

Threat Hunt Creation

1. Create the Hypothesis

Threat Hunt Hypothesis

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.

2. Create a Virtual Machine at <https://portal.azure.com/>.

Virtual machine		Networking	
Computer name	Win11VMBruce	Public IP address ⓘ	-
Operating system	Windows (Windows 11 Pro)	Public IP address (IPv6)	-
VM generation	V2	Private IP address	10.1.0.142
VM architecture	x64	Private IP address (IPv6)	-
Agent status	Ready	Virtual network/subnet	Cyber-Range-2-VNet/Cyber-Range-2-Subnet
Agent version	2.7.41491.1172	DNS name	-

3. Onboard this Virtual Machine to Microsoft Defender for Endpoint.

First, log in to the Virtual Machine using Remote Desktop via Bastion within Azure and enable the Virtual Machine to be onboarded to Microsoft Defender for Endpoint.

```
Administrator: C:\Windows\S... x + -
This script is for onboarding machines to the Microsoft Defender for Endpoint services, including security and compliance products.
Once completed, the machine should light up in the portal within 5-30 minutes, depending on this machine's Internet connectivity availability and machine power state (plugged in vs. battery powered).
IMPORTANT: This script is optimized for onboarding a single machine and should not be used for large scale deployment. For more information on large scale deployment, please consult the MDE documentation (links available in the MDE portal under the endpoint onboarding section).

Press (Y) to confirm and continue or (N) to cancel and exit: y

Starting Microsoft Defender for Endpoint onboarding process...

Testing administrator privileges
Script is running with sufficient privileges

Performing onboarding operations

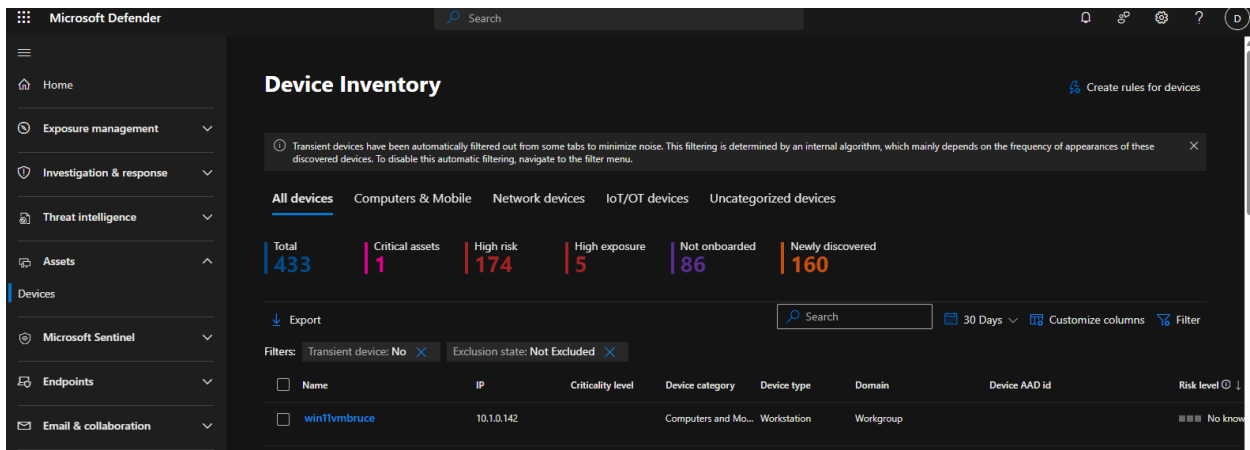
Starting the service, if not already running

Finished performing onboarding operations

Waiting for the service to start

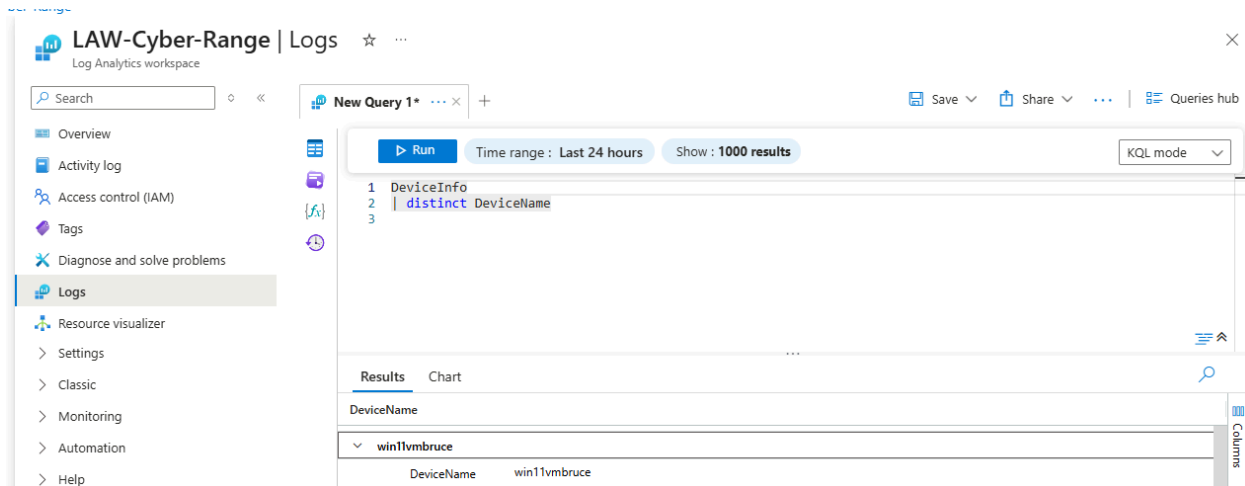
Successfully onboarded machine to Microsoft Defender for Endpoint
|
```

