Threat Hunting Summary Report

Tor Browser Installation and Usage Investigation

Analyst: Dan Chui
Date of Investigation: March 10, 2026
Platform: Microsoft Defender XDR Advanced Hunting
Endpoint: vm-hunt-tyo
User Account: dan
Incident Type: Unauthorized Privacy Tool Installation / Potential Policy Violation

Executive Summary

During a proactive threat hunting exercise, activity related to the Tor Browser was identified on endpoint **vm-hunt-tyo**. Investigation of Microsoft Defender telemetry (DeviceFileEvents, DeviceProcessEvents, and DeviceNetworkEvents) confirmed that the user downloaded and executed the Tor Browser portable installer. Following execution, Tor application files were extracted to the system and the processes **tor.exe** and **firefox.exe** were launched. Shortly after execution, the endpoint established outbound communication with the IP address **15.204.223.128** over **port 9001**, which is commonly associated with Tor relay communication. Additional encrypted traffic over port 443 suggested active browsing activity through the Tor network. Later in the timeline, a file named **tor-shopping-list.txt** was created on the Desktop, potentially related to the user's Tor browsing activity. The investigation confirms that Tor Browser was successfully installed and used on the endpoint.

Investigation Overview

Field	Value
Investigation Type	Threat Hunt
Detection Method	KQL Log Analysis
Primary Artifact	Tor Browser Installer
Endpoint	vm-hunt-tyo
User	dan

Key Timeline of Events

Time (UTC)	Event
00:18:19	Tor installer downloaded
00:21:44	Tor installer executed
00:22:04–00:22:12	Tor files extracted to Desktop
00:22:22	Tor Browser launched
00:22:34	Connection established to Tor relay node (15.204.223.128:9001)
00:22:37–00:27:54	Continued Tor browsing activity
00:35:58	tor-shopping-list.txt created

Indicators of Compromise (IOCs)

Type	Indicator
File	tor-browser-windows-x86_64-portable-15.0.7.exe
File	tor-shopping-list.txt
Process	tor.exe
Process	firefox.exe
IP Address	15.204.223.128
Port	9001

MITRE ATT&CK; Mapping

Technique	ID	Description
User Execution	T1204	User executed downloaded Tor installer
Ingress Tool Transfer	T1105	Tor installer downloaded from internet
Application Layer Protocol	T1071	Tor network communications
Encrypted Channel	T1573	Encrypted communication via Tor

Recommendations

Endpoint Response
• Investigate contents of tor-shopping-list.txt
• Remove Tor Browser from the endpoint
• Review endpoint security policies regarding anonymizing tools

Monitoring Improvements
• Implement detection rules for Tor installer downloads
• Monitor execution of tor.exe
• Monitor connections to known Tor ports

Network Security
Consider blocking outbound traffic to common Tor ports such as 9001, 9030, 9050, 9051, and 9150.

Conclusion

This investigation confirmed that Tor Browser was downloaded, installed, and used on endpoint **vm-hunt-tyo**. Network telemetry confirmed communication with Tor relay infrastructure, enabling anonymous browsing through the Tor network. Although no additional malicious payloads were detected during the investigation, the presence of anonymizing tools in enterprise environments may represent a policy violation and potential security risk.