ultraviolet

CONFIDENTIAL

THREAT REPORT:

Hiding In Plain Sight with Tor's New WebTunnel

Services Performed By:
UltraViolet Cyber
Casey Latham
(443) 351-7630
info@uvcyber.com

Published Date:
03/13/2024

Contents

1 Executive Summary

The Tor Browser/Network has been a vehicle to fight censorship in oppressive regimes, provide security for home users with anonymous browsing, and, unfortunately, provide a hidden network for bad actors to deal in Cyber Crime. Just in time for World Day Against Cyber Censorship Day (March 12, 2024) the Tor Project, developers of Tor, have announced the release of their new WebTunnel. This new technology according to the Tor Project is, "...a new type of Tor bridge designed to assist users in heavily censored regions to connect to the Tor network."[i] On the face of it, this is fantastic news that will allow users and news organizations to operate behind oppressive opposition. However, this technology is also available to bad actors. This is a new security concern that needs to be addressed.

2 Technical Analysis

The Tor Project announced the release of WebTunnel. WebTunnel is a pluggable transport, that can mimic encrypted web (HTTP) traffic. This mimic of traffic is completed over a bridge and "...works by wrapping the payload connection into a WebSocket-like HTTPS connection, appearing to network observers as an ordinary HTTPS (WebSocket) connection."[ii] This provides an obfuscated network connection wherein bad actors can appear as legitimate web surfers navigating through encrypted traffic. This provides a layer of protection for the bad actor as their traffic, it is advertised, will be blended into what appears to be normal https traffic.

Describing the technology behind this new WebTunnel delves deep into the workings of advanced Network Operations, thankfully the Tor Project has provided a brief, albeit chilling, explanation into the operation of WebTunnel.

> "In fact, WebTunnel is so similar to ordinary web traffic that it can coexist with a website on the same network endpoint, meaning the same domain, IP address, and port. This coexistence allows a standard traffic reverse proxy to forward both ordinary web traffic and WebTunnel to their respective application servers. As a result, when someone attempts to visit the website at the shared network address, they will simply perceive the content of that website address and won't notice the existence of a secret bridge (WebTunnel)." [iii]

The Tor WebTunnel was just announced hours before the writing of this Threat Bulletin. The implications of an encrypted traffic mimicking technology will unfold as the release of Tor's WebTunnel is broadcasted throughout the internet. A brief investigation into the availability of WebTunnel currently shows 65 available nodes, advertising up to 9.89 MiBs in bandwidth.[iv]

3 What UltraViolet Cyber is Doing

- UltraViolet Cyber regularly updates our IOC database to ensure alerting is up to date
- Monitoring commands that are associated with malicious activity from threat actors
- Monitoring network logs for traffic to known malicious sites

4 What Customers Can Do

- Increase enterprise awareness and scrutiny towards Tor traffic.
- Never assume that all HTTPS is legitimate. Security vendors will continue development on detections to locate mimicked HTTPS traffic for analysis.
- Review company policies and procedures on the usage of Tor by employees. If Tor usage is not allowed in your enterprise, deny regular Tor traffic if this does not affect business operations.

5 References

- Gatlan, S. (2024, March 12). Tor's new WebTunnel bridges mimic HTTPS traffic to evade censorship. *BleepingComputer*. https://www.bleepingcomputer.com/news/security/tors-new-webtunnel-bridges-mimic-https-traffic-to-evade-censorship/
- *Hiding in plain sight: Introducing WebTunnel | Tor Project*. (n.d.). https://blog.torproject.org/introducing-webtunnel-evading-censorship-by-hiding-in-plain-sight/
- *Relay search*. (n.d.). https://metrics.torproject.org/rs.html#search/transport:webtunnel?fields=transports

[i] Hiding in plain sight: Introducing WebTunnel | Tor Project. (n.d.). https://blog.torproject.org/introducing-webtunnel-evading-censorship-by-hiding-in-plain-sight/
[ii] Hiding in plain sight: Introducing WebTunnel | Tor Project. (n.d.). https://blog.torproject.org/introducing-webtunnel-evading-censorship-by-hiding-in-plain-sight/
[iii] Hiding in plain sight: Introducing WebTunnel | Tor Project. (n.d.). https://blog.torproject.org/introducing-webtunnel-evading-censorship-by-hiding-in-plain-sight/
[iv] Relay search. (n.d.). https://metrics.torproject.org/rs.html#search/transport:webtunnel?fields=transports

(443) 351-7630 | info@uvcyber.com