**<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 |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |