

# DROPPING DOCS ON DARKNETS: HOW PEOPLE GOT CAUGHT

Adrian Crenshaw



# About Adrian

- ❑ I run Irlongeek.com
- ❑ I have an interest in InfoSec education
- ❑ I don't know everything - I'm just a geek with time on my hands
- ❑ Sr. Information Security Consultant at TrustedSec

Twitter: @Irlongeek\_ADC



- ❑ Co-Founder of Derbycon  
<http://www.derbycon.com>



# Perspective and General Warnings

- ❑ I will be taking two perspectives
  - People trying to stay anonymous
  - People trying to de-anonymize users
- ❑ I'm not really a privacy guy
- ❑ IANAL
- ❑ Be careful where you surf, contraband awaits



# BASICS OF HOW TOR WORKS



TrustedSec

<http://Irongeek.com>

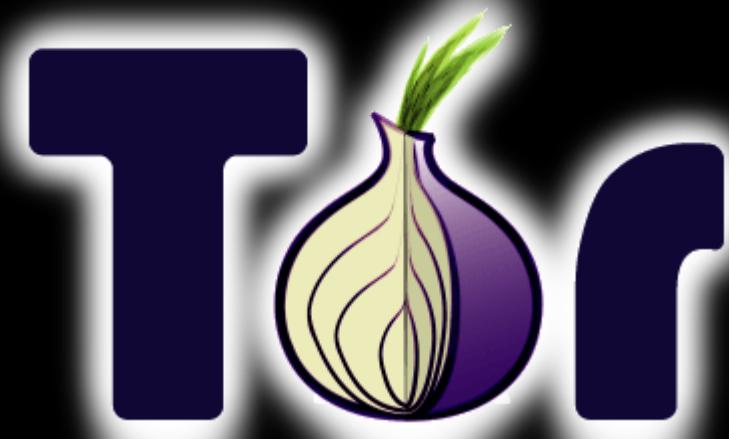


# A little background...

## Darknets

- ❑ There are many definitions, but mine is “anonymizing private network”
- ❑ Use of encryption and proxies (some times other peers) to obfuscate who is communicating to whom
- ❑ Sometimes referred to as Cipherspace (love that term)





The Onion Router



# Overview

## □ Who?

First the US Naval Research Laboratory, then the EFF and now the Tor Project (501c3 non-profit).

<http://www.torproject.org/>

## □ Why?

“Tor is free software and an open network that helps you defend against a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security known as traffic analysis.” ~ As defined by their site

## □ What?

Access normal Internet sites anonymously, and Tor hidden services.

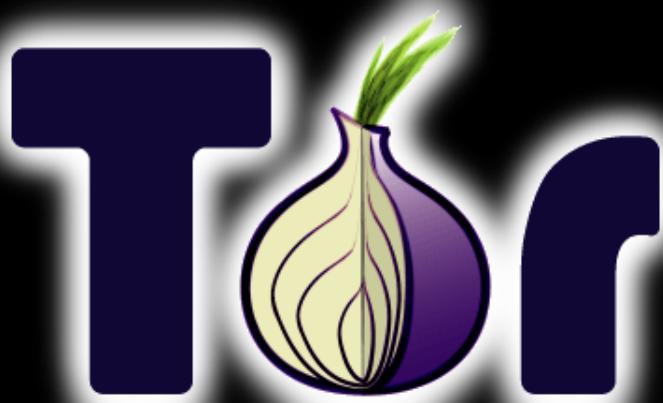
## □ How?

Locally run SOCKS proxy that connects to the Tor network.



# Tor: The Onion Router

- ❑ Layered encryption
- ❑ Bi-directional tunnels
- ❑ Has directory servers
- ❑ Mostly focused on out proxying to the Internet
- ❑ More info at <https://www.torproject.org>



