argas Advanced Technologies Group, Inc.
Keeping You Connected To Technology

The Battle Against Anonymous Browsing:

The Security Challenges Presented by Tor

Brief Introduction

- David A. Vargas
  - Work
    - President, VATG, Inc.
  - Teaching
    - Professor of Networking and Network Security
  - Education
    - BA, The George Washington University
    - MS, The Johns Hopkins University
  - Training:
    - Navy Cryptography
    - Army Counterintelligence
    - Security Audit, Malware Analysis, Digital Forensics, etc.
  - Primary certs:
    - CISSP, CISM, and CEHv7

Presentation Outline

- Introduction to the Dark Web - Hiding in Darkness
- What is Tor?
- Detecting Tor
- Chinks in the Armor - The Exit Node Problem
- Tor Attacks and Takedowns
- Does Tor Have a Future?

ATG

argas Advanced Technologies Group, Inc.
Keeping You Connected To Technology

Introduction to the Dark Web - Hiding in Darkness

Introduction to the Dark Web - Hiding in Darkness

- Surface Web:
  - The visible web that we are most familiar with

Introduction to the Dark Web - Hiding in Darkness

- What you find when you look deeper:

ATG

Introduction to the Dark Web - Hiding in Darkness

- Dark Web:
  - Consists of sites that are private or at least accessible only by those who know what they are looking for
  - Because of its anonymity, frequently used by deviant subcultures (criminals, pedophiles, etc.)

Aside: A comment on the terms

Introduction to the Dark Web - Hiding in Darkness

Surface Web (where most of you surf)

Dark Web (where only *some* of you surf – in some cases the FBI would like to meet with you)

Estimates have suggested that the deep web is *4,000 to 5,000 times* larger than the surface web.

ATG

Searching the Dark

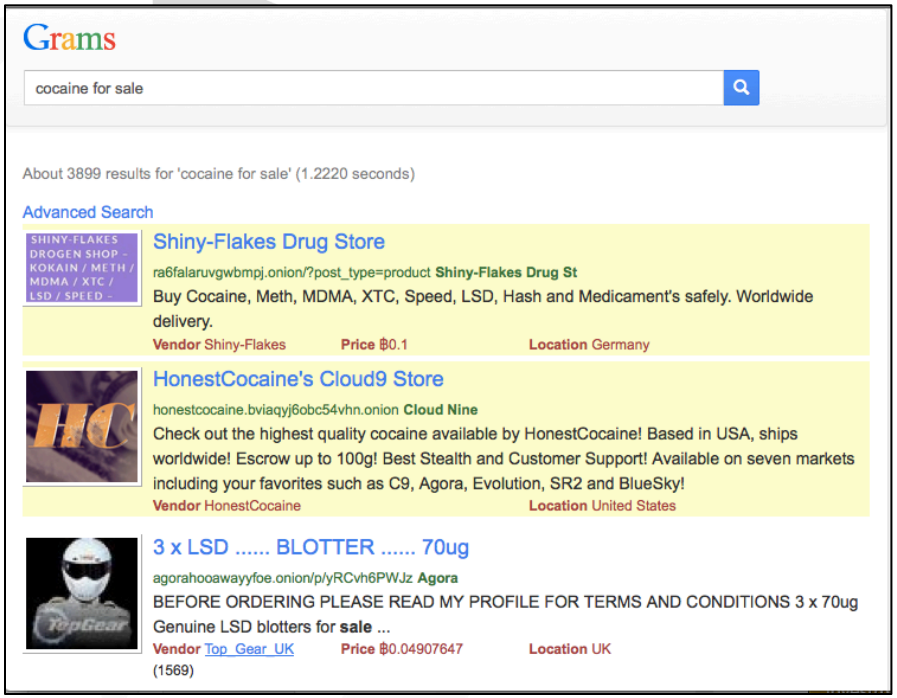
- Although the dark web exists on the very same physical infrastructure as the surface web, it cannot be indexed by traditional search engines
  - As a result, its contents do not appear as the result of common web searches
- Special search engines and sites are required

Grams Darknet Market Search Engine:

http://grams7enufi7jmdl.onion/

Searching the Dark

- Grams Darknet Market Search Engine
  - No-frills interface similar to Google's
    - Copies Google's "I'm Feeling Lucky" button
  - Requires the user be on the Tor network



Searching the Dark

- The Hidden Wiki

The Hidden Wiki

zqktlwi4fecvo6ri.onion/wiki/index.

create account log in

page | discussion | view source | history

The Hidden Wiki

navigation
- Main page
- Recent changes
- Random page
- Rules of the site

search
Search
Go Search

tools
- What links here
- Related changes
- Special pages
- Printable version
- Permanent link
- Page information

Main Page

Welcome to The Hidden Wiki

New hidden wiki url 2014 http://zqktlwi4fecvo6ri.onion Add it to bookmarks and spread it!!

Editor's picks

Bored? Pick a random page from the article index and replace one of the three slots with it

1. The Matrix - Very nice to read.
2. How to Exit the Matrix - Learn how to Protect yourself and your rights, online and off
3. Verifying PGP signatures - A short and simple how-to guide.

Volunteer

Here are five different things that you can help us out with.

1. Plunder other hidden service lists for links and place them here
2. File the SnapBBSIndex links wherever they go.
3. Set external links to HTTPS where available, good certificate, and same content.
4. Care to start recording onionland's history? Check out Onionland's Museum
5. Perform Dead Services Duties.

Introduction Points

- Ahmia.fi - Clearnet search engine for Tor Hidden Services (allows you to add new sites to its database).
- TorSearch Search engine for Tor Hidden Services.

Contents [hide]

Erotica

- Young Teens On Webcam Little Cute Girls And Perfect Amateur Teens On Cam
- X Teen Chan Only The Best Tiny Non Nude Teen Models And Sweet Naked Teens

Noncommercial (E)

- Pink Meth - Tor mirror of pinkmeth.com.
- (Y)APE - Down - Yet Another Porn Exchange.
- Darkscandals Site with Real Rape, Blackmail and Forced videos! (Pack 3 is out now - August)
- Fly On The Wall - Real Hacked Pics, Videos & Webcam Recordings from Girl's Computers

Commercial (E)

- bittit NSFW, clearnet - Buy or sell original NSFW pictures for Bitcoins.
- Lisa Hidden Cam - Watch 18 year old
- The Voyeur Underground - Voyeur pi
- Meet my Sisters - Two gorgeous girls

Under Age

- Hard Candy
- Jailbait

page | discussion | view source | history

Hard Candy

Attention Tor Browser Bundle users! Javascript is NOT disabled in the Tor Browser by default.
It is dangerous to access links on this page without first manually disabling Javascript.
Click on the blue **S** on the top left of your browser, then select **Forbid Scripts Globally (advised)**.
Also, some antis are changing links over and over, and deleting or manipulating things. So look at the history everytime.

Purpose & Background of this page

This wiki page discusses resources specifically for people who are attracted to children. This includes everything from discussion groups to modeling images of children to hard core pornography.

This wiki is a group effort and everybody will get the most out of it if everybody makes quality contributions so feel free to add any resource you know of. This page is constantly vandalized. Please make backups for yourself. If you're a person looking to vandalize please don't. Please respect our free speech rights as well.

