Threat hunt report prepared for

<Insert Company Logo>

CLASSIFICATION OF HUNTS:

**Lateral Movement Techniques**

Assessment start date: <Year>-<Month>-<Day>

Assessment end date: <Year>-<Month>-<Day>

[**Executive Summary**](#_rkq2wnsyir8e) **3**

[Assessment Overview](#_jsx5r2mf0023) 3

[Remediations Required](#_5p4wdeuqbcgs) 3

[**Technical Findings**](#_hb0gerk89tje) **4**

[**Threat Hunt (W-2023-001): PsExec Executing Remote Payload**](#_65dx2lf8ufhb) **4**

[Assumption](#_kqh5ebm5ux8q) 4

[Tactic(s)](#_o0ic09co8f9) 4

[MITRE ATT&CK Details](#_h1oxgd2gdt93) 4

[Operating System(s) in Scope:](#_swk5ot3bovsl) 4

[Adversary Details](#_xyzgwzd915jo) 4

[Query 1 Details](#_l13gltvrt8zw) 5

[Platform Used:](#_nc2oe2mz4d7r) 5

[Query Logic](#_g8qgxn47fr0g) 5

[Timeframe](#_d31z19cr34jp) 5

[Query Breakdown](#_caj4udo032fm) 5

[Detailed Analysis](#_o040euqezvk9) 5

[**Threat Hunt (W-2023-002): WinRM Executing Remote Command**](#_dbmq1v49gk3w) **6**

[Assumption](#_izpdsv1ut06l) 6

[Tactic(s)](#_y5ksnyyath4) 6

[MITRE ATT&CK Details](#_3h28uts7m75s) 6

[Operating System(s) in Scope:](#_kj8uinj5qvte) 6

[Adversary Details](#_4e9jgiiqmkt2) 6

[Query 1 Details](#_umskc5fyronm) 7

[Platform Used:](#_8jkd4skqrdjw) 7

[Query Logic](#_aqbgvqnd8f24) 7

[Timeframe](#_mapjxe3b219o) 7

[Query Breakdown](#_pucqytyc9gr2) 7

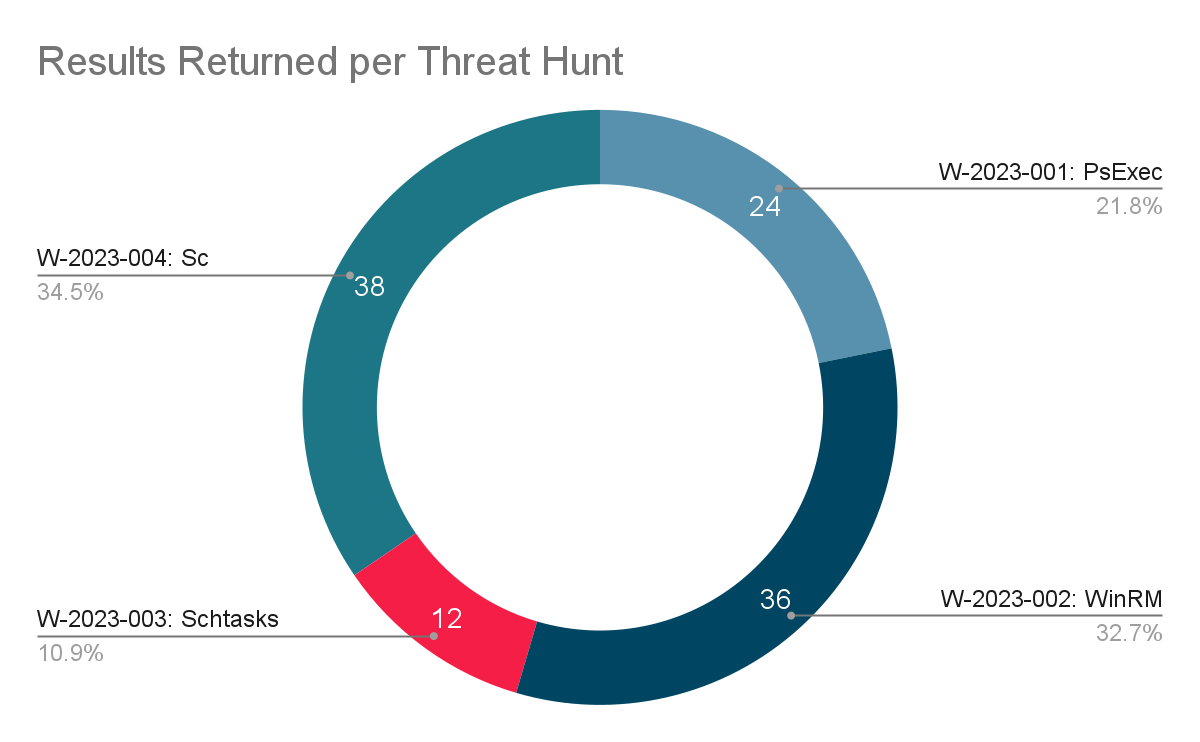
[Detailed Analysis](#_55ka5nug1132) 7

# **Executive Summary**

Hunting Adversaries performed the threat hunts listed below in Demo Company’s environment from January 1st, 2023 to February 1st, 2023. The following sections provide a high-level overview of the anomalous activity discovered and the threat hunts performed. Hunting Adversaries selected the following threat hunts based on recent threat intelligence trends, as adversaries such as APT28, Koadic, and APT38, among others, have been observed leveraging the associated TTPs (Tactics, Techniques, & Procedures).

## **Assessment Overview**

Hunting Adversaries ran three threat hunts in total, focusing on the [*Lateral Movement*](https://attack.mitre.org/tactics/TA0008/)tactic. Hunting Adversaries engineered 3 detection queries in total which returned 45 results in total after the expected activity was excluded from the initial queries. The breakdown of the results can be seen below:



## **Remediations Required**

| **Finding** | **Recommendation** | **Severity** |
| --- | --- | --- |
| W-2023-001: PsExec Executing Remote Payload | Verify whether PsExec is authorized for use in the environment. Follow up by checking the legitimacy of the remote execution of procdump on hostname-dc, by user joebloggs. | **Critical** |
| W-2023-003: Schtasks Creating Remote Scheduled Task | Confirm the legitimacy of the scheduled task remotely created by user01, on host hostname456. | **High** |

# **Technical Findings**

## **Threat Hunt (W-2023-001): PsExec Executing Remote Payload**

### **Assumption**

An adversary is attempting to move through the environment by executing remote payloads using PsExec.

### **Tactic(s)**

* **Lateral Movement -** techniques that adversaries use to enter and control remote systems on a network.
* **Execution -** techniques that result in adversary-controlled code running on a local or remote system.

### **MITRE ATT&CK Details**

**Primary TTP:** System Services: Service Execution ([T1569.002](https://attack.mitre.org/techniques/T1569/002/))

### **Operating System(s) in Scope:**

* Microsoft Windows

### **Adversary Details**

Attackers are capable of using the Sysinternals PsExec tool to perform lateral movement. PsExec can be used to connect to remote workstations with compromised credentials to execute files and executables on the remote host.

**Example Attacker Command:** psexec.exe \\<IP ADDRESS> -u <DOMAIN>\Administrator -p "<PASSWORD>" -s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe

*Reference:* [*Quantum Ransomware*](https://thedfirreport.com/2022/04/25/quantum-ransomware/)

### **Query 1 Details**

#### Platform Used:

Crowdstrike

#### Query Logic

event\_simpleName=ProcessRollup2 FileName=psexec.exe AND CommandLine="\*\\\\\*"

#### Timeframe

December 21, 2022 to January 20, 2023 (30 day search)

#### Query Breakdown

| **Field** | **Rationale** |
| --- | --- |
| event\_simpleName | This is where we specified that we are looking at process creation logs. |
| FileName | This field contains the process associated with this TTP. |
| CommandLine | This is where we specify that we are looking for command line activity containing “\\”, which indicates that an adversary is executing the file on a remote host. |

#### Detailed Analysis

* Hunting Adversaries received 24 events from two hosts in relation to remote execution using PsExec:
  + 4 out of the 24 events occurred on hostname321. The user responsible for this activity was joebloggs. The user, joebloggs, executed procdump.exe on one remote host (hostname-dc). Further investigation shows credentials being dumped on the remote host. This activity appears to be suspicious and requires escalation. We created INC45678 to track the remediation process.
  + 20 out of the 24 events originated from hostname123. The user, adm-johndoe, executed cmd.exe on four remote hosts using psexec.exe. Upon further investigation, Hunting Adversaries discovered ticket INC12345 in relation to this activity. It appears admin John Doe was performing troubleshooting activity on the four hosts. This activity was verified and therefore does not require further investigation.

## **Threat Hunt (W-2023-002): WinRM Executing Remote Command**

### **Assumption**

<Add threat hunt hypothesis>

### **Tactic(s)**

* **<Tactic> -** <Tactic Description>
* **<Tactic> -** <Tactic Description>

### **MITRE ATT&CK Details**

**Primary TTP:** <System Services: Service Execution> ([<T1569.002>](https://attack.mitre.org/techniques/T1569/002/))

**Alternate TTP:** <TTP Title> (<MITRE ID Link>)

### **Operating System(s) in Scope:**

* <Target operating system>

### **Adversary Details**

<provide details about how and why and adversary uses the technique>

**Example Attacker Command:** <enter example command>

*Reference:* [*<reference>*](https://google.com)

### **Query 1 Details**

#### Platform Used:

<platform used to query data>

#### Query Logic

<query used to pull back data>

#### Timeframe

<month> <date>, <year> to <month> <date>, <year> (<no. of days>-day search)

#### Query Breakdown

| **Field** | **Rationale** |
| --- | --- |
| <field name> | <why you are looking in that field> |
|  |  |
|  |  |

#### Detailed Analysis

* <write analysis notes here>