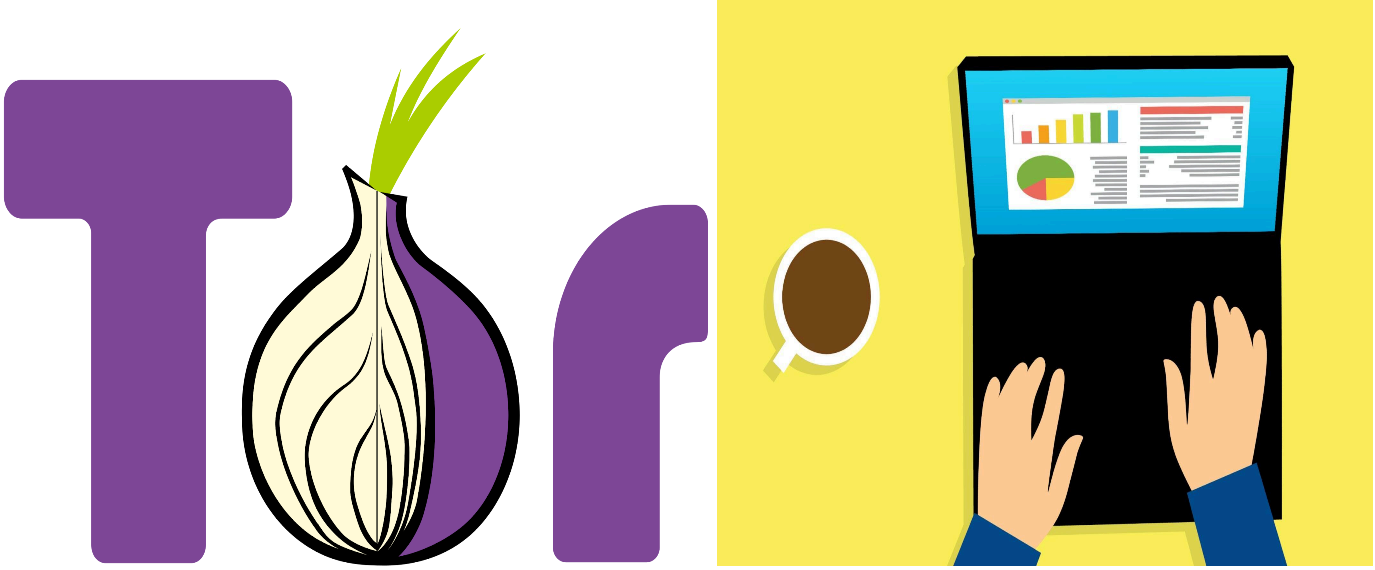


Threat Hunt Report

Family Member Compromise Leads to Unauthorized TOR Usage

Detection of Unauthorized TOR Browser Installation and Use on Workstation: **win11vmbruce**

Scenario:

A non-employee (family member) has used an employee’s workstation to install and use the TOR browser for browsing the dark web, creating traces of unauthorized software installation, network connections to TOR nodes, and the creation/deletion of suspicious text files. This behavior indicates potential insider misuse or an external compromise vector requiring investigation. 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 IoC Discovery Plan

Purpose: quickly discover and triage evidence of TOR installation and use on endpoints using Microsoft Defender for Endpoint (MDE) telemetry and Azure Sentinel. The goal is to find installer activity, process executions, and anonymized network connections, then escalate to containment if confirmed.

Quick overview

Search endpoint file, process, and network telemetry for TOR-related filenames/processes (e.g., `tor.exe`, `tor-browser`, `firefox.exe` inside Tor bundle) and outbound connections on TOR ports (9001, 9030, 9040, 9050, 9051, 9150).

Priority checklist

1. **File evidence** — `DeviceFileEvents`: detect installer downloads and tor-related files on disk (high confidence, quick).
2. **Process evidence** — `DeviceProcessEvents`: detect silent install command lines and `tor.exe` / bundled `firefox.exe` executions (high confidence).
3. **Network evidence** — `DeviceNetworkEvents`: detect outbound connections from `tor.exe`/`firefox.exe` to known TOR ports / unusual IPs (confirmation).
4. **Correlate** timestamps across the three sources to construct timeline and attribute to a user/device.
5. **Triage & Contain** if events are confirmed (isolate endpoint, capture artifacts).

Steps Taken

1. Searched the DeviceFileEvents table for ANY file that contained the string “tor” in it and discovered that the user: “threathunt” has downloaded a “tor” installer. This has resulted in numerous “tor” related files being created, and a file being created on the desktop named “tor-shopping-list.txt,” which was created on: 2025-10-20T22:26:17.2212683Z
—
These following events began at this time: 2025-10-20T21:38:15.4884203Z

At approximately **9:38 PM UTC on October 20, 2025**, the workstation **win11vmbruce** recorded a `FileRenamed` event under the account **threathunt** for the file **tor-browser-windows-x86_64-portable-14.5.8.exe** in the **Downloads** directory. Additional file creation events followed, including the creation of several executable and text files associated with the TOR browser package (`tor.exe`, `tor.txt`, `Torbutton.txt`, `Tor-Launcher.txt`), indicating that a new software package was unpacked or modified within the user's directory.

