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

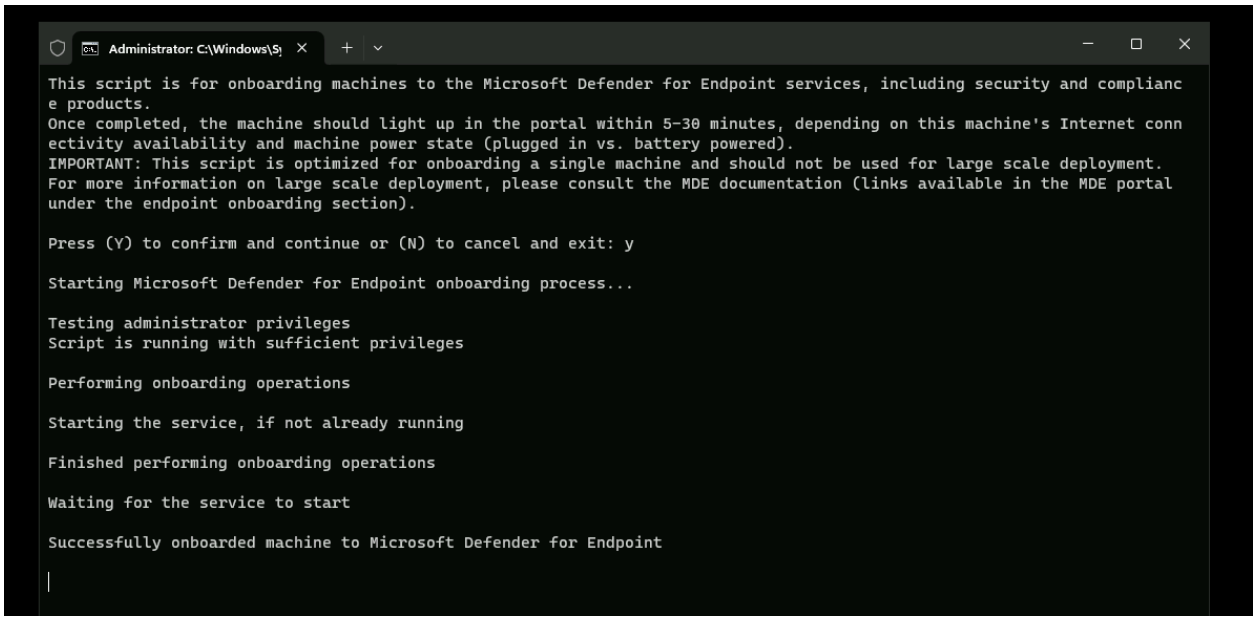
Computer name	Win11VMBruce
Operating system	Windows (Windows 11 Pro)
VM generation	V2
VM architecture	x64
Agent status	Ready
Agent version	2.7.41491.1172

Networking

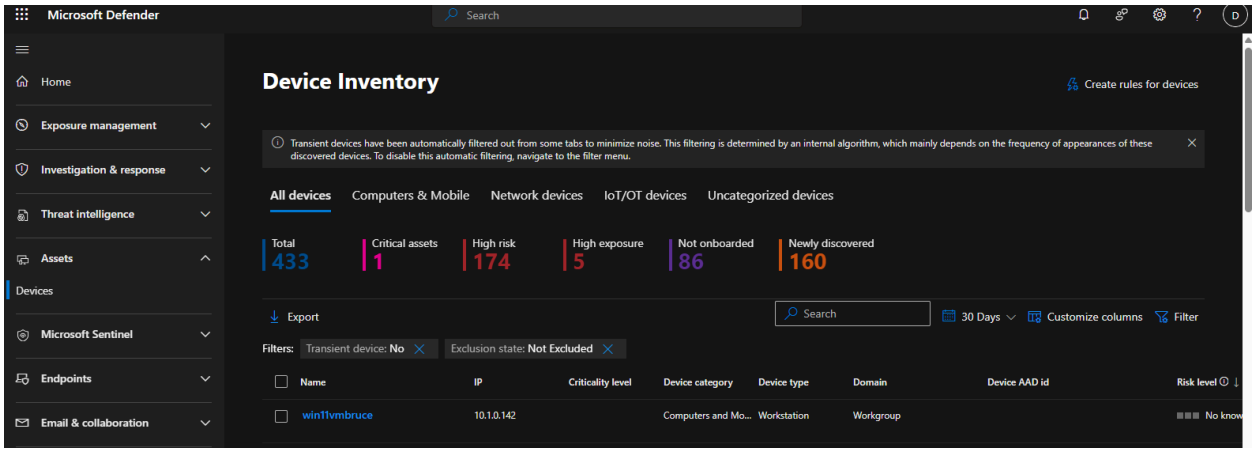
Public IP address	-
Public IP address (IPv6)	-
Private IP address	10.1.0.142
Private IP address (IPv6)	-
Virtual network/subnet	Cyber-Range-2-VNet/Cyber-Range-2-Subnet
DNS name	-

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.