It is important that you stay as safe as possible when browsing these sites. Consider reading

Contents [hide]

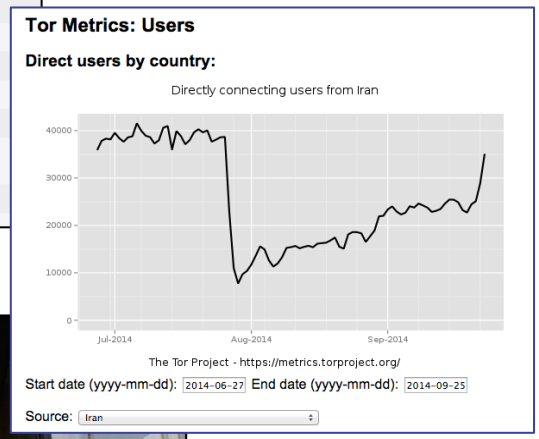
ATG

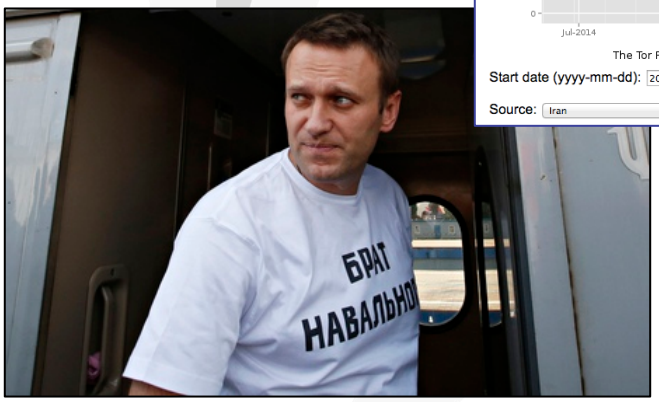
Legal Activities on the Dark Web

- Use the dark web legally:
  - Normal People (Firewalled)
  - Military
  - Law Enforcement
  - Businesses
  - IT Professionals
  - Journalists and Bloggers
  - Political Dissidents
  - Activists
  - Whistleblowers
  - NGOs

ONI ranking of each country for internet censorship
Click heading to sort table. Download this data

Country	Political filtering	Social filtering	Internet tools filtering	Conflict/security filtering
China	pervasive	substantial	substantial	pervasive
Burma (Myanmar)	pervasive	substantial	substantial	substantial
Sudan	selective	substantial	substantial	no evidence
Bahrain	pervasive	pervasive	substantial	selective
Oman	selective	pervasive	substantial	no evidence
Vietnam	pervasive	selective	substantial	selective
Morocco	no evidence	selective	selective	selective
Turkey	selective	selective	selective	no evidence
Pakistan	selective	selective	selective	substantial

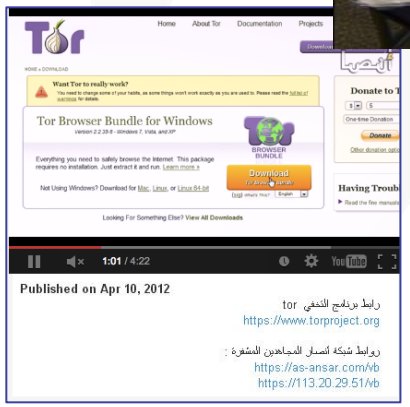




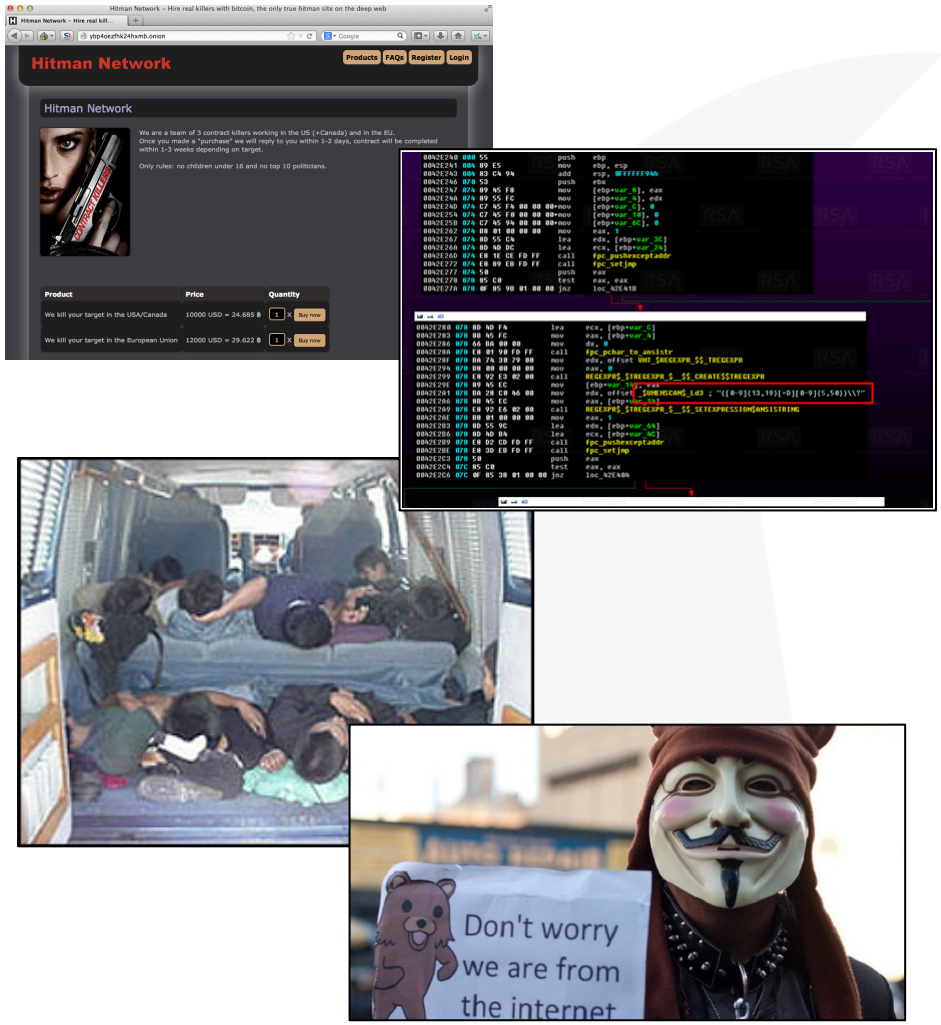
Anti-corruption crusader Alexei Navalny's blog was blocked by Russian authorities and now can only be accessed through Tor

Illegal Activities on the Dark Web

- Examples of illegal uses:
  - Sale and distribution of child pornography
  - Sale of drugs and drug paraphernalia
  - Distribution of recipes for drug manufacture
  - Terrorist communication
  - Bitcoin use anonymity
  - Sale of pirated software



