Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization

A. Biryukov, I. Pustogarov, R.P. Weinmann
University of Luxembourg
Ivan.pustogarov@uni.lu

May 20, 2013
Overview

- Background
- Measuring the popularity of hidden services
- DoSing hidden services.
- Harvesting onion addresses.
- Revealing the guards.
- Opportunistic deanonymisation.
Overview

- **Background**
- Measuring the popularity of hidden services
- DoSing hidden services.
- Harvesting onion addresses.
- Revealing the guards.
- Opportunistic deanonymisation.
Tor anonymity network

Client Anonymity

Alice

Bob
Server Anonymity

Tor anonymity network

Alice → R1 → R2 → R3 → R4 → R5 → Bob
## Consensus

<table>
<thead>
<tr>
<th>Node</th>
<th>Score</th>
<th>Port</th>
<th>IP Address/Host Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>menTor</td>
<td>1737</td>
<td>55863896.cust.multi.fi [85.134.56.150]</td>
<td></td>
</tr>
<tr>
<td>microshaft</td>
<td>2820</td>
<td>tor-exit.microshaft.org [208.201.249.3]</td>
<td></td>
</tr>
<tr>
<td>minisausage</td>
<td>3348</td>
<td>50.7.184.58 [50.7.184.58]</td>
<td></td>
</tr>
<tr>
<td>morphium</td>
<td>298</td>
<td>this.is.a.Tor.server.please see.tor.morphium.info [91.143.90.25]</td>
<td></td>
</tr>
<tr>
<td>NetromAc</td>
<td>2115</td>
<td>1385160742.business.dbnet.dk [82.143.224.38]</td>
<td></td>
</tr>
<tr>
<td>Nitr0x</td>
<td>175</td>
<td>50.97.1.36-static.reverse.softlayer.com [50.97.1.36]</td>
<td></td>
</tr>
<tr>
<td>OhCanada</td>
<td>419</td>
<td>van1.zworg.com [209.17.191.117]</td>
<td></td>
</tr>
<tr>
<td>onconnett80</td>
<td>392</td>
<td>tor01.onconnett.com [184.105.231.11]</td>
<td></td>
</tr>
<tr>
<td>PasToutAFaitNet1</td>
<td>261</td>
<td>91.229.20.159 [91.229.20.159]</td>
<td></td>
</tr>
<tr>
<td>PasToutAFaitNet2</td>
<td>763</td>
<td>tor2.pastoutafait.net [95.130.11.247]</td>
<td></td>
</tr>
<tr>
<td>plebia</td>
<td>3599</td>
<td>tor-exit.plebia.org [37.59.162.218]</td>
<td></td>
</tr>
<tr>
<td>pps</td>
<td>9</td>
<td>184-22-164-107.static.hostnoc.net [184.22.164.107]</td>
<td></td>
</tr>
<tr>
<td>PrivaT0Reu</td>
<td>4229</td>
<td>torexit.privator.eu [88.208.90.1]</td>
<td></td>
</tr>
<tr>
<td>programmercpp</td>
<td>149</td>
<td>proxy [213.171.220.40]</td>
<td></td>
</tr>
<tr>
<td>PsyNetNP</td>
<td>155</td>
<td>broadband-95-84-148-164.nationalcablenetworks.ru [95.84.148.164]</td>
<td></td>
</tr>
<tr>
<td>Qwerty</td>
<td>91</td>
<td>93.167.245.178 [93.167.245.178]</td>
<td></td>
</tr>
</tbody>
</table>

http://torstatus.blutmagie.de/
Guards

Guard = high uptime + high bandwidth

Every client has 3 Guard nodes
Guards

Guard = high uptime + high bandwidth

Every client has 3 Guard nodes
Guard = high uptime + high bandwidth

Every client has 3 Guard nodes
Examples of Tor HS

Public Library of US Diplomacy: Kissinger Cables
2013-04-08

The Kissinger Cables are part of today’s launch of the WikiLeaks Public Library of US Diplomacy (PlusD), which holds the world’s largest searchable collection of United States confidential, or formerly confidential, diplomatic communications. As of its launch on April 8, 2013 it holds 2 million records comprising approximately 1 billion words.

Detainee Policies
2012-10-24

WikiLeaks has begun releasing the 'Detainee Policies': more than 100 classified or otherwise restricted files from the United States Department of Defense covering the rules and procedures for detainees in U.S. military custody. Over the next month, WikiLeaks will release in chronological order the United States’ military detention policies followed for more than a
Examples of Tor HS

Duck Duck Go is a search engine based in Valley Forge, Pennsylvania that uses information from crowd-sourced sites (like Wikipedia) with the aim of augmenting traditional results and improving relevance.