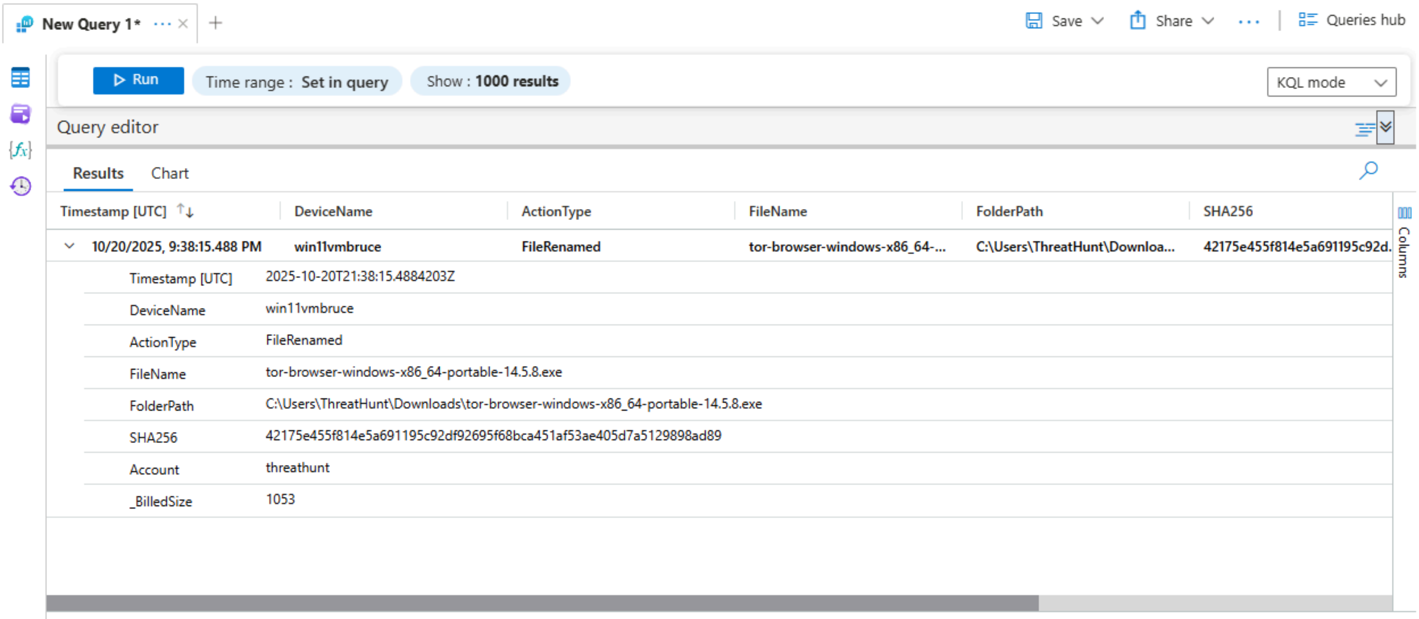
These file creation and renaming events mark the **initial observable signs of software installation activity** on the device. At this point in the investigation, it is too early to determine intent or identify the user's exact motivation. However, the presence of multiple TOR-related files suggests the early stages of a new application setup.

Given that this system is shared between an employee and a **family member**, it remains plausible that the non-employee user may have initiated these actions without awareness of security restrictions. Analysts should continue monitoring subsequent process and network telemetry to establish whether this installation progressed into unauthorized activity or external communication.

Query to locate this event:

```
DeviceFileEvents
| where FileName startswith "tor"
| where DeviceName == "win11vmbruce"
| where InitiatingProcessAccountName has "threathunt"
| where Timestamp == todatetime('2025-10-20T21:38:15.4884203Z')
| project Timestamp, DeviceName, ActionType, FileName, FolderPath, SHA256, Account =
InitiatingProcessAccountName
```

Return:



Timestamp [UTC]	DeviceName	ActionType	FileName	FolderPath	SHA256
10/20/2025, 9:38:15.488 PM	win11vmbruce	FileRenamed	tor-browser-windows-x86_64-...	C:\Users\ThreatHunt\Downloa...	42175e455f814e5a691195c92d.

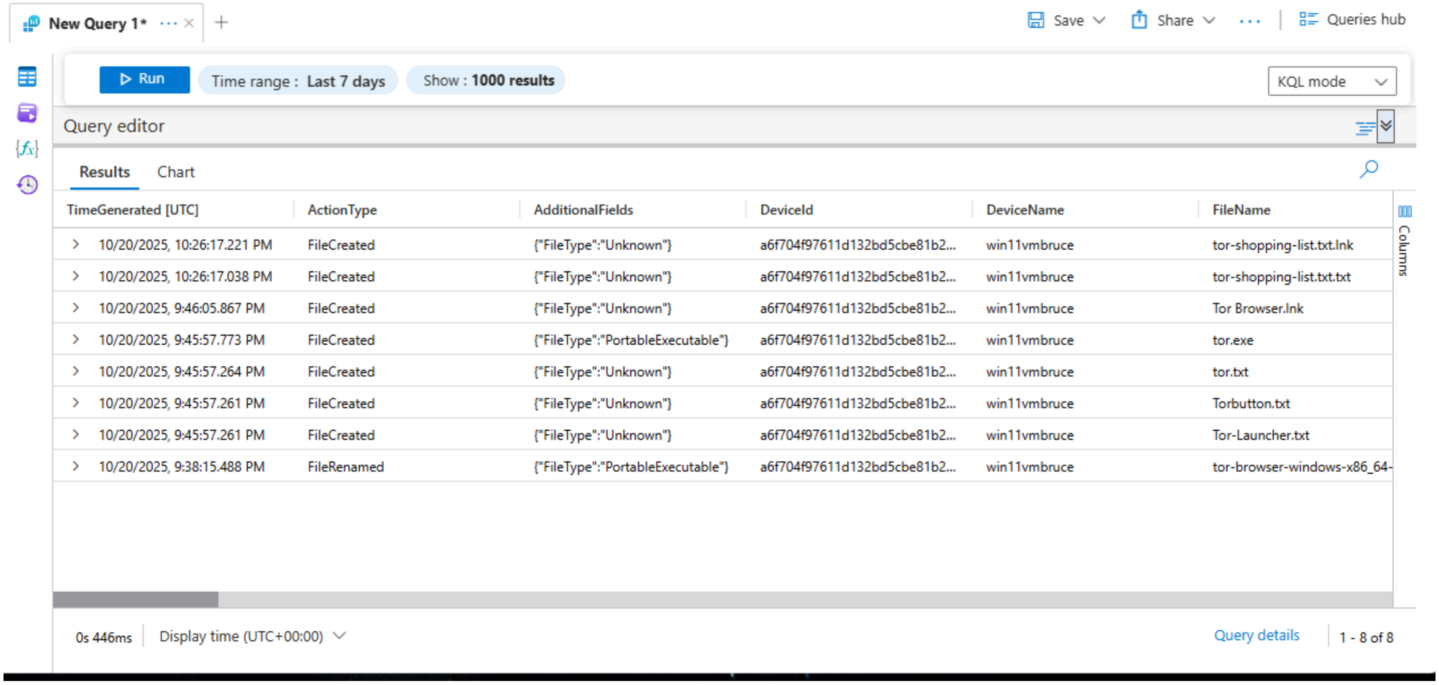
Timestamp [UTC]	2025-10-20T21:38:15.4884203Z
DeviceName	win11vmbruce
ActionType	FileRenamed
FileName	tor-browser-windows-x86_64-portable-14.5.8.exe
FolderPath	C:\Users\ThreatHunt\Downloads\tor-browser-windows-x86_64-portable-14.5.8.exe
SHA256	42175e455f814e5a691195c92df92695f68bca451af53ae405d7a5129898ad89
Account	threathunt
_BilledSize	1053

