***Intrusion Analysis*** *template use cases:*

* ***Author:*** *CTI Team*
* ***Audience:*** *SOC, IR, Hunt*
* ***Key Decisions:*** *Look for additional adversary behavior beyond the initial alert; Stop the adversary from reaching their goals and contain the threats.*
* ***Decision-Enabling Data Points****: intelligence assessment of potential intrusion scenarios; Set of techniques used in past adversary behavior.*

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*The* ***mandatory*** *fields in this template are denoted with an asterisk (\*), e.g., Report Date, Report Title, Executive Summary, and Key Points. However, most fields are* ***optional*** *and can be removed/adjusted for external sharing.*

***Criticality****: This field communicates the urgency of the report and helps prioritize for recipients. Criticality’s selections are: FYSA, Low, Medium, High, Critical.*

**<Report Date\*> < Criticality\*>**

**Report Title\***

# **Executive Summary\***

# This is a brief narrative explaining the significance of the report. This should focus on the decision the CTI summary is supporting and the change in circumstances that makes this timely and actionable.

# This should focus on:

# BLUF (Bottom Line Up Front) as the single largest takeaway from the CTI analysis

# What is the new information?

# Why it is important for the audience to understand this now?

# This section should not summarize the underlying reports used to create the analysis.

# This should be able to convey the most important analysis to the reader, so that they can skip the rest of the report and still be able to take an informed action.

# The Executive Summary should not be longer than 2 -3 paragraphs, according to best practices. For this report, we recommend trying to keep it to a paragraph

# **Key Points\***

These bullets should summarize:

* What data anchors the analysis?
* Where the data falls in the intrusion chain
* Threat actors associated with the data and
* Malicious activity generally observed before and after the known activity.

# **Indicator Analysis**

# This section should provide:

# An assessment of what other TTPs are likely to be in a network based on the initial information provided by the SOC or IR team.

# Include corresponding detections in the Signature section below, if applicable (i.e., YARA signatures, etc.)

# Once possible, provide attribution to a threat actor with a level of confidence.

# An Attack Flow for that threat actor should then be included \*IF CURRENTLY AVAILABLE\*

# If not available, a description of end goal TTPs is most important to aid in initial containment steps.

# Only take the time to create a full Attack Flow once the IR has moved into eradication and remediation.

# If multiple threat actors could be responsible based on observed data, provide the above for each threat actor ordered by confidence in attribution and secondarily by potential harm caused. This should provide key hunt recommendations for the different threat actors that may be responsible to help the IR team find additional malicious activity and increase the intelligence assessment of attribution.

# **MITRE ATT&CK Table (based on v12): TTPs Likely to Be in the Network**

This table should show the MITRE tactics and techniques/Sub-techniques not yet observed but likely to be in the network. The procedure column details a particular instance of how a technique/sub-technique has been used. The D3FEND column includes the corresponding MITRE D3FEND countermeasure technique, if available.  If using the tool, the tactics and techniques can be automatically generated from an Attack Flow document using the plug-in.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Attribution** | **Tactics** | **Techniques** | **Sub Technique** | **Procedure** | **D3FEND** | **Deployed Control** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

# **MITRE ATT&CK Table (based on v12): TTPs Observed in the Intrusion**

This table should show the MITRE tactics, techniques/sub-techniques, and procedures observed during the intrusion based on data provided by the SOC or IR team. Analysts can include the corresponding MITRE DEFEND countermeasure technique, if available.  If using the tool, the tactics and techniques can be automatically generated from an Attack Flow document using the plug-in.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tactics** | **Techniques** | **Sub Technique** | **Procedure** | **D3FEND** |
| Sample text goes here |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# **Indicators of Compromise for Hunting**

This section consists of three IOC tables [Malware, Network, and System Artifacts] associated with the Campaign.

# Malware

This table should detail the malware and tools associated with the campaign. The “Associated Files Hash” column can include any files related to the tool or malware, e.g., downloader for a memory dropper. The “Brief Malware Description” column should provide a short description for context, as well as where the activity falls in the intrusion chain. The first and last reported fields are intended to memorialize the longevity of a particular piece of malware, providing additional insight into trends in malicious behavior.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Attribution | Malicious Tool Name | Hash Type | File Hash | Associated Files Hash | Brief Description | Malware Analysis Report (Hyperlink, or N/A) | First Reported | Last Reported |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

# Network

This table should detail the network indicators associated with the campaign, e.g., domains and IP addresses. The “Intrusion Phase” column includes Initial Access, Command and Control, and Exfiltration. The first and last reported fields are intended to memorialize the longevity of a particular network artifact, providing additional insight into trends in malicious behavior.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribution | Network Artifact | Details | Intrusion Phase | First Reported | Last Reported |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# System Artifacts

This table should detail any unique artifacts associated with the campaign that could be observed on a host, e.g., processes, DLLs, registry keys. The first and last reported fields are intended to memorialize the longevity of a particular system artifact, providing additional insight into trends in malicious behavior.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Attribution | Host Artifact | Type | Details | Tactic | First Reported | Last Reported |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

# Common Vulnerabilities and Exposures (CVEs)

CVEs associated with the campaign. The date reported field is designed to capture the date when the CVE became public knowledge. To adequately fill out this table, it may require information from other internal teams.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Attribution | CVE Number | CVSS Score | Patch Available (Y/N) | Other Remediation | Date Reported | Patch Applied (Y/N/UNK/NA) |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

# **Signatures**

This section should include detections (e.g., Yara signature) that correspond to the malware or malicious activity associated with the campaign.

1. Malware or malicious activity name
   1. Detection
2. Malware or malicious activity name
   1. Detection

# **Attached Attack Flow and/or Navigator Heat Maps, if applicable**

# **Probability Matrix**

We recommend that analysts properly express and explain uncertainties associated with major analytic judgments.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Almost no chance | Very unlikely | Unlikely | Roughly Even Chance | Likely | Very likely | Almost certain(ly) |
| 01–05% | 05–20% | 20–45% | 45–55% | 55–80% | 80–95% | 95–99% |

# **Intelligence Requirements**

Brief citation of CTI requirements(s) addressed by this report.

# **Feedback**

Provide a point of contact (e.g., an email address) for customer feedback on the published CTI report, such as whether the report addressed the customers’ Intelligence Requirements, how the report could be more actionable, additional Intelligence Requirement questions to answer, etc.

|  |  |
| --- | --- |
| Data Sources: | * Cite external CTI Report with hyperlink if available. * Cite Internal Telemetry sources provided by the SOC as needed. This field is not designed to preserve Intrusion Analysis data and should only include data necessary to justify the analytic assessments. |

The metadata table below is for automation purposes and provides discrete fields for tool extraction. If you are not using the tool, we recommend removing the table.

|  |  |
| --- | --- |
| Threat Actor: | * Primary Threat Actor Name(s) or Unknown * Associated Group Names/Aliases or N/A |
| Actor Motivation: | * Cyber Espionage, Data Theft, Cyber Crime, Ransomware, Destructive Attack, Hacktivism, Other, Unknown |