THE TOR PROJECT

OONI

Vasilis Ververis (andz@torproject.org)

GPG Fingerprint: 8FD5 CF5F 39FC 03EB B382 7470 5FBF 70B1 D126 0162

Public Key: https://pgp.mit.edu/pks/lookup?op=get&search=0x5FBF70B1D1260162
The Tor project

Mission: be the global resource for technology, advocacy, research and education in the ongoing pursuit of freedom of speech, privacy rights online, and censorship circumvention.
What is Tor?

- Online anonymity
  - FL/OSS
  - Open (volunteer based) network
- Community: researchers, developers, users, relay operators, [...]
- U.S. 501(c)(3) non-profit organization
Estimated 2,500,000+ Tor users (daily)
HOW INTERNET WORKS?
Source: Mapa analítico de Internet basado en la información obtenida del sitio opte.org el 15 de enero de 2005
A gigantic network of "computers", servers and devices
Every PC, server, device, refrigerator,... requires a unique identifier - "IP address"
• Internet is not the WWW (World Wide Web)
• Internet is the infrastructure
• Web is a service of this infrastructure
WE KNOW WHERE YOU ARE

Source: Rhododendrites
On the Internet we are sending (a lot) of private data:

- Source/destination IP address
- Geographical location
- WWW (World Wide Web):
  - Web Browser
  - Operating system
  - Addons/Extensions
Other services: e-mail, telephone, chat (IRC, IM), file sharing,...
UNDERSTANDING YOUR THREAD MODEL:

I use encryption (HTTPS, ...) my ISP cannot see my traffic! Maybe it cannot see your traffic (in cleartext), *but* it tracks:

- Websites visited
- Locations logs
- IP address logs
- ..archived for x time: Data retention
VPN / Proxy Providers

Alice1

E(Bob3, “X”)

Alice2

E(Bob1, “Y”)

Alice3

E(Bob2, “Z”)

Relay

Bob1

“Z”

Bob2

“X”

Bob3
VPN / Proxy Providers: (often) single point of failure
VPN / Proxy Providers: (often) single point of bypass
ANONYMITY: DIFFERENT INTERESTS FOR DIFFERENT USER GROUPS

POWERED BY Tor
ANONYMITY: DIFFERENT INTERESTS FOR DIFFERENT USER GROUPS

Anonymity

“It's privacy!”

Private citizens
ANONYMITY: DIFFERENT INTERESTS FOR DIFFERENT USER GROUPS

"It's privacy!"

Anonymity

Private citizens

"It's network security!"

Businesses
ANONYMITY: DIFFERENT INTERESTS FOR DIFFERENT USER GROUPS

“*It's traffic-analysis resistance!*”

Governments

Anonymity

Businesses

“*It's network security!*”

“*It's privacy!*”

Private citizens
ANONYMITY: DIFFERENT INTERESTS FOR DIFFERENT USER GROUPS

- **Governments**: “It's traffic-analysis resistance!”
- **Human rights activists**
- **Anonymity**: “It's reachability!”
- **Businesses**: “It's network security!”
- **Private citizens**: “It's privacy!”
A Alice criptografa o seu pedido online para o Bob três vezes, e envia-o para o primeiro servidor.

O primeiro servidor remove a primeira camada de criptografia, mas não consegue saber que o pedido é dirigido ao Bob.

O segundo servidor remove outra camada de criptografia e reencaminha o pedido.

O terceiro servidor remove a última camada de criptografia e entrega o pedido ao Bob, mas não consegue saber que o pedido veio da Alice.

O Bob não sabe que o pedido online foi feito pela Alice, a menos que ela mesma o diga.
Cómo Funciona Tor: 1

Paso 1: El cliente Tor de Alicia obtiene una lista de nodos Tor desde un servidor de directorio.
Cómo Funciona Tor: 2

Paso 2: El cliente Tor de Alicia elige un camino aleatorio al servidor de destino. Los enlaces verdes están encriptados, los enlaces rojos van en claro.
Cómo Funciona Tor: 3

Paso 3: Si el usuario quiere acceder a otro sitio, el cliente Tor de Alicia selecciona un segundo camino aleatorio. De nuevo, los enlaces verdes están encriptados, los enlaces rojos van en claro.
Total relay bandwidth

Advertised bandwidth and Bandwidth history

Source: Tor metrics

The Tor Project - https://metrics.torproject.org/
Tor's safety comes from diversity

- Diversity of relays
- Diversity of users
Transparency for Tor is key

- FL/OSS
- Public design documents and specifications
But what about the bad people?

- (remember) the millions of daily users
- Still a two-edged sword?
- Good people need Tor much more than bad people need it
Onion services

- Self authenticated
- End-to-end encrypted
- Built-in NAT punching
- Limit surface area
- No need to “exit” from Tor
• About 3% of Tor's traffic has to do with onion services at all
• Onion services are still in the "neat toy" stage
• Terbium labs (and others) found ~7000 useful onion sites
1 Million People use Facebook over Tor

People who choose to communicate over Tor do so for a variety of reasons related to privacy, security and safety. As we've written previously it's important to us to provide methods for people to use our services securely - particularly if they lack reliable methods to do so.

This is why in the last two years we built the Facebook onion site and onion-mobile site, helped standardise the “.onion” domain name, and implemented Tor connectivity for our Android mobile app by enabling connections through Orbot.
... and many others

Package repository
http://vwakviie2ienjx6t.onion/

apt-get install apt-tor-transport
Submit documents for the first time

If this is your first time submitting documents to journalists, start here.