Directory Server



Internet Server

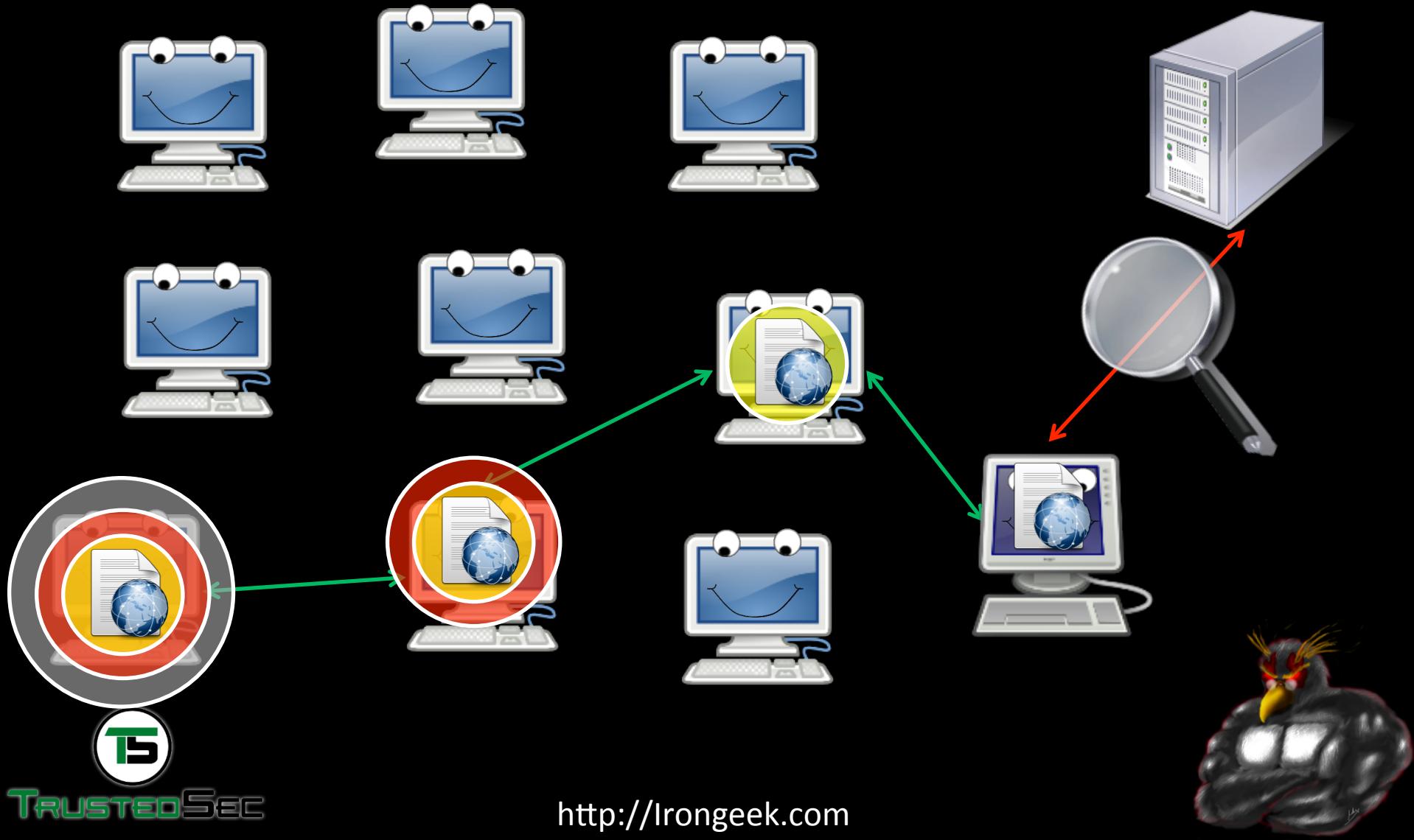
<http://Irongeek.com>



TRUSTEDSEC



# Layers like an Ogre



# Layout to connect to Hidden Service

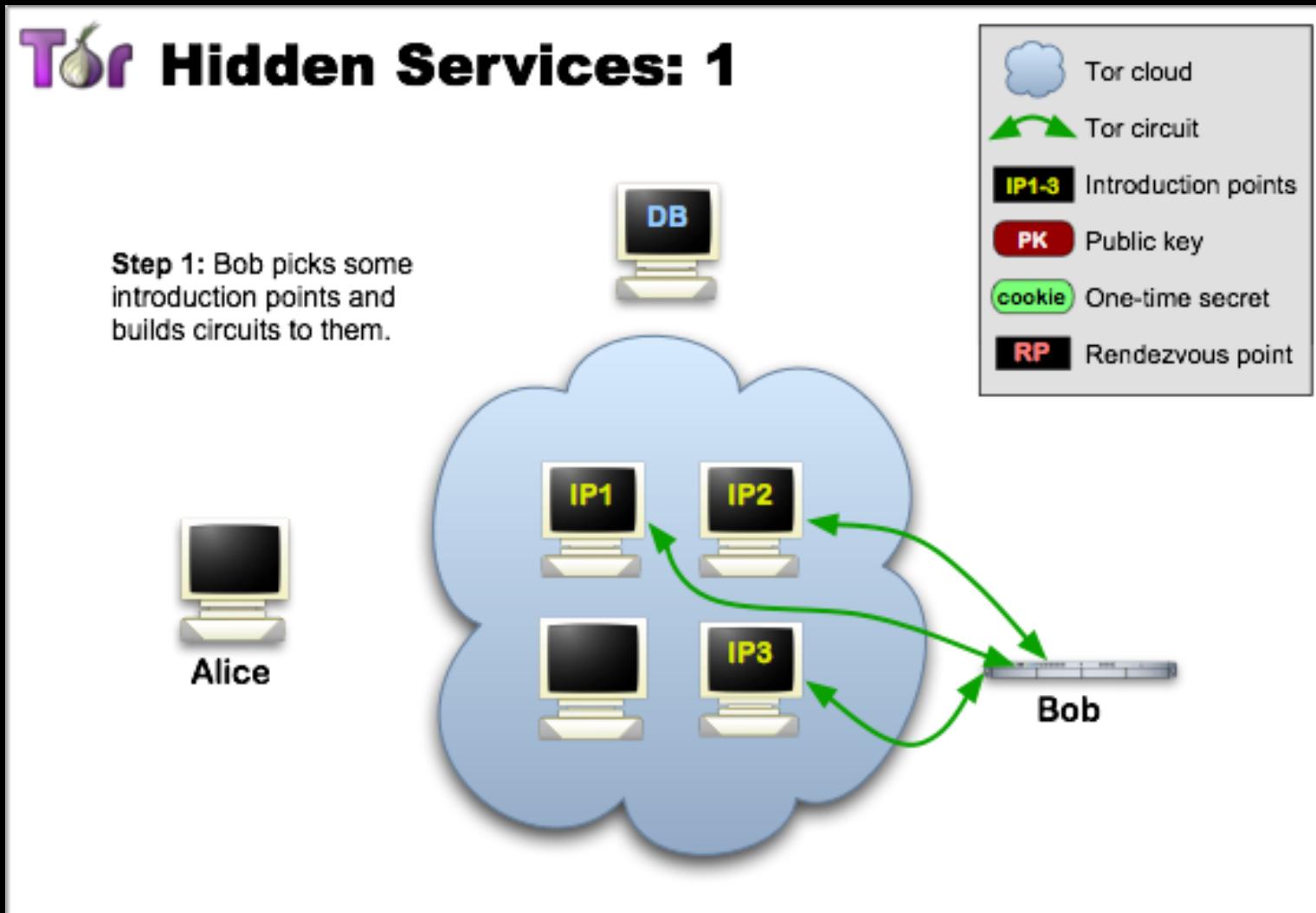


Image from <http://www.torproject.org/hidden-services.html.en>  
<http://Irongeek.com>



# Layout to connect to Hidden Service

## Tor Hidden Services: 2

Step 2: Bob advertises his hidden service -- XYZ.onion -- at the database.