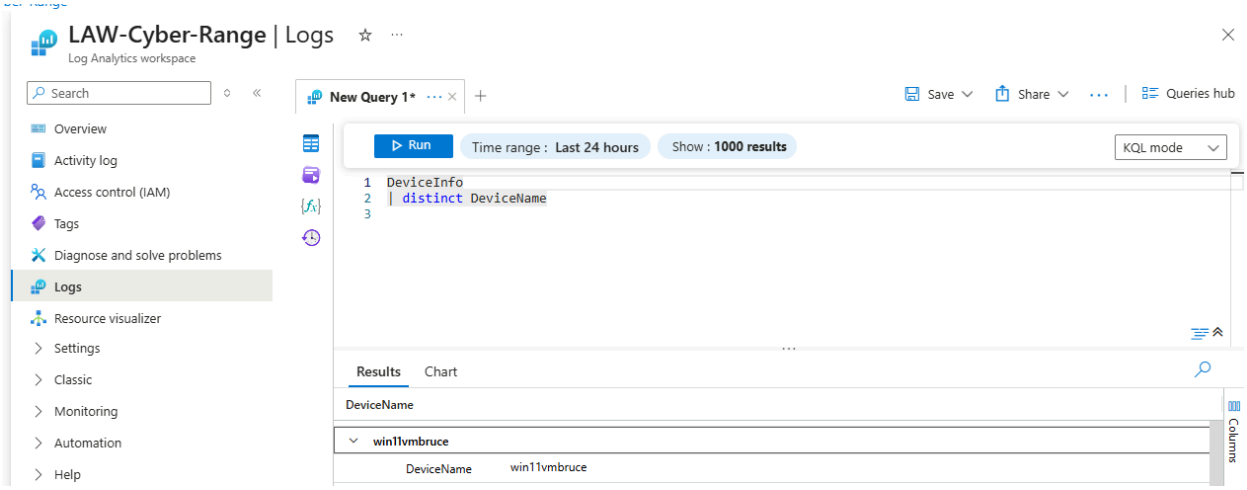


Check within Microsoft Defender for Endpoint that the Virtual Machine has successfully onboarded at https://security.microsoft.com/

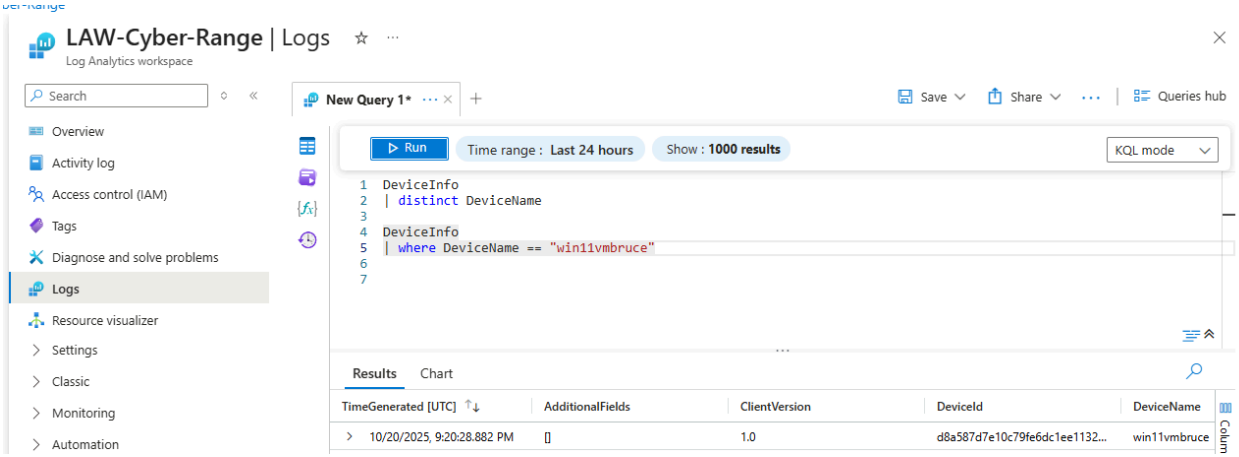


Virtual Machine created successfully and onboarded to Microsoft Defender for Endpoint.

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.