SUBMIT DOCUMENTS

Already submitted something?

If you have already submitted documents in the past, log in here to check for responses. You will need to know your code name.

CHECK FOR A RESPONSE

Like all software, SecureDrop may contain security bugs. Use at your own risk.

Powered by SecureDrop 0.3development.
Salut Korben !

ça fonctionne, c'est cool. A qui ai je l'honneur ?

Oui, c'est cool. Je suis un lecteur de ton site, Paul.

enchanté !

j'ai commenté qu'une fois un article sur Mario64 porté sur plateforme x86
onionshare_jedtgt.zip

64.2 MiB (compressed)

This zip file contains the following contents:

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>folder</td>
<td>leaks</td>
<td>196.9 MiB</td>
</tr>
<tr>
<td>file</td>
<td>instructions.rtf</td>
<td>1.2 KiB</td>
</tr>
</tbody>
</table>
Since 2012, OONI (Open Observatory of Network Interference) has collected millions of network measurements across more than 200 countries around the world, shedding light on various instances of network interference.
WHAT IS OONI?
Detect censorship and signs of network tampering

Shares observations and data about the nature, methods, and prevalence of censorship and network tampering around the world, through the use of open methodologies and FLOSS tools.
OPEN DATA MODEL

- Network measurement data (reports) submitted by volunteers
- Complete dataset (from 2012) available to use/download
EVIDENCE OF INTERNET CENSORSHIP

- Transparency: What is blocked, where and how? What is the *health* of the network that we are using?
- Legality: Can the blocking of specific types of sites and services be legally justified?
- Story-telling & Advocacy: What is the impact of censorship on human rights?
DATA REPRESENTATION

OONI explorer
OONI TESTING METHODOLOGY
• Blocking of websites
• Blocking of instant messaging apps
• Blocking of censorship circumvention tools (Tor, VPN, Psiphon, Lantern)
• Detection of *middle boxes* proxy technologies that could be responsible for censorship and/or surveillance
• Speed and network performance tests (NDT)
OONI MEASUREMENTS IN LATAM
PIRATEBAY BLOCKED IN ARGENTINA
Web Connectivity 2017-03-23 06:24:01 UTC

20170323T062328Z_AS7303_UYQj7sql3cX8qzQXjRGZ4QCHf6lCnALEmLqcOjoFxpyIshSmI4

Test runtime: 1.82408 seconds

Network: Telecom Argentina S.A., AR ( AS7303 )  Name: ooniprobe-android  Version: 1.1.2

This measurement contains data that could be a sign of network tampering or censorship.

https://thepiratebay.se
Option for blocking: dns
measurements for URL
NEWS WEBSITE NTN24 BLOCKED IN VENEZUELA
Web Connectivity 2017-03-03 03:48:36 UTC

20170303T034153Z_AS8048_3ndo86P4sVdRgJ7N9CPMX5ft97YeHcbpCkofTTKol42forLpfN

Test runtime: 4.69504 seconds

Network: CANTV Servicios, Venezuela, VE (AS8048)  Name: ooniprobe  Version: 2.0.1

This measurement contains data that could be a sign of network tampering or censorship.

---

http://ntn24.com

Reason for blocking: dns

measurements for URL
WHATSAPP BLOCKED IN BRAZIL

# OONI Probe Report for http_requests (0.2.5)
# Mon May 2 23:17:02 2016

probe_asn: AS26615
probe_cc: BR
software_name: ooniprobe
software_version: 1.4.2
test_helpers: {}
test_name: http_requests
test_start_time: '2016-05-02 21:17:02'
test_version: 0.2.5

agent: agent
body_length_match: null
OONI RESULTS (1/4)

- March 2017: Thailand blocked news and censorship circumvention tool websites
- December 2016: Malaysia block pages and censorship
- December 2016: Ethiopia DPI used to block media websites during major political protests
OONI RESULTS (2/4)

- December 2016: Belarus blocked Tor
- October 2016: Zambia blocked websites during general elections
- May 2016: Uganda blocking of social media
OONI RESULTS (3/4)

- May 2016: Brazil blocked WhatsApp
- June 2015: Greece and EEEP blocklists
- July 2013: Zambia, a country under Deep Packet Inspection
May 2013: Uzbekistan and Turkmenistan Internet filtering and DPI

April 2012: Hadara Palestine Internet agency Hadara restricts access to certain content for users in Bethlehem

March 2012: T-Mobile USA Web Guard Parental controls blocked number of websites (Newgrounds, Cosmopolitan Magazine, and the Tor Project)
OONI STATISTICS
• Millions of network measurements collected from 200+ countries
• 2766+ unique ASNs
INTERNET HAS A LOT OF ENEMIES
Reporters Without Borders
HELP REVEAL INTERNET CENSORSHIP
Install ooniprobe

To install ooniprobe on Raspberry pi devices see our [lepidopter install guide](#).

To install ooniprobe on unix based systems read our [installation guide](#).
• Available for: Linux, Mac OS, Raspberry Pi, IOS, Android
• Source code:
  https://github.com/TheTorProject/ooni-probe
HOW CAN YOU HELP TOR?

- Run a relay (or a bridge)
- Teach your friends about Tor, and privacy in general
- Help fix -- and fix -- bugs
- Work on open research problems (petsymposium.org)
Protect your privacy

https://www.torproject.org/download/download-easy.html/