Check within Microsoft Defender for Endpoint that the Virtual Machine has successfully onboarded at <https://security.microsoft.com/>

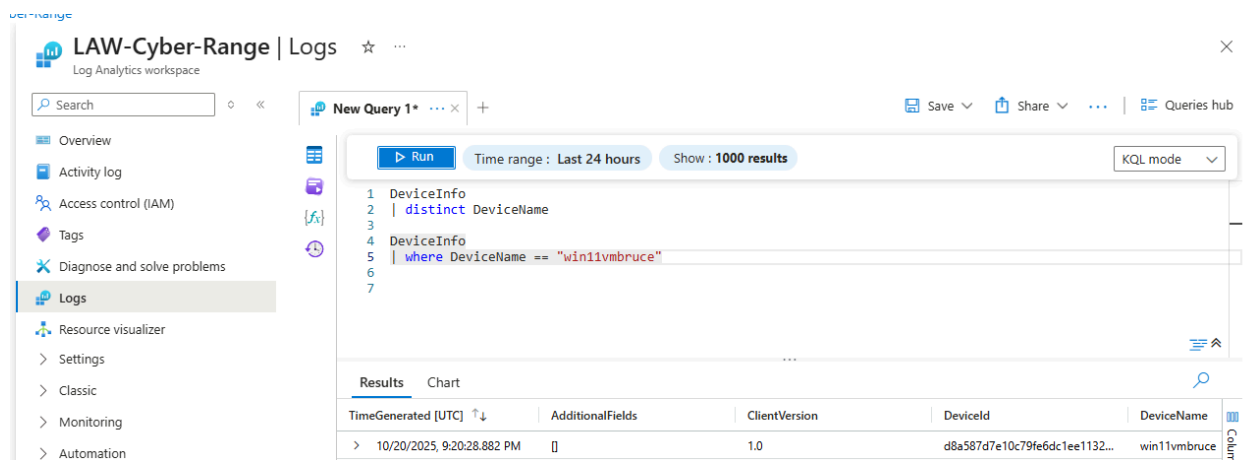


Virtual Machine created successfully and onboarded to Microsoft Defender for Endpoint.

I will ensure that I can access log data and find my Virtual Machine through Azure Sentinel.



Here is proof of discovery in these screenshots from Azure Sentinel.