Alice

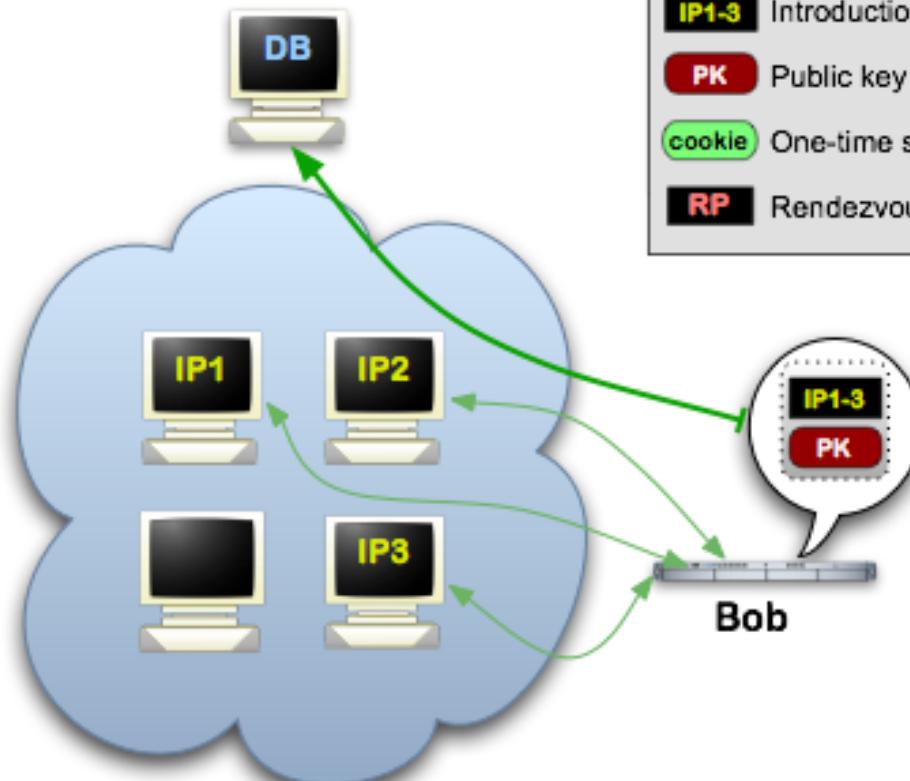


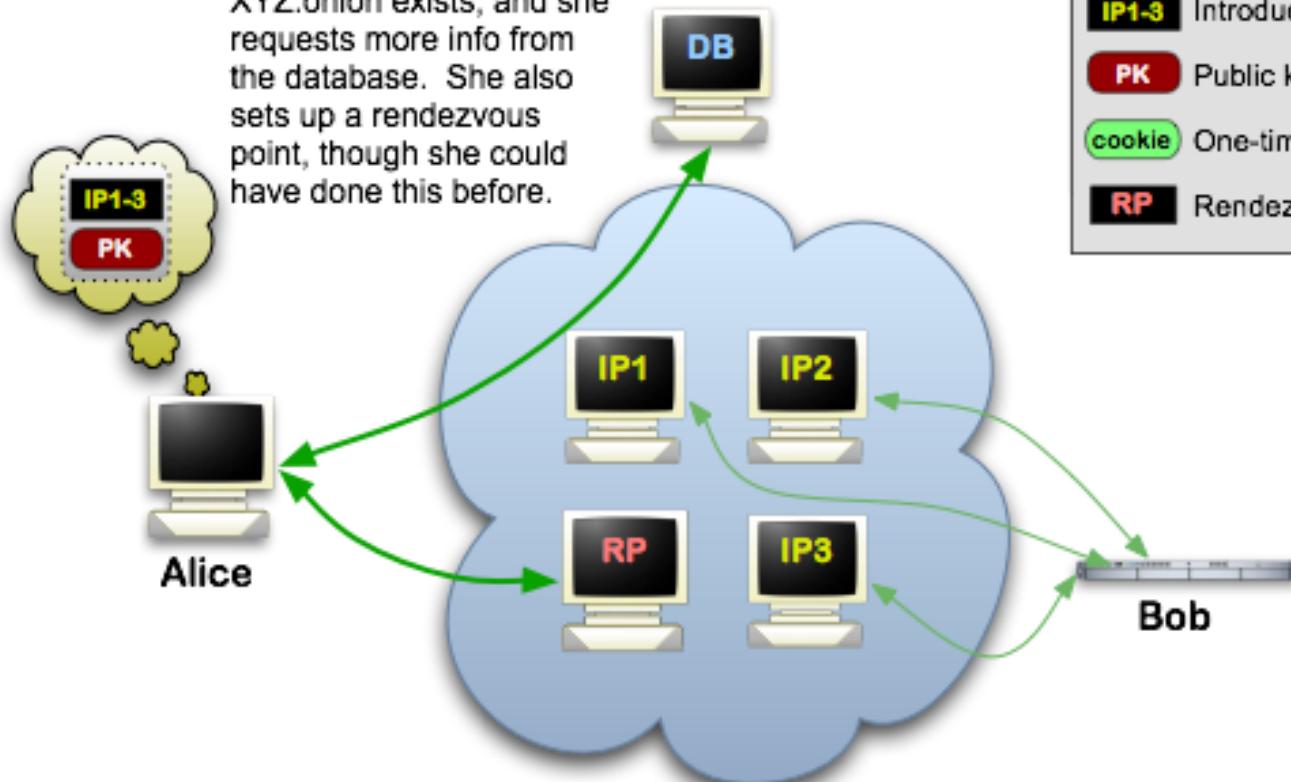
Image from <http://www.torproject.org/hidden-services.html.en>  
<http://Irongeek.com>



# Layout to connect to Hidden Service

## Tor Hidden Services: 3

Step 3: Alice hears that XYZ.onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.



	Tor cloud
	Tor circuit
	IP1-3 Introduction points
	PK Public key
	cookie One-time secret
	RP Rendezvous point