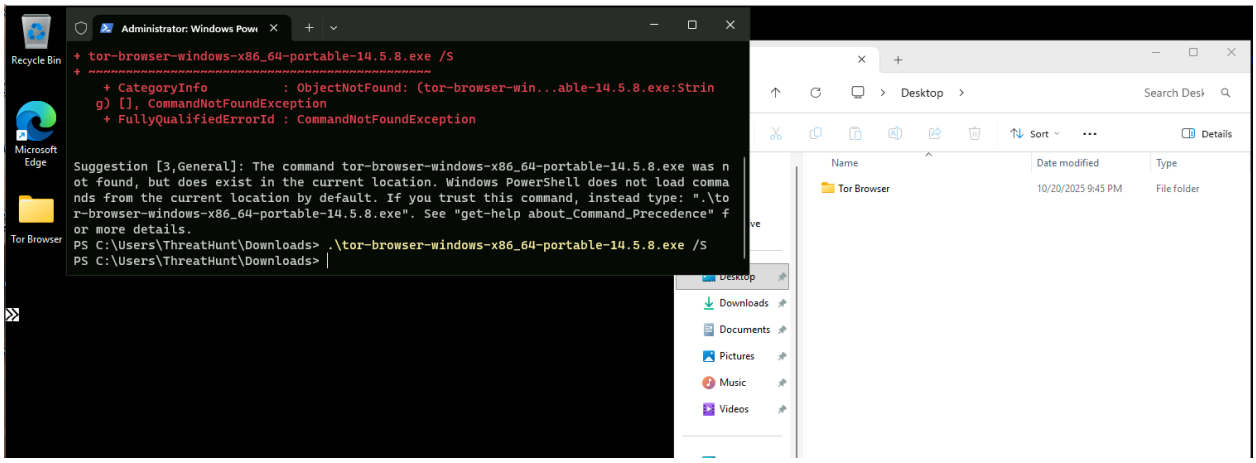


4. **<u>Perform the steps the "Bad Actor" took Create Logs and IoCs</u>.**

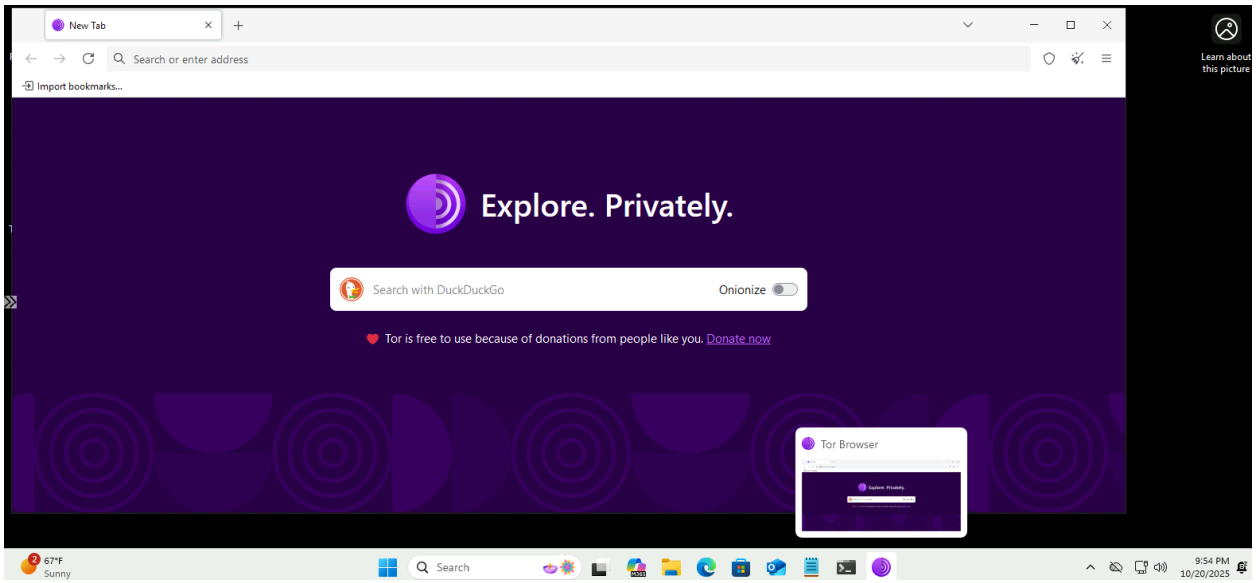
First I downloaded the Tor browser and installed it **silently** on the Virtual Machine.

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

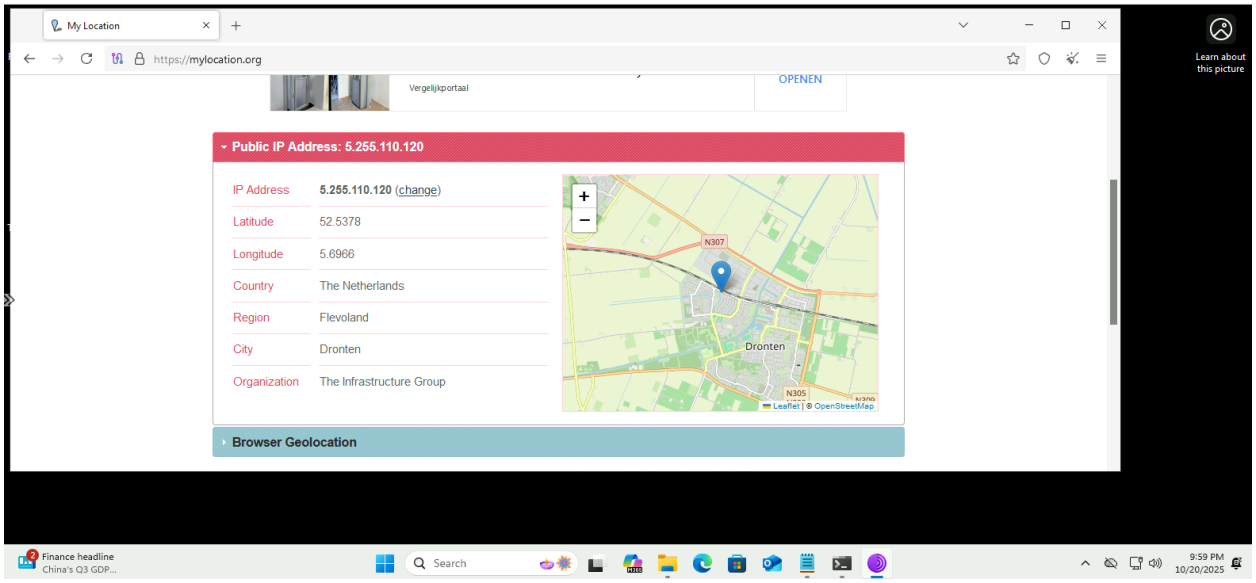
The Virtual Machine has successfully placed the Tor browser on the desktop silently.



