To: IT Management; Head of Security

Subject: URGENT: Critical Security Incident - Active Ransomware Attack

This is an urgent notification from the Security Operations Center (SOC).

At approximately 09:10 AM, we detected an **active ransomware attack** on our network. The host 172.16.0.3 (user bob) triggered a "Ransomware Behavior" alert.

This appears to be the final stage of a larger, coordinated attack that also involved rootkits and trojans to compromise multiple systems.

Impact: High. Data encryption is likely in progress, and multiple systems are compromised.

Action Taken: We are taking immediate steps to contain the threat, starting with isolating the affected machines from the network.

A full incident report will follow.

Thank you,

Rohit Pawar SOC Analyst