**----------------------------------------------------START OF TICKET----------------------------------------------------**

**Reporting Analyst(s):**

**Executive Summary:** Provide a brief “story-like” narrative of the Incident Detection. Include items such as:

• Detect Date and Time

• Incident Threat Details (Example: CrowdStrike (CS) AI identified a high confidence malicious file.)

• Any actions you take or that CS took

• OSINT information

**CrowdStrike Incident link(s) here:**

-------------------------------------------------------------------------------------------------------------------------------

**Incident Detection Details**

**Severity Level:**

**Tactic & Technique:**

**CS Action(s) Taken:**

**Host Details**

• Host Name:

• Host Type:

• Username:

• Host IP Address:

**IOA Name and Description:**

**File name:**

**Associated File:**

**Command Line:**

**File path:**

**File Hash:**

**Any Network Operations:** (Y/N, how many, anything significant that stands out)

**Any DNS Requests:** (Y/N, how many, anything significant that stands out)

**Any Registry Operations:** (Y/N, how many, anything significant that stands out)

**Root Cause Information: (How did the incident start? Found a potential file download source?)**

**----------------------------------------------------------OSINT INFORMATION---------------------------------------------------**

**Malicious File(s)**

**Malicious File # 1:**

• File Name:

• File Hash(es):

• VirusTotal Link:

o Risk Score:

• Other OSINT Resources:

**Malicious File # 2:**

• File Name:

• File Hash(es):

• VirusTotal Link:

o Risk Score:

**• Other OSINT Resources:**

**IP Address(es) Reputation**

**IP Address # 1:**

• VirusTotal Link:

o Risk Score:

• AbuseIPDB Link:

o Number of Times reported:

o Confidence of Abuse:

• URLScan.io Link:

o Verdict:

**IP Address # 2:**

• VirusTotal Link:

o Risk Score:

• AbuseIPDB Link:

o Number of Times reported:

o Confidence of Abuse:

• URLScan.io Link:

o Verdict:

**Malicious URLs (Defanged) [Potential file download source(s)]**

**Malicious Link # 1:**

• VirusTotal Link:

o Risk Score:

• Other OSINT Resources:

**Malicious Link # 2:**

• VirusTotal Link:

o Risk Score:

• Other OSINT Resources:

**-------------------------------------------------------------------------------------------------------------------------------**

**Additional Information:**

**-------------------------------------------------------------------------------------------------------------------------------**

**Declaration:**

**-------------------------------------------------------------------------------------------------------------------------------**

**Recommendations**

**Block IP Address(es):**

**Block URL(s):**

**Credentials Reset:**

**Other:**

**------------------------------------------------------END OF TICKET-----------------------------------------------------**

**Notes to Reporting Analysts from CNL:**

**[1] Enhance your Jira tickets and reports by adding pictures and screenshots when applicable.**

**[2] An example of ‘Additional Information’ could be an explanation of the type of malware VirusTotal found in a file attachment. If VT found Mimikatz malware then explain what that is so your readers will understand the danger involved.**