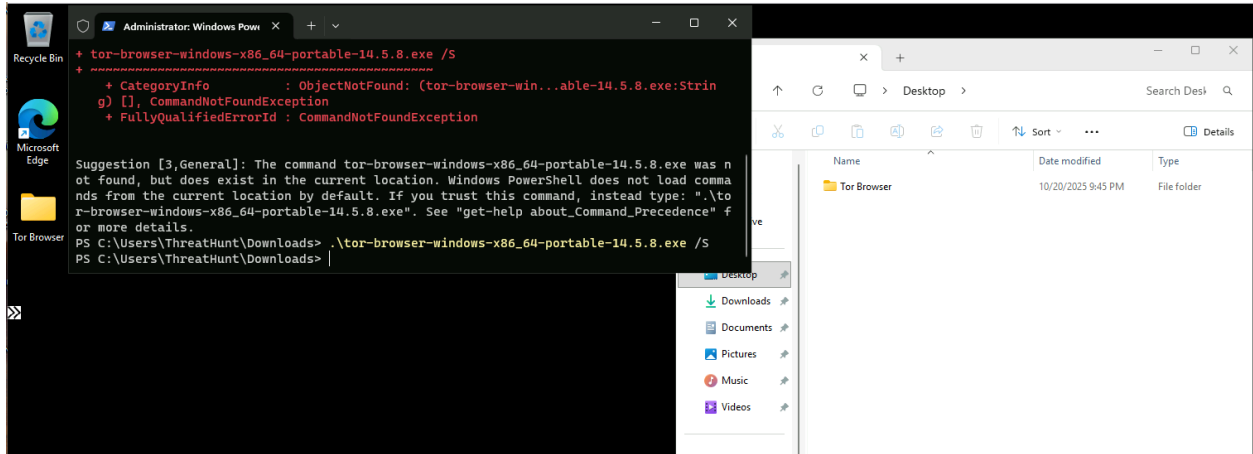


4. Perform the steps the "Bad Actor" took Create Logs and IoCs.

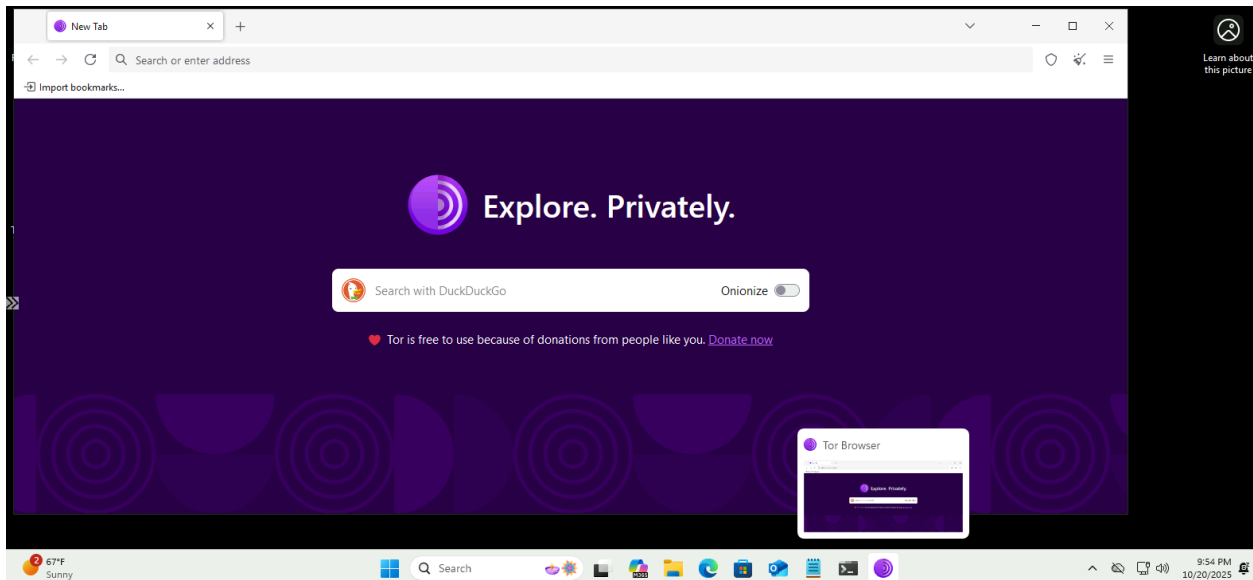
First I downloaded the Tor browser and installed it **silently** on the Virtual Machine.

The first attempt at silently downloading the Tor browser failed due to an error. I have added “.” and now it is successful.

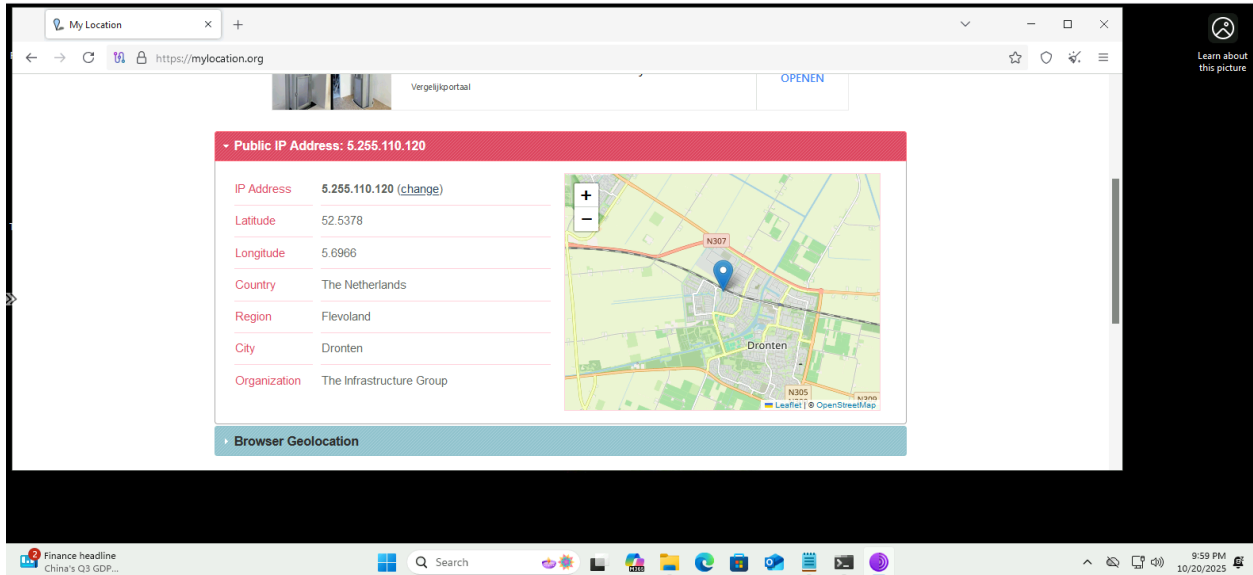
The Virtual Machine has successfully placed the Tor browser on the desktop silently.