# Layout to connect to Hidden Service

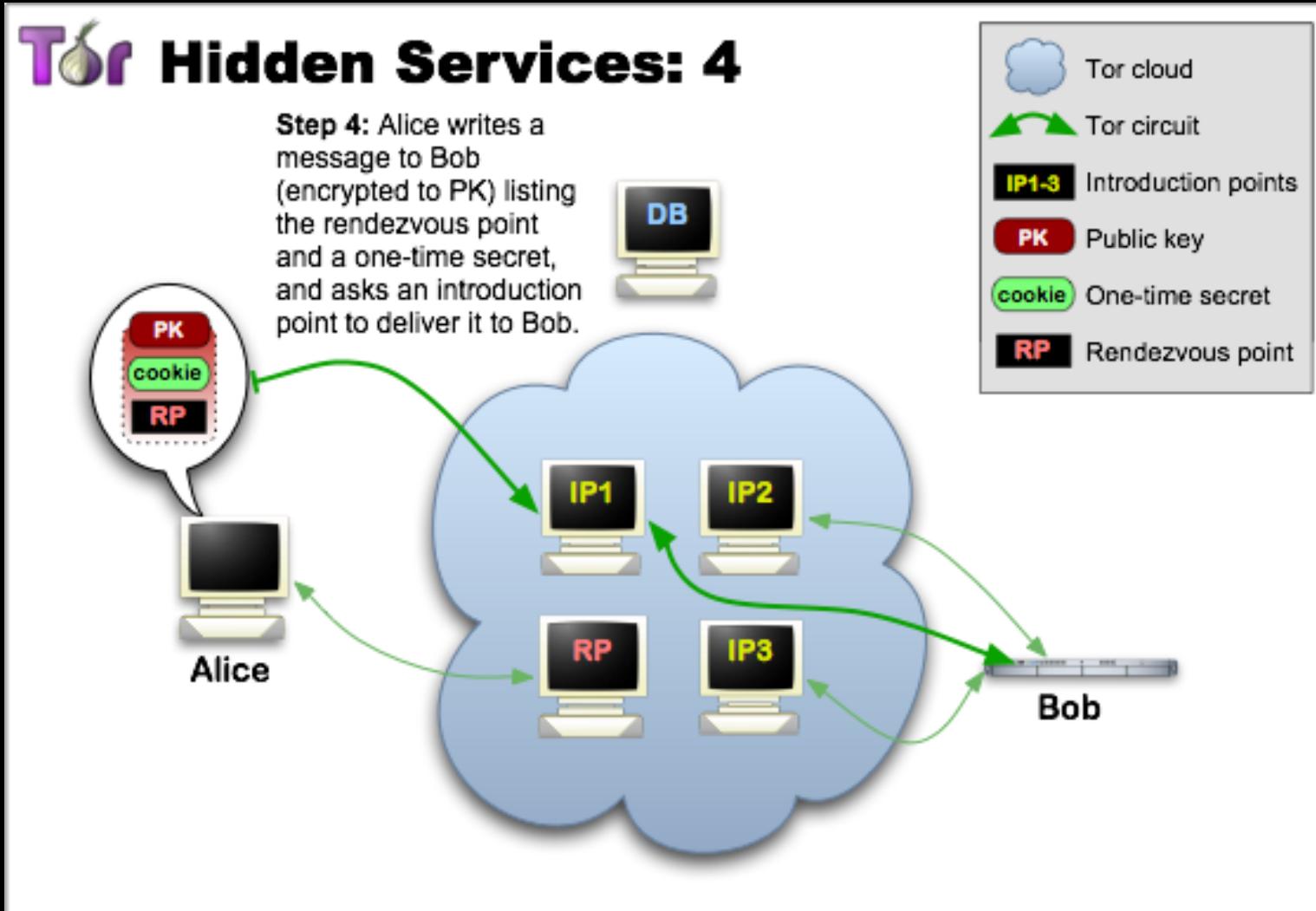


Image from <http://www.torproject.org/hidden-services.html.en>  
<http://Irongeek.com>



# Layout to connect to Hidden Service

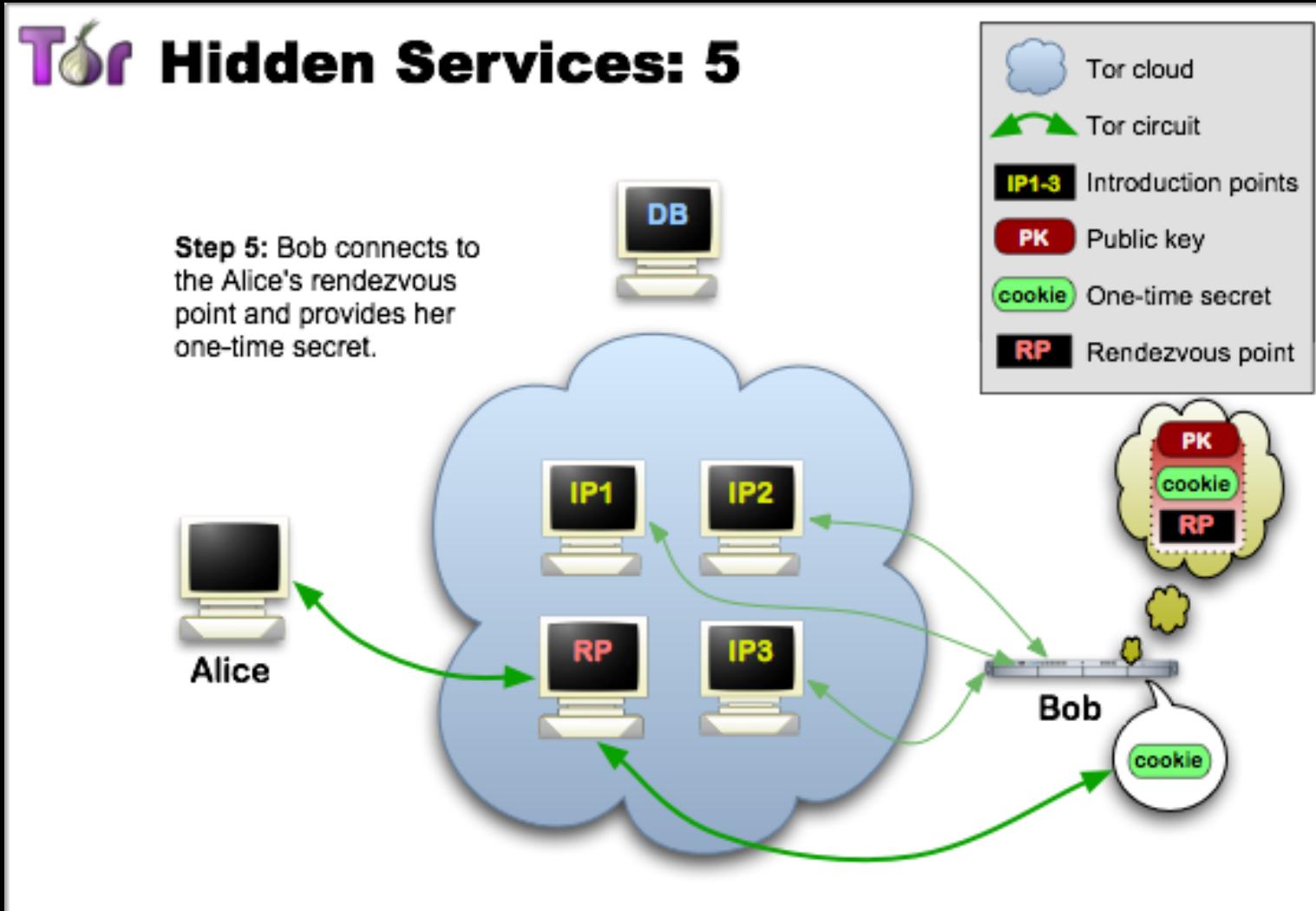


Image from <http://www.torproject.org/hidden-services.html.en>  
<http://Irongeek.com>



