# Rogue Tor Browser: When Search for Anonymity Leads to Exposure Instead

## Table of Contents



## Executive Report

Anyone who wishes to browse the Internet without the prospect of being spied upon by others, whether for legal or illegal purposes, can always rely on using the Tor browser if they're so inclined. But for countries where Tor usage is deemed unlawful, accessing the browser's official download page may not be an option.

That said, users decided on using the Tor browser may need to rely on relatively unknown and possibly accessible download sites. Therein may lie the problem, given that some like the recently publicized malicious download link distributed via YouTube, could be distributing a poisoned version.

To ensure protection, WhoisXML API researchers sought to expand a list of indicators of compromise (IoCs) containing two domains—torbrowser[.]io and tor-browser[.]io—published by AlienVault. Our in-depth investigation revealed:

- Four shared IP addresses to which the IoCs resolved, one of which is malicious
- At least 302 domains that shared the IoCs' IP hosts, one of which is classified as a malware host
- 113 additional domains containing the string "torbrowser," one of which is a confirmed spam host

### What We Know Already about the Malicious Tor Browser Installer

Kaspersky published a report on the malicious installer early this month, dubbing it "OnionPoison." It was being widely distributed via a popular Chinese YouTube channel devoted to promoting anonymity on the Web.

Contrary to the Tor browser's promise, OnionPoison was designed to steal all the information they stored in their browsers and entered into web forms. All this is sent to the attackers' command-and-control (C&C) server.

As making the Internet safer for all is our primary goal, we hope to expand the list of IoCs by identifying connected artifacts that could put those duped by OnionPoison at great risk.

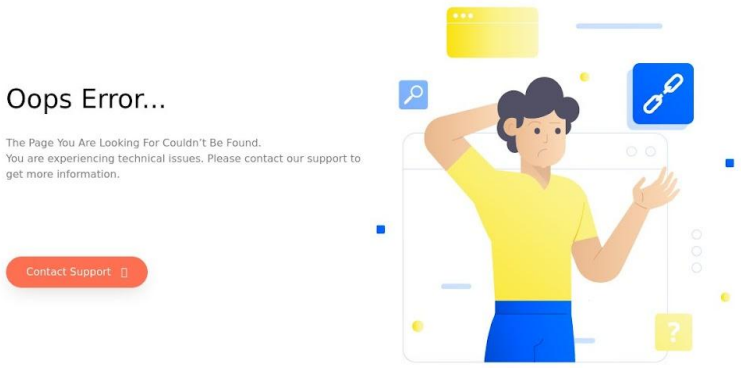
## IoC List Expansion Details

Using the two domains identified as IoCs as DNS lookup search terms provided four unique IP addresses to which they resolved, namely:

- 172[.]67[.]203[.]37
- 104[.]21[.]74[.]133
- 104[.]21[.]87[.]4
- 172[.]67[.]139[.]26

Malware checks showed that one of the IP hosts—172[.]67[.]203[.]37—requires blocking, as several malware engines deemed it malicious. All of them are geolocated in the U.S. and indicated Cloudflare, Inc. as Internet service provider (ISP).

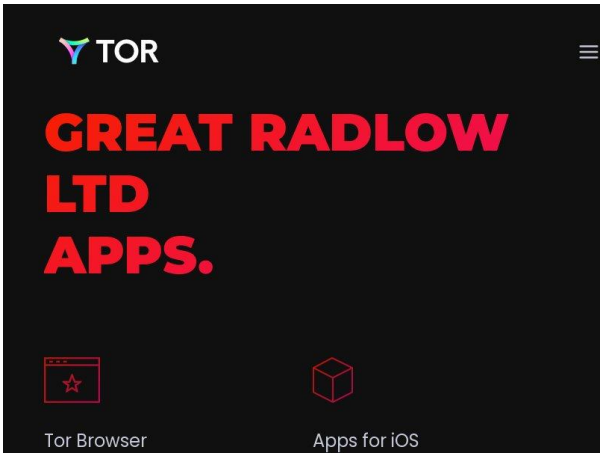
To identify additional threat artifacts, we subjected the IP addresses to reverse IP lookups that led to the discovery of at least 302 domains. One of them—disasgar[.]xyz—should particularly be avoided since it's been dubbed a malware host. Currently, though, a screenshot lookup for it led to an error page.



