Threat Hunt Report (Unauthorised TOR Usage)

Detection of unauthorised TOR Browser Installation and Use on Workstation: **mm-mde-onboard**i

Example Scenario:

Management suspects that some employees may be using TOR browsers to bypass network security controls because recent network logs show unusual encrypted traffic patterns and connections to known TOR entry nodes. Additionally, there have been anonymous reports of employees discussing ways to access restricted sites during work hours. The goal is to detect any TOR usage and analyse related security incidents to mitigate potential risks. If any use of TOR is found, notify management.

High-Level TOR related IoC Discovery Plan:

1. Check DeviceFileEvents for any tor(.exe) or firefox(.exe) file events
2. Check DeviceProcessEvents for any signs of installation or usage
3. Check DeviceNetworkEvents for any signs of outgoing connections over known TOR ports

---

Steps Taken

The first search was conducted in the DeviceFileEvents for any file containing the string “tor”. The results reveal that a labuser1 had something to do with the tor file.

Query used to get this information:

```
DeviceFileEvents
| where DeviceName == "mm-mde-onboardi"
| where FileName startswith "tor"
|project Timestamp, DeviceName, FileName, InitiatingProcessAccountName, InitiatingProcessFileName
```

A file that looked interesting was one that had a name tor-browser-windows-x86_64-portable-15.0.2.exe.

```
DeviceProcessEvents
| where DeviceName == "mm-mde-onboardi"
| where ProcessCommandLine contains "tor-browser-windows-x86_64-portable-15.0.2.exe  /S"
| project Timestamp, DeviceName, AccountName, ActionType, FileName, ProcessCommandLine
```

The result showed that the file was executed at time stamp Nov 29, 2025 12:18:27 PM by the user labuser1

To find out is the file was downloaded I used the query:

```
DeviceFileEvents
| where FileName has_any ("tor.exe", "firefox.exe")
| where DeviceName == "mm-mde-onboardi"
| order by Timestamp desc
| project  Timestamp, DeviceName, RequestAccountName, ActionType, InitiatingProcessCommandLine
```

Results show that tor and firefox processes were created by labuser account name.

To check if the files were executed, I used the query

```
DeviceProcessEvents
| where ProcessCommandLine has_any("tor.exe","firefox.exe")
| where DeviceName == "mm-mde-onboardi"
| project  Timestamp, DeviceName, AccountName, ActionType, ProcessCommandLine
```

Further investigation revealed that there was network activity

```
DeviceNetworkEvents
| where InitiatingProcessFileName in ("tor.exe", "firefox.exe")
| where DeviceName == "mm-mde-onboardi"
| where RemotePort in (9001, 9030, 9040, 9050, 9051, 9150)
| project Timestamp, DeviceName, InitiatingProcessAccountName, InitiatingProcessFileName, RemoteIP,
RemotePort, RemoteUrl
| order by Timestamp desc
```

Time stamp: Nov 29, 2025 12:19:33 PM successful connection to IP address 45.137.70.158 on port 9001

Nov 29, 2025 12:28:57 PM T11

```
DeviceFileEvents
| where DeviceName == "mm-mde-onboardi"
| where FileName contains "shopping list.txt"
| project Timestamp, DeviceName, ActionType, FileName, InitiatingProcessAccountName,
FolderPath,  InitiatingProcessCreationTime
```

Chronological Assessment

Time	Event Type	Details	User / Process	Additional Notes
11:49:28 AM	ProcessCreation (from Shopping List	Initiating the process that later created *Shopping List.txt* started	labuser1	This is only the creation time of the process not the file itself.
12:18:27 PM	ProcessCreated	Tor Browser silent installer executed: tor-browser-windows-x86_64-portable-15.0.2.exe /S	labuser1	Beginning of Tor Browser installation.
12:19:14 PM	ProcessCreated	firefox.exe (Tor Browser UI) started	labuser1	Tor Browser launches Firefox as its frontend.
12:19:14 – 12:19:24 PM	Multiple ProcessCreated	Series of Firefox content processes created (-contentproc, gpu, tab, rdd, utility)	labuser1	Normal Tor Browser multi-process architecture.
12:19:20 PM	ProcessCreated	Firefox GPU process started	labuser1	Expected browser sub-process.
12:19:21 PM	ProcessCreated	Firefox content process (tab)	labuser1	Browser rendering pipeline.
12:19:22 PM	ProcessCreated	tor.exe started with full torrc configuration	labuser1	Tor routing service starts.
12:19:22 PM	ProcessCreated	Additional Firefox tab processes	labuser1	Normal Tor Browser internal processes.
12:19:33 PM	DeviceNetworkEvent	tor.exe → 45.137.70.158:9001	labuser1	First Tor network connection to an entry node.
12:19:35 PM	DeviceNetworkEvent	tor.exe → 45.137.70.158:9001 (again)	labuser1	Additional Tor circuit building.
12:19:44 PM	ProcessCreated	Firefox content process (tab 8)	labuser1	User likely opening or loading the Tor Browser UI.
12:19:51 PM	DeviceNetworkEvent	firefox.exe → 127.0.0.1:9150 (local Tor SOCKS proxy)	labuser1	Browser traffic routing into Tor network.
12:28:57 PM	FileCreated	"Shopping List.txt" created at C:\Users\labuser1\Desktop\Shopping List.txt	labuser1	User-created file on desktop. Not created by Tor Browser.

Summary

Summary Report

This report summarises the user and system activity observed on the endpoint mm-mde-onboardi on 29 November 2025, focusing on the installation and operation of the Tor Browser and the subsequent creation of a user-generated text file.

1. Initial Process Activity
At 11:49:28 AM, a process associated with labuser1 was started. Although this process did not immediately create any files, it is later identified as the parent process responsible for creating *Shopping List.txt*. This timestamp represents the process creation, not the file creation itself.

2. Tor Browser Installation and Launch
Between 12:18 PM and 12:19 PM, the Tor Browser portable installer was executed silently (/S flag silently), signalling the start of installation. Shortly afterwards, multiple Firefox-related processes were created, representing:

At 12:19:22 PM, the tor.exe process began running using the system's Tor configuration. This marks the point where the Tor routing service initialises and begins establishing encrypted circuits.

3. Tor Network Communications
Network telemetry shows Tor network activity beginning at 12:19:33 PM, with tor.exe connecting to IP address 45.137.70.158 on port 9001. A second connection to the same node was made shortly afterwards. These appear to be standard Tor entry/guard node connections.

4. File Creation Unrelated to Tor
At 12:28:57 PM, the file Shopping List.txt was created on the desktop by user labuser1. This action is not related to Tor Browser activity and appears to be a normal user-generated file.

Response Taken

TOR usage was confirmed on endpoint mm.mde.onboardi. The device was isolated, and the user's direct manager was notified.