# Layout to connect to Hidden Service

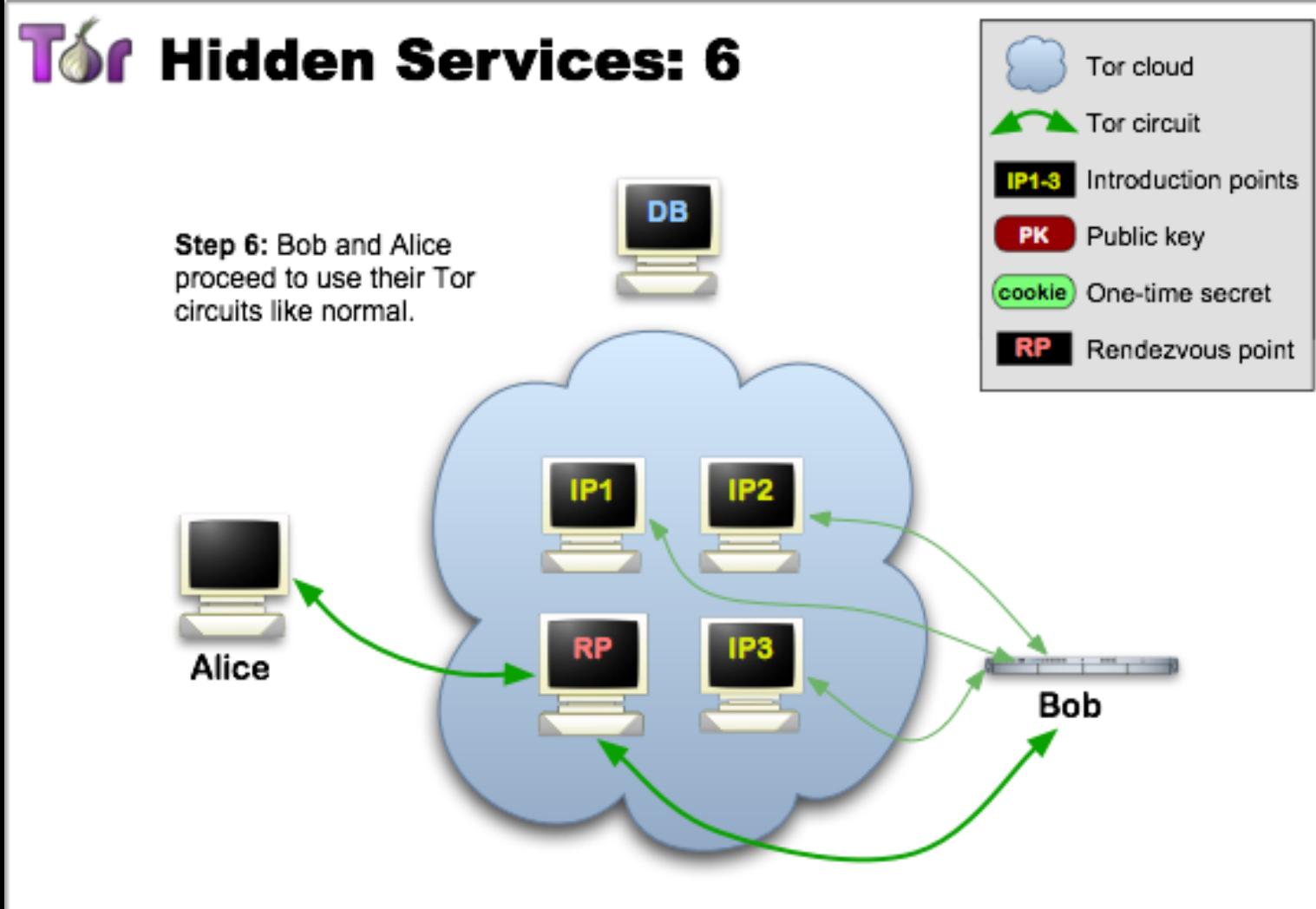


Image from <http://www.torproject.org/hidden-services.html.en>  
<http://Irongeek.com>

# Node types

- ❑ Client  
Just a user
- ❑ Relays  
These relay traffic, and can act as exit points
- ❑ Bridges  
Relays not advertised in the directory servers, so harder to block
- ❑ Guard Nodes  
Used to mitigate some traffic analysis attacks
- ❑ Introduction Points  
Helpers in making connections to hidden services
- ❑ Rendezvous Point  
Used for relaying/establishing connections to hidden services



# What does it look like to the user?

The image shows a screenshot of a computer desktop with two windows open. On the left is a TorBrowser window displaying the IronGeek.com homepage. The browser's status bar indicates it is connecting to www.irongeek.com. The page itself shows the IronGeek logo, a green onion icon, and a message encouraging users to include their content via RSS. A sidebar on the left includes links to InfoSec Daily, Root Secure.net, and DreamHost. The main content area features a large "irongeek.com" logo and a welcome message from Adrian Crenshaw. On the right is the Vidalia Control Panel, which shows a status window indicating "Connected to the Tor network!" and a "Vidalia Shortcuts" section with icons for Stop Tor, View the Network, Use a New Identity, Bandwidth Graph, Help, Message Log, Settings, and Exit. At the bottom of the control panel is a checkbox for "Show this window on startup" and a "Hide" button.

