To: Management, SOC Lead
From: Fasi Sika - SOC Analyst
Date: 19 November, 2025
Priority: **Medium**

Executive Summary

On **12 November, 2025**, logs indicate that user '**John.Doe**' on workstation '**fasi-threat-hun**', downloaded a **TOR** browser installer and silently installed it to their desktop. Shortly afterward, '**tor.exe**' established outbound connections to multiple external IPs on common TOR related ports, confirming active TOR usage over the corporate network. During this period, the user also created and modified the file '**tor goodies hehe.txt**', which appears related to their browsing activity. Once their browsing activity stopped, TOR-related files, including the main binary and installer, were deleted from the Desktop folder, Downloads folder, and Recycle bin. This sequence of actions constitutes unauthorized use of anonymizing software on a corporate asset, violating company policy and creating elevated risk of unmonitored browsing and potential data exfiltration over the TOR network.

Findings

File Downloaded
The user `john.doe` was able to download the Tor browser installer directly from the Tor download site onto their Downloads folder.

- Timestamp: 2025-11-12T03:56:29.652104Z
- Action: FileRenamed
- File Name: tor-browser-windows-x86_64-portable-15.0.1.exe
- File Path: C:\Users\john.doe\Downloads\tor-browser-windows-x86_64-portable-15.0.1.exe
- File Hash (SHA256): 66793f7208919a15087bac96d8e31151ff53f9620d9fd7bfd340794fa6d5f86c

File Installed
Using command prompt, the user was able to successfully install the using the silent flag (/S)

- Timestamp: 2025-11-12T03:56:48.605522Z
- Action: ProcessCreated
- Command: tor-browser-windows-x86_64-portable-15.0.1.exe /S
- File Path: C:\Users\john.doe\Downloads\tor-browser-windows-x86_64-portable-15.0.1.exe
- File Hash (SHA26): 66793f7208919a15087bac96d8e31151ff53f9620d9fd7bfd340794fa6d5f86c

Browser Executed

Following the installation, Tor (`tor.exe`) was launched from the Tor browser directory on the Desktop.

- Timestamp: 2025-11-12T03:57:44.9374005Z
- Action: ProcessCreated
- File Path: C:\Users\john.doe\Desktop\Tor Browser\Browser\TorBrowser\Tor\tor.exe
- File Hash (SHA256): f78d87ff967bbdebbc43c58c2b5376522d2bbc975c98727c75bf28e2eb23ffd0

Network Activity

Multiple outbound connections to external IP addresses over port 9001 were captured. The associated hostnames were randomized to anonymize traffic activity.

Initial Network Connections

- Timestamp: 2025-11-12T04:00:15.5356762Z
- Action: ConnectionSuccess
- Remote IP: 75[.]184[.]13[.]239
- Remote Port: 9001
- Remote URL: hxxps[:]//www[.]xbvi5e5kbgs5yeaetixqhd[.]com

Additional Network Connections

- Timestamp: 2025-11-12T04:01:33.4118235Z
- Remote IP: 65[.]21[.]132[.]179
- Remote Port: 9001
- Remote URL: hxxps[://]www[.]znkfu2v6h4q[.]com

- Timestamp: 2025-11-12T04:02:42.0786733Z
- Remote IP: 84[.]1[.]55[.]201
- Remote Port: 9001
- Remote URL: hxxps[://]www[.]gbridgaxtjdubtzsimnj3[.]com

- Timestamp: 2025-11-12T04:03:48.3024522Z
- Action: ConnectionFailed
- Remote IP: 45[.]148[.]121[.]112
- Remote Port: 9001
- Remote URL: N/A

- Timestamp: 2025-11-12T04:04:49.7953786Z
- Remote IP: 51[.]159[.]104[.]35
- Remote Port: 9001
- Remote URL: hxxps[://]www[.]rvyvjcnbejfrlbbtxetmdcc[.]com

- Timestamp: 2025-11-12T04:09:28.1399383Z
- Remote IP: 151[.]115[.]77[.]195
- Remote Port: 9001
- Remote URL: hxxps[://]www[.]rvyvjcnbejfrlbbtxetmdcc[.]com