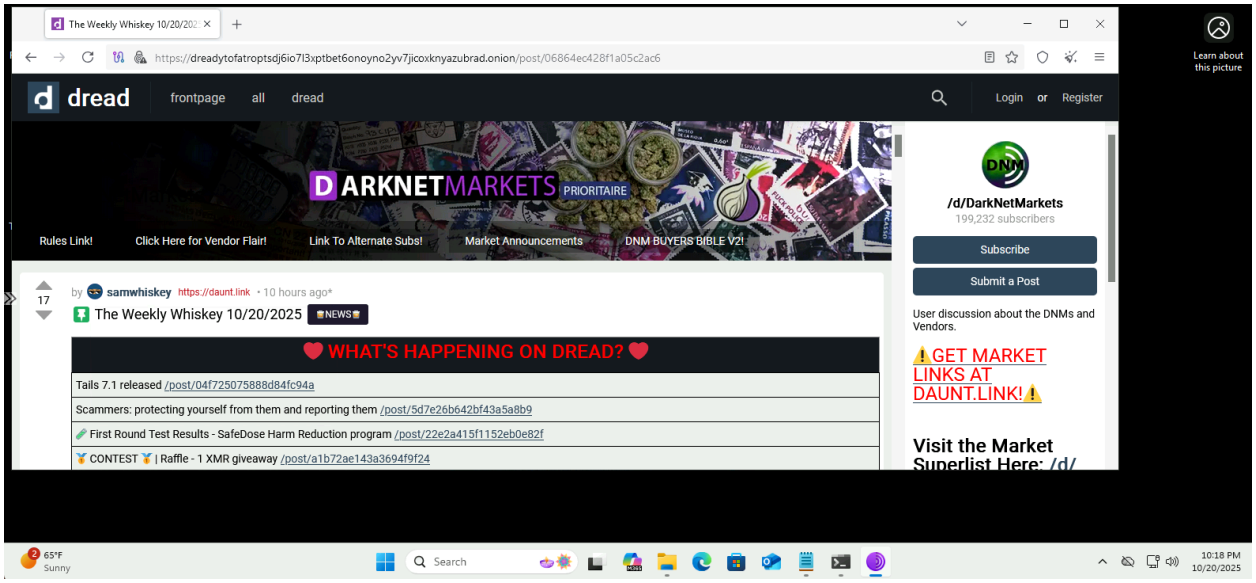
I will open up the Tor browser and begin “surfing” the internet/Web.

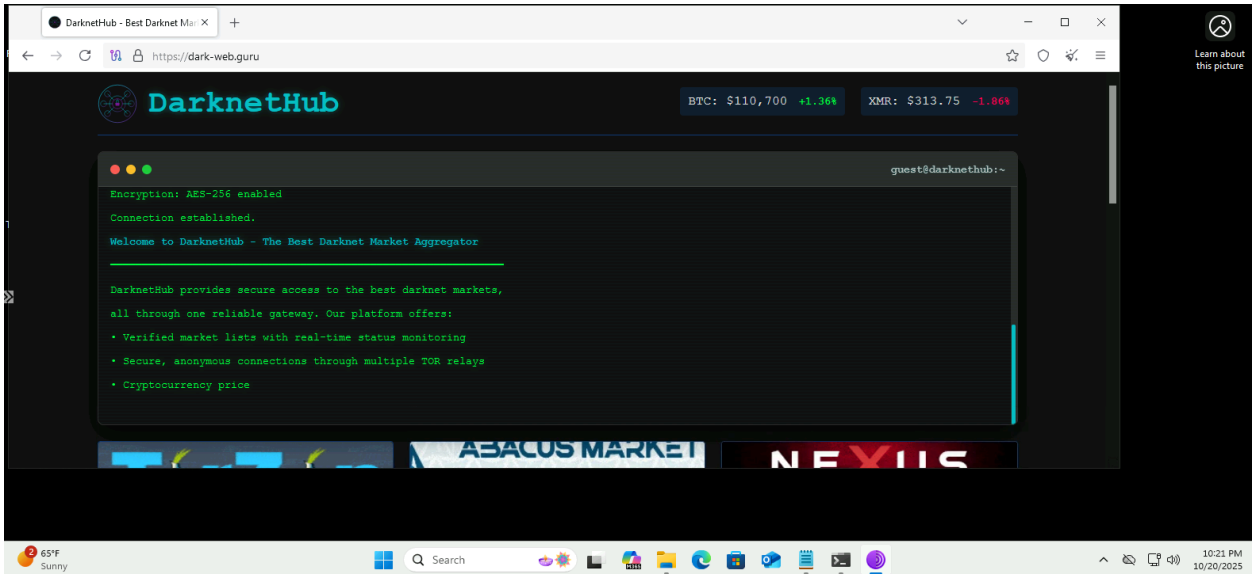


After entering Google into the field, I enter “geo locate me” and the return is this screenshot:



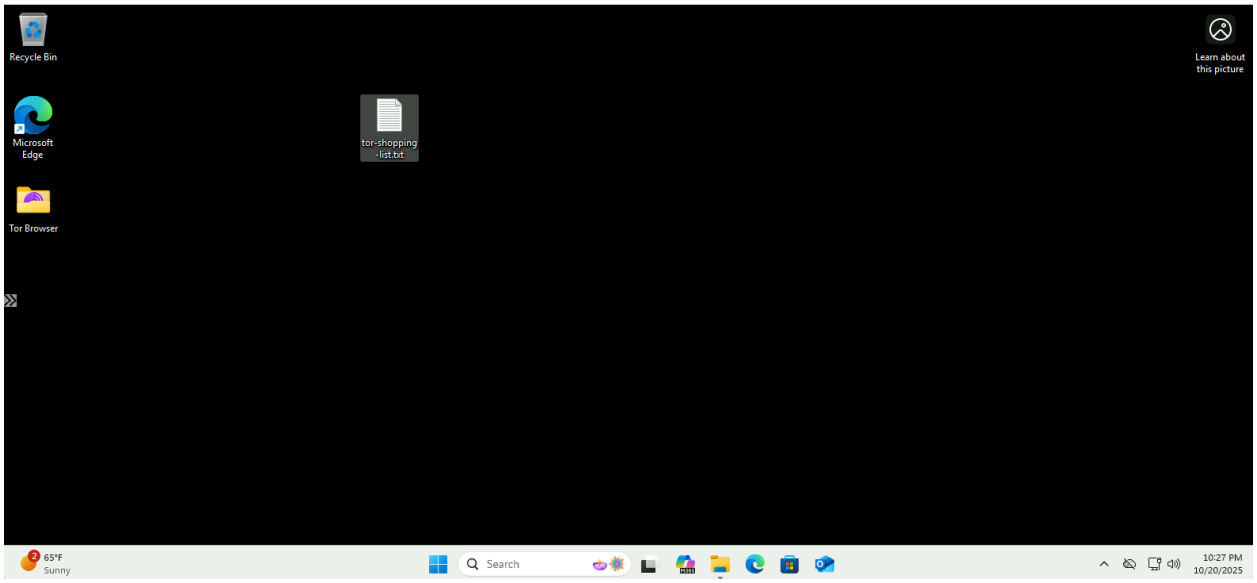
Took some time to open up a few sites on this browser as seen in these screenshots:

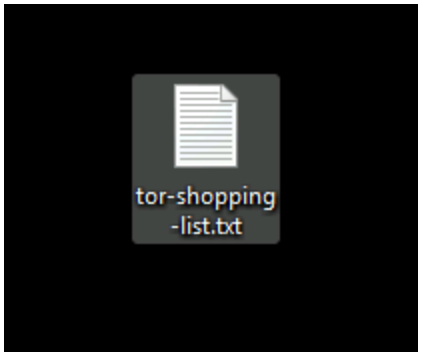




And I have successfully created a “shopping list” on the desktop of the Virtual Machine, called:

tor-shopping-list.txt

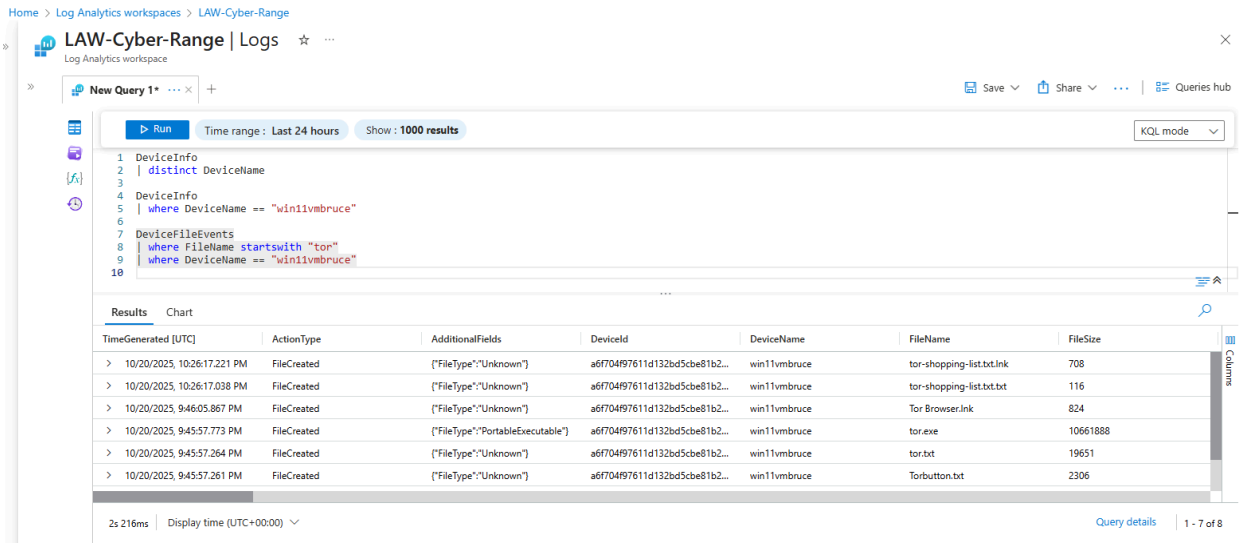




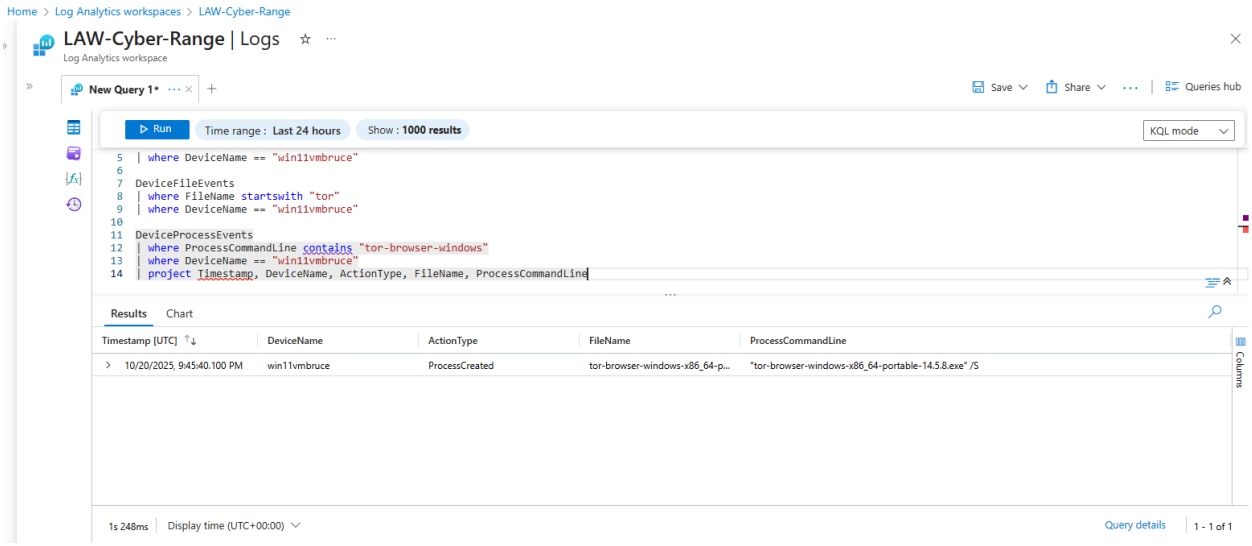
5. **<u>Ensure that the “Evidence” of malicious activity has been placed where it needs to be to be hunted.</u>**

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.