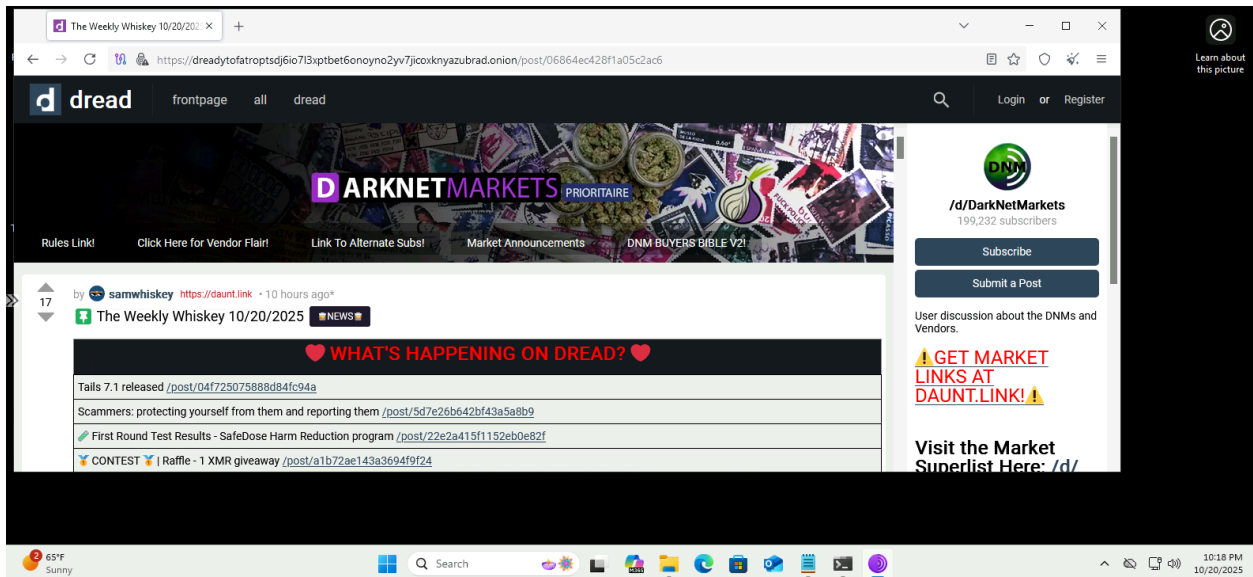
I will open up the Tor browser and begin “surfing” the internet/Web.

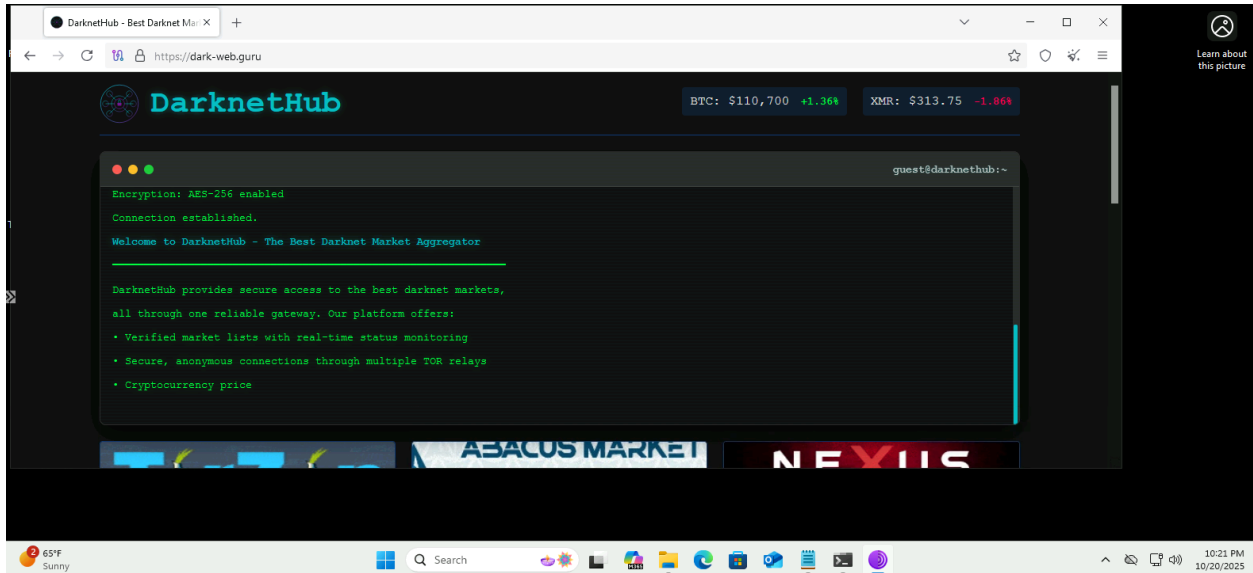


After entering Google into the field, I enter “geo locate me” and the return is this screenshot:



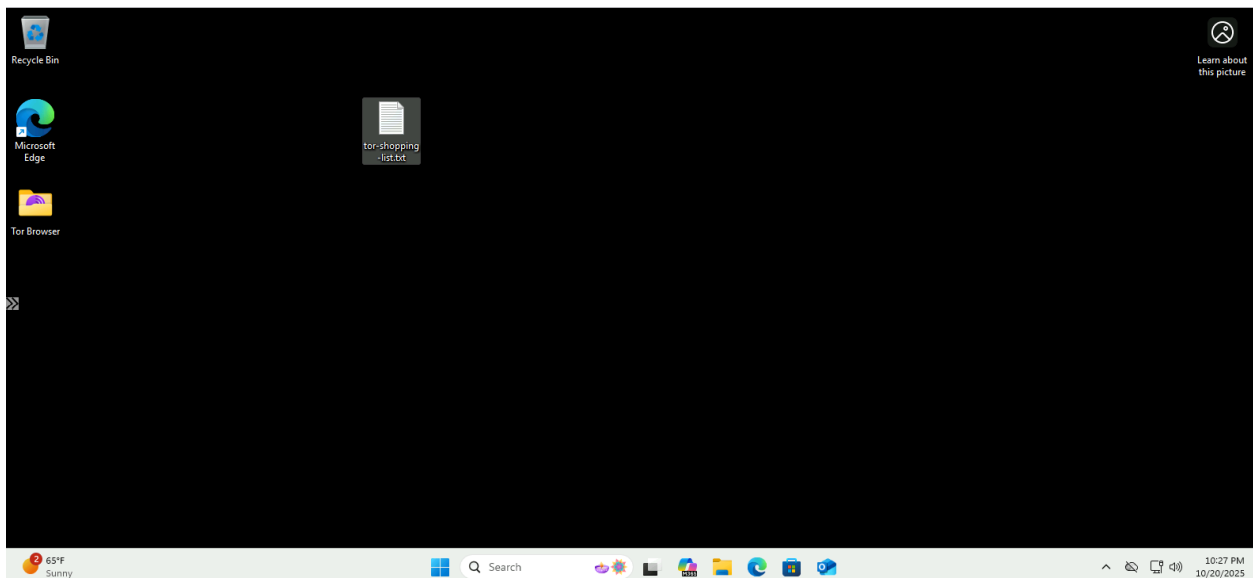
Took some time to open up a few sites on this browser as seen in these screenshots:

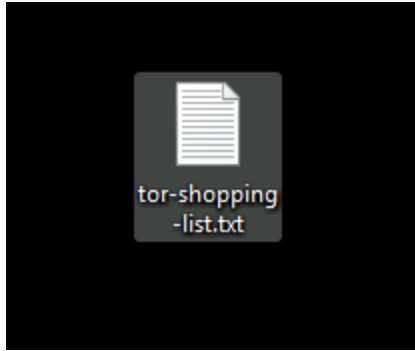




And I have successfully created a “shopping list” on the desktop of the Virtual Machine, called:

tor-shopping-list.txt





5. Ensure that the “Evidence” of malicious activity has been placed where it needs to be to be hunted.

I will use the following KQL commands to see evidence of the “malicious actor,” and to have “Flags” that are available to be hunted for.

```
// Installer name == tor-browser-windows-x86_64-portable-(version).exe
// Detect the installer being downloaded
DeviceFileEvents
| where FileName startswith "tor"
| where DeviceName == "win11vmbruce"
```

Home > Log Analytics workspaces > LAW-Cyber-Range

LAW-Cyber-Range | Logs

New Query 1*

Run Time range: Last 24 hours Show: 1000 results KQL mode

```
1 DeviceInfo
2 | distinct DeviceName
3
4 DeviceInfo
5 | where DeviceName == "win11vmbruce"
6
7 DeviceFileEvents
8 | where FileName startswith "tor"
9 | where DeviceName == "win11vmbruce"
10
```