Query to locate these events:

```
DeviceFileEvents
```

```
| where FileName startswith "tor"
| where DeviceName == "win11vmbruce"
| where InitiatingProcessAccountName has "threathunt"
```

Returns:



TimeGenerated [UTC]	ActionType	AdditionalFields	DeviceId	DeviceName	FileName
10/20/2025, 10:26:17.221 PM	FileCreated	{"FileType":"Unknown"}	a6f704f97611d132bd5cbe81b2...	win11vmbruce	tor-shopping-list.txt.lnk
10/20/2025, 10:26:17.038 PM	FileCreated	{"FileType":"Unknown"}	a6f704f97611d132bd5cbe81b2...	win11vmbruce	tor-shopping-list.txt.txt
10/20/2025, 9:46:05.867 PM	FileCreated	{"FileType":"Unknown"}	a6f704f97611d132bd5cbe81b2...	win11vmbruce	Tor Browser.lnk
10/20/2025, 9:45:57.773 PM	FileCreated	{"FileType":"PortableExecutable"}	a6f704f97611d132bd5cbe81b2...	win11vmbruce	tor.exe
10/20/2025, 9:45:57.264 PM	FileCreated	{"FileType":"Unknown"}	a6f704f97611d132bd5cbe81b2...	win11vmbruce	tor.txt
10/20/2025, 9:45:57.261 PM	FileCreated	{"FileType":"Unknown"}	a6f704f97611d132bd5cbe81b2...	win11vmbruce	Torbutton.txt
10/20/2025, 9:45:57.261 PM	FileCreated	{"FileType":"Unknown"}	a6f704f97611d132bd5cbe81b2...	win11vmbruce	Tor-Launcher.txt
10/20/2025, 9:38:15.488 PM	FileRenamed	{"FileType":"PortableExecutable"}	a6f704f97611d132bd5cbe81b2...	win11vmbruce	tor-browser-windows-x86_64-

---

2. Searched the DeviceProcessEvents table for any ProcessCommandLine that contained the string: “tor-browser-windows-x86_64-portable-14.5.8.exe”

Based on the logs returned on October 20, 2025, at approximately 9:45 PM UTC

Timestamp: 2025-10-20T21:45:40.1006109Z

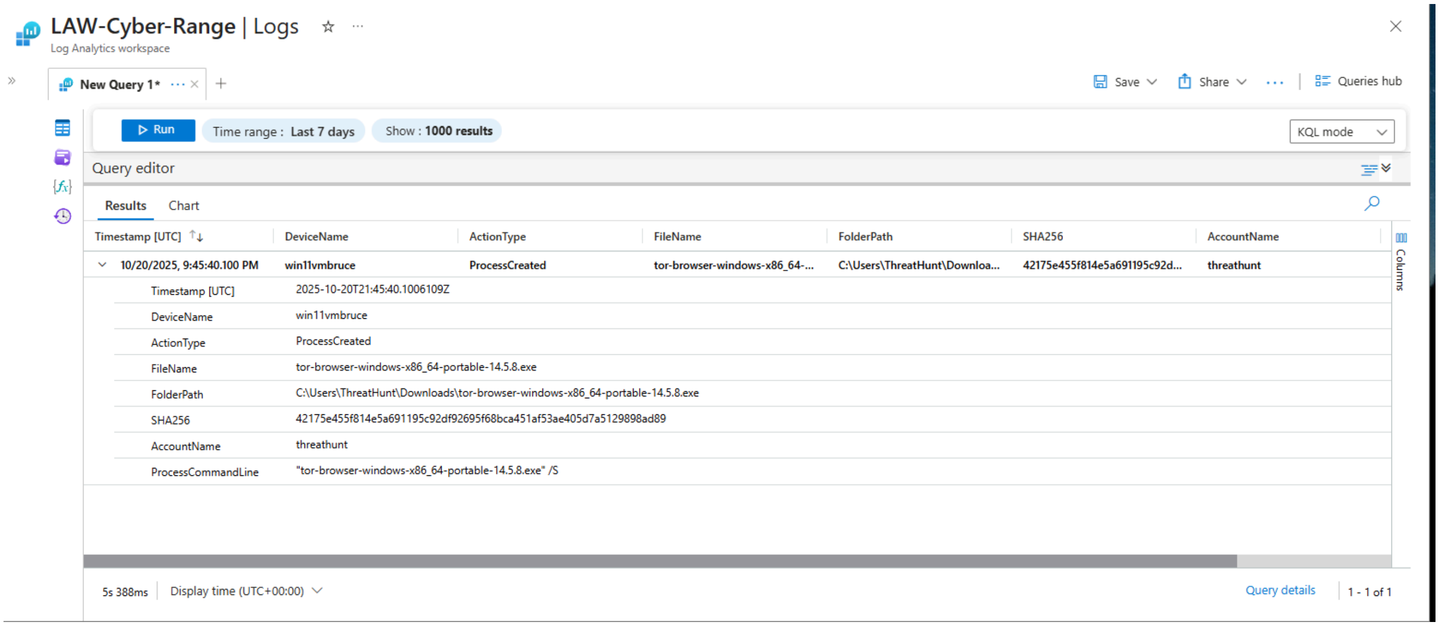
The user account “threathunt” on the workstation win11vmbruce silently executed the TOR browser installer (tor-browser-windows-x86_64-portable-14.5.8.exe) from the Downloads directory. The command-line argument “/S” indicates that the installation was performed silently, without user prompts, suggesting an attempt to install the software discreetly.

This event signifies the initial phase of unauthorized TOR browser installation. The use of a silent installation flag (/S) is atypical for legitimate users and often associated with scripted or concealed application deployments. In this case, contextual evidence suggests that the activity was not initiated by the employee directly, but rather by a family member who had access to the workstation. This supports the hypothesis that a non-employee user—acting without awareness of security policies—introduced unauthorized software and potential risk into the corporate environment.

