Immagine che contiene cielo, blu, grattacielo, edificio

Descrizione generata automaticamente

Abstract

Incident Report

{{ doc\_id }} {{ date }}

{{ case.name }}

Incident Report

# Executive summary

## Context

This report summarizes the principal elements emerged during the handling of incident the incident  "{{ case.name }}", following up events detected in date {{ case.open\_date}} in the context of {{ case.for\_customer }}.

{{ case.description|markdown }}

## Analysis timeline

|  |  |
| --- | --- |
| Date | Event |
| Date | Request received by the SOC |
| {{ case.open\_date }} | Start of the analysis |
| {{ date }} | End of the analysis and report |

{% if assets|count %}

# Assets

The table below summarize the assets seen during the investigation.

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

As shown on the table above, the following assets where found compromised.

{% for asset in assets %} {% if asset.compromised %}

### {{ asset.asset\_name }}

{{ asset.asset\_description }}

The following IOC were found on the asset.

{%if asset.asset\_ioc| count %}

|  |  |  |
| --- | --- | --- |
| Value | Type | Description |
| {%tr for item in asset.asset\_ioc %} | | |
| {{ item.ioc\_value }} | {{ item.ioc\_type }} | {{ item.ioc\_description }} |
| {%tr endfor %} | | |

{% endif %} {% endif %}{% endfor %}{% endif %}

1. Changelog

|  |  |  |
| --- | --- | --- |
| Date | Version | Author |
| {{ date }} | v1.0 | {{ user }} |

1. Timeline

{% if timeline|count %}

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Category | Assets | Event |
| {%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 %}

1. Received files

The following files have been received and analysed during this investigation.

|  |  |  |
| --- | --- | --- |
| File | Date received | SHA256 |
| {%tr for item in evidences %} | | |
| {{ item.filename }} | {{ item.date\_added }} | {{ item.file\_hash }} |
| {%tr endfor %} | | |

{% endif %}

{% if iocs |count %}

1. Indicators of compromise

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

{% endif %}