Results Chart

TimeGenerated [UTC]	ActionType	AdditionalFields	DeviceId	DeviceName	FileName	FileSize
> 10/20/2025, 10:26:17.221 PM	FileCreated	("FileType":"Unknown")	a6f70497611d132bd5cbe81b2...	win11vmbruce	tor-shopping-list.txt.lnk	708
> 10/20/2025, 10:26:17.038 PM	FileCreated	("FileType":"Unknown")	a6f70497611d132bd5cbe81b2...	win11vmbruce	tor-shopping-list.txt.txt	116
> 10/20/2025, 9:46:05.867 PM	FileCreated	("FileType":"Unknown")	a6f70497611d132bd5cbe81b2...	win11vmbruce	Tor Browser.lnk	824
> 10/20/2025, 9:45:57.773 PM	FileCreated	("FileType":"PortableExecutable")	a6f70497611d132bd5cbe81b2...	win11vmbruce	tor.exe	10661888
> 10/20/2025, 9:45:57.264 PM	FileCreated	("FileType":"Unknown")	a6f70497611d132bd5cbe81b2...	win11vmbruce	tor.txt	19651
> 10/20/2025, 9:45:57.261 PM	FileCreated	("FileType":"Unknown")	a6f70497611d132bd5cbe81b2...	win11vmbruce	Torbutton.txt	2306

2s 216ms Display time (UTC+00:00) Query details 1 - 7 of 8

```
// TOR Browser being silently installed
DeviceProcessEvents
| where ProcessCommandLine contains "tor-browser-windows"
| where DeviceName == "win11vmbruce"
| project Timestamp, DeviceName, ActionType, FileName, ProcessCommandLine
```

Home > Log Analytics workspaces > LAW-Cyber-Range

LAW-Cyber-Range | Logs ☆ ...

Log Analytics workspace

New Query 1* ... +

Save Share ... Queries hub

Run Time range: Last 24 hours Show: 1000 results KQL mode

```
5 | where DeviceName == "win11vmbruce"
6
7 DeviceFileEvents
8 | where FileName startswith "tor"
9 | where DeviceName == "win11vmbruce"
10
11 DeviceProcessEvents
12 | where ProcessCommandLine contains "tor-browser-windows"
13 | where DeviceName == "win11vmbruce"
14 | project Timestamp, DeviceName, ActionType, FileName, ProcessCommandLine
```

Results Chart

Timestamp [UTC] ↑↓	DeviceName	ActionType	FileName	ProcessCommandLine
> 10/20/2025, 9:45:40.100 PM	win11vmbruce	ProcessCreated	tor-browser-windows-x86_64-p...	"tor-browser-windows-x86_64-portable-14.5.8.exe" /S

1s 248ms Display time (UTC+00:00) Query details 1 - 1 of 1

```
// TOR Browser or service was successfully installed and is present on the disk
DeviceFileEvents
| where FileName has_any ("tor.exe", "firefox.exe")
| where DeviceName == "win11vmbruce"
| project Timestamp, DeviceName, RequestAccountName, ActionType,
InitiatingProcessCommandLine
```


Home > Log Analytics workspaces > LAW-Cyber-Range

LAW-Cyber-Range | Logs

New Query 1*

Run Time range: Last 24 hours Show: 1000 results KQL mode

```
10 DeviceProcessEvents
11 | where ProcessCommandLine contains "tor-browser-windows"
12 | where DeviceName == "win11vmbruce"
13 | project Timestamp, DeviceName, ActionType, FileName, ProcessCommandLine
14
15 DeviceFileEvents
16 | where FileName has_any ("tor.exe", "firefox.exe")
17 | where DeviceName == "win11vmbruce"
18 | project Timestamp, DeviceName, RequestAccountName, ActionType, InitiatingProcessCommandLine
19
```

Results Chart

Timestamp [UTC]	DeviceName	RequestAccountName	ActionType	InitiatingProcessCommandLine
> 10/20/2025, 9:45:57.773 PM	win11vmbruce	ThreatHunt	FileCreated	"tor-browser-windows-x86_64-portable-14.5.8.exe" /S
> 10/20/2025, 9:45:40.930 PM	win11vmbruce	ThreatHunt	FileCreated	"tor-browser-windows-x86_64-portable-14.5.8.exe" /S

0s 590ms Display time (UTC+00:00) Query details 1 - 2 of 2

```
// TOR Browser or service was launched
DeviceProcessEvents
| where ProcessCommandLine has_any("tor.exe","firefox.exe")
| where DeviceName == "win11vmbruce"
| project Timestamp, DeviceName, AccountName, ActionType, ProcessCommandLine
```

Home > Log Analytics workspaces > LAW-Cyber-Range

LAW-Cyber-Range | Logs

New Query 1*

Run Time range: Last 24 hours Show: 1000 results KQL mode

```
16 DeviceFileEvents
17 | where FileName has_any ("tor.exe", "firefox.exe")
18 | where DeviceName == "win11vmbruce"
19 | project Timestamp, DeviceName, RequestAccountName, ActionType, InitiatingProcessCommandLine
20
21 DeviceProcessEvents
22 | where ProcessCommandLine has_any ("tor.exe", "firefox.exe")
23 | where DeviceName == "win11vmbruce"
24 | project Timestamp, DeviceName, AccountName, ActionType, ProcessCommandLine
25
```

