***Threat Actor Profile*** *template use cases:*

* ***Author:*** *CTI Team*
* ***Audience:*** *SOC*
* ***Key Decisions:*** *Determine alert prioritization and triaging; Identify TTPs that may require new or updated detections.*
* ***Decision-Enabling Data Points****: Context and relevance of the threat to the organization; Adversary behavior and potential goals; IOC enrichment; Associated malware and tools; Newly observed TTPs*

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

* ***Author:*** *CTI Team*
* ***Audience:*** *Threat Hunt*
* ***Key Decisions:*** *Conduct tailored, specific searches in the network for the reported malicious behavior.*
* ***Decision-Enabling Data Points****: Adversary behavior and potential goals; IOC enrichment; Associated malware and tools; Observed TTPs; Difference from existing TTPs – net new capabilities, slight modifications, etc.*

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

* ***Author:*** *CTI Team*
* ***Audience:*** *Red/Purple Team*
* ***Key Decisions:*** *Conduct updated, threat-informed adversary emulation to better assess an organization’s defensive posture against the reported malicious activity.*
* ***Decision-Enabling Data Points****: Adversary behavior and potential goals; IOC enrichment; Associated malware and tools; Observed TTPs*

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

*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 section should focus on the decision the CTI summary is supporting and the change in circumstances that makes this timely and actionable.

It should focus on:

* The single largest takeaway from the CTI analysis.
* Why it is important for the audience to understand?
* How does this fit into the larger risk landscape?

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.

# **Key Points\***

These bullets should summarize:

* Who is the report about?
* What did they do?
* How they did it?
* Why does it matter to the audience of the CTI analysis?

# **Assessment**

This section should contain:

* Key Judgement: This threat actor demonstrates X that has the potential to impact Y.
* Change Analysis: Threat actor has a new TTP that creates capability Y, leverages vulnerability X, etc.
* Relation to Your Organization: This threat actor historically targets our sector; we have previous detections of malware associated with this threat actor; the malware leverages vulnerabilities in our software stack, etc.

# **Threat Actor Summary**

This section should contain relevant information outlining the key differentiating features of the intrusion set. Start with an overarching summary: This intrusion set, associated with county Y, organization X, mainly targets sectors 1,2,3 and countries A, B, C. They have been openly tracked since XX/XX/XXXX.

**Tactics, Techniques, & Procedures**

This sub section should list out the types of tools and TTPs they leverage. This does not need to be an exhaustive list of tool names (that will be listed in the table below), but rather a description of how they operate.

EXAMPLE: Threat actor X leverages legitimate administrative tools during their intrusions to avoid detection and attribution. They primarily rely on exploitation of vulnerabilities in internet facing devices for initial access, etc.

**Infrastructure**

This sub section should list the types of infrastructure the threat actor leverages for command and control, initial intrusion, and exfiltration from networks.

EXAMPLE: Threat actor X leverages VPS providers for managing C2 communication and exfiltration but prefers to compromise open exchange relays to send phishing emails for initial intrusion.

**Victims**

This sub section should list the countries and industries targeted by the threat actor. It should also note if there is a pattern shift in this activity over time.

EXAMPLE: Threat actor X primarily targeted Western Europe defense and advanced technology sectors from 2015- 2021. However, in 2022 the targeting saw a shift to include Latin America and financial services.

**Attribution**

This sub section should focus on what is known about the intrusion set from an attribution perspective. As attribution is often subjective, each organization will have to come to their own threshold for attributing activity internally. Reserve this section to discuss the known facts that could support attribution to a particular country or organization.

EXAMPLE: Threat actor X is attributed to China by several cybersecurity vendors because Chinese language artifacts are present in different malware utilized by the threat actor. Operating times generally correlate to China’s time zone and there is a lull in activity around major Chinese holidays. Additionally, the victims of this activity align with Chinese national interests in Southeast Asia.

# **Timeline of Activity**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Attribution** | **Start Date** | **End Date** | **Location** | **Sector** | **Activity** |
| Sample text goes here |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# **Key Intelligence Gaps**

* Brief bullet summary of additional information the CTI team is seeking to further evaluate risk. Call out explicit gaps in understanding and what will change assessment because you don’t have information yet.

# **MITRE ATT&CK Table (based on v12)**

Table of the MITRE ATT&CK tactics and techniques/sub-techniques from the campaign. 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** |
| Sample text goes here |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

# **Victims**

This table should detail known victims, including sector and geographic location, of this threat actor.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Date Reported** | | **Sector** | **City/State/Province/etc.** | **Country/Region** |
|  |  |  | |  |  |
|  |  |  | |  |  |
|  |  |  | |  |  |

# **Indicators of Compromise (IOC)**

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 telemetry 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 |
| Victim Location: | * Drop-down list of countries |
| Sectors: | * Drop-down list of NAICS industries |
| Infrastructure Used | * Infrastructure used by adversary |
| Actor Motivation: | * Cyber Espionage, Data Theft, Cyber Crime, Ransomware, Destructive Attack, Hacktivism, Other, Unknown |