User File Created
During the period of TOR network activity, a TOR-related file name appears in the user's Recent Items, indicating that a text file named `tor goodies hehe.txt` was opened or edited

- Timestamp: 2025-11-12T04:08:56.8641165Z
- Action: FileCreated
- File Name: tor goodies hehe.txt
- File Path: C:/Users/john.doe/AppData/Roaming/Microsoft/Windows/Recent/tor%20goodies%20hehe.lnk)
- File Hash (SHA256): 3846e3e7e8208fc5b9ef32b4239d882c2d28202317df97e7e6fa55de7c7b897a

File Deletion
After TOR browsing was completed, TOR-related files were deleted from their original locations and from the Recycle Bin. This suggests a deliberate attempt to remove evidence of TOR Browser from the system after use

- Timestamp: 2025-11-12T04:34:04.5293334Z
- Action: FileDeleted
- File: tor-browser-windows-x86_64-portable-15.0.1.exe
- File Path: C:\Users\john.doe\Downloads\tor-browser-windows-x86_64-portable-15.0.1.exe

- Timestamp: 2025-11-12T04:34:57.61735Z
- Action: FileDeleted
- File: firefox.exe
- File Path: C:\Users\john.doe\Desktop\Tor Browser\Browser\firefox.exe

- Timestamp: 2025-11-12T04:34:57.7315916Z
- Action: FileDeleted
- File: tor.exe
- File Path: C:\Users\john.doe\Desktop\Tor Browser\Browser\TorBrowser\Tor\tor.exe

- Timestamp: 2025-11-12T04:35:02.3841697Z
- Action: FileDeleted
- File: tor.exe

- File Path: C:\$Recycle.Bin\S-1-5-21-745193952-4091496363-3212887824-500\$RP148BR\Browser\TorBrowser\Tor\tor.exe

Recommendations

Incident Response:

- Immediately isolate the affected workstation and collect any relevant logs and artefacts
- Conduct antivirus/EDR scan to check for additional tools, scripts, or malware that may have been installed
- Search network for signs of suspicious or unusual activity from the host

Network Controls

- Block access to known TOR download domains and their mirror sites at the proxy or firewall
- Add detection rules for TOR-related traffic:
    - outbound connections to the following ports: `9001`, `9030`, `9040`, `9050`, `9051`, and `9150`

Endpoint Controls

- Prevent regular users from installing software outside of approved applications catalog
- Implement EDR or application control policies to detect and block known TOR components
- Block known TOR binaries and installers (e.g. `tor.exe` and `tor-browser-windows-x86_64-portable`)
- Monitor for TOR browser folders under user profiles (e.g., `C:\Users\<user>\Desktop\Tor Browser\...`)

Security Awareness

- Remind employees of acceptable use and security policies that prohibit unauthorized applications on company workstations.
- Encourage employees to reach out to IT/Security regarding additions to approved software list

Appendix A - Evidence Summary

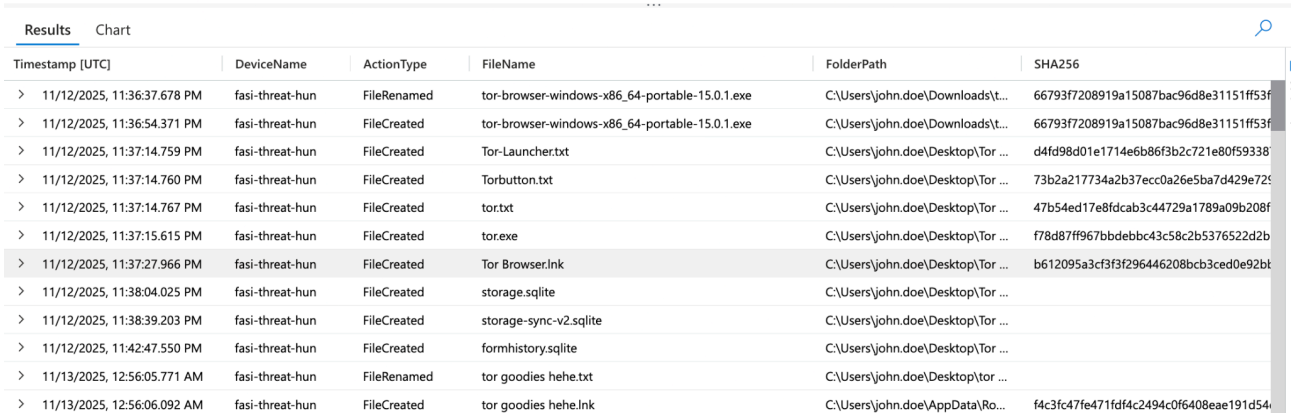
Discovery of TOR-related activity within the network

```
DeviceFileEvents
| where FileName contains "tor"
| order by TimeGenerated asc
```