Results Chart

Timestamp [UTC]	DeviceName	AccountName	ActionType	ProcessCommandLine
> 10/20/2025, 10:06:56.242 PM	win11vmbruce	threathunt	ProcessCreated	"tor.exe" -f "C:\Users\ThreatHunt\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor\torrc" DataDirectory "..."
> 10/20/2025, 10:06:54.176 PM	win11vmbruce	threathunt	ProcessCreated	"firefox.exe"
> 10/20/2025, 10:06:54.137 PM	win11vmbruce	threathunt	ProcessCreated	"firefox.exe"
> 10/20/2025, 9:57:51.860 PM	win11vmbruce	threathunt	ProcessCreated	"firefox.exe" -contentproc --channel=6004 -childID 16 -isForBrowser -prefHandle 5864 -prefMapHandle 45...
> 10/20/2025, 9:57:51.835 PM	win11vmbruce	threathunt	ProcessCreated	"firefox.exe" -contentproc --channel=4524 -childID 15 -isForBrowser -prefHandle 1808 -prefMapHandle 59...
> 10/20/2025, 9:57:49.701 PM	win11vmbruce	threathunt	ProcessCreated	"firefox.exe" -contentproc --channel=5576 -childID 14 -isForBrowser -prefHandle 5568 -prefMapHandle 55...

3s 873ms Display time (UTC+00:00) Query details 1 - 7 of 28

19	project	Timestamp, DeviceName, InitiatingProcessAccountName, InitiatingProcessFileName
20		
21	DeviceProcessEvents	
22	where ProcessCommandLine has_any ("tor.exe", "firefox.exe")	
23	where DeviceName == "win11vmbruce"	
24	project	Timestamp, DeviceName, AccountName, ActionType, ProcessCommandLine
25		

Timestamp [UTC]	DeviceName	AccountName	ActionType	ProcessCommandLine
> 10/20/2025, 10:06:54.176 PM	win11vmbruce	threathunt	ProcessCreated	"tor.exe" -f "C:\Users\ThreatHunt\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor\torrc" DataDirectory "C:\Users\ThreatHunt\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor" ClientOnionAuthDir "C:\Users\ThreatHunt\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor\geop6" --defaults-torrc "C:\Users\ThreatHunt\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor\geop6" --socks-port 127.0.0.1:9150 ExtendedErrors IPv6Traffic PreferIPv6 KeepAliveIsolateSOCKSAuth" eNetwork 1
> 10/20/2025, 10:06:54.137 PM	win11vmbruce	threathunt	ProcessCreated	"firefox.exe"

3s 873ms | Display time (UTC+00:00) | Query details | 1 - 3 of 28

// TOR Browser or service is being used and is actively creating network connections

DeviceNetworkEvents

| where InitiatingProcessFileName in~ ("tor.exe", "firefox.exe")

| where DeviceName == "win11vmbruce"

| where RemotePort in (9001, 9030, 9040, 9050, 9051, 9150)

| project Timestamp, DeviceName, InitiatingProcessAccountName, InitiatingProcessFileName,

RemoteIP, RemotePort, RemoteUrl

| order by Timestamp desc

Home > Log Analytics workspaces > LAW-Cyber-Range

LAW-Cyber-Range | Logs

Log Analytics workspace

New Query 1*

Time range: Last 24 hours

Show: 1000 results

KQL mode

```
22 | where ProcessCommandLine has_any("tor.exe","firefox.exe")
23 | where DeviceName == "win11vmbruce"
24 | project Timestamp, DeviceName, AccountName, ActionType, ProcessCommandLine
25
26 DeviceNetworkEvents
27 | where InitiatingProcessFileName in~ ("tor.exe", "firefox.exe")
28 | where DeviceName == "win11vmbruce"
29 | where RemotePort in (9001, 9030, 9040, 9050, 9051, 9150)
30 | project Timestamp, DeviceName, InitiatingProcessAccountName, InitiatingProcessFileName, RemoteIP, RemotePort, RemoteUrl
31 | order by Timestamp desc
32
```

Results

Chart

Timestamp [UTC]	DeviceName	InitiatingProcessAccountNa...	InitiatingProcessFileName	RemoteIP	RemotePort	RemoteUrl
> 10/20/2025, 9:52:39.905 PM	win11vmbruce	threathunt	firefox.exe	127.0.0.1	9150	
> 10/20/2025, 9:52:34.442 PM	win11vmbruce	threathunt	tor.exe	37.120.168.158	9001	https://www.kfdy6j7wlupt56h...
> 10/20/2025, 9:52:33.953 PM	win11vmbruce	threathunt	tor.exe	37.120.168.158	9001	
> 10/20/2025, 9:52:33.938 PM	win11vmbruce	threathunt	tor.exe	66.111.2.16	9001	https://www.zsh67ng4fgodd.com
> 10/20/2025, 9:52:32.452 PM	win11vmbruce	threathunt	tor.exe	66.111.2.16	9001	

