unusual activity in your account. Please click the link below to verify your identity and restore access.

[Click Here to Restore Access]

Failure to act will result in permanent account suspension.

Sincerely,

The IT Team