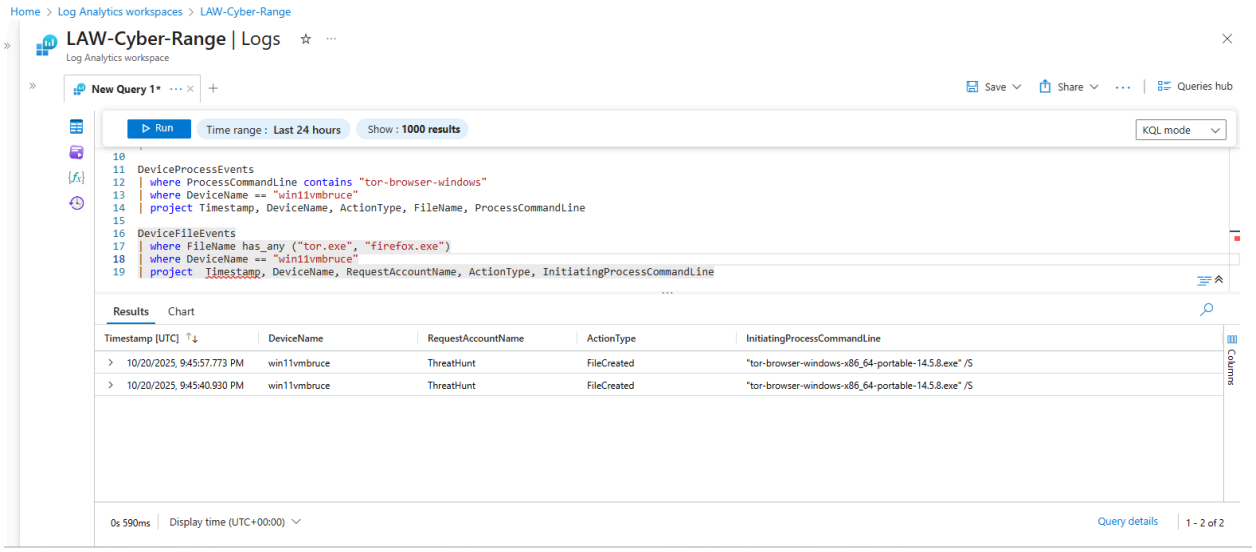
```
// Installer name == tor-browser-windows-x86_64-portable-(version).exe
// Detect the installer being downloaded
DeviceFileEvents
| where FileName startswith "tor"
| where DeviceName == "win11vmbruce"
```



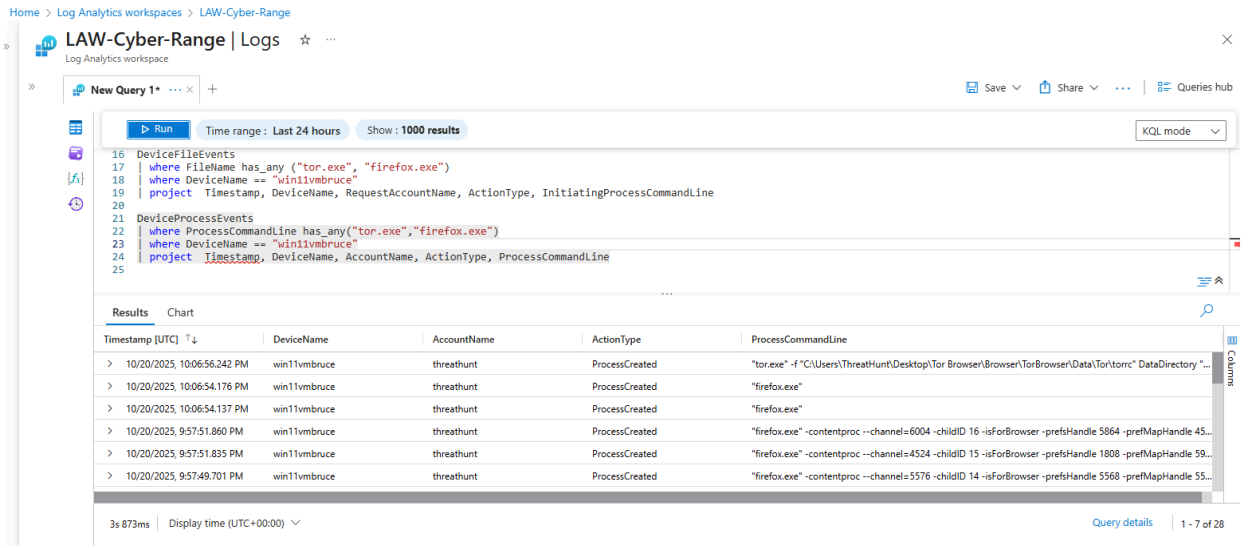
// TOR Browser being silently installed
DeviceProcessEvents
| where ProcessCommandLine contains "tor-browser-windows"
| where DeviceName == "win11vmbruce"
| project Timestamp, DeviceName, ActionType, FileName, ProcessCommandLine