Illegal Activities on the Dark Web



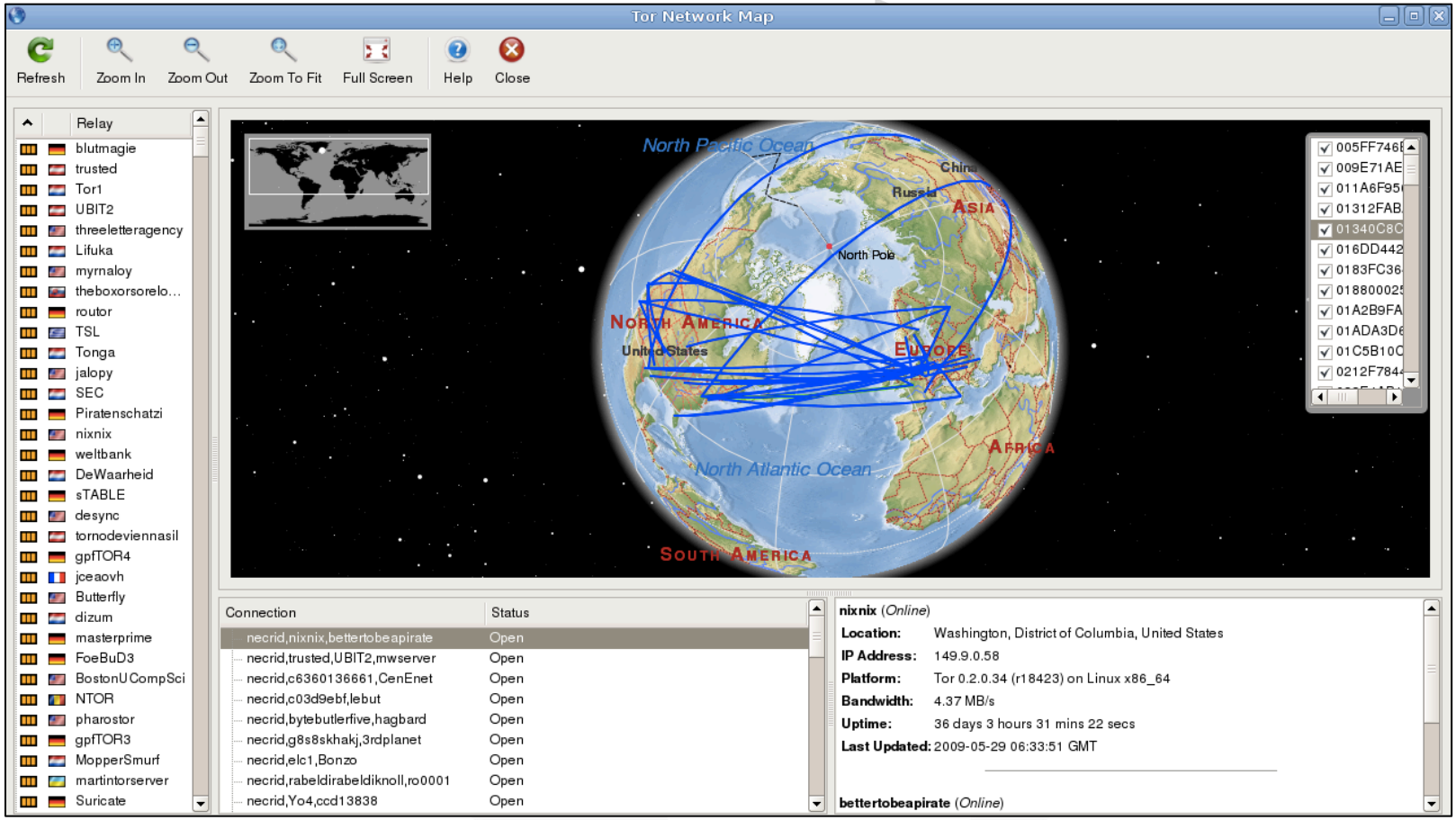
- *Continued:*
  - Hiring of hit men
  - Human-trafficking
  - Malware distribution
  - Botnet control and sale
  - DDoS services
  - Hide from law enforcement
  - Attacker communications
  - Posting of stolen hacktivist information
  - Etc….

What is Tor?

What is Tor?

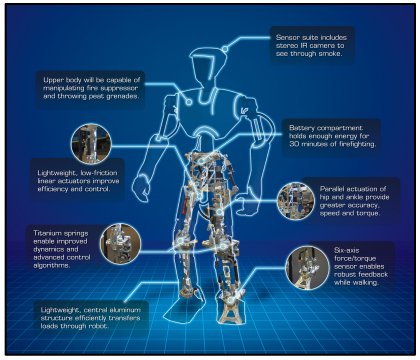
- Most popular method of accessing the dark web
- Tor is a *network of virtual tunnels* that provide anonymous browsing using a layered encryption system called "onion routing"
  - Takes the original data and encrypts and re-encrypts it several times before it reaches its final destination

What is Tor?

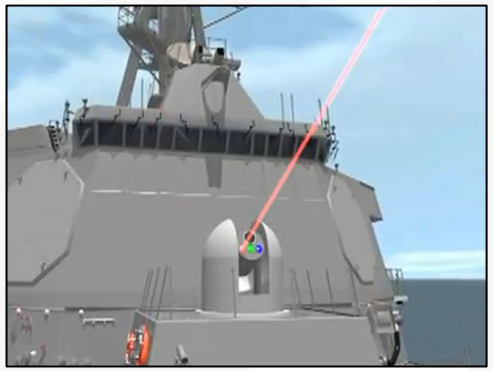


Tor Network Map

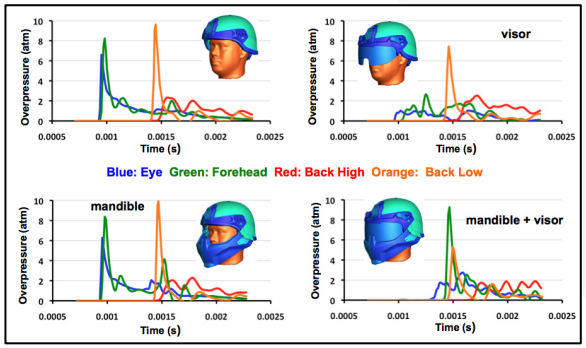
What is Tor?



Firefighting Robots



Laser Weapons



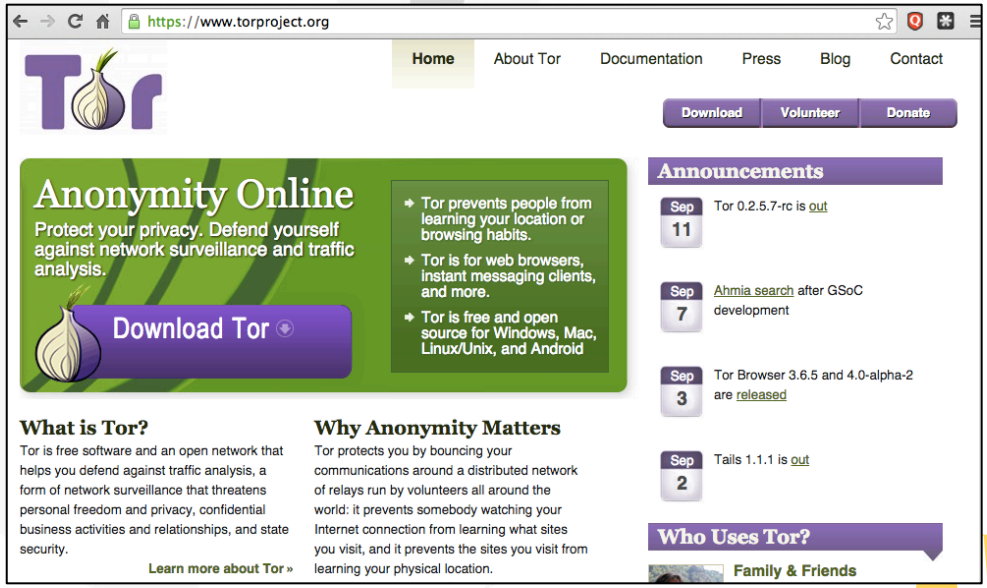
IED Blast Wave Research

- Developed in the mid-1990s by U.S. Naval Research Laboratory (NRL) with the purpose of protecting U.S. intelligence communications online

What is Tor?

