Subject: [CRITICAL] Security Alert: Ransomware Detected on Server-X

Hello Tier 2 Analyst,

A ransomware infection has been detected on Server-X within the corporate network. Initial analysis indicates that the malware is actively encrypting files and may have accessed shared resources. Immediate containment measures have been taken: the affected server has been isolated, and a memory dump, along with relevant log files, has been collected for further forensic investigation.

Key Indicators of Compromise (IOCs):

- File: `crypto_locker.exe`
- Source IP: `192.168.1.50`
- Affected user: Bob Smith
- Observed malicious processes: `Miranda_Tate_unveiled.dotm`
- Suspicious domain accessed: `cerberhhyed5frqa.xmfir0.win`

Recommended next steps:

1. Conduct a full endpoint forensic analysis.
2. Investigate potential lateral movement or access to file servers.
3. Identify persistence mechanisms and remove malicious artifacts.
4. Update network and endpoint defenses to prevent further spread.

Regards,
Lokesh,
SOC Analyst Intern