TimeGenerated [UTC]	ActionType	AdditionalFields	DeviceId	DeviceName	FileName
11/12/2025, 3:00:08.753 AM	FileRenamed	{"FileType":"PortableExecutable"}	45db0cb63e38f0e6b8f918d253...	fasi-mde-test	drvstore.dll
11/12/2025, 3:00:10.039 AM	FileRenamed	{"FileType":"PortableExecutable"}	45db0cb63e38f0e6b8f918d253...	fasi-mde-test	drvstore.dll
11/12/2025, 3:00:18.717 AM	FileRenamed	{"FileType":"Error"}	45db0cb63e38f0e6b8f918d253...	fasi-mde-test	drvstore.dll
11/12/2025, 3:00:18.729 AM	FileRenamed	{"FileType":"Error"}	45db0cb63e38f0e6b8f918d253...	fasi-mde-test	drvstore.dll
11/12/2025, 3:00:18.878 AM	FileRenamed	{"FileType":"Error"}	45db0cb63e38f0e6b8f918d253...	fasi-mde-test	3c43667a8053dc01fd0000004c...
11/12/2025, 3:00:19.305 AM	FileRenamed	{"FileType":"PortableExecutable"}	45db0cb63e38f0e6b8f918d253...	fasi-mde-test	drvstore.dll
11/12/2025, 3:00:19.319 AM	FileRenamed	{"FileType":"PortableExecutable"}	45db0cb63e38f0e6b8f918d253...	fasi-mde-test	drvstore.dll
11/12/2025, 3:02:51.447 AM	FileRenamed	{"FileType":"Unknown"}	45db0cb63e38f0e6b8f918d253...	fasi-mde-test	@storagesensetoasticon.png
11/12/2025, 3:02:52.389 AM	FileRenamed	{"FileType":"Unknown"}	45db0cb63e38f0e6b8f918d253...	fasi-mde-test	active directory sites and servic...
11/12/2025, 3:02:53.289 AM	FileRenamed	{"FileType":"Unknown"}	45db0cb63e38f0e6b8f918d253...	fasi-mde-test	aggregatorhost.exe
11/12/2025, 3:02:53.823 AM	FileRenamed	{"FileType":"Unknown"}	45db0cb63e38f0e6b8f918d253...	fasi-mde-test	appidcertstorecheck.exe
11/12/2025, 3:02:54.285 AM	FileRenamed	{"FileType":"Unknown"}	45db0cb63e38f0e6b8f918d253...	fasi-mde-test	appobjectfactory.js
11/12/2025, 3:03:02.351 AM	FileRenamed	{"FileType":"Unknown"}	45db0cb63e38f0e6b8f918d253...	fasi-mde-test	bytecodegenerator.exe

Narrow search to single workstation

```
DeviceFileEvents
| where DeviceName contains "fasi-threat"
| where FileName contains "tor"
| order by TimeGenerated asc
| where TimeGenerated >= todatetime('2025-11-12T23:36:37.6787105Z')
| project Timestamp, DeviceName, ActionType, FileName, FolderPath, SHA256, Account =
InitiatingProcessAccountName
```