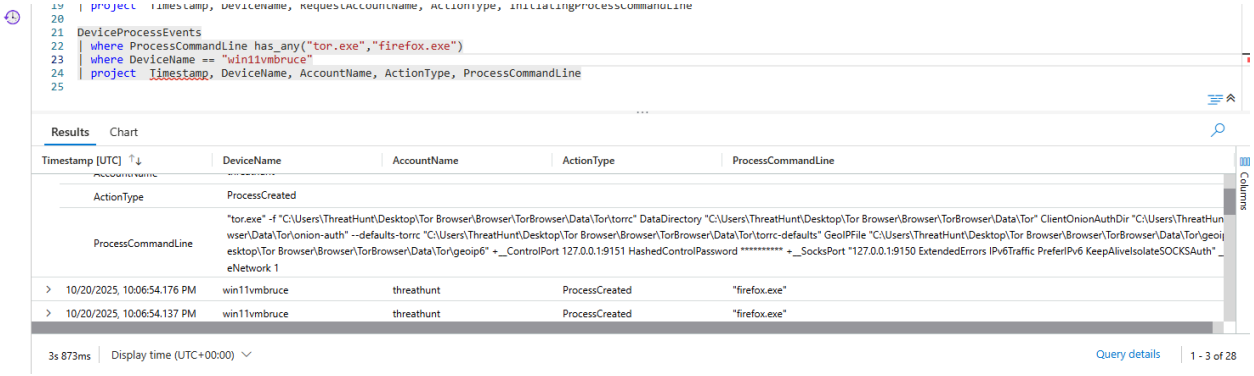


// TOR Browser or service was successfully installed and is present on the disk
DeviceFileEvents
| where FileName has_any ("tor.exe", "firefox.exe")
| where DeviceName == "win11vmbruce"
| project Timestamp, DeviceName, RequestAccountName, ActionType, InitiatingProcessCommandLine

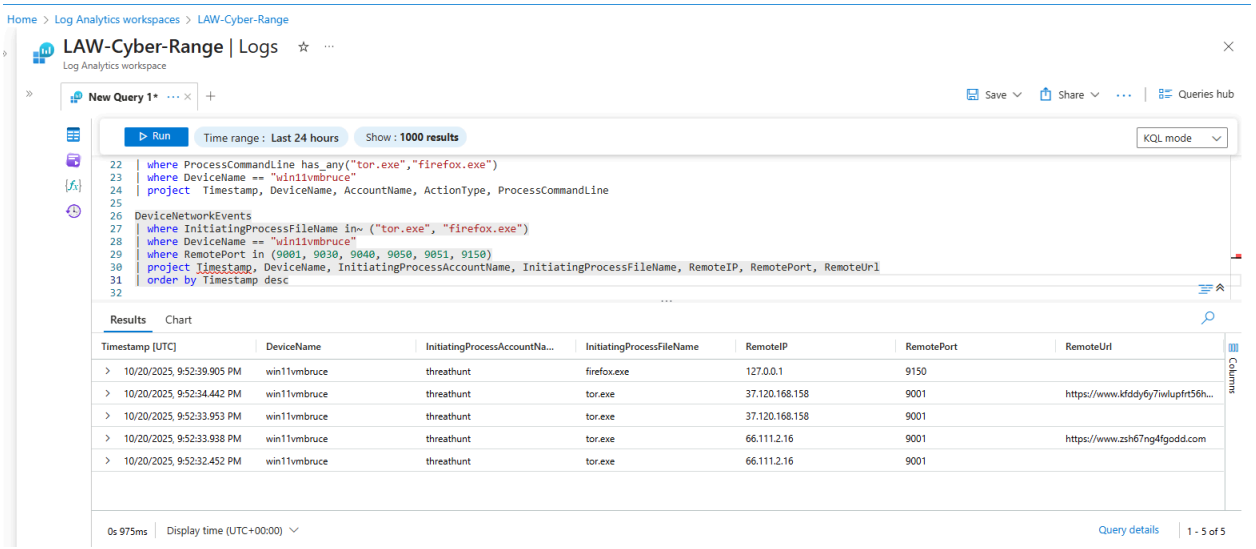


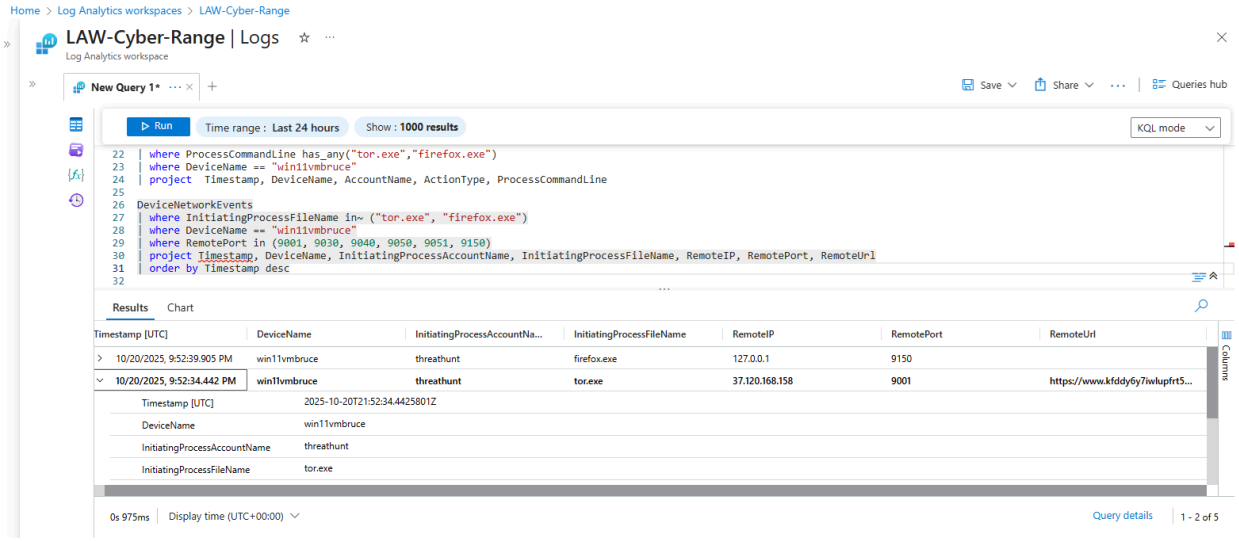
// TOR Browser or service was launched
DeviceProcessEvents
| where ProcessCommandLine has_any("tor.exe","firefox.exe")
| where DeviceName == "win11vmbruce"
| project Timestamp, DeviceName, AccountName, ActionType, ProcessCommandLine



