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

**Reporting Analyst(s):**

**Executive Summary**

**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:**

**Any DNS Requests:**

**Any Registry Operations:**

**Root Cause Information:**

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