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

**Reporting Analyst(s):**

**Executive Summary:**

**SentinelOne incident link(s) here:**

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

**Incident Dispositions**

Incident Classification:

Family:

OSINT name for malware:

Threat objective:

Threat status:

AI Confidence Level:

Mitigation actions:

Root cause:

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

**User, Endpoint, and Threat Information**

User:

Device name/Endpoint:

Detection type(s):

Process user:

Originating process:

Threat file name:

File path(s):

File hash(es):

Engine:

Network connections:

**----------------------------------------------------------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:

• Other OSINT Resources:

**IP Address # 2:**

• VirusTotal Link:

o Risk Score:

• AbuseIPDB Link:

o Number of Times reported:

o Confidence of Abuse:

• URLScan.io Link:

o Verdict:

• Other OSINT Resources:

**Malicious URLs (Defanged)**

**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:**

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