Query to locate this event:

```
DeviceProcessEvents
| where DeviceName == "win11vmbruce"
| where ProcessCommandLine contains "tor-browser-windows-x86_64-portable-14.5.8.exe"
| project Timestamp, DeviceName, ActionType, FileName, FolderPath, SHA256, AccountName,
ProcessCommandLine
```

Returns:



Timestamp [UTC]	DeviceName	ActionType	FileName	FolderPath	SHA256	AccountName
10/20/2025, 9:45:40.100 PM	win11vmbruce	ProcessCreated	tor-browser-windows-x86_64-...	C:\Users\ThreatHunt\Downloa...	42175e455f814e5a691195c92d...	threathunt

Timestamp [UTC]	2025-10-20T21:45:40.1006109Z
DeviceName	win11vmbruce
ActionType	ProcessCreated
FileName	tor-browser-windows-x86_64-portable-14.5.8.exe
FolderPath	C:\Users\ThreatHunt\Downloads\tor-browser-windows-x86_64-portable-14.5.8.exe
SHA256	42175e455f814e5a691195c92df92695f68bca451af53ae405d7a5129898ad89
AccountName	threathunt
ProcessCommandLine	"tor-browser-windows-x86_64-portable-14.5.8.exe" /S

5s 388ms Display time (UTC+00:00) Query details 1 - 1 of 1

---

3. Searched the DeviceProcessEvents table for any evidence of the several “aliases” that the “tor browser” can be found under, and any evidence that the “employee family member” on the win11vmbruce workstation used the “tor” browser or any of its “aliases.”

There is evidence that the “employee family member” did indeed use this browser at: 2025-10-20T21:51:30.4896967Z

At approximately **9:51 PM UTC on October 20, 2025**, the workstation **win11vmbruce** initiated multiple process creation events for **firefox.exe**, the executable component of the TOR browser bundle. These processes originated from the directory path:

C:\Users\ThreatHunt\Desktop\Tor Browser\Browser

Under the user account **threathunt**. The repeated `ProcessCreated` events indicate the successful launch and active use of the TOR browser shortly after installation.

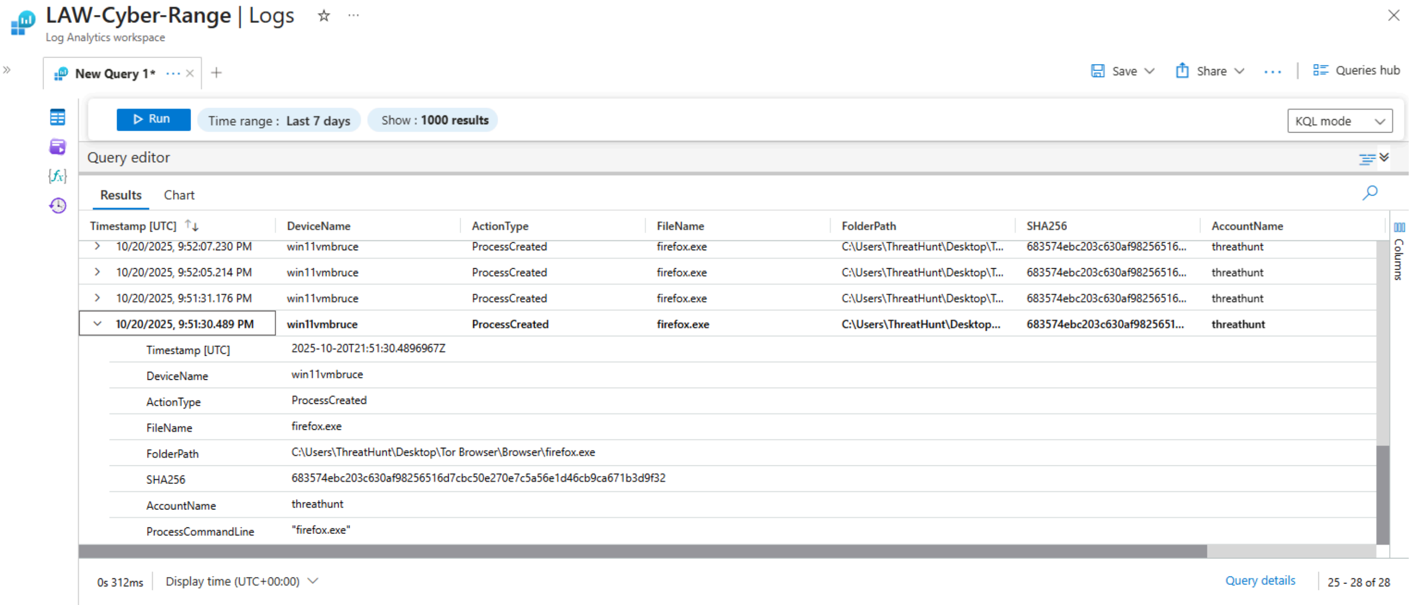
This sequence of process creation events confirms that the TOR browser was not only installed but also actively launched on the employee's workstation. The timing of these events—occurring minutes after the silent TOR installation—indicates immediate use of the application.

Correlating this behavior with prior context suggests that the **employee's family member** initiated the TOR browser, likely exploring or accessing dark web content without understanding the organizational risk. This activity directly violates acceptable use policies and introduces potential security exposure through anonymized browsing channels, further substantiating the hypothesis of **unintentional compromise through non-employee interaction**.

Query to locate these events:

```
DeviceProcessEvents
| where DeviceName == "win11vmbruce"
| where FileName has_any ("tor.exe", "firefox.exe", "tor-browser.exe")
| project Timestamp, DeviceName, ActionType, FileName, FolderPath, SHA256, AccountName, ProcessCommandLine
```

Returns:



Timestamp [UTC]	DeviceName	ActionType	FileName	FolderPath	SHA256	AccountName
10/20/2025, 9:52:07.230 PM	win11vmbruce	ProcessCreated	firefox.exe	C:\Users\ThreatHunt\Desktop\T...	683574ebc203c630af98256516...	threathunt
10/20/2025, 9:52:05.214 PM	win11vmbruce	ProcessCreated	firefox.exe	C:\Users\ThreatHunt\Desktop\T...	683574ebc203c630af98256516...	threathunt
10/20/2025, 9:51:31.176 PM	win11vmbruce	ProcessCreated	firefox.exe	C:\Users\ThreatHunt\Desktop\T...	683574ebc203c630af98256516...	threathunt
10/20/2025, 9:51:30.489 PM	win11vmbruce	ProcessCreated	firefox.exe	C:\Users\ThreatHunt\Desktop...	683574ebc203c630af9825651...	threathunt

Timestamp [UTC]	2025-10-20T21:51:30.4896967Z
DeviceName	win11vmbruce
ActionType	ProcessCreated
FileName	firefox.exe
FolderPath	C:\Users\ThreatHunt\Desktop\Tor Browser\Browser\firefox.exe
SHA256	683574ebc203c630af98256516d7cbc50e270e7c5a56e1d46cb9ca671b3d9f32
AccountName	threathunt
ProcessCommandLine	"firefox.exe"

0s 312ms | Display time (UTC+00:00) | 25 - 28 of 28

---

4. Searched the DeviceNetworkEvents table for any evidence from:

DeviceName, InitiatingProcessAccountName, ActionType, RemoteIP, RemotePort, RemoteUrl, InitiatingProcessFileName, and InitiatingProcessFolderPath; with a distinct focus on RemotePort for known "tor" browser used ports and possible connections to remote IP addresses, and remote URL's.

