Threat Hunt Report (Unauthorized TOR Usage)

Detection of Unauthorized TOR Browser Installation and Use on Workstation: mde-test

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 analyze 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

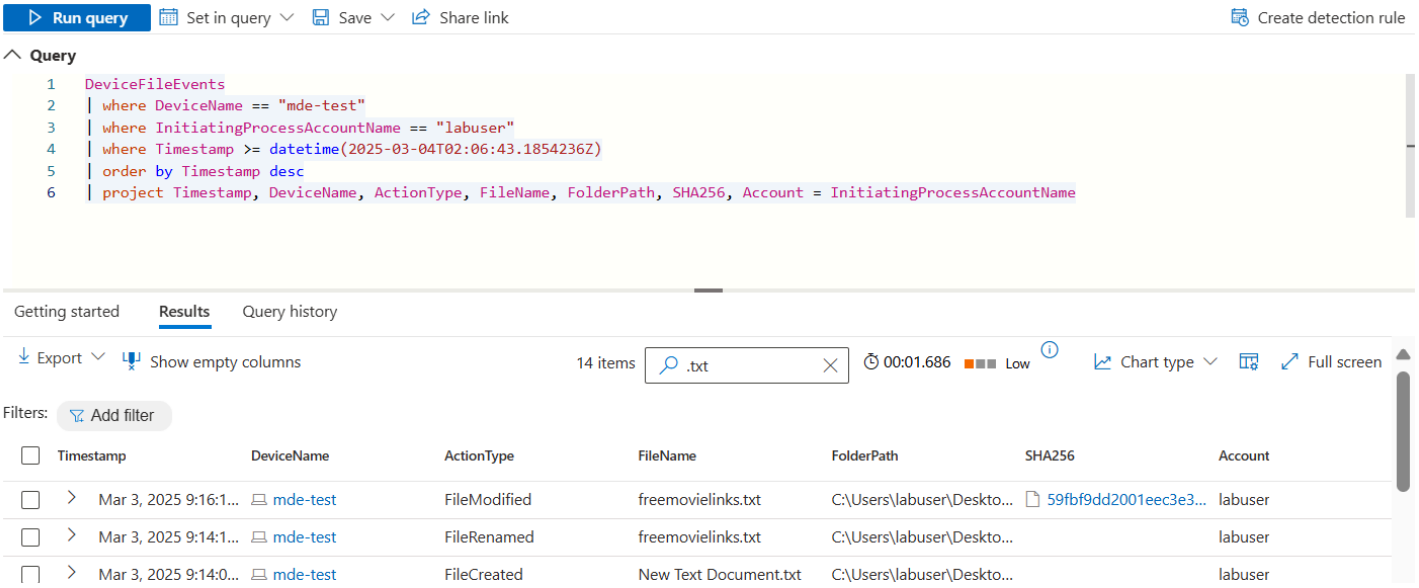
---

Steps Taken

1. Searched the DeviceFileEvents table for ANY file that had the string containing “tor” in it and discovered what looked like the user “labuser” downloaded a tor installer, did something that resulted in many tor-related files being copied to the Desktop. These events began at: 2025-03-04T02:06:43.1854236Z

```
DeviceFileEvents
| where DeviceName == "mde-test"
| where InitiatingProcessAccountName == "labuser"
| where FileName contains "tor"
| order by Timestamp desc
| project Timestamp, DeviceName, ActionType, FileName, FolderPath, SHA256, Account = InitiatingProcessAccountName
```

2. Additionally, searching for the creation of files around the same time period yielded more suspicious findings. A suspicious file named freemovielinks.txt was located. The file was created at 2025-03-04T02:14:00.3936439Z.



3. Searched the DeviceProcessEvents table for any ProcessCommandLine that contained the string “tor-browser-windows”. Based on the logs returned, at 2025-03-04T02:09:07.4267766Z, an employee on the “mde-test” device ran the file tor-browser-windows-x86_64-portable-14.0.6.exe from their Downloads folder, using a command that triggered a silent installation.

Query used to locate event:

```
DeviceProcessEvents
| where DeviceName == "mde-test"
| where ProcessCommandLine contains "tor-browser-windows"
| project Timestamp, DeviceName, AccountName, ActionType, FileName, FolderPath, SHA256, ProcessCommandLine
```

4. Searched the DeviceProcessEvents table for any indication that user “labuser” actually opened the tor browser. There was evidence that they did open it at 2025-03-04T02:09:28.4580295Z. There were several other instances of firefox.exe (Tor) as well as tor.exe spawned afterwards.
Query used to locate events:

```
DeviceProcessEvents
| where DeviceName == "mde-test"
| where FileName has_any ("tor.exe", "firefox.exe", "tor-browser.exe")
| project Timestamp, DeviceName, AccountName, ActionType, FileName, FolderPath, SHA256, ProcessCommandLine
| order by Timestamp desc
```

5. Searched the DeviceNetworkEvents table for any indication the tor browser was used to establish a connection using any of the known tor ports. At 2025-03-04T02:10:35.471503Z, an employee on the “mde-test” device successfully established a connection to the remote IP address 185.246.86.175 on port 9001. The connection was initiated by the process tor.exe, located in the

folder c:\users\labuser\desktop\tor browser\browser\torbrowser\tor\tor.exe. There were a couple other connections to sites over port 443.