More at Wikipedia | Official site: duckduckgo.com

DuckDuckGo | BEGIN-DOWNLOAD.com
Free Download flv app Fast & Simple.
begin-download.com

DuckDuckGo | CrunchBase Profile
DuckDuckGo is a search engine, like Google. Use it to get more Zero-click Info, more privacy, less spam, !bang syntax and lots of other goodies.
crunchbase.com/company/duck-duck-go

DuckDuckGo Challenges Google on Privacy (With a Billboard) | Wired Business...
DuckDuckGo, a one-man band search engine based out of Valley Forge, Pennsylvania, is aiming at Google’s privacy practices with an unusual tactic: a billboard.
wired.com/business/2011/01/duckduckgo-google-privacy/
Examples of Tor HS

THE NEW YORKER

STRONGBOX

SECURELY SUBMIT FILES TO WRITERS AND EDITORS

You can use this site to submit information, messages, and files to writers and editors at The New Yorker.

GET STARTED
Load times may vary.
Examples of Tor HS

Silk Road

Shop by Category

Food 5
- Beverages 2
- Apparel 168
- Art 4
- Books 865
- Collectibles 8
- Computer equipment 30
- Custom Orders 47
- Digital goods 365
- Drug paraphernalia 174
- Drugs 4,217
- Electronics 37
- Erotica 389
- Forgeries 92
- Hardware 3
- Herbs & Supplements 14
- Home & Garden 3
- Jewelry 32
- Lab Supplies 29
- Lotteries & games 30
- Medical 31
- Money 100
- Packaging 25
- Services 37
- Weight loss 19
- Writing 2
- Yubikeys 3

sort by: bestselling
- Domestic only
- update

Cocaine Energy Drink - Banned
- seller: namedeclined(100)
- ships from: United States of America
- $0.74
- add to cart

Kefir grains - water kefir
- seller: etizolam(97)
- ships from: United States of America
- $0.83
- add to cart

3Jane Stealth Listing Feedback
- no image
- seller: 3Jane(100)
- ships from: Canada
- $0.00
- add to cart

Kefir grains - milk kefir
- seller: etizolam(97)
- ships from: United States of America
- $0.90
- add to cart

Security Editor

You can use this

GET STARTED
Load times may vary.
Examples of Tor HS

Skynet, a Tor-powered botnet straight from Reddit

Posted by Claudio Guarnieri in Information Security on Dec 6, 2012 2:51:13 PM

Wandering through the dark alleys of the Internet we encountered an unusual malware artifact, something that was a night.

The more we spent time looking at it, the more it started to look unusually familiar. As a matter of fact it turned out be origin named “throwaway236236” described in a very popular / Am A thread you can read here.

This is an overview of this malware labelled by the creator as Skynet: a Tor-powered trojan with DDoS, Bitcoin mining, and Usenet.

Were the warez

"People download software from Usenet and install it in the offices or at friends pretty often. Also Usenet isn’t the most hosting. Most Providers have their own Usenet client for idiot proof downloads”
**Tor rendezvous protocol**

**Step 1:** Bob picks some introduction points and builds circuits to them.
Step 2: Bob advertises his hidden service – <z>.onion – at the database.
Tor rendezvous protocol

**Step 3:** Alice requests introduction points from the database. She also sets up a rendezvous point.
**Step 4:** Alice sends a message to Bob listing the rendezvous point and asks the introduction points from to deliver it.
**Step 5:** Alice and Bob
Connect at the Rendezvous point
Tor rendezvous protocol

Alice

RP

IP1

IP2

IP3

Bob

HSDir Storage
Responsible hidden service directories

HSDir Storage

IDs+

= HSDir = 25 hours of uptime

Hash(\text{\text{\textkey}} + \text{\textclock} + \text{Secret} + (0|1) )
Responsible hidden service directories

\[\text{Hash(} \text{Key} + \text{Time} + \text{Secret} + (0|1) \text{)}\]

\(= \text{HSDir} = 25 \text{ hours of uptime}\)
Responsible hidden service directories

- IDs change every 24 hours at some time during the day
- Re-upload every hour
Overview

- Background
- **Measuring the popularity of hidden services**
- **DoSing hidden services.**
- Harvesting onion addresses.
- Revealing the guards.
- Opportunistic deanonymisation.
Impersonating Hidden service directory

HSDir = 25 hours of uptime

Bob

IDS+
Impersonating Hidden service directory

HSDir = 25 hours of uptime

Bob

IDS+
Impersonating Hidden service directory

Bob

IDS+

HSDir

Storage

= HSDir = 25 hours of uptime
Impersonating Hidden service directory

- By impersonating 1 directory, we can track the popularity
- By impersonating all 6 directories, we can DoS.