TorBrowser Connecting... www.irongeek.com

IronGeek.com 213.141.129.248  
Hello  
Tor User :)  
Amsterdam NL

Feel free to include my content in your page via my  
RSS feed irongeek.com

Irongeek Security Hacking Illustrated Videos InfoSec Articles Mobile Pen-testing Tools Apps/Scripts Reviews RSS Your IP Podcasts Contact Forums Workout Nutrition Supplements Humor Irongeek Campuses Fed Watch Books Store About

Search Irongeek.com:

Search

Affiliates:

InfoSec DAILY  
Root Secure.net  
REGISTER NOW  
irongeek.com

Welcome to Irongeek.com, Adrian Crenshaw's Information Security site (along with a bit about fancy). As I write articles and tutorials I will be posting them here. If you would like to republish one of the print journal please e-mail me. Enjoy the site and write us if you have any good ideas for articles or links

Adrian

News/Change Log:

[ShmooCon Firetalks 2014](#)  
These are the videos for the ShmooCon Firetalks 2014. Day 2 I overslept, but [Squidly1](#)  
[http://www.MediaArchives.tv/](#)

Vidalia Control Panel

Status: Connected to the Tor network!

Vidalia Shortcuts:

- Stop Tor
- View the Network
- Use a New Identity
- Bandwidth Graph
- Help
- Message Log
- Settings
- Exit

Show this window on startup  Hide

# Applications/Sites

- ❑ Tails: The Amnesic Incognito Live System  
<https://tails.boum.org/>
- ❑ Tor2Web Proxy  
<http://tor2web.org>
- ❑ Tor Hidden Wiki:  
<http://kpvt7ki2v5agwt35.onion>
- ❑ Scallion (make host names)  
<https://github.com/lachesis/scallion>
- ❑ Onion Cat  
<http://www.cypherpunk.at/onioncat/>
- ❑ Reddit Onions  
<http://www.reddit.com/r/onions>



# Tor Pros and Cons

## Pros

- ❑ If you can tunnel it through a SOCKS proxy, you can make just about any protocol work.
- ❑ Three levels of proxying, each node not knowing the one before last, makes things very anonymous.

## Cons

- ❑ Slow
- ❑ Do you trust your exit node?
- ❑ Semi-fixed Infrastructure:  
Sept 25th 2009, Great Firewall of China blocks 80% of Tor relays listed in the Directory, but all hail bridges!!!  
<https://blog.torproject.org/blog/tor-partially-blocked-china>  
<http://yro.slashdot.org/story/09/10/15/1910229/China-Strangles-Tor-Ahead-of-National-Day>
- ❑ Fairly easy to tell someone is using it from the server side  
<http://www.irongeek.com/i.php?page=security/detect-tor-exit-node-in-php>



# What does the traffic look like?

(Keep in mind, this is just the defaults)

- ❑ Local

- 9050/tcp Tor SOCKS proxy

- 9051/tcp Tor control port

- (9150 and 9151 on Tor Browser Bundle)

- ❑ Remote

- 443/tcp and 80/tcp mostly

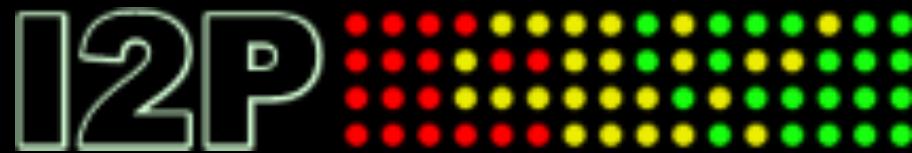
- Servers may also listen on port 9001/tcp, and directory information on 9030.

- ❑ More details

- <http://www.irongeek.com/i.php?page=security/detect-tor-exit-node-in-php>

- <http://www.room362.com/tor-the-yin-or-the-yang>





# SHOUT OUT TO I2P

<http://geti2p.net>



TRUSTEDSEC

<http://Irongeek.com>



# Bitcoin?

- ❑ Crypto Currency
- ❑ Proof of work
- ❑ Bitcoin Addresses & Private Keys
- ❑ Block Chain (ledger)
- ❑ Tumblers (laundering)
- ❑ Way more info by Bob Weiss

<http://www.irongeek.com/i.php?page=videos/bsidesde2013/2-6-hacking-benjamins-bob-weiss-pwcrack-into-to-bitcoin>



# Case 0: Harvard Bomb Threat

- On Dec. 16th 2013 a bomb threat was made to Harvard's student news paper and some officials.
- The person used <https://www.guerrillamail.com> to send email after shrapnel bombs placed in:  
science center  
sever hall  
emerson hall  
thayer hall  
2/4.  
guess correctly.  
be quick for they will go off soon
- Guerrilla Mail is a web-based email system that allows users to send and receive email without having to download or install any software. It is designed to be secure and easy to use. It also offers features such as spam filtering, virus scanning, and the ability to send attachments.