- Although Tor was originally developed to protect government communications, it is now maintained and developed through a non-profit organization known as The Tor Project:

The Tor Project is a Massachusetts-based 501(c)(3) research-education nonprofit organization responsible for maintaining Tor



https://www.torproject.org/

What is Tor?

- In 2014, the following organizations have indicated their support for Tor by contributing financially:
  - SRI International
  - US Department of State Bureau of Democracy, Human Rights, and Labor
  - National Science Foundation joint with Georgia Tech and Princeton University
  - Radio Free Asia
  - The Ford Foundation
  - Google Summer of Code

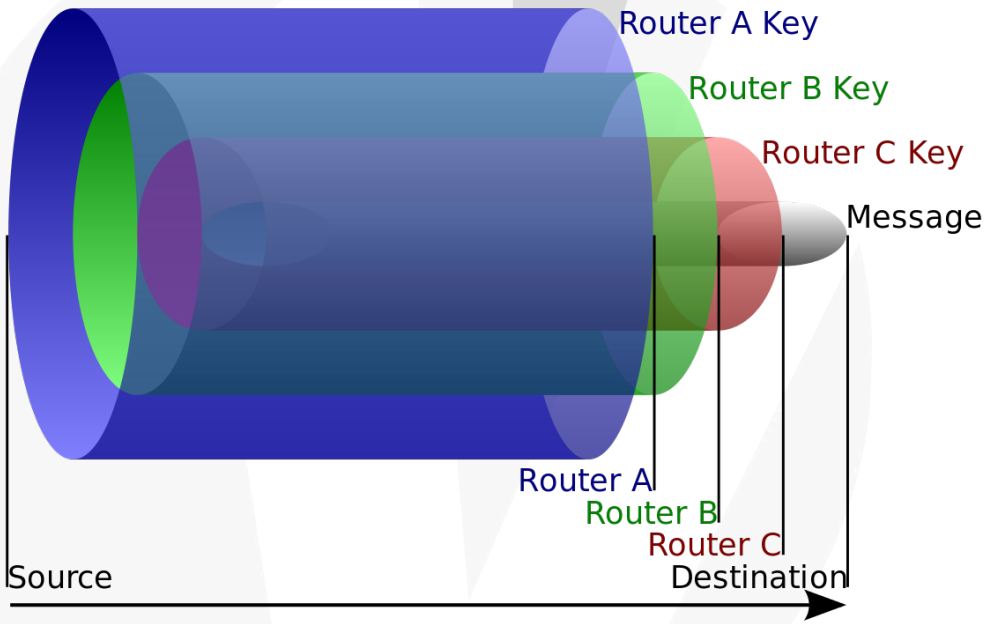
ATG

Tor's Foundation: Onion Routing

- The core principle behind Tor is the concept of onion routing
  - An onion is formed by wrapping the original message with successive layers of encryption
  - Each layer can be decrypted like the layer of an onion by one intermediary in a succession of intermediaries, with the original plaintext message only viewable by:
    - Sender
    - Exit node
    - Recipient

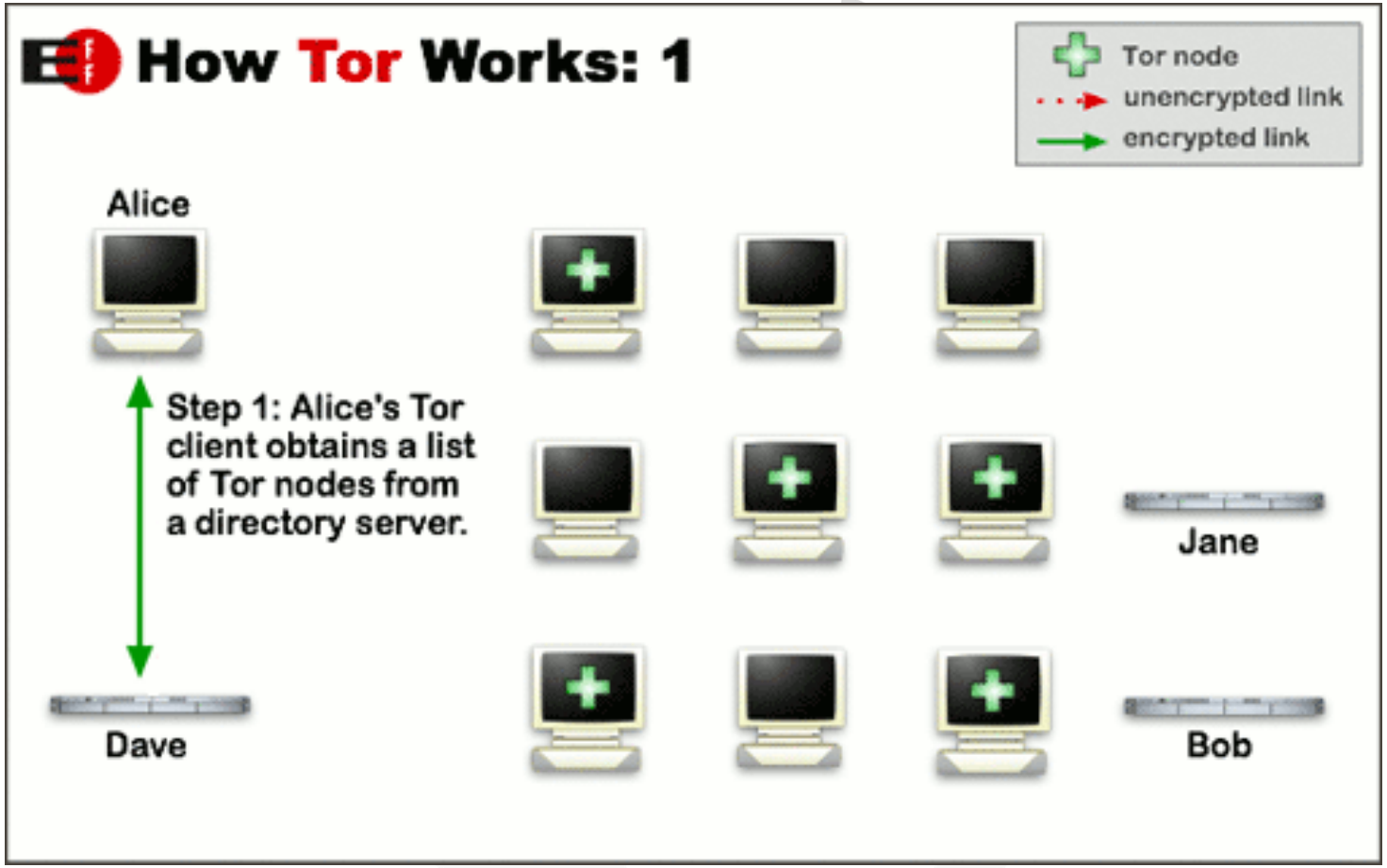
Tor's Foundation: Onion Routing

Example Onion:



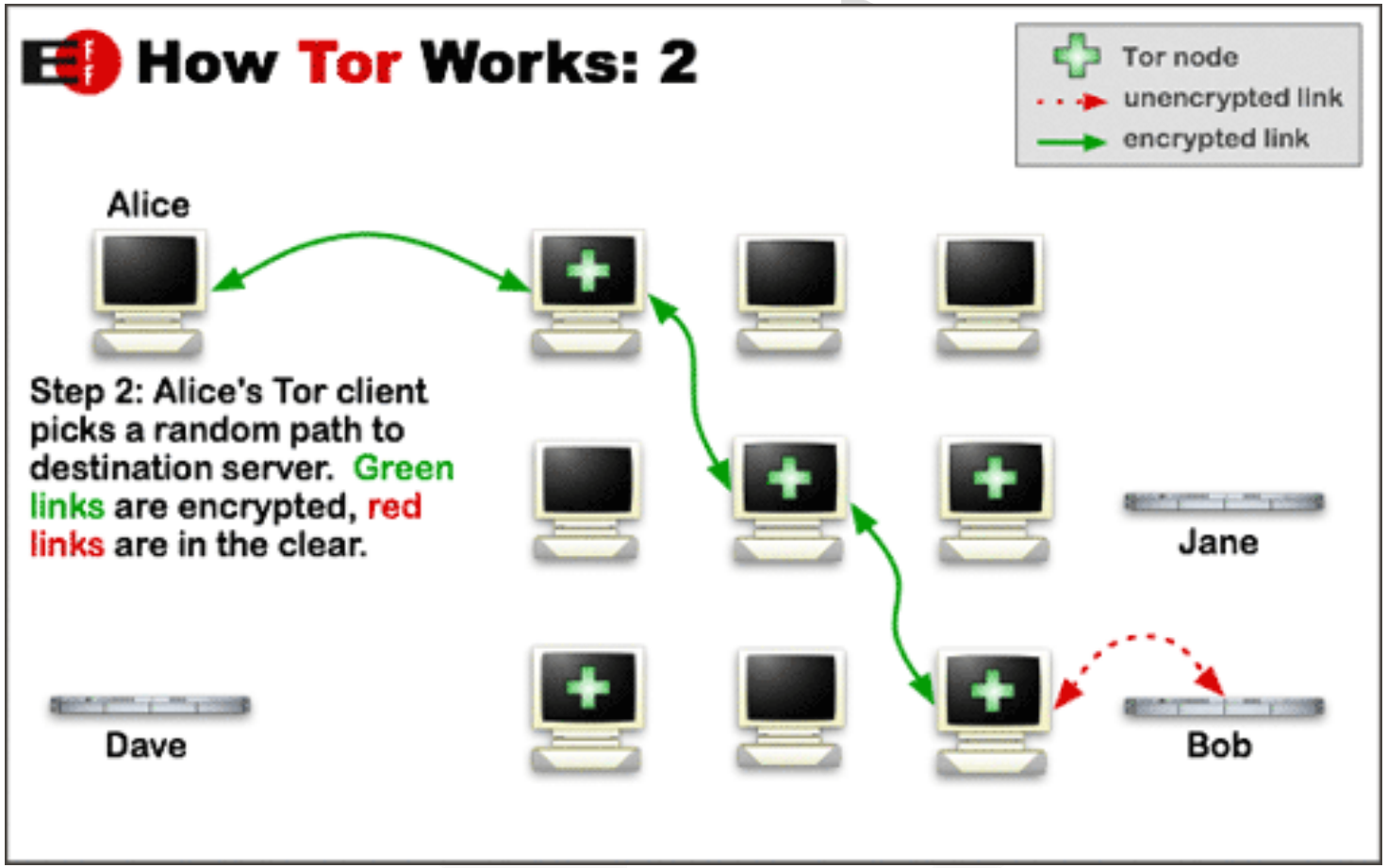
Source: http://en.wikipedia.org/wiki/Onion_routing

Tor's Foundation: Onion Routing

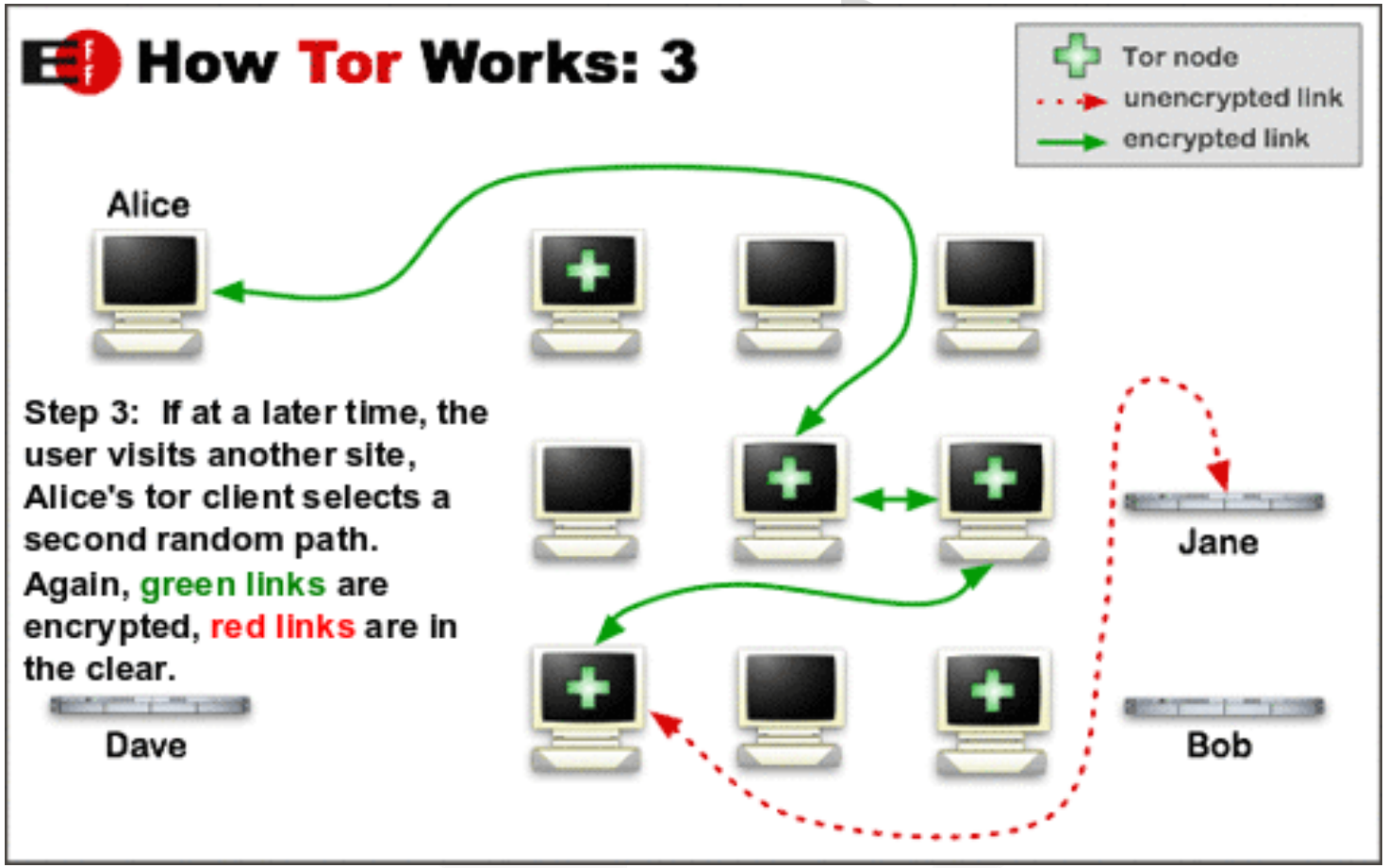


Source: https://www.torproject.org/about/overview.html.en#thesolution

Tor's Foundation: Onion Routing



Tor's Foundation: Onion Routing



Tor Relays

- Tor supports three different types of relays:

1. Middle Relays
   - Add to the speed and robustness of the network without making the owner of the relay look like the source of the traffic
   - Advertise their presence to the rest of the Tor network so that any Tor user can connect to them
2. Bridges
   - Not publicly listed as part of the Tor network.
   - Provide the ability to circumvent censorship in countries that regularly block the IP addresses of all publicly listed Tor relays (ie, China)

ATG

Tor Relays

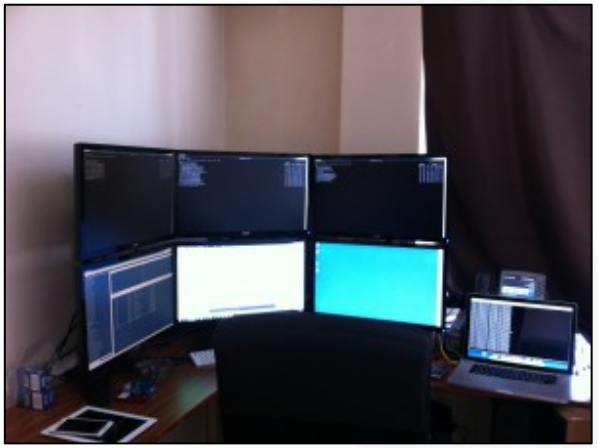
3. Exit Relays
   - Final relay that data passes through before it reaches its destination
   - Advertise their presence to the entire Tor network so that others can connect to them
   - Since this is where all the traffic exits, it also could be determined as the source
     - There is a possibility that if any illegal information is obtained through an exit relay, the owner of the relay might be blamed. Really! Don’t believe me…?

ATG

Tor Relays

One man's blog post title:
(http://raided4tor.cryto.net)

RAIDED FOR OPERATING
A TOR EXIT NODE



Before Raid

After Raid

Tor's Primary Services

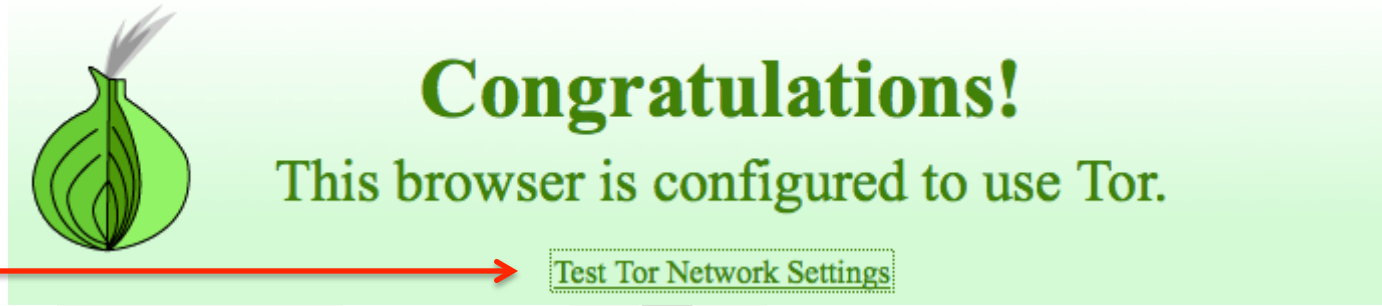
- The two primary services that Tor provides are:

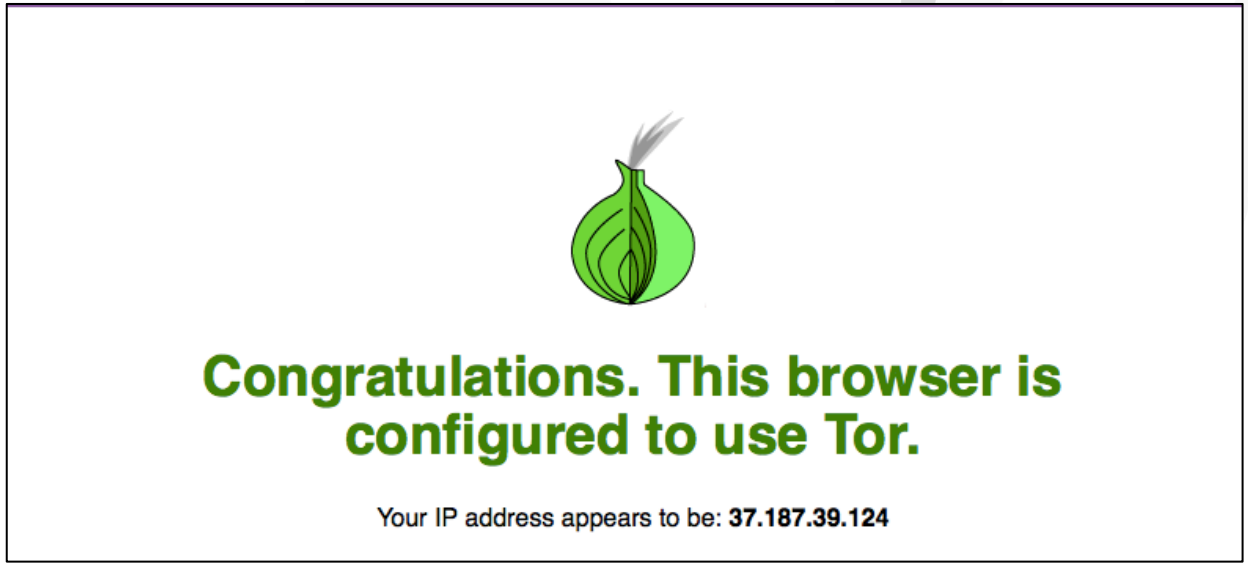
  1. Anonymity

  2. Hidden Services

Tor and Anonymity

Confirming on Tor Network:





Tor and Anonymity

IP Address via Chrome:

Your IP Address Is:
216.4.249.66

Your IP Details:

ISP: XO Communications
Services: Confirmed Proxy Server
Country: United States

Don't want this known? Hide your IP details

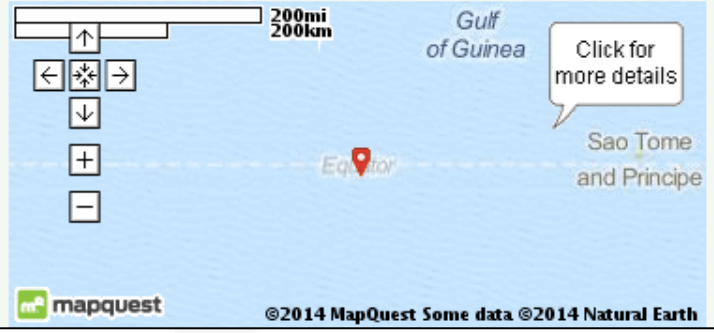
IP Address via TorBrowser:

Your IP Address Is:
94.242.255.236

Your IP Details:

ISP: root SA
Services: Confirmed Proxy Server
Recently report forum spam source.
Country: Anonymous Proxy