The evidence shows that at this time: 2025-10-20T21:52:33.9386116Z

At approximately **9:52 PM UTC on October 20, 2025**, the workstation **win11vmbruce** initiated two successful outbound network connections over **port 9001**, a port commonly associated with the TOR network. The connections were established by the process **tor.exe**, located in the directory `C:\Users\threathunt\Desktop\tor browser\browser\torbrowser\tor\tor.exe`.

- The first connection was made to remote IP **66.111.2.16** (URL: `https://www.zsh67ng4fgodd.com`).

- The second connection followed seconds later to remote IP **37.120.168.158** (URL: `https://www.kfddy6y7iwluprft56hql.com`).
  Both were logged as **ConnectionSuccess** events under the user account **threathunt**.

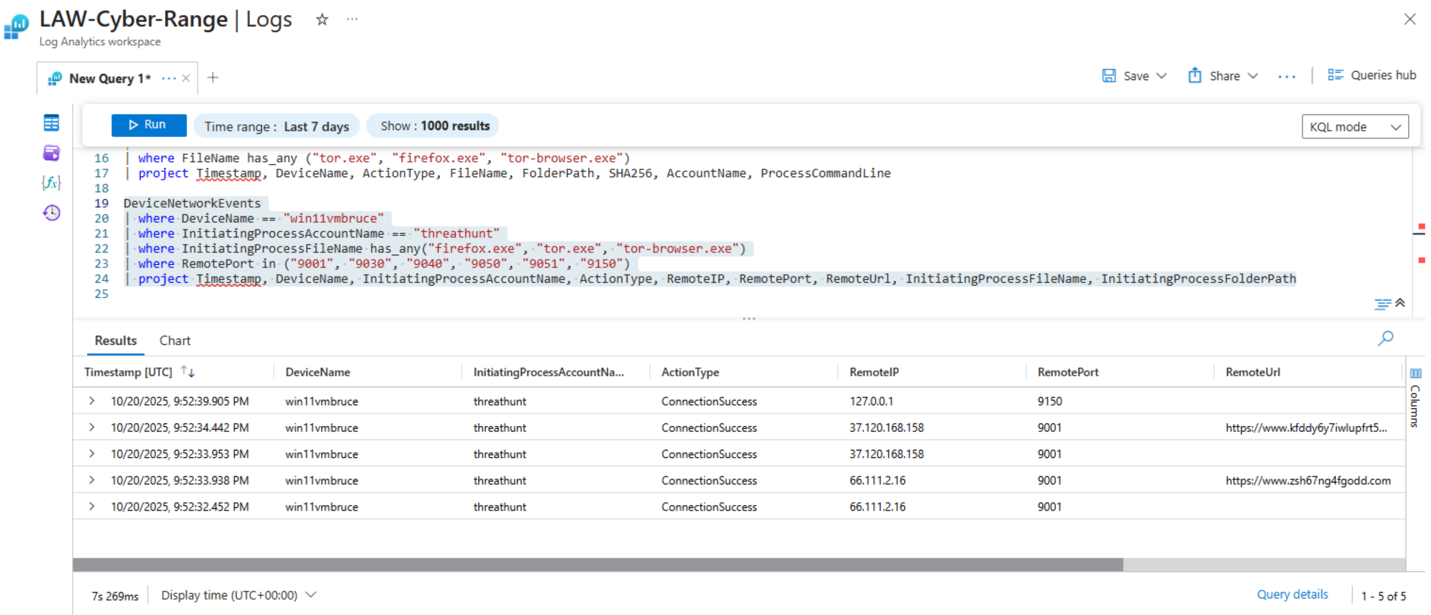
These events confirm that the TOR application successfully connected to external TOR relay nodes shortly after its silent installation. This activity demonstrates the transition from software installation to active TOR network usage, establishing an anonymized communication channel from within the corporate environment.

Contextual analysis suggests that the employee's **family member**—who previously installed the browser—initiated this session out of curiosity, personal browsing or possibly hearing the employee discussing this kind of activity, unaware of the security implications. By connecting to external TOR nodes, this action bypassed standard network visibility controls and potentially exposed the organization to unmonitored traffic paths, reinforcing the threat hypothesis of **indirect compromise via non-employee activity**.

Query to locate these events:

```
DeviceNetworkEvents
| where DeviceName == "win11vmbruce"
| where InitiatingProcessAccountName == "threathunt"
| where InitiatingProcessFileName has_any("firefox.exe", "tor.exe", "tor-browser.exe")
| where RemotePort in ("9001", "9030", "9040", "9050", "9051", "9150")
| project Timestamp, DeviceName, InitiatingProcessAccountName, ActionType, RemoteIP, RemotePort, RemoteUrl, InitiatingProcessFileName, InitiatingProcessFolderPath
```

Returns:



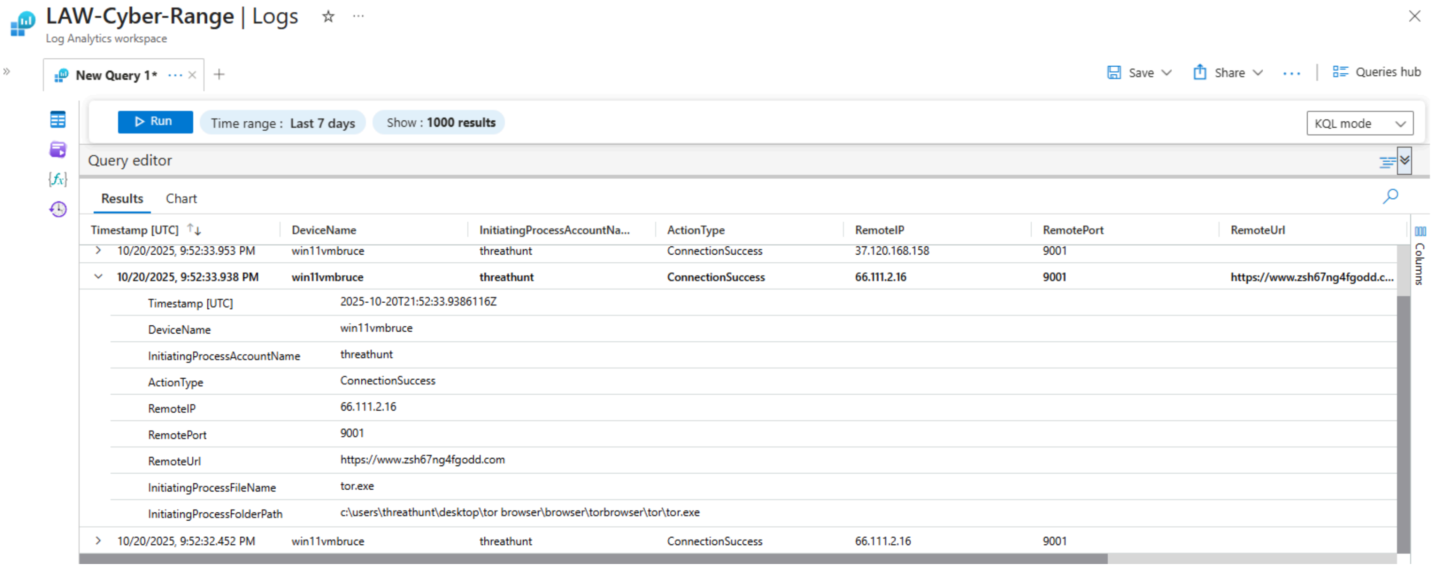
```
| where FileName has_any ("tor.exe", "firefox.exe", "tor-browser.exe")
| project Timestamp, DeviceName, ActionType, FileName, FolderPath, SHA256, AccountName, ProcessCommandLine

DeviceNetworkEvents
| where DeviceName == "win11vmbruce"
| where InitiatingProcessAccountName == "threathunt"
| where InitiatingProcessFileName has_any("firefox.exe", "tor.exe", "tor-browser.exe")
| where RemotePort in ("9001", "9030", "9040", "9050", "9051", "9150")
| project Timestamp, DeviceName, InitiatingProcessAccountName, ActionType, RemoteIP, RemotePort, RemoteUrl, InitiatingProcessFileName, InitiatingProcessFolderPath

```

Timestamp [UTC]	DeviceName	InitiatingProcessAccountNa...	ActionType	RemoteIP	RemotePort	RemoteUrl
10/20/2025, 9:52:39.905 PM	win11vmbruce	threathunt	ConnectionSuccess	127.0.0.1	9150	
10/20/2025, 9:52:34.442 PM	win11vmbruce	threathunt	ConnectionSuccess	37.120.168.158	9001	https://www.kfddy6y7iwlupfrt5...
10/20/2025, 9:52:33.953 PM	win11vmbruce	threathunt	ConnectionSuccess	37.120.168.158	9001	
10/20/2025, 9:52:33.938 PM	win11vmbruce	threathunt	ConnectionSuccess	66.111.2.16	9001	https://www.zsh67ng4fgodd.com
10/20/2025, 9:52:32.452 PM	win11vmbruce	threathunt	ConnectionSuccess	66.111.2.16	9001	

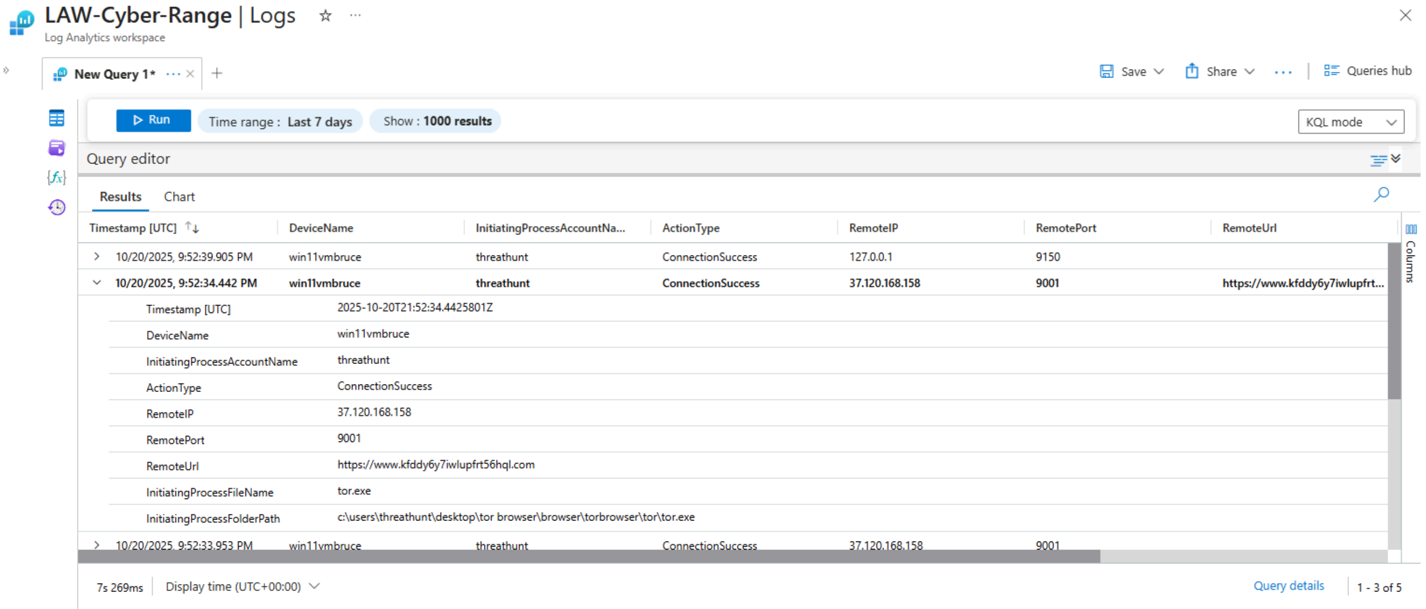
7s 269ms Display time (UTC+00:00) 1 - 5 of 5



Timestamp [UTC]	DeviceName	InitiatingProcessAccountNa...	ActionType	RemoteIP	RemotePort	RemoteUrl
10/20/2025, 9:52:33.953 PM	win11vmbruce	threathunt	ConnectionSuccess	37.120.168.158	9001	
10/20/2025, 9:52:33.938 PM	**win11vmbruce**	**threathunt**	**ConnectionSuccess**	**66.111.2.16**	**9001**	**https://www.zsh67ng4fgodd.c...**

Timestamp [UTC]	2025-10-20T21:52:33.9386116Z
DeviceName	win11vmbruce
InitiatingProcessAccountName	threathunt
ActionType	ConnectionSuccess
RemoteIP	66.111.2.16
RemotePort	9001
RemoteUrl	https://www.zsh67ng4fgodd.com
InitiatingProcessFileName	tor.exe
InitiatingProcessFolderPath	c:\users\threathunt\desktop\tor browser\browser\torbrowser\tor\tor.exe