# Case 0: Harvard Bomb Threat

- All Tor nodes are publicly known (except bridges):  
<http://torstatus.blutmagie.de>
- Easy to correlate who was attached to Harvard network and using Tor at the same time the email was sent (unless you use a bridge).
- Eldo Kim was connected to the Tor network around that time.
- Suspect Eldo Kim wanted to get out of a final and admitted he made the bomb threat when interviewed.
- More Details:  
<http://arstechnica.com/security/2013/12/use-of-tor-helped-fbi-finger-bomb-hoax-suspect/>  
<http://www.scribd.com/doc/192371742/Kim-El-Do-Harvard>



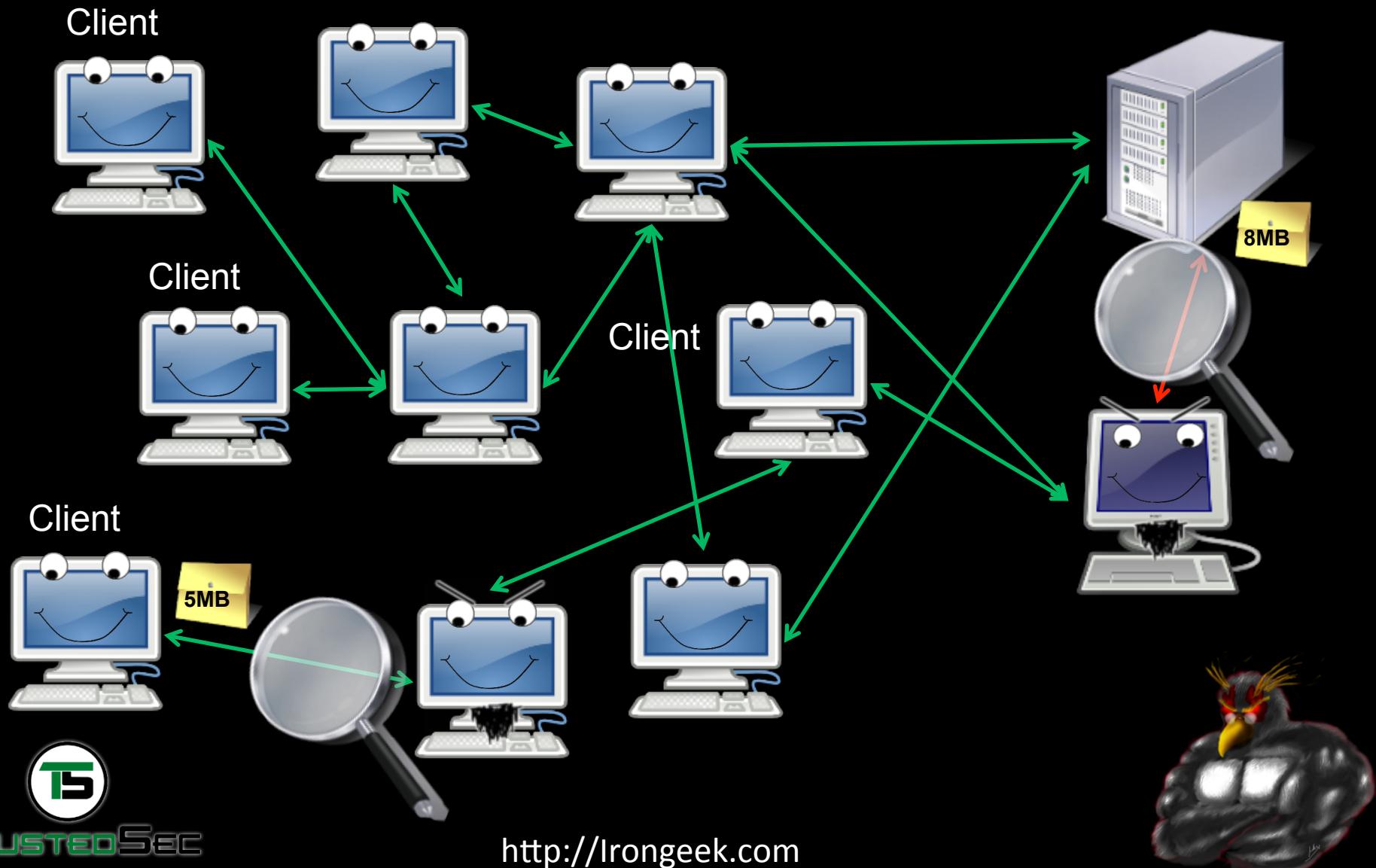
# Case 0: Harvard Bomb Threat

## Lessons Learned:

