1,000+ Customers, **12 years** of best-in-class solutions

LOGPOINT

Products Solutions Pricing Resources & Support Partner resources Book a demo

Detecting Tor use with LogPoint

July 21st, 2020 - 6 min read

By Bhabesh Raj Rai, Associate Security Analytics Engineer, LogPoint

On July 1, 2020, the Cybersecurity and Infrastructure Security Agency (CISA), along with contributions from the Federal Bureau of Investigation (FBI), released an advisory highlighting risks associated with Tor, including technical details and mitigation recommendations. CISA and the FBI recommend that organizations assess their risk of compromise via Tor and take appropriate mitigations to block or closely monitor network traffic to and from Tor exit nodes.

On July 1, 2020, the Cybersecurity and Infrastructure Security Agency (CISA), along with contributions from the Federal Bureau of Investigation (FBI), released an advisory highlighting risks associated with Tor, including technical details and mitigation recommendations. CISA and the FBI recommend that organizations assess their risk of compromise via Tor and take appropriate mitigations to block or closely monitor network traffic to and from Tor exit nodes.

Tor uses the Onion Routing Protocol to obfuscate the user's identity from anyone seeking to monitor online activity. Tor uses a network comprised of thousands of volunteer-run servers known as Tor relays, which obfuscates the source and destination of a network connection. Anyone conducting monitoring or analysis will only see the traffic coming from the Tor exit node and will not be able to determine the original IP address of the request. Tor also has a browser-based on Firefox ESR that aims to make all users look the same, making it difficult for anyone to be fingerprinted based on their browser and device information.

Although Tor's primary purpose is to protect its users' privacy, it is increasingly used by threat actors to hide their malware's network traffic. In 2013, Trend Micro blogged about the Mevede malware using Tor to hide their C&C servers. Kaspersky also noted that a few banking malware families, such as 64-bit ZeuS Trojans, use Tor connections. There are also some ransomware variants like Onion that use Tor to hide their C&C servers. To make matters simple for malware to access a website hosted in the Tor, free services like Tor2web enable anyone to connect to an onion site with any regular browser. Just by appending the .to extension to almost any onion link makes it accessible from the clearnet. This way, the malware doesn't require the bells and whistles of a full-blown Tor client.

FireEye has observed Russian nation-state attackers APT29 employing domain fronting with Tor for stealthy backdoor access to victim environments on the APT side. The increasing trend of malware using Tor means that administrators should consider how to detect, and if necessary, block, Tor use in their enterprise.

Malicious tactics and techniques aided by Tor

Adversaries use Tor to create a layer of anonymity to conceal malicious activity at different stages of network compromise. Their tactics and techniques include:

- Initial Access [TA0001]
    - Exploit Public-Facing Applications [T1190]
- Command and Control [TA0011]
    - Commonly Used Port [T1043]
    - Connection Proxy [T1090]

- - Custom Command and Control Protocol [T1094]

  - Custom Cryptographic Protocol [T1024]

  - Multi-hop Proxy [T1188]

  - Multilayer Encryption [T1079]

  - Standard Application Layer Protocol [T1071]
- Exfiltration [TA0010]

- Impact [TA0040]

  - Data Encrypted for Impact [T1486]

  - Endpoint Denial of Service [T1499]

  - Network Denial of Service [T1498]

LogPoint supports a wide range of MITRE ATT&CK analytics. We recommend businesses keep up-to-date with our alert rules to increase incident detection capabilities.

LogPoint detection to Tor use

On the detection side, enterprises can detect Tor use by leveraging the various network, endpoint and security appliance logs. According to CISA, using an indicator-based approach, network defenders can leverage SIEMs and other log analysis platforms to flag suspicious activities involving known Tor exit nodes' IP addresses. With a behavior-based approach, blue teams can uncover suspicious Tor activity by searching for Tor client software and protocols' operational patterns and protocols, for example, port use commonly affiliated with Tor.

Tor use, both malicious or legitimate, is easy to detect using LogPoint. Firewalls, proxy servers and endpoint logs can pinpoint the endpoint from where the Tor connection originates.

Detection from firewalls and proxy servers

At the very least, it is required to maintain a list named TOR_ENTRY_IPS, which contains up-to-date IP addresses of known Tor entry (also called guard) nodes. Such a list can be periodically fetched from many sites with additional filtering to select only the guard nodes. An alternative is to create a list named TOR_IPS that contains all the Tor node's IP addresses.

Egress Filtering for Tor Connections

```
source_address IN HOMENET destination_address IN TOR_IPS
```

Egress Filtering for Tor Ports

```
source_address IN HOMENET destination_address IN TOR_IPS
```

Tor2web detection

The following query can detect any use of the Tor2web service for connecting to onion sites.

```
(resource="*.onion.*" OR url="*.onion.*")
```

At the Windows endpoint, DNS queries can be monitored for detecting any Tor2web use.

```
norm_id=WindowsSysmon label=DNS label=Query query="*onion.*"
```

Detection from IDS/IPS

IDS/IPS, such as Snort or Suricata, are also capable of detecting Tor use if the required rules are activated.

```
(norm_id=Snort OR norm_id=SuricataIDS) (message="* Tor *" OR message="* TorRules *")
```

Detection from endpoint

Tor client execution can be picked up from Windows Event Logs or Sysmon.

```
norm_id=WindowsSysmon label="Process" label=Create image="*tor.exe"
```

Use of the Tor browser can be detected from the same events.

```
norm_id=WindowsSysmon label="Process" label=Create image="*\Tor Browser\Browser\firefox.exe"
```

Installation of the Tor browser can be detected from the registry logs.

```
norm_id=WindowsSysmon event_id=13 target_object="*\Root\InventoryApplicationFile\torbrowser*"
```

Network connection logs from Sysmon can detect Tor use from the endpoint.

```
norm_id=WindowsSysmon label=Network label=Connect destination_port IN [443, 8443] source_address IN HOMENET
destination_address IN TOR_IPS
```

Windows Filtering Platform logs also help detect HTTP proxy listening for Tor connections.

```
norm_id=WinServer event_id=5154 source_port=9050
```

Windows's native AppLocker can be used to block the execution of Tor. This query will detect any instance of Tor execution blocked by AppLocker.

```
norm_id=WinServer event_id=8004 event_source=Microsoft-Windows-AppLocker rule="*tor.exe"
```

A variant of ZeuS maintained a tor.exe utility inside its body, which it later injects into svchost.exe. In the ZueS variant, it is the svchost.exe that is running tor.exe. Similar behaviors can be detected by looking at the execution of Windows's native processes having command lines options of tor.exe.

```
norm_id=WindowsSysmon label="Process" label=Create image="*svchost.exe" command IN ["*-HiddenServiceDir*", "*-
HiddenServicePort*"]
```

Sometimes, malware like ChewBacca drops tor.exe in the user's temp directory and runs it with a default listing on localhost:9050.

```
norm_id=WindowsSysmon event_id=11 path="*\Temp\" file="tor.exe"
```

In conclusion

In the end, we strongly advise that administrators use Tor detection capabilities within their deployed WAFs, firewalls, IPS/IDS, etc. Sinkholing of DNS queries can be done to prevent the use of services like Tor2web. However, sophisticated threat actors may leverage additional anonymization technologies—such as VPNs and Tor bridges to circumvent detection and blocking. Ultimately, each entity must consider its risk tolerance level when determining which risk mitigation approach to use for Tor.

Discover More About Logpoint

Book a demo

Customer cases

Customer reviews

Related Posts

Uncover more resources with Logpoint's latest release

October 30th, 2024

Latrodectus: The Wrath of Black Widow

October 22nd, 2024

LOGPOINT

Products   Why Logpoint?   Company   Support   Contact

Detect. Manage. Respond.

SIEM

Automation

Case Management

Behavior Analytics

Cyber Defense Platform

Pricing

Sizing Calculator

Product Recognition

Customer Cases

EAL3+ Certificate

Newsletter

About us

Management

Careers at Logpoint

Media Room

Logpoint in the media

Blog & Webinars

Cyber Library

Service Desk

Documentation

Community

Contact

Status

info@logpoint.com

+45 7060 6100