Results Chart

Timestamp [UTC]	DeviceName	ActionType	FileName	FolderPath	SHA256
11/12/2025, 11:36:37.678 PM	fasi-threat-hun	FileRenamed	tor-browser-windows-x86_64-portable-15.0.1.exe	C:\Users\john.doe\Downloads\t...	66793f7208919a15087bac96d8e31151ff53f
11/12/2025, 11:36:54.371 PM	fasi-threat-hun	FileCreated	tor-browser-windows-x86_64-portable-15.0.1.exe	C:\Users\john.doe\Downloads\t...	66793f7208919a15087bac96d8e31151ff53f
11/12/2025, 11:37:14.759 PM	fasi-threat-hun	FileCreated	Tor-Launcher.txt	C:\Users\john.doe\Desktop\Tor ...	d4fd98d01e1714e6b86f3b2c721e80f59338
11/12/2025, 11:37:14.760 PM	fasi-threat-hun	FileCreated	Torbutton.txt	C:\Users\john.doe\Desktop\Tor ...	73b2a217734a2b37ecc0a26e5ba7d429e729
11/12/2025, 11:37:14.767 PM	fasi-threat-hun	FileCreated	tor.txt	C:\Users\john.doe\Desktop\Tor ...	47b54ed17e8fdcab3c44729a1789a09b208f
11/12/2025, 11:37:15.615 PM	fasi-threat-hun	FileCreated	tor.exe	C:\Users\john.doe\Desktop\Tor ...	f78d87ff967bbdebbc43c58c2b5376522d2b
11/12/2025, 11:37:27.966 PM	fasi-threat-hun	FileCreated	Tor Browser.lnk	C:\Users\john.doe\Desktop\Tor ...	b612095a3cf3f3f296446208bcb3ced0e92bb
11/12/2025, 11:38:04.025 PM	fasi-threat-hun	FileCreated	storage.sqlite	C:\Users\john.doe\Desktop\Tor ...	
11/12/2025, 11:38:39.203 PM	fasi-threat-hun	FileCreated	storage-sync-v2.sqlite	C:\Users\john.doe\Desktop\Tor ...	
11/12/2025, 11:42:47.550 PM	fasi-threat-hun	FileCreated	formhistory.sqlite	C:\Users\john.doe\Desktop\Tor ...	
11/13/2025, 12:56:05.771 AM	fasi-threat-hun	FileRenamed	tor goodies hehe.txt	C:\Users\john.doe\Desktop\tor ...	
11/13/2025, 12:56:06.092 AM	fasi-threat-hun	FileCreated	tor goodies hehe.lnk	C:\Users\john.doe\AppData\Ro...	f4c3fc47fe471fdf4c2494c0f6408eae191d54

Confirmation of unauthorized application installation

```
DeviceProcessEvents
| where DeviceName contains "Fasi-Threat"
| where ProcessCommandLine contains
"tor-browser-windows-x86_64-portable-15.0.1.exe"
| where TimeGenerated >= todatetime('2025-11-12T23:36:37.6787105Z')
| project TimeGenerated, DeviceName, ActionType, ProcessCommandLine, FileName,
FolderPath, Account = InitiatingProcessAccountName, SHA256
```

TimeGenerated [UTC]	DeviceName	ActionType	ProcessCommandLine	FileName	FolderPath	Account	SHA256
11/12/2025, 11:36:57.210 PM	fasi-threat-hun	ProcessCreated	tor-browser-windows-x86_64-p...	tor-browser-windows-x86_64-p...	C:\Users\john.doe\Downloads\t...	john.doe	66793f720891

Confirmation of unauthorized application launched on workstation

```
DeviceProcessEvents
| where DeviceName contains "Fasi-Threat"
| where FileName has_any ("tor.exe", "tor-browser.exe", "firefox.exe")
| project Timestamp, DeviceName, AccountName, ActionType, ProcessCommandLine,
FileName, FolderPath, SHA256
| order by Timestamp desc
```