0s 975ms

Display time (UTC+00:00)

Query details

1 - 5 of 5

Home > Log Analytics workspaces > LAW-Cyber-Range

LAW-Cyber-Range | Logs

Log Analytics workspace

New Query 1*

Time range: Last 24 hours Show: 1000 results KQL mode

```
22 | where ProcessCommandLine has_any("tor.exe", "firefox.exe")
23 | where DeviceName == "win11vmbruce"
24 | project Timestamp, DeviceName, AccountName, ActionType, ProcessCommandLine
25
26 DeviceNetworkEvents
27 | where InitiatingProcessFileName in~ ("tor.exe", "firefox.exe")
28 | where DeviceName == "win11vmbruce"
29 | where RemotePort in (9001, 9030, 9040, 9050, 9051, 9150)
30 | project Timestamp, DeviceName, InitiatingProcessAccountName, InitiatingProcessFileName, RemoteIP, RemotePort, RemoteUrl
31 | order by Timestamp desc
32
```

Results Chart

Timestamp [UTC]	DeviceName	InitiatingProcessAccountNa...	InitiatingProcessFileName	RemoteIP	RemotePort	RemoteUrl
> 10/20/2025, 9:52:39.905 PM	win11vmbruce	threatunt	firefox.exe	127.0.0.1	9150	
10/20/2025, 9:52:34.442 PM	win11vmbruce	threatunt	tor.exe	37.120.168.158	9001	https://www.kfddy6y7wlpufrt5...

0s 975ms Display time (UTC+00:00) Query details 1 - 2 of 5

// User shopping list was created and, changed, or deleted
DeviceFileEvents
| where FileName contains "shopping-list.txt"
| where DeviceName == "win11vmbruce"

Home > Log Analytics workspaces > LAW-Cyber-Range

LAW-Cyber-Range | Logs

Log Analytics workspace

New Query 1*

Time range: Last 24 hours Show: 1000 results KQL mode

```
26 DeviceNetworkEvents
27 | where InitiatingProcessFileName in~ ("tor.exe", "firefox.exe")
28 | where DeviceName == "win11vmbruce"
29 | where RemotePort in (9001, 9030, 9040, 9050, 9051, 9150)
30 | project Timestamp, DeviceName, InitiatingProcessAccountName, InitiatingProcessFileName, RemoteIP, RemotePort, RemoteUrl
31 | order by Timestamp desc
32
33 DeviceFileEvents
34 | where FileName contains "shopping-list.txt"
35 | where DeviceName == "win11vmbruce"
36
```

Results Chart

TimeGenerated [UTC]	ActionType	AdditionalFields	DeviceId	DeviceName	FileName	FileSize
> 10/20/2025, 10:26:17.221 PM	FileCreated	["FileType": "Unknown"]	a6704f97611d132bd5cbe81b2...	win11vmbruce	tor-shopping-list.txt.lnk	708
> 10/20/2025, 10:26:17.038 PM	FileCreated	["FileType": "Unknown"]	a6704f97611d132bd5cbe81b2...	win11vmbruce	tor-shopping-list.txt.txt	116

0s 669ms Display time (UTC+00:00) Query details 1 - 2 of 2

Home > Log Analytics workspaces > LAW-Cyber-Range

LAW-Cyber-Range | Logs ☆ ...

Log Analytics workspace

New Query 1* ... × +

Save Share ... Queries hub

Run Time range: Last 24 hours Show: 1000 results KQL mode

Query editor

Results Chart

TimeGenerated [UTC]	ActionType	AdditionalFields	DeviceId	DeviceName	FileName	FileSize
10/20/2025, 10:26:17.221 PM	FileCreated	{"FileType": "Unknown"}	a6f70497611d132bd5cbe81b2...	win11vmbruce	tor-shopping-list.txt.Ink	708
		TenantId	60c7f53e-249a-4077-b68e-55a4ae877d7c			
		ActionType	FileCreated			
		> AdditionalFields	{"FileType": "Unknown"}			
		DeviceId	a6f70497611d132bd5cbe81b218056b16aaecab			
		DeviceName	win11vmbruce			
		FileName	tor-shopping-list.txt.Ink			
		FileSize	708			
		FolderPath	C:\Users\ThreatHunt\AppData\Roaming\Microsoft\Windows\Recent\tor-shopping-list.txt.Ink			
		InitiatingProcessAccountDomain	win11vmbruce			
		InitiatingProcessAccountName	threathunt			

0s 669ms | Display time (UTC+00:00) Query details | 1 of 2

Created By:

- Author Name: Bruce Thornton
- Author Contact: www.linkedin.com/in/bruce-thornton-3b0b80350
- Date: October 20, 2025