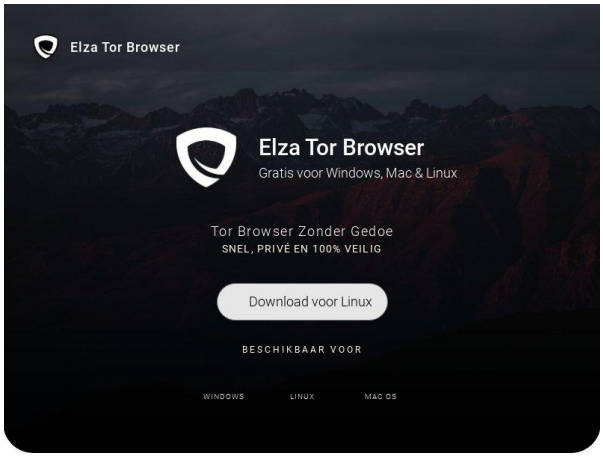

*Screenshot of malicious site disasgar[.]xyz*

We then looked for more domains containing the string “torbrowser” via Domains & Subdomains Discovery. Our investigation uncovered 113 additional artifacts.

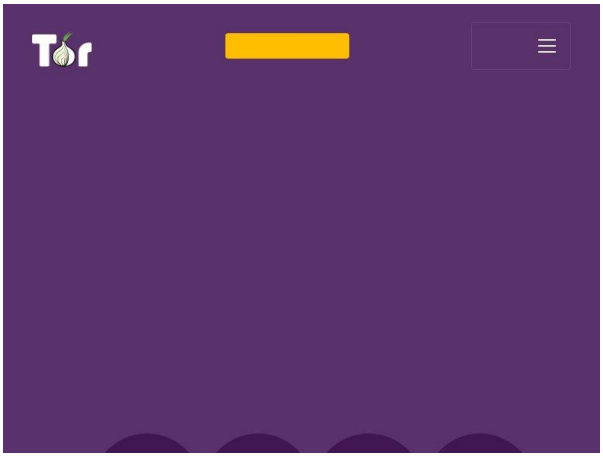
While only one of the additional “torbrowser” domains was dubbed “malicious” by various malware engines—torbrowser-rus[.]ru, six could pose dangers should the download buttons for the supposed Tor browser turn out to be malware-laden. These sites are torbrowser[.]in, torbrowser[.]nl, torbrowser[.]top, torbrowserpro[.]ru, torbrowserwin[.]com, and torbrowser-free[.]ru.




*Screenshot of torbrowser[.]in*

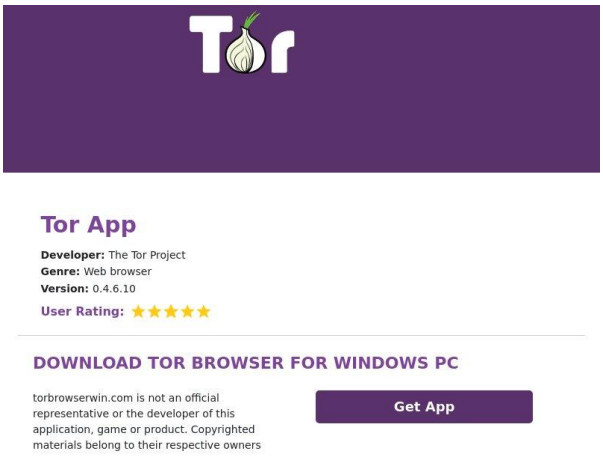



*Screenshot of torbrowser[.]nl*



*Screenshot of torbrowser[.]top*

*Screenshot of torbrowserpro[.]ru*




*Screenshot of torbrowserwin[.]com*


*Screenshot of torbrowser-free[.]ru*

As the screenshots show, computers regardless of operating system (OS) could get infected. A bulk WHOIS lookup for the domains also revealed that none of them were owned by the Tor Project, given that their records don't share "The Tor Project, Inc." as registrant organization with the legitimate domain torproject[.]org.