Results Chart

Timestamp [UTC]	DeviceName	AccountName	ActionType	ProcessCommandLine	FileName	FolderPath	SHA256
11/12/2025, 11:39:06.028 PM	fasi-threat-hun	john.doe	ProcessCreated	"tor.exe" -f "C:\Users\john.doe\...	tor.exe	C:\Users\john.doe\Desktop\Tor ...	f78d87ff967bbdeb
11/12/2025, 11:38:01.170 PM	fasi-threat-hun	john.doe	ProcessCreated	"firefox.exe"	firefox.exe	C:\Users\john.doe\Desktop\Tor ...	3807eab0d5d069c
11/12/2025, 11:38:00.713 PM	fasi-threat-hun	john.doe	ProcessCreated	"firefox.exe"	firefox.exe	C:\Users\john.doe\Desktop\Tor ...	3807eab0d5d069c
11/12/2025, 4:34:02.375 AM	fasi-threat-hun	john.doe	ProcessCreated	"firefox.exe" -contentproc -isFor...	firefox.exe	C:\Users\john.doe\Desktop\Tor ...	3807eab0d5d069c
11/12/2025, 4:07:42.962 AM	fasi-threat-hun	john.doe	ProcessCreated	"firefox.exe" -contentproc -isFor...	firefox.exe	C:\Users\john.doe\Desktop\Tor ...	3807eab0d5d069c
11/12/2025, 4:07:37.982 AM	fasi-threat-hun	john.doe	ProcessCreated	"firefox.exe" -contentproc -isFor...	firefox.exe	C:\Users\john.doe\Desktop\Tor ...	3807eab0d5d069c
11/12/2025, 4:07:36.923 AM	fasi-threat-hun	john.doe	ProcessCreated	"firefox.exe" -contentproc -isFor...	firefox.exe	C:\Users\john.doe\Desktop\Tor ...	3807eab0d5d069c
11/12/2025, 4:05:31.080 AM	fasi-threat-hun	john.doe	ProcessCreated	"firefox.exe" -contentproc -isFor...	firefox.exe	C:\Users\john.doe\Desktop\Tor ...	3807eab0d5d069c
11/12/2025, 4:03:31.246 AM	fasi-threat-hun	john.doe	ProcessCreated	"firefox.exe" -contentproc -isFor...	firefox.exe	C:\Users\john.doe\Desktop\Tor ...	3807eab0d5d069c
11/12/2025, 4:03:31.197 AM	fasi-threat-hun	john.doe	ProcessCreated	"firefox.exe" -contentproc -isFor...	firefox.exe	C:\Users\john.doe\Desktop\Tor ...	3807eab0d5d069c
11/12/2025, 4:03:02.251 AM	fasi-threat-hun	john.doe	ProcessCreated	"firefox.exe" -contentproc -isFor...	firefox.exe	C:\Users\john.doe\Desktop\Tor ...	3807eab0d5d069c
11/12/2025, 4:01:19.295 AM	fasi-threat-hun	john.doe	ProcessCreated	"firefox.exe" -contentproc -isFor...	firefox.exe	C:\Users\john.doe\Desktop\Tor ...	3807eab0d5d069c
11/12/2025, 4:00:14.561 AM	fasi-threat-hun	john.doe	ProcessCreated	"firefox.exe" -contentproc -isFor...	firefox.exe	C:\Users\john.doe\Desktop\Tor ...	3807eab0d5d069c

Network activity on common TOR-related ports

```
DeviceNetworkEvents
| where DeviceName contains "Fasi-Threat"
| where InitiatingProcessFileName in ("tor.exe", "firefox.exe")
| where RemotePort in ("9001", "9030", "9040", "9050", "9051", "9150")
| project Timestamp, DeviceName, InitiatingProcessAccountName, ActionType, RemoteIP,
RemotePort, RemoteUrl, InitiatingProcessFileName, InitiatingProcessFolderPath
```