Timestamp [UTC]	DeviceName	InitiatingProcessAccountNa...	ActionType	RemoteIP	RemotePort	RemoteUrl
10/20/2025, 9:52:32.452 PM	win11vmbruce	threathunt	ConnectionSuccess	66.111.2.16	9001	



Timestamp [UTC]	DeviceName	InitiatingProcessAccountNa...	ActionType	RemoteIP	RemotePort	RemoteUrl
10/20/2025, 9:52:39.905 PM	win11vmbruce	threathunt	ConnectionSuccess	127.0.0.1	9150	
10/20/2025, 9:52:34.442 PM	**win11vmbruce**	**threathunt**	**ConnectionSuccess**	**37.120.168.158**	**9001**	**https://www.kfddy6y7iwlupfrt...**

Timestamp [UTC]	2025-10-20T21:52:34.4425801Z
DeviceName	win11vmbruce
InitiatingProcessAccountName	threathunt
ActionType	ConnectionSuccess
RemoteIP	37.120.168.158
RemotePort	9001
RemoteUrl	https://www.kfddy6y7iwlupfrt56hql.com
InitiatingProcessFileName	tor.exe
InitiatingProcessFolderPath	c:\users\threathunt\desktop\tor browser\browser\torbrowser\tor\tor.exe

Timestamp [UTC]	DeviceName	InitiatingProcessAccountNa...	ActionType	RemoteIP	RemotePort	RemoteUrl
10/20/2025, 9:52:33.953 PM	win11vmbruce	threathunt	ConnectionSuccess	37.120.168.158	9001	

7s 269ms Display time (UTC+00:00) 1 - 3 of 5

5. Searched the DeviceFileEvents table for any evidence of file creation onto the workstation: win11vmbruce.

At this time: 2025-10-20T22:26:17.2212683Z, tor-shopping-list.txt was created.

At approximately **10:26 PM UTC on October 20, 2025**, the workstation **win11vmbruce** generated two file-creation events under the user account **threathunt**.

- The first event recorded the creation of the shortcut file **tor-shopping-list.txt.lnk**, initiated by **explorer.exe**.

- The second event, seconds later, showed the creation of the actual text file **tor-shopping-list.txt**, initiated by **notepad.exe**.
  Both events confirm that a user on the system manually created a text file and began editing it, consistent with interactive desktop activity.

These file-creation events confirm direct user interaction following TOR browser usage. The creation of a text file named **“tor-shopping-list.txt”**—and its corresponding link—suggests that the user intended to record items or information gathered during dark-web browsing.

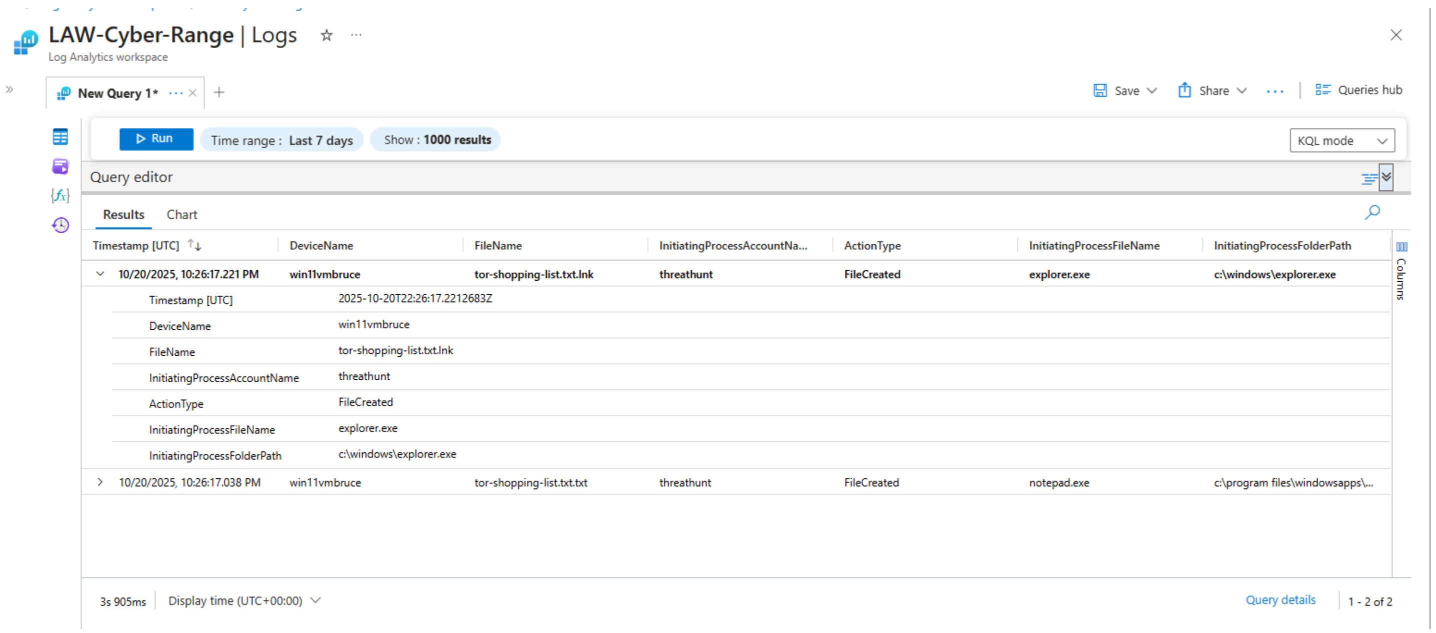
Based on contextual evidence from earlier in the investigation, this behavior was likely performed by the **employee’s family member**, who was using the system unsupervised. The action reinforces the narrative of **unintentional insider risk**, where a non-employee, unaware of corporate security expectations, engaged in activities that introduced policy violations and potential exposure of the organization’s endpoint.

The use of **notepad.exe** and **explorer.exe** as initiating processes confirms local, manual creation rather than automated or malicious scripting, painting a clear picture of curiosity-driven but risky user behavior.

Query to locate this event:

```
DeviceFileEvents
| where DeviceName == "win11vmbruce"
| where FileName contains "tor-shopping-list"
| project Timestamp, DeviceName, FileName, InitiatingProcessAccountName, ActionType,
InitiatingProcessFileName, InitiatingProcessFolderPath
```

Return:



Timestamp [UTC]	DeviceName	FileName	InitiatingProcessAccountNa...	ActionType	InitiatingProcessFileName	InitiatingProcessFolderPath
10/20/2025, 10:26:17.221 PM	win11vmbruce	tor-shopping-list.txt.lnk	threathunt	FileCreated	explorer.exe	c:\windows\explorer.exe
10/20/2025, 10:26:17.038 PM	win11vmbruce	tor-shopping-list.txt.txt	threathunt	FileCreated	notepad.exe	c:\program files\windowsapps\...