—

Online anonymity isn't easy to procure. In OnionPoison's case, instead of guaranteeing one's privacy, the tool steals precious personal data and more instead. Avoiding access to the IoCs and additional artifacts obtained via WHOIS, IP, and DNS intelligence sources featured here, however, could be a step toward DNS security.

***If you wish to perform a similar investigation or get access to the full data behind this research, please don't hesitate to contact us.***

# Appendix: Sample Artifacts and IoCs

## Sample Domains That Shared the IoCs' IP Hosts

- 0yznsihpf[.]club
- 204863[.]com
- 209mm[.]com
- 2ndplaceinportugal[.]com
- 383betsat[.]com
- 521ay[.]com
- 789digital[.]com
- 89ixl[.]com
- a-prime-us-ux-design-courses[.]zone
- a-school5[.]ru
- aaa[.]napilsya[.]ru
- aaa20[.]cc
- aab[.]napilsya[.]ru
- aac[.]napilsya[.]ru
- aad[.]napilsya[.]ru
- aagamgroup[.]in
- abenbounmithssove[.]gq
- abu10[.]cc
- aceropam[.]tk
- acretag[.]com
- addysbelarolje[.]tk
- adraning[.]ga
- advertisinginpune[.]com
- ag99[.]ru
- agencyimmo03[.]fr
- ajz[.]stone-official[.]pl
- alagporhytig[.]tk
- alinebender[.]com
- allacsybutlo[.]ga
- alsospolicyohcivils[.]cfd
- amadocs[.]com
- amatospassa[.]tk
- amatsilu[.]ml
- amzavip[.]com
- an-it-uk-funeral-cost-ok[.]live
- aneggatlou[.]tk
- angara[.]fr

- anleworddilo[.]cf
- annathpootethale[.]ga
- anprivolib[.]tk
- antenthumbpassvenfi[.]ml
- aperosplone[.]org
- apesad[.]tk
- appscurtain[.]xyz
- arancycco[.]ml
- arexviou[.]gq
- arizonarp[.]com[.]br
- aromasecure[.]fr
- arraratideter[.]tk
- arunabhaphotography[.]in

## Sample Domains Containing the String “torbrowser”

- torbrowser[.]nu
- torbrowser[.]us
- torbrowser[.]ch
- torbrowser[.]io
- torbrowser[.]me
- torbrowser[.]de
- torbrowser[.]fr
- torbrowser[.]in
- torbrowser[.]su
- torbrowser[.]nl
- torbrowser[.]tk
- torbrowser[.]co
- torbrowser[.]ru
- torbrowser[.]cn
- torbrowser[.]com
- torbrowser[.]net
- torbrowser[.]xyz
- xn--torbrwser-zxb[.]com
- torbrowser[.]app
- torbrowsers[.]ru
- torbrowsers[.]tk
- torbrowser[.]org
- torbrowser[.]top
- torbrowser[.]pro
- torbrowser[.]info
- torbrowser[.]live
- 5gtorbrowser[.]com
- motorbrowser[.]com
- torbrowserrus[.]ru
- torbrowser-pc[.]ru
- torbrowser[.]pp[.]ua
- 5gtorbrowser[.]app
- torbrowserpro[.]ru
- rotorbrowser[.]com
- mytorbrowser[.]org
- tutorbrowser[.]com
- gettorbrowser[.]com
- hectorbrowser[.]com
- thetorbrowser[.]com
- torbrowser-rus[.]ru
- torbrowser[.]online
- doctorbrowser[.]com
- freetorbrowser[.]ru
- torbrowserwin[.]com
- vectorbrowser[.]com
- viatorbrowser[.]com
- realtorbrowser[.]com
- freetorbrowser[.]com
- rotatorbrowser[.]com
- proctorbrowser[.]com