![Graph showing distance between HS directories fingerprints over time, with annotations for 1 second and ~20 seconds.](image-url)
Tracking popularity

- We tracked popularity of Skynet C&C, Silkroad, and DuckDuckGo
Overview

- Background
- Measuring the popularity of hidden services
- DoSing hidden services.
- **Harvesting onion addresses.**
- Revealing the guards.
- Opportunistic deanonymisation.
Shadowing

- Active
- Shadow

158.64.76.40

Consensus

 Authorities
Shadowing

- Active
- Shadow

Authorities

Internal database

158.64.76.40

Consensus
Shadowing

- Active
- Shadow

Consensus

Authorities

Internal database
Shadowing

- Active
- Shadow

 Authorities
 Internal database

158.64.76.40

Consensus

...
Collecting onion addresses

- Active
- Shadow
Collecting onion addresses

- Active
- Shadow

• Naive approach will require ~350 IP addresses.
Collecting onion addresses

- Active
- Shadow

- Naive approach will require \(~350\) IP addresses.
- Descriptors don't relocate within 24 hours.
- Prepare shadow HSDir relays and gradually pull to consensus.
Collecting onion addresses

- Active
- Shadow

- Naive approach will require ~350 IP addresses.
- Descriptors don't relocate within 24 hours.
- Prepare shadow HSDir relays and gradually pull to consensus.

158.64.76.40
Collecting onion addresses

- Active
- Shadow

- Naive approach will require ~350 IP addresses.
- Descriptors don't relocate within 24 hours.
- Prepare shadow HSDir relays and gradually pull to consensus.
Collecting onion addresses

- Active
- Shadow

- Naive approach will require ~350 IP addresses.
- Descriptors don't relocate within 24 hours.
- Prepare shadow HSDir relays and gradually pull to consensus.

158.64.76.40
Harvest results

• We used 58 IP addresses from Amazon EC2 and spent 57 USD

• We collected 39824 unique onion addresses in 49 hours (on hidden wikis one can find ~2500 addresses only)

• Some interesting note: 12 onion addresses in the form silkroad*****.onion.
Overview

- Background
- Measuring the popularity of hidden services
- DoSing hidden services.
- Harvesting onion addresses.
- Revealing the guards.
- Opportunistic deanonymisation.
Revealing Guard Nodes
Revealing Guard Nodes
Revealing Guard Nodes

Eve

RP

Guard

Eve's Node

Traffic Signature

Bob
Revealing Guard Nodes

Eve's Node

Eve

RP

Guard

Traffic Signature

Bob
Revealing Guard Nodes

~40 minutes to reveal the guard nodes for a 5Mb/s node
Opportunistic deanonymisation
Opportunistic deanonymisation

How long does it take to become a Guard of a hidden service?
Opportunistic deanonymisation

- Rent a server for 60 USD per month => 0.6% probability to be chosen as a Guard.
- Deanonymisation \(\sim 150\) hidden services per month (for \(60\) USD per month)
- By running 23 such servers, the probability to deanonymize any long-running hidden service within 8 months is 99%. (\(~11,000\) USD total).
Side effect (flag assignment)

- Large number of shadow relays with bw <= 1 accelerated flag assignment.

Number of relays with relay flags assigned

The Tor Project - https://metrics.torproject.org/
# Conclusions

<table>
<thead>
<tr>
<th>Tracking</th>
<th>□ 150 addresses per month (60 USD) □ Any HS (8 months+11000 USD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denial of Service</td>
<td>□</td>
</tr>
<tr>
<td>Collecting onion addresses</td>
<td>□</td>
</tr>
<tr>
<td>Revealing Guard Nodes</td>
<td>□</td>
</tr>
<tr>
<td>Deanonymisation</td>
<td>• 150 addresses per month (60 USD) • Any HS (8 months+11000 USD)</td>
</tr>
</tbody>
</table>
Support slide 1

• Triggered
  – #8243: Getting the HSDir flag should require more effort
  – #8243: Getting the HSDir flag should require more effort

• Related
  – Changing of the Guards: A Framework for Understanding and Improving Entry Guard Selection in Tor", WPES 2012
  – #8240: Raise our guard rotation period
    (patch to raise it to 9.5 month still pending)
Support slide 2

• Not included into the presentation
  – Finding guard nodes using topological properties
  – Bandwidth inflation