Don't want this known? Hide your IP details



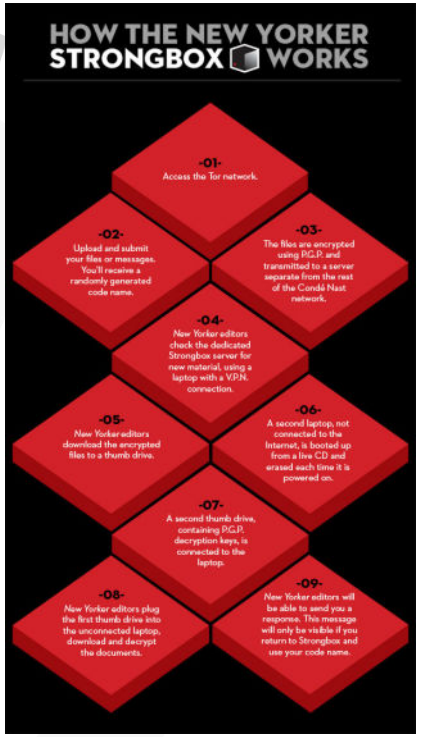
Tor and Anonymity

- According to the ip2location.com website, the IP address 94.242.255.236 is located in Luxembourg:

IP Address	94.242.255.236
Location	LUXEMBOURG, LUXEMBOURG, STEINSEL
Latitude & Longitude	49.676940, 6.123890 (49°40'37"N 6°7'26"E)
ISP	ROOT SA
Local Time	26 Sep, 2014 06:51 PM (UTC +02:00)
Domain	ROOT.LU
Net Speed	(COMP) Company/T1
IDD & Area Code	(352) 026
ZIP Code	L-7349
Weather Station	LUXEMBOURG (LUXX0003)
Mobile Country Code (MCC)	-
Mobile Network Code (MNC)	-
Carrier Name	-
Elevation	243m
Usage Type	(DCH) Data Center/Web Hosting/Transit
Anonymous Proxy	No
Shortcut	http://www.ip2location.com/94.242.255.236

Tor's Hidden Services

- Tor's onion-routing technology enables the creation of hidden services, websites that can hide their identity from its users and are only accessible via Tor
- In May 2013, *The New Yorker* magazine launched a Tor-hidden service so whistleblowers can securely leave documents or messages



StrongBox site was by Aaron Swartz and Kevin Poulsen

The TorBrowser

- Preconfigured web browser based on Firefox
  - Most recent stable version is 3.6.6 (32 and 64-bit)
  - Can access both Tor and non-Tor sites
  - Multi-platform (OSes, Android, etc.)
  - Can run off of a flash drive
  - Has many features related to more secure browsing

Tor and Traffic Analysis

- Traffic analysis is a technique that intercepts and examines traffic in order to deduce information from communication patterns
  - Because it analyzes communication patterns, it can be performed when when the messages are encrypted
- Tor is supposed to protect against traffic analysis because it hides the source and destination of your Internet traffic

argas Advanced Technologies Group, Inc.
Keeping You Connected To Technology

Detecting Tor

Detecting Tor

- If have local access, look for the application
- Difficult to detect by observing network traffic because uses TLS (v1):

107	2.267706	198.27.97.223	10.0.0.126	TLSv1	803	Server Hello, Certificate, Server Key Exchange, Server Hello Done
125	2.281025	66.18.12.197	10.0.0.126	TLSv1	994	Server Hello, Certificate, Server Key Exchange, Server Hello Done
141	2.320225	212.83.140.45	10.0.0.126	TLSv1	801	Server Hello, Certificate, Server Key Exchange, Server Hello Done
143	2.320285	64.62.249.222	10.0.0.126	TLSv1	788	Server Hello, Certificate, Server Key Exchange, Server Hello Done
175	2.349662	31.7.186.228	10.0.0.126	TLSv1	809	Server Hello, Certificate, Server Key Exchange, Server Hello Done
184	2.366189	82.96.35.8	10.0.0.126	TLSv1	802	Server Hello, Certificate, Server Key Exchange, Server Hello Done
186	2.366273	95.211.225.167	10.0.0.126	TLSv1	815	Server Hello, Certificate, Server Key Exchange, Server Hello Done
202	2.384445	88.159.20.120	10.0.0.126	TLSv1	1001	Server Hello, Certificate, Server Key Exchange, Server Hello Done
204	2.384602	212.83.158.5	10.0.0.126	TLSv1	807	Server Hello, Certificate, Server Key Exchange, Server Hello Done

Detecting Tor

- Look for nodes:

dan.ec

You're connected from 216.4.249.66 (via AS2828: XO Communications from , US) using a 128-bit SSL IPv4 connection.
Local (Bolton, UK) weather: 12.7°C - Humidity: 73% - Wind: 3.1mph W - Rain: 0.3mm - Forecast: Settled fine

Navigation

- Index
- Login
- About Me (Dan)
- Amateur Radio 2E0NNX
- BGP Looking Glass
- BGP Lookup Tool
- Blog (Tech Hints & Tips)
- DNS Blacklists (dnsbl)
- DNS Server Info
- Filter List Generator
- IP Information Tool
- IP Subnet Calculator

TOR Node List

This page contains a full TOR nodelist (no more than 30 minutes old) in the format below.
There are tags of __BEGIN_TOR_NODE_LIST__ and __END_TOR_NODE_LIST__ for easy scripting use of this page.

You can also fetch https://www.dan.me.uk/torlist/ for a list of ips only, one per line - updated every 30 minutes. Ideal for constructing your own tor banlists.

<ip>|<name>|<router-port>|<directory-port>|<flags>|<uptime>|<version>|<contactinfo>

Total number of nodes is: 6298

100.0.120.66|FreeDomainRadio|34819|47216|FHRSDV|1058624|Tor 0.2.4.23|Matt <MellowMatt (AA-TT) gmx.com>
100.0.180.181|FuckPRISM|9001|9030|FGHRSDV|1805567|Tor 0.2.3.25|sorry@noway.com
100.0.67.218|crowcastletor|9001|9030|FGHRSDVX|9674479|Tor 0.2.5.4-alpha|net.crowcastle@pc-toradmin [reversed]
100.1.94.104|default|443|9030|FHRDV|248583|Tor 0.2.4.23|
100.33.8.35|IgniteTOR|443|9030|FGHRSDV|402721|Tor 0.2.4.23|TORInfo@itc-productions.com
100.37.110.51|Unnamed|9002|9031|FGHRSDV|2100171|Tor 0.2.4.22|
100.38.78.246|magalien|443|80|FHRSDV|194590|Tor 0.2.4.23|
101.142.101.111|Unnamed|9001|0|FRSV|209681|Tor 0.2.4.23|
101.142.37.250|Unnamed|9001|9030|FRDV|226798|Tor 0.2.4.23|
101.99.64.150|sumatra|9001|0|EFRSV|5263158|Tor 0.2.4.22|
103.10.197.50|loki3|443|80|EFHRSDV|3354155|Tor 0.2.4.23|abuse<__aT>icetor{_DoT===}is -

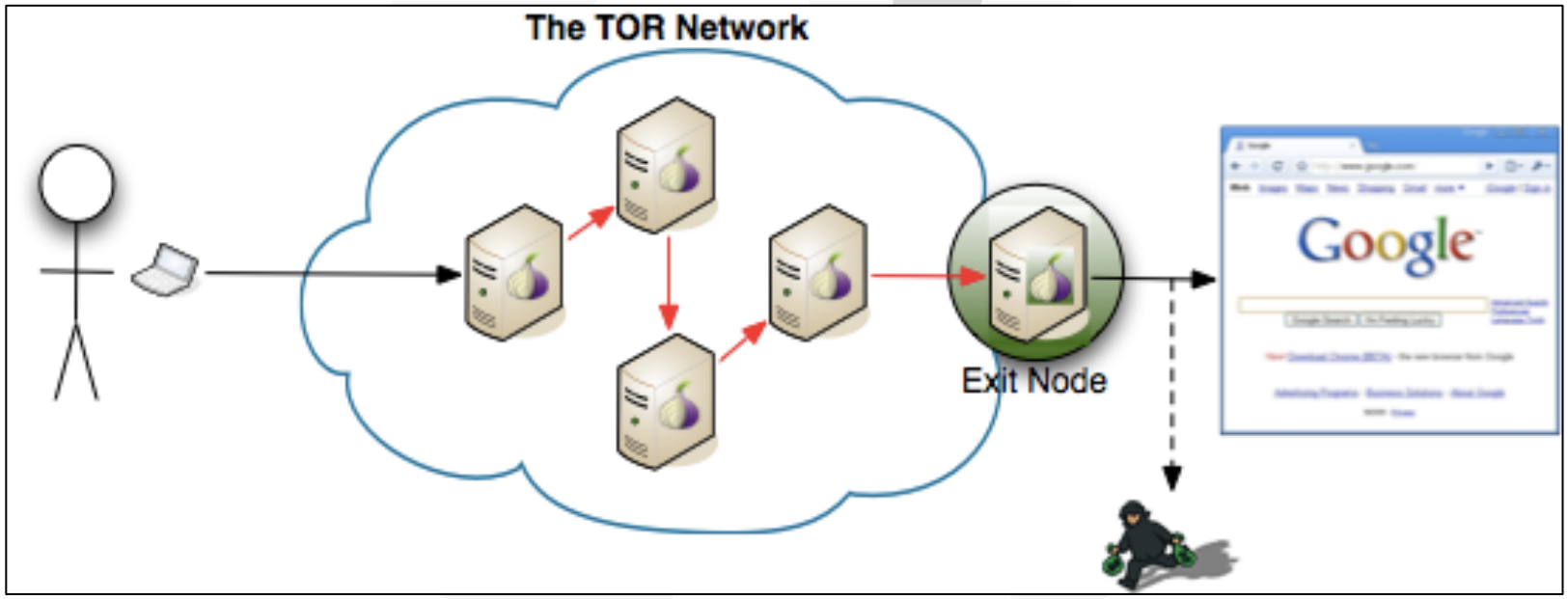
ATG

argas Advanced Technologies Group, Inc.
Keeping You Connected To Technology

The Exit Node Problem

The Exit Node Problem

- Main vulnerability right now is people masquerading as exit nodes



argas Advanced Technologies Group, Inc.
Keeping You Connected To Technology

Chinks in the Armor - Tor Attacks and Takedowns

Chinks in the Armor – Tor Attacks and Takedowns

- In 2007, Metasploit creator H.D. Moore attacked Tor
  - Set up a series of fake nodes that did the opposite of what a real Tor node would do -- they looked at traffic that was passing through and did some tricks to tag that traffic and follow it back to its source
  - The people using Tor could be identified

Exploitation

By *admin*
Created *03/20/2007 - 11:06pm*

Testing the limits of vulnerability

› annalee@techsploitation.com [1]

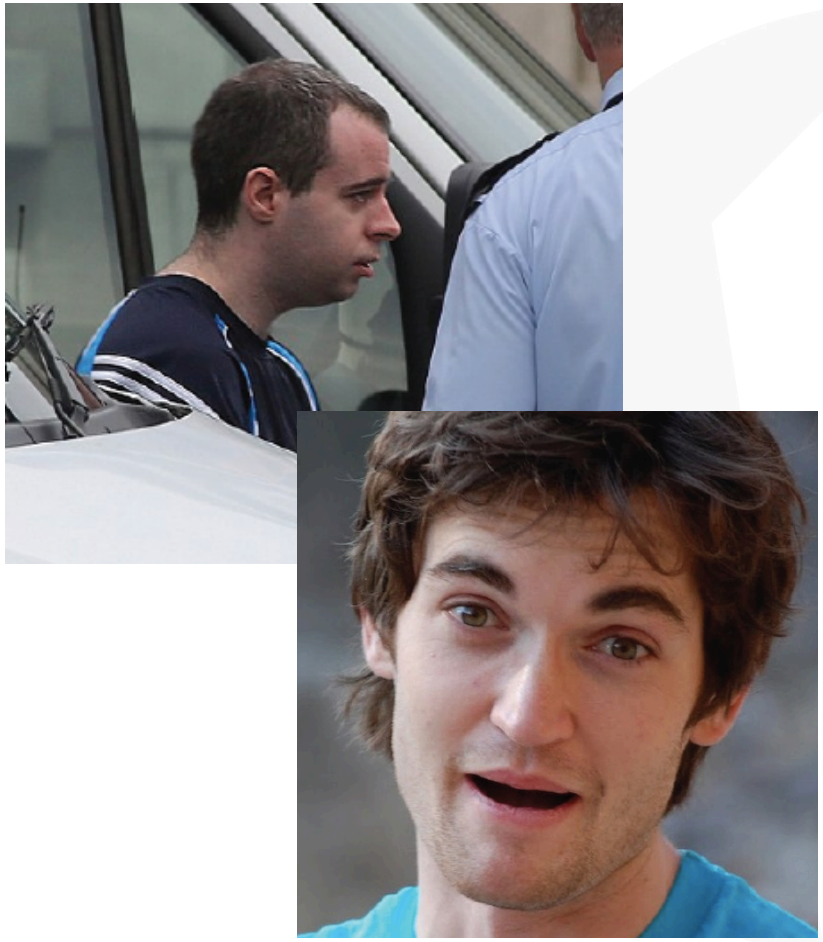
TECHSPLOITATION Among hackers, exploitation is a social good. Exploiting a piece of software means discovering a little chink in its armor, a vulnerability that could allow a crook to slip through and do unwanted things to innocent people's computers. Researchers write an exploit — a little program that takes advantage of the vulnerability — and then show it to everybody involved so that the vulnerability can be patched up.

But things are not always so tidy, and a case in point
researcher named HD Moore. He publicized a vulner
facilitates anonymous Web surfing and online publish
journalists, and people who just want additional priva
special network of protected servers run by thousand

To run his exploit, dubbed Torment, Moore set up a s
opposite of what a real Tor node would do: they looke
and did some tricks to tag that traffic and follow it bac
Tor could be identified. Like many exploits, Torment
misconfigured Tor. So anyone who has faithfully follo
is still safe — but of course, even the most anal-reten
when installing and configuring software.

Moore has said that he decided to launch this attack
pornographers are using the anonymous network to
than that. Via e-mail, he told me, "If anything, I want
warning for anyone who believes their Web traffic is

Chinks in the Armor – Tor Attacks and Takedowns



- 2013 August: FBI Tor Takedown of Child Pornographer Eric Marques (Freedom Hosting)
- 2013 October: FBI Takedown of The Silk Road (and Ross William Ulbricht/Dread Pirate Roberts)

Chinks in the Armor – Tor Attacks and Takedowns

- 2014 July: Black Hat presentation on Tor suddenly cancelled because of vulnerabilities that were going to be disclosed
- 2014 July: Russian Ministry of Internal Affairs (MVD) offered prize money totaling nearly four million rubles ($114,000) to anyone who could find a way to identify normally Tor users

ATG

argas Advanced Technologies Group, Inc.
Keeping You Connected To Technology

Does Tor Have a Future?

Does Tor Have a Future?

vs.

Questions?

ATG

Thank You!

David Vargas, MS, CISSP, CISM, CEH(v7)
President, VATG Inc. (dvargas@vatg.com)
and
Professorial Lecturer, High Technology Crime Investigation Program, The George Washington University (dvargas@gwu.edu - *preferred*)