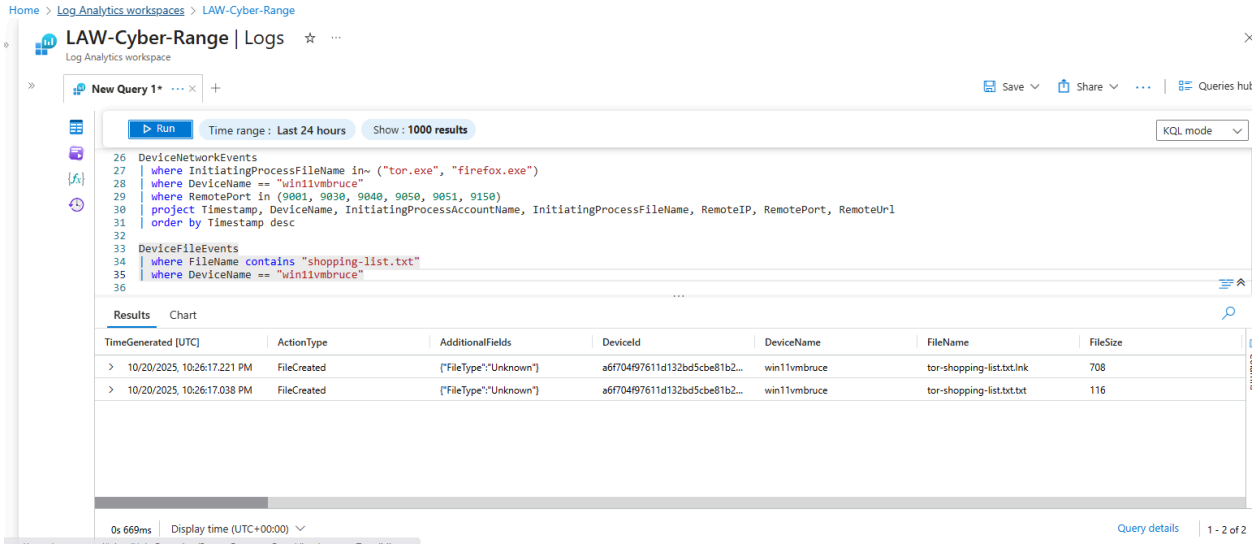


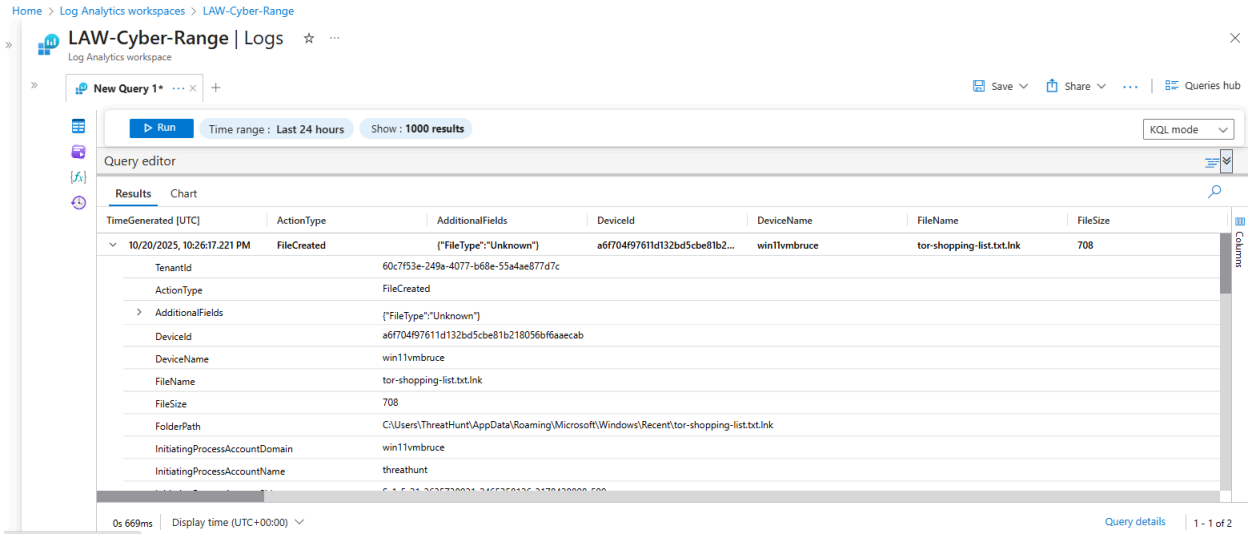
// TOR Browser or service is being used and is actively creating network connections
DeviceNetworkEvents
| where InitiatingProcessFileName in~ ("tor.exe", "firefox.exe")
| where DeviceName == "win11vmbruce"
| where RemotePort in (9001, 9030, 9040, 9050, 9051, 9150)
| project Timestamp, DeviceName, InitiatingProcessAccountName, InitiatingProcessFileName, RemoteIP, RemotePort, RemoteUrl
| order by Timestamp desc





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





Created By:

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