Query used to locate events:

```
DeviceNetworkEvents
| where DeviceName == "mde-test"
| where InitiatingProcessAccountName != "system"
| where InitiatingProcessFileName in (“tor.exe”, “firefox.exe”)
| where RemotePort in ("9001", "9030", "9040", "9050", "9051", "9150")
| project Timestamp, DeviceName, InitiatingProcessAccountName, ActionType, RemoteIP, RemotePort, RemoteUrl, InitiatingProcessFileName, InitiatingProcessFolderPath
```

Chronological Events

1. Tor Browser Installer Download & Preparation

- **Timestamp (UTC):** 2025-03-04T02:06:43Z
  - **Event:** File renamed to `tor-browser-windows-x86_64-portable-14.0.6.exe` in `C:\Users\labuser\Downloads`.
  - **Source:** `tor-download.csv` (FileRenamed action).

---

2. Initial Execution of Tor Installer

- **Timestamp (UTC):** 2025-03-04T02:07:57Z
  - **Event:** Process `tor-browser-windows-x86_64-portable-14.0.6.exe` created in `C:\Users\labuser\Downloads`.
  - **Source:** `tor-install.csv` (ProcessCreated action).

---

3. Silent Installation of Tor Browser

- **Timestamp (UTC):** 2025-03-04T02:09:07Z
  - **Event:** Silent installation triggered via command: `tor-browser-windows-x86_64-portable-14.0.6.exe /S`.
  - **Source:** `tor-install.csv` (ProcessCreated action).

---

4. Tor Browser Setup & File Creation

- **Timestamp (UTC):** 2025-03-04T02:09:25Z
    - **Event:** License files (`Tor.txt`, `Torbutton.txt`, `Tor-Launcher.txt`) created in `C:\Users\labuser\Desktop\Tor Browser\Browser\TorBrowser\Docs\Licenses`.
    - **Source:** `tor-download.csv` (FileCreated action).

---

5. Launch of Tor Browser Components

- **Timestamp (UTC):** 2025-03-04T02:09:28Z
    - **Event:** First `firefox.exe` process spawned from `C:\Users\labuser\Desktop\Tor Browser\Browser\firefox.exe`.
    - **Source:** `tor-process-creation.csv` (ProcessCreated action).
    - **Details:** Multiple child processes of `firefox.exe` created afterward, indicating Tor Browser startup.
- **Timestamp (UTC):** 2025-03-04T02:09:42Z
    - **Event:** `tor.exe` process started from `C:\Users\labuser\Desktop\Tor Browser\Browser\TorBrowser\Tor\tor.exe`.
    - **Source:** `tor-process-creation.csv` (ProcessCreated action).
    - **Command Line:** Configured to use Tor control port `9151` and SOCKS proxy `127.0.0.1:9150`.

---

6. Tor Network Connections

- **Timestamp (UTC):** 2025-03-04T02:10:13Z
    - **Event: ConnectionFailed** to `127.0.0.1:9150` via `firefox.exe`.
    - **Source:** `tor-usage.csv`.
- **Timestamp (UTC):** 2025-03-04T02:10:34Z
    - **Event: ConnectionSuccess** to Tor node `185.246.86.175:9001` via `tor.exe`.
    - **Source:** `tor-usage.csv`.
- **Timestamp (UTC):** 2025-03-04T02:10:42Z
    - **Event: ConnectionSuccess** to local SOCKS proxy `127.0.0.1:9150` via `firefox.exe`.
    - **Source:** `tor-usage.csv`.
- **Timestamp (UTC):** 2025-03-04T02:10:52Z
    - **Event: ConnectionFailed** to `107.189.5.25:9001` via `tor.exe`.
    - **Source:** `tor-usage.csv`.

---

7. Suspicious File Creation

- **Timestamp (UTC):** 2025-03-04T02:14:00Z
    - **Event:** File `freemovielinks.txt` created (found during threat hunt).
    - **Details:** Not present in provided logs but detected via threat hunt queries. Potential indicator of data exfiltration or unauthorized activity.

---

8. Browser Profile Modifications

- **Timestamp (UTC):** 2025-03-04T03:02:15Z
    - **Event:** Browser profile files (`storage.sqlite`, `formhistory.sqlite`, `webappsstore.sqlite`) modified in `C:\Users\labuser\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default`.
    - **Source:** `tor-download.csv` (FileModified/FileCreated actions).

Summary

1. **Installation Phase:**
    - Labuser downloaded and silently installed Tor Browser, bypassing typical user prompts.
    - Critical Tor components (`tor.exe`, `firefox.exe`) and configuration files were deployed to the Desktop.
2. **Execution & Network Activity:**
    - Tor Browser launched, establishing connections to Tor nodes (`185.246.86.175:9001`).
    - Local SOCKS proxy (`127.0.0.1:9150`) usage confirmed, consistent with Tor traffic routing.
3. **Post-Usage Activity:**
    - Suspicious file `freemovielinks.txt` created shortly after Tor usage, suggesting potential data exfiltration or access to unauthorized content.
    - Browser profile modifications indicate user activity (e.g., form history, storage updates).

Response Taken

TOR usage was confirmed on endpoint **mde-test** by the user **labuser**. The device was isolated and the user's direct manager was notified.