Threat Hunt Report (Unauthorized TOR Usage)

Detection of Unauthorized TOR Browser Installation and Use on Workstation: _______________

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. Created a rule in Microsoft Sentinel to help with detection of any tor(.exe) or firefox(.exe) events that may have taken place in DeviceFileEvents, DeviceProcessEvents, and DeviceNetworkEvents. The query I used will be located at the bottom of the report.
2. Once the alert was triggered indicating any signs of tor or firefox usage, I assigned the investigation to myself, declared it active, and began to investigate.
3. To start my investigation, I took a screenshot of all processes, IPs, and DeviceNames captured by the rule. There were 10+ processes, 3 IPs, and 2 Devices that triggered the rule.
4. Then, I proceeded to examine all the logs using the same query so they were all in one place.
5. From the logs, I gathered all relevant information in screenshots.
6. I wrote a summary of all events and included full details at the bottom of the report.
7. I marked the incident as closed and kept the rule running for security purposes.

Chronological Events

1. The timeline begins at (2025-12-24T00:48:54.5084843Z) with Tor(.exe) being downloaded directly to the device.
2. Next, Powershell was used to install Tor silently to bypass any EDR alerts.
3. Between 2025-12-24T00:55:53.5387343Z and 2025-12-24T01:02:05.6748412Z, Tor was executed many times. The most probable cause was that the user was trying to troubleshoot.

4. At 2025-12-24T01:02:34.1642381Z, the user successfully connected with the Tor browser using Firefox. The device was using the IP 89.234.157.254 and communicating over port 9001.
5. At 2025-12-24T01:18:01.8090358Z, the user creates a file named “tor-shopping-list.txt

---

Summary

This threat hunt was conducted to identify unauthorized TOR browser usage following concerns that employees may be attempting to bypass network security controls. A Microsoft Sentinel analytics rule was created to correlate file, process, and network telemetry across DeviceFileEvents, DeviceProcessEvents, and DeviceNetworkEvents. The rule successfully identified TOR-related file creation, execution, and outbound network connections on endpoint **NickScenario2**, including communication over known TOR ports. Investigation confirmed that TOR was downloaded, installed, and executed multiple times, with network activity consistent with attempts to connect to the TOR network. Although no evidence of successful access to external TOR-hosted websites was observed, unauthorized TOR usage was confirmed. The affected device was isolated, management was notified, and the detection rule remains active to monitor for similar activity in the future.