Timestamp [UTC]	2025-10-20T22:26:17.2212683Z
DeviceName	win11vmbruce
FileName	tor-shopping-list.txt.lnk
InitiatingProcessAccountName	threathunt
ActionType	FileCreated
InitiatingProcessFileName	explorer.exe
InitiatingProcessFolderPath	c:\windows\explorer.exe

Chronological Events

Overview

Date of Activity: October 20, 2025
System: `win11vmbruce`
User Account: `threathunt`
Summary:
A sequence of events showing the download, silent installation, and use of the TOR browser by a non-employee (family member) on a corporate-managed workstation. Activity included outbound TOR connections and the creation of a “shopping list” file — indicating interactive use.

Timeline of Events

1. File Renamed – TOR Installer Appears

Time: 9:38:15 PM UTC
Action: `FileRenamed`
File: `tor-browser-windows-x86_64-portable-14.5.8.exe`

Location: `C:\Users\ThreatHunt\Downloads\`
Account: `threathunt`

Observation:
The TOR browser installer was renamed or modified in the Downloads directory — marking the first visible sign of TOR-related activity.

Analyst Note:
Early evidence of software introduction. The action likely represents the point where the family member either downloaded or prepared the installer but had not yet executed it.

---

2. Process Created – Silent Installation

Time: 9:45:40 PM UTC
Action: `ProcessCreated`
Process: `"tor-browser-windows-x86_64-portable-14.5.8.exe" /S`
Account: `threathunt`

Observation:
The TOR installer was executed with a `/S` argument — indicating a **silent installation** without user prompts.

Analyst Interpretation:
This suggests an intentional or scripted installation method. Given the context, it's likely that the employee's **family member** initiated this, unaware that it violated organizational policy or introduced risk.

---

3. File Created – TOR Components Unpacked

Time: 9:45:57 PM UTC
Action: `FileCreated`
Files: `tor.exe`, `Torbutton.txt`, `Tor-Launcher.txt`, `tor.txt`
Account: `threathunt`

Observation:
Several TOR-related executables and text files were created seconds after installation, confirming the unpacking of the TOR bundle.

Analyst Interpretation:
This marks the successful installation of the TOR environment on the endpoint. The rapid creation of multiple files supports that this was an automated extraction process.

4. Process Created – TOR Browser Launches

Time: 9:51:30–9:52:07 PM UTC
Action: `ProcessCreated`
Process: `firefox.exe`
Folder: `C:\Users\ThreatHunt\Desktop\Tor Browser\Browser\`
Account: `threathunt`

Observation:
Multiple `firefox.exe` process creation events occurred within a short time frame.

Analyst Interpretation:
This confirms user interaction — the TOR browser was opened and possibly restarted multiple times.
Correlating this behavior with previous events suggests the family member began actively using the browser immediately after installation.

5. Network Connections – TOR Relay Nodes

Time: 9:52:33 PM & 9:52:34 PM UTC
Action: `ConnectionSuccess`
Process: `tor.exe`
Remote IPs:

- `66.111.2.16:9001` → `https://www.zsh67ng4fgodd.com`
- `37.120.168.158:9001` → `https://www.kfddy6y7iwluprft56hql.com`

Observation:
Two outbound connections from `tor.exe` were made over **port 9001**, which is typically used for TOR network relays.

Analyst Interpretation:
These events confirm the TOR browser successfully connected to external relay nodes, creating encrypted and anonymized network traffic.
This aligns with the hypothesis that a **non-employee family member** was using TOR for personal browsing without realizing it introduced unmonitored network exposure.

6. File Created – “Shopping List” Document

Time: 10:26:17 PM UTC
Action: `FileCreated`
Files:

- `tor-shopping-list.txt`
- `tor-shopping-list.txt.lnk`
  Processes: `notepad.exe` and `explorer.exe`
  Account: `threathunt`

Observation:
A text file and corresponding shortcut were created, likely representing a manually typed list by the user.

Analyst Interpretation:
This is a clear sign of **human interaction**. The file name and timing suggest that while browsing TOR content, the family member began writing or saving notes.
While not malicious, this behavior demonstrates unsafe user actions and further supports the **family member compromise** narrative.

Summary of Events

Between **9:38 PM and 10:26 PM UTC**, the workstation `win11vmbruce` underwent a complete cycle of TOR browser installation and use.

1. The **installer appeared and was renamed** in the Downloads folder.
2. It was **executed silently**, unpacking TOR components.
3. **Browser processes launched**, indicating user activity.
4. **Connections to TOR nodes** established over known relay ports.
5. A **“shopping list” text file** was manually created and deleted later, showing direct engagement.

The consistent use of the **`threathunt`** account and the timeline of events align with the previously established hypothesis that the system was accessed by the **employee’s family member**.
This individual, likely unaware of the organizational implications, introduced unauthorized software and connected to anonymizing networks, unintentionally creating security and compliance risks.

Analyst Conclusion

The incident reflects an **unintentional insider risk** scenario.
The family member’s actions demonstrate a lack of awareness rather than malicious intent — however, the result was a clear breach of acceptable use policy and potential network exposure through TOR connectivity.

MITRE ATT&CK mapping

- **T1204** — User Execution (user launched installer / opened browser)
- **T1071** — Application Layer Protocol (TOR uses application layer for anonymized comms)
- **T1090** — Proxy (TOR acts as anonymizing proxy)
- **T1547** — (if persistence mechanisms are found) — Boot or service persistence

---

Response Taken

TOR usage was confirmed on endpoint **win11vmbruce**. The device was isolated and the user's direct manager was notified.

Recommended Next Steps:

- Implement application control (AppLocker or Defender Application Control).
- Restrict administrative rights for shared systems.
- Increase user awareness training regarding shared device usage.
- Enhance monitoring for TOR process and port activity in MDE / Sentinel.

Suggested alert rule (pseudocode):

IF (DeviceProcessEvents.ProcessCommandLine contains "tor-browser" OR DeviceFileEvents.FileName startswith "tor-browser")

AND (DeviceNetworkEvents.InitiatingProcessFileName in ("tor.exe","firefox.exe") AND RemotePort in (9001,9050,9150))

THEN Alert: "Possible TOR Installation and Use on Endpoint"

Severity: High