Results | Chart

Timestamp [UTC]	DeviceName	InitiatingProcessAccountNa...	ActionType	RemoteIP	RemotePort
11/12/2025, 11:39:17.125 PM	fasi-threat-hun	john.doe	ConnectionSuccess	75.145.166.75	9001
11/12/2025, 11:39:14.053 PM	fasi-threat-hun	john.doe	ConnectionSuccess	75.145.166.75	9001
11/12/2025, 4:09:28.139 AM	fasi-threat-hun	john.doe	ConnectionSuccess	151.115.77.195	9001
11/12/2025, 4:09:27.420 AM	fasi-threat-hun	john.doe	ConnectionSuccess	151.115.77.195	9001
11/12/2025, 4:04:49.795 AM	fasi-threat-hun	john.doe	ConnectionSuccess	51.159.104.35	9001
11/12/2025, 4:04:27.355 AM	fasi-threat-hun	john.doe	ConnectionSuccess	51.159.104.35	9001
11/12/2025, 4:03:48.302 AM	fasi-threat-hun	john.doe	ConnectionFailed	45.148.121.112	9001
11/12/2025, 4:02:42.078 AM	fasi-threat-hun	john.doe	ConnectionSuccess	84.1.55.201	9001
11/12/2025, 4:02:27.354 AM	fasi-threat-hun	john.doe	ConnectionSuccess	84.1.55.201	9001
11/12/2025, 4:01:33.411 AM	fasi-threat-hun	john.doe	ConnectionSuccess	65.21.132.179	9001
11/12/2025, 4:01:19.235 AM	fasi-threat-hun	john.doe	ConnectionSuccess	127.0.0.1	9150
11/12/2025, 4:01:17.329 AM	fasi-threat-hun	john.doe	ConnectionSuccess	65.21.132.179	9001
11/12/2025, 4:00:15.705 AM	fasi-threat-hun	john.doe	ConnectionSuccess	75.184.13.239	9001

Appendix B - Event Timeline

Time (UTC)	Event
03:56:29	Tor browser installer downloaded to workstation
03:56:48	User silently installed application
03:57:44	Tor browser execution
04:00:15	Initial network activity over TOR network (port 9001)
04:08:56	“tor shopping list.txt” created
04:09:28	Last TOR site connected to
04:34:52	Tor browser installer deleted from Downloads folder
04:34:57	Tor browser directory deleted from Desktop
04:35:02	Recycle bin cleared

Appendix C - Indicators of Compromise (IOCs)

Indicators of Compromise

Category	IOC	Hash	Folder Path	Notes
File	tor-browser-windows-x86_64-portable-15.0.1.exe	66793f7208919a15087bac96d8e31151ff53f9620d9fd7bfd340794fa6d5f86c	C:\Users\john.doe\Downloads\tor-browser-windows-x86_64-portable-15.0.1.exe	Tor installer
File	tor.exe	f78d87ff967bbdebbc43c58c2b5376522d2bbc975c98727c75bf28e2eb23ffd0	C:\Users\john.doe\Desktop\Tor Browser\Browser\TorBrowser\Tor\tor.exe	Tor browser file
File	Tor Browser.lnk	b612095a3cf3f3f296446208bcb3ced0e92bbafac910637769217c589946ebcf	C:\Users\john.doe\Desktop\Tor Browser\Tor Browser.lnk	Tor browser shortcut
File	Tor goodies hehe.txt	3846e3e7e8208fc5b9ef32b4239d882c2d28202317df97e7e6fa55de7c7b897a	C:\Users\john.doe\Desktop\tor goodies hehe.txt	User created file
IP	75.145.166.75			External IP connected when browsing on TOR
IP	151. 115.77.195			External IP connected when browsing on TOR
IP	51.159.104.35			External IP connected when browsing on TOR
IP	45.148.121.112			External IP connected when browsing on TOR
IP	84.1.55.201			External IP connected when browsing on TOR
IP	65.21.132.79			External IP connected when

				browsing on TOR
IP	75.184.13.239			External IP connected when browsing on TOR
Port	9001			Port used when browsing on TOR
Port	9150			Port used for localhost 127.0.0.1

Appendix D - MITRE ATT&CK Framework

ID	Techniques	Notes
T1105	Ingress Tool Transfer	Downloading unauthorized file from the internet into Downloads folder
T1059.003	Command and Scripting Interpreter: Windows Command Shell	The Tor installer was executed through Windows command prompt using the silent flag (/S)
T1204.002	User Execution: Malicious File	User opened the Tor browser executable on their Desktop
T1090	Proxy	Tor established outbound connections across multiple external IPs over port 9001 to anonymize network data
T1573	Encrypted Channel	Encrypted outbound channels TOR traffic between the host and TOR nodes
T1070.004	Indicator Removal: File Deletion	User tried clearing their tracks by deleting all Tor related files from their machine