



{{ case.name }}

Technical report

***Contributor*** *: Company Name*

***Customer*** *: {{ case.client.customer\_name }}*

***Case ID*** *: {{ case.case\_id }}*

***Incident type****: {{ case.classification.name }}*

***Severity of the incident****: {{ case.severity.severity\_name }}*

***Date****: {{ date }}*

Contents

[Context 3](#_Toc172020702)

[Contributors 3](#_Toc172020703)

[Summary 3](#_Toc172020704)

[Intervention timeline 3](#_Toc172020705)

[Technical Analysis 4](#_Toc172020706)

[Annex 1 - Assets 5](#_Toc172020707)

[Annex 2 - Timeline 6](#_Toc172020708)

[Annex 3 - Evidence 7](#_Toc172020709)

[Annex 4 – Indicators of compromise (IOCS) 8](#_Toc172020710)

[Annex 5 – Accomplished tasks 9](#_Toc172020711)

[Annex 6 – Pattern of infection 10](#_Toc172020712)

# Context

Following the cyber incident suspicion on the {{ case.client.customer\_name }} information system, the decision to send a cyber intervention group (CIG) was taken.

{{ case.description }}

# Contributors

Group leader :

* \*\* FILL \*\*

Analyst :

* \*\* FILL \*\*
* \*\* FILL \*\*

# Summary

# Intervention timeline

|  |  |
| --- | --- |
| Date | Evènements |
| \*\* FILL DATE \*\* | SOC Alert – {{ case.soc\_id }} |
| {{ case.open\_date }} | Start of investigation |
|  |  |
|  |  |
|  |  |

# Technical Analysis

# Annex 1 - Assets

The table below contains all assets found during the investigation.

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | Status | Description |
| {%tr for asset in assets%} | | | |
| {{ asset.asset\_name }} | {{ asset.type }} | {{ asset.asset\_compromise\_status }} | {{ asset.light\_asset\_description }} |
| {%tr endfor %} | | | |

# Annex 2 - Timeline

{% if timeline|count %}

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Categories | Assets | Events |
| {%tr for event in timeline %} | | | |
| {{ event.event\_date }} | {{ event.category }} | {% for asset in event.assets %}  {{ asset }}  {%endfor %} | {{ event.event\_title }}  *{{ event.event\_content }}* |
| {%tr endfor %} | | | |

{% endif %} {% if evidences|count %}

# Annex 3 - Evidence

|  |  |  |
| --- | --- | --- |
| Filename | Escrow date | File hash (SHA256) |
| {%tr for item in evidences %} | | |
| {{ item.filename }} | {{ item.date\_added }} | {{ item.file\_hash }} |
| {%tr endfor %} | | |

{% endif %}

# Annex 4 – Indicators of compromise (IOCS)

{% if iocs |count %}

|  |  |  |  |
| --- | --- | --- | --- |
| Valeurs | Type | Description | TLP |
| {%tr for item in iocs %} | | | |
| {{ item.ioc\_value }} | {{ item.type\_name }} | {{ item.ioc\_description }} | {{ item. tlp\_name }} |
| {%tr endfor %} | | | |

{% endif %}

# Annex 5 – Accomplished tasks

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Title | Start date | End date | Description | Analysts |
| {%tr for task in tasks %} | | | |  |
| {{ task.task\_title }} | {{ task.task\_open\_date }} | {{ task.task\_close\_date }} | {{ task.task\_description }} | {% for user in task.task\_assignees %} {{ user.name }}  {% endfor %} |
| {%tr endfor %} | | | |  |

# Annex 6 – Pattern of infection