**THREAT INTELLIGENCE REPORT: TITLE**

*Reporter Name* – May 5, 2024

**EXECUTIVE SUMMARY**

{Executive summary highlighting important high-level notes designed primarily for review by Senior leadership/C-Level eyes}

**ABSTRACT**

{Abstract, summary of findings indicating methodology and summary of findings including limited technical detail.}

**HYPOTHESIS**

{Hypothesis}

**TECHNICAL SUMMARY**

Overview

OUTCOME

{Outcome options: Escalation, Detection Gap, Visibility Gap, Policy Violation, N/A}

ESCALATION DETAILS

{Detailed escalation write up. Discuss briefly the artifacts/findings found leading to the outcome and what the outcome exactly was.}

Hunt Packages

TTP TITLE

Threat Description

{Description of the TTP being investigated and its relevance to the Hypothesis}

MITRE Information

*MITRE ATT&CK Tactic*

{Initial Access, Persistence, Lateral Movement, Privilege Escalation, Discovery}

*MITRE ATT&CK Techniques*

{Ex. Registry Run Keys / Startup Folder}

*MITRE ATT&CK Id*

{ex. [T1547.001](https://attack.mitre.org/techniques/T1547/001/) – this should link to the proper MITRE Entry}

Analysis

1. {Tool Name – Log Type,   
   ex. Microsoft Defender XDR – endpoint:DeviceProcessEvents}

*Initial Query* ({Query Language} ex. KQL):

A close-up of a computer screen

Description automatically generated{Insert formatted query/script/etc, use: [Carbon.now.sh](https://carbon.now.sh/)}

*Description*

{Brief description of query to explain rationale}

Pivot Query X (KQL | Lucene | FQL | SPL | AQL | etc.):

{query}

Mitigation Recommendations:

{Write up of how to stop this threat be it IR procedures, detection engineering, IOAs, IOCs, etc.}

Detection Engineering:

{Write up explaining steps taken to create, implement, and verify new detection rules in response to threat hunt findings}

**CONCLUSION**

{Write up of threat hunt conclusions referencing findings to support conclusion.}

**RECOMMENDATIONS**

Hunt 1: TTP Name

{Provide key findings/logs/etc. for each hunt package, separate findings from the initial

query and subsequent pivot queries. This should walk the reader through the line of findings and supporting information rationalizing pivoting}