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

**Reporting Analyst(s):**

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

• Reported Time

• Incident Threat Details (Example: Malicious file download of “the file name under Threat Details”)

• Endpoint Policy at Detection

• Detection Type (Static, Dynamic, Both)

• Any actions you take or that SentinelOne took

• OSINT information

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

• Note that SentinelOne groups incidents by hash number

• Multiple incidents for the same hash number will have a number next to the dashboard incident shield

• You should include a link to all the incidents here

• Yes, that means all the incidents should be investigated together and reported together

*(There are exceptions. You will see incidents with dozens, hundreds, or over 1000 grouped together; do not do these all at once -- just choose one of them).*

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

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

**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.**