SOC - Standard Operating Procedure

Possible Ransomware detection

Usage: *All rights reserved. For Internal Use Only.*

Table of Contents

1. Introduction 3

1.1 Purpose And Scope 3

1.2 Audience 3

1.3 Background 3

2. Procedure 1

2.1. Identification 4

2.2. Investigation 4

2.3. Containment 5

3. Remediation 6

4. Recovery 6

5. Review 6

6. Important Links 7

7. Contact Point List 7

8. Glossary 7

1. Introduction
   1. Purpose and Scope

This document describes the Capgemini Standard Operating Procedure for Ransomware related security incidents in Matalan environment. This document provides detailed work instruction to work upon this security incident when occurred. Escalation matrix will be followed in case it breached SLA. The scope of this document includes any security incidents pertaining to ransomware events or alerts which are observed and reported. The procedure which is described in this document to be followed to mitigate or resolve the incident.

* 1. Audience

DL IN MSSP Sentinel GSOC <msspsentinelgsoc@capgemini.com>

* 1. Background

Ransomware is malware that employs encryption to hold a victim’s information at ransom. A user or organization’s critical data is encrypted so that they cannot access files, databases, or applications. A ransom is then demanded to provide access. Ransomware is often designed to spread across a network and target database and file servers and can thus quickly paralyze an entire organization. It is a growing threat, generating billions of dollars in payments to cybercriminals and inflicting significant damage and expenses for businesses and governmental organizations.

1. Procedure

The following steps are to be followed for the Investigation.

* 1. Identification

The Identification stage deals with the identification and initial scoping of a security alert.

* Possible Ransomware is either identified by SIEM solution detected by Antivirus or IPS/IDS console.
* End-user reported after observing suspicious behavior on a system by calling service desk, raise ticket in ITSM tool.
  1. Investigation

The Investigation & Resolution stage deals with investigating and resolving the security incident in detail including fully scoping and documenting incidents.

Analyse the information in the incident record or information captured in offense in SIEM tool.

The first step of any ransomware attack is to get the malware installed on the host system. This typically occurs using:

1. Spear phishing - where the victim receives an attachment or link that they click.
2. Drive-by - where an attacker can exploit a vulnerability in the web browser or related applications.
3. Exploitation - where an attacker can exploit a vulnerability and gain access to a remote system or allow the ransomware to propagate automatically.
4. Valid accounts - where an attacker has valid credentials to the target system and can authenticate to it.
5. RDP – attacker brute force and steal RDP credentials.
6. Mass file Extension modifications. Suspicious PowerShell CMDs execution.
7. Shadow copy deletion to prevent recovery.
8. We have different use cases configured to detect possible ransomware detected for Matalan account like Possible phishing alert, Privilege escalation, Suspicious outbound communication, unusual volume of data transfer etc.,
9. When we get the alert for any of the above scenario’s investigation should be done on based on triggering indicator.
10. In case where the alert is related to user activity like Possible phishing alert, Privilege escalation, investigate based on user recent and past(historical) logs to check if user has received any phishing email and clicked on any suspicious URL or opened/accessed any attachment that came along with phish mail, as Phishing is one of the most common ways that a ransomware attack begins.
11. The next, step is to identify unusual behaviour related to user account changes in AD gaining access to accounts across the network.
12. In case where suspicious activities are observed, incidents are created with proper analysis details and passed to Wintel team queue (‘**IS - CG Wintel Backoffice**’) team(in case of windows devices) or O365 queue (‘**IS - CG O365 Support**’)team(in case of cloud alerts) for further investigation with user.
13. In case where the alert is related to network activity like Suspicious outbound communication, unusual volume of data transfer, we investigate based on network logs, i.e.- logs coming from firewall, IPS/IDS, ASA etc to identify.
14. Unusual/suspicious behaviour related to data exfiltration to external domains or communication with malicious/unsafe external IP address or communication with external IP address from unusual location, which could be the connections towards attacker's command and control server.
15. In case where suspicious activities are observed, incidents are created with proper analysis details and passed to Network security team queue (‘**IS - L2-SecNetNEU\_Tower**’) team for further investigation.
16. Perform correlation across the log sources to check for suspicious activities.
17. In case where the alert is related to detection of malicious file related to ransomware, Check the Defender status/action if it is (Blocked/Not Blocked) in logs.
18. In case Remediation action field is 'null' or empty, create an incident with AV team to further check of the defender end and take necessary remediation steps in case the source file detected does not have any business dependency and is malicious.
    1. Containment

Once the infection has been confirmed, the next step is its containment. Note that containment is not meant to be the definitive solution to an infection, but a temporary fix to prevent the spread of the malware and limit its impact.

1. In case the user account is suspected to be compromised, Wintelteam will take necessary actions related to disabling the user account temporarily and to reset the user account password.
2. Revoke the MFA sessions and cancel all active sessions of the user.
3. If the detection is based on network logs (related to suspicious IP), Network security team will take necessary actions to block the external IP at perimeter level.
4. First, identify how many devices or Users are involved in this attack.
5. If we identified malicious code or suspicious detection over the device, first Isolate all the involved devices from the Network, so that it should spread to other devices. Later the Offshore AV team needs to scan the endpoints or infected system. Incase, the device is not reachable, initiate the scan with help of Service Desk team.
6. Once scanning is done, AV team also ensures that the malware was successfully removed.
7. After the Scan if nothing is detected, Un-Isolate the Device and take it back to the internet if required.
8. Remediation
9. Vulnerability Management team need to perform network and vulnerability scans to identify any gaps/vulnerabilities on network devices and servers for any undetected vulnerabilities.
10. Respective tower teams need to fix the operating system vulnerabilities by patching them using documented patching policy and also patch any vulnerabilities found while performing vulnerability scan in the environment.
11. EPS team needs to run full scan on the System with up-to-date antivirus to check for any other unwanted file and if present, please remove/uninstall them.
12. EPS team to automatically update signature files and scan engines whenever the vendor publishes updates.
13. Sentinel team will Deploy a new use case to closely monitor Suspicious activities with respect to the compromised devices or users.

4. Recovery

Recovery stage deals with recovering the files or systems which were infected and disconnected from the network. It mainly includes the following set of steps:

1. Add the system back to the network which was isolated from the Network.
2. Reopen the Network traffic which was closed during containment.
3. Reconnect the area to the Internet.

5. Review

The review stage is conducted post incident ensuring nothing is overlooked and process improvement. . It mainly includes the following set of steps:

1. Lessons learnt will be reviewed with respective teams in session set up by GSOC to discuss process improvements.
2. Prior to the meeting, ensure that the incident record has documented any controls that failed to prevent/detect the Malware.
3. SOC will suggest improvements on:

3.1 IOCs

3.2 Procedure Documentation

3.3 Technical and Policy Controls

**7. Contact Point list**

**8. Glossary**

|  |  |
| --- | --- |
| **Acronym/Abbreviation** | **Explanation** |
| GSOC | Global Security Operations Centre – Capgemini |
| EPS | End Point Security |
| IDS | Intrusion Detection System |
| IPS | Intrusion Prevention System |
| IOCs | Indicators of Compromise |
| SIEM | Security Information and Event Management |

**Document Control**

**Document Review Cycle:**  Yearly

**Ownership**

| **Version** | **Date** | **Owner** | **Function, Role, Title** |
| --- | --- | --- | --- |
| 1.0 | 09-05-2025 | Sentinel SOC | SOC L3 |

**Reviewers**

| **Version** | **Date** | **Reviewer(s)** | **Function, Role, Title** |
| --- | --- | --- | --- |
| 1.0 | 09-05-2025 | anand.misal@capgemini.com | Security Manager |
| 1.1 | 09-05-2025 | ayyazahmed.nandgadi@capgemini.com | SOC Lead. |