Response Taken

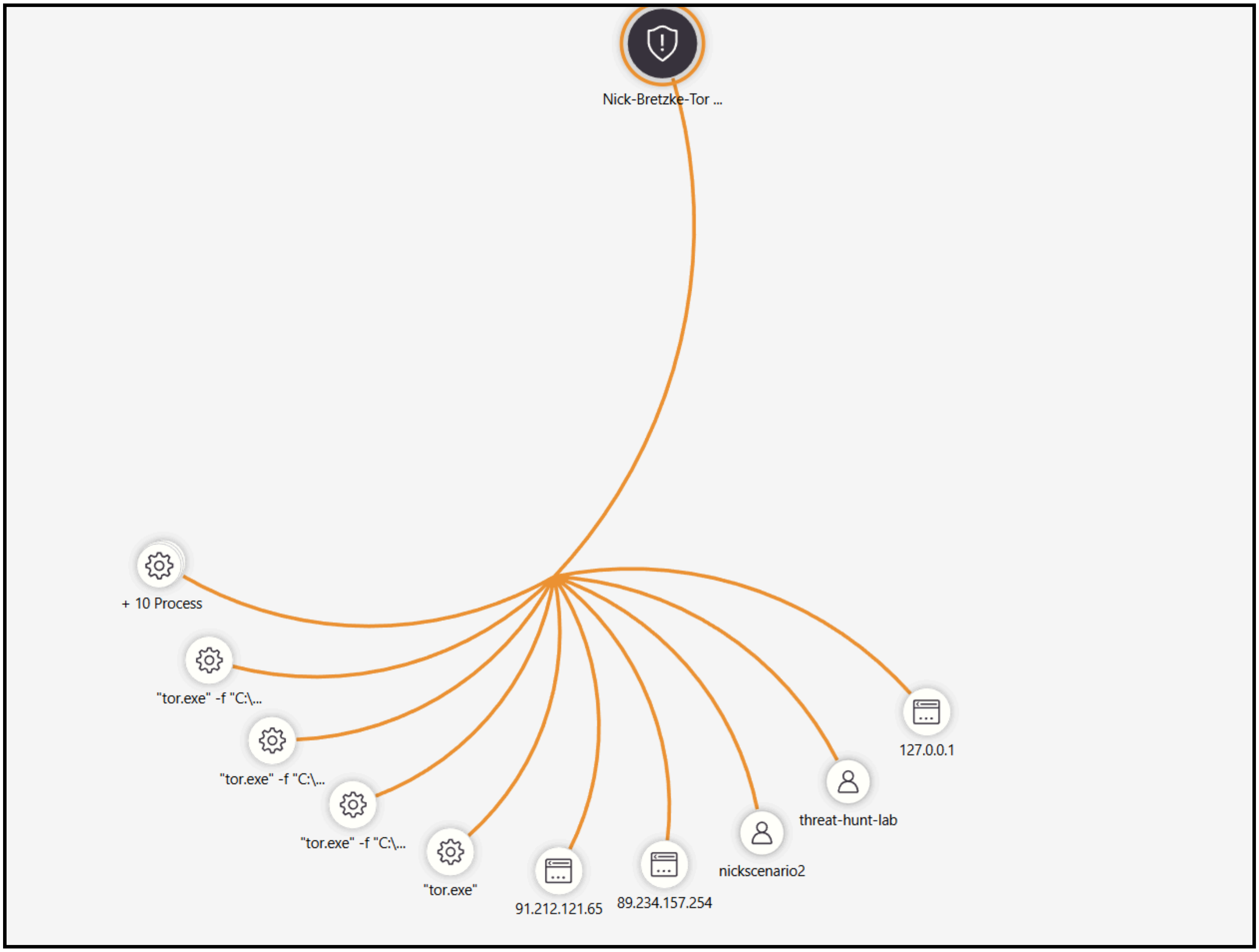
TOR usage was confirmed on endpoint NickScenario2. The device was isolated and the user's direct manager was notified.

Additional Information:

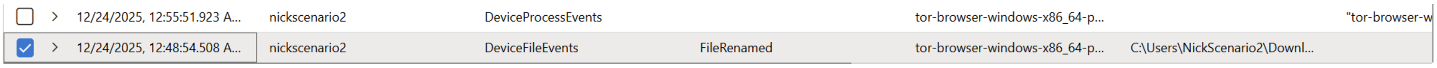
Query used in detection:

```
let lookback = 24h;

union
(
    DeviceFileEvents
    | where TimeGenerated >= ago(lookback)
    | where FileName has_any ("tor","onion")
    | extend SourceTable = "DeviceFileEvents"
    | project TimeGenerated, DeviceName, SourceTable, FileName, FolderPath
),
(
    DeviceProcessEvents
    | where TimeGenerated >= ago(lookback)
    | where FileName has_any ("tor","onion")
    | extend SourceTable = "DeviceProcessEvents"
    | project TimeGenerated, DeviceName, SourceTable, FileName, ProcessCommandLine
),
(
    DeviceNetworkEvents
    | where TimeGenerated >= ago(lookback)
    | where ActionType in ("ConnectionAttempt", "ConnectionSuccess")
    | where RemotePort in (9001, 9030, 9040, 9050, 9051, 9150)
    | where InitiatingProcessFileName has_any ("tor", "firefox")
    | extend SourceTable = "DeviceNetworkEvents"
    | project TimeGenerated, DeviceName, SourceTable,
              InitiatingProcessFileName, InitiatingProcessCommandLine,
              RemoteIP, RemotePort
)
| order by TimeGenerated desc
```

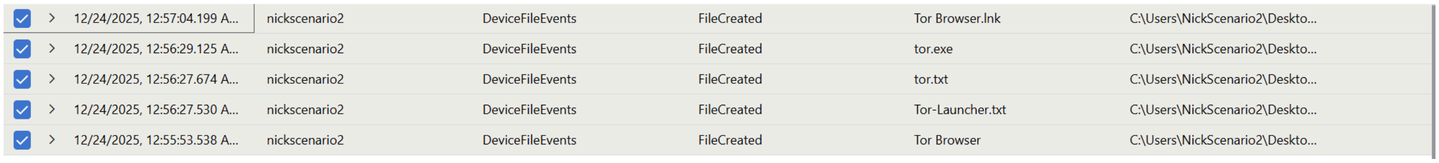


Tor Browser was downloaded:



