# **Root Cause Analysis - Report Template**

# Incident Title

Provide a title that describes the incident.

# Date

Date of Investigation (report completion)

# Authors

Names of Incident Responder(s)

# TLP of document

TLP:RED

TLP:RED

Not for disclosure, restricted to incident responders only.

# **Executive Summary**

Length: no more than 1 page.

Provide an incident summary for a non-technical audience. What is the potential (or real) impact on the business as a result of the incident. To make a good executive summary, take the place of a non-technical executive that needs to understand WHAT happened, HOW it happened, and the key takeaways from the incident. Note that this should be the last part you write.

# **Incident Timeline**

Length: no more than 1 page - may be a screenshot / image / drawing / photo of a drawing.

Provide an illustration of the incident timeline, focusing on key activities. Make sure each event is timestamped and provides value. The aim of the incident timeline is to provide a high-level view of the succession of key events from entry / initial infection to the reception of the extortion email.

Note: the timeline does not need to be to scale, details should remain strictly minimal - no need more than an event title and 1-liner description alongside the timestamp. The timeline is an illustration of the story of the incident so someone non-technical and not-acquainted with the events should be able to gain a general grasp of the incident. You should build this timeline only when you have completed the full technical analysis.

# **Technical Analysis**

Length: as-needed, aim for quality over quantity. Illustrations / diagrams may be used as-needed.

In this section, describe low level / tactical details on the incident. This includes exact timelines and artifacts such as screenshots, code snippets, additional documents, external resources, etc.

Elements of your analysis should include all artifacts, key subsections include:

* PCAP Analysis
* Logs Analysis
* Data Impact Analysis
* Succession of attacker activities & movements (from Patient Zero to final activity) - this will help in then illustrating the incident timeline.

# **Recommendations**

Length: no more than 1 page per recommendation.

In this section you will provide your professional advice as an incident responder on:

1. Whether the company should pay the ransom or not.
2. What steps should be taken to remediate and recover from the incident.
3. Post-incident activities to strengthen the security posture of the company.

## Ransom Payment Guidance

Provide clear guidance for the company leadership to take a decision on the ransom pay/no-pay decision. This should include an official recommendation (pay or no-pay) in your professional opinion (with justification).

## Incident Remediation & Recovery Recommendations

These recommendations should provide the leadership & incident responders with answers to the following questions:

* What are the recommended actions to contain and remediate the incident.
* What are the recommended actions to recover / return to business as usual (BAU).

Ideally you should describe a list of sequential activities the firm needs to take starting from now (assume they follow your advice on pay/no-pay decision) until the business fully returns to normal. The more specific/detailed the better.

## Post-Incident Recommendations

These recommendations should provide the leadership with insights into potential future projects they should consider to greatly reduce the likelihood and/or impact of a similar incident in the future. Aim for at least 10 recommendations, each with at least a paragraph of explanation, and implementation guidance.

Note: you may work on assumptions but aim to list the most critical controls/practices/insights to ensure this specific type of incident is most unlikely to reoccur.

Here is a Post-Incident Recommendation table example you can leverage:

| **#1 -** Recommendation Title |
| --- |
| **NIST Domain:** Identify/Protect/Detect/Respond/Recover |
| **Observation:**  The company lacks X. |
| **Recommendation details:**  The company should implement X on Y assets for Z reasons.  [Add any guidance on implementation/deployment of X] |

# Appendix

Appendices may be used for any reference material, definitions, and data tables.

Note: do not put the original artifacts in Appendix, simply reference them as-needed in the body of your analysis.