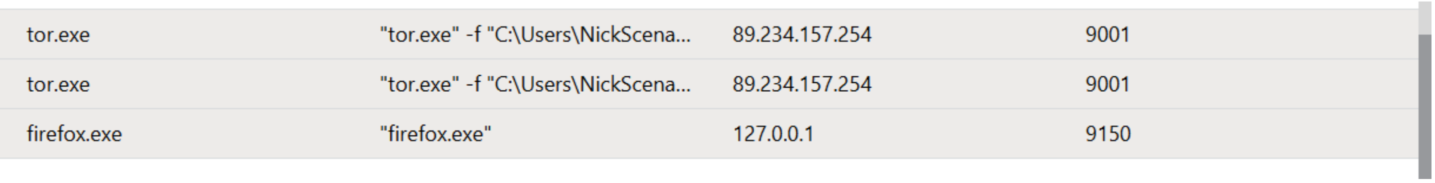
□	>	12/24/2025, 12:55:51.923 A...	nickscenario2	DeviceProcessEvents		tor-browser-windows-x86_64-p...		"tor-browser-w
☑	>	12/24/2025, 12:48:54.508 A...	nickscenario2	DeviceFileEvents	FileRenamed	tor-browser-windows-x86_64-p...	C:\Users\NickScenario2\Downl...	

Tor files were successfully created:



☑	>	12/24/2025, 12:57:04.199 A...	nickscenario2	DeviceFileEvents	FileCreated	Tor Browser.lnk	C:\Users\NickScenario2\Deskto...
☑	>	12/24/2025, 12:56:29.125 A...	nickscenario2	DeviceFileEvents	FileCreated	tor.exe	C:\Users\NickScenario2\Deskto...
☑	>	12/24/2025, 12:56:27.674 A...	nickscenario2	DeviceFileEvents	FileCreated	tor.txt	C:\Users\NickScenario2\Deskto...
☑	>	12/24/2025, 12:56:27.530 A...	nickscenario2	DeviceFileEvents	FileCreated	Tor-Launcher.txt	C:\Users\NickScenario2\Deskto...
☑	>	12/24/2025, 12:55:53.538 A...	nickscenario2	DeviceFileEvents	FileCreated	Tor Browser	C:\Users\NickScenario2\Deskto...

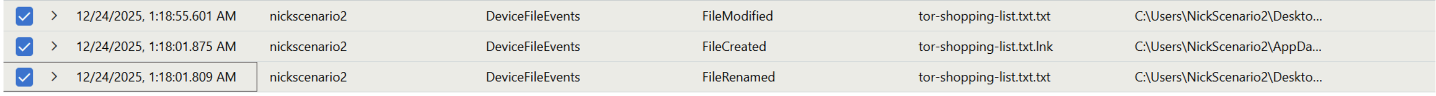
Tor was successfully ran on the device using firefox and then connected to the tor browser within Firefox.



tor.exe	"tor.exe" -f "C:\Users\NickScena...	89.234.157.254	9001
tor.exe	"tor.exe" -f "C:\Users\NickScena...	89.234.157.254	9001
firefox.exe	"firefox.exe"	127.0.0.1	9150

I do not see any evidence of successful connection with any websites.

The user created a file called Tor shopping list.



☑	>	12/24/2025, 1:18:55.601 AM	nickscenario2	DeviceFileEvents	FileModified	tor-shopping-list.txt.txt	C:\Users\NickScenario2\Deskto...
☑	>	12/24/2025, 1:18:01.875 AM	nickscenario2	DeviceFileEvents	FileCreated	tor-shopping-list.txt.lnk	C:\Users\NickScenario2\AppDa...
☑	>	12/24/2025, 1:18:01.809 AM	nickscenario2	DeviceFileEvents	FileRenamed	tor-shopping-list.txt.txt	C:\Users\NickScenario2\Deskto...

The user has not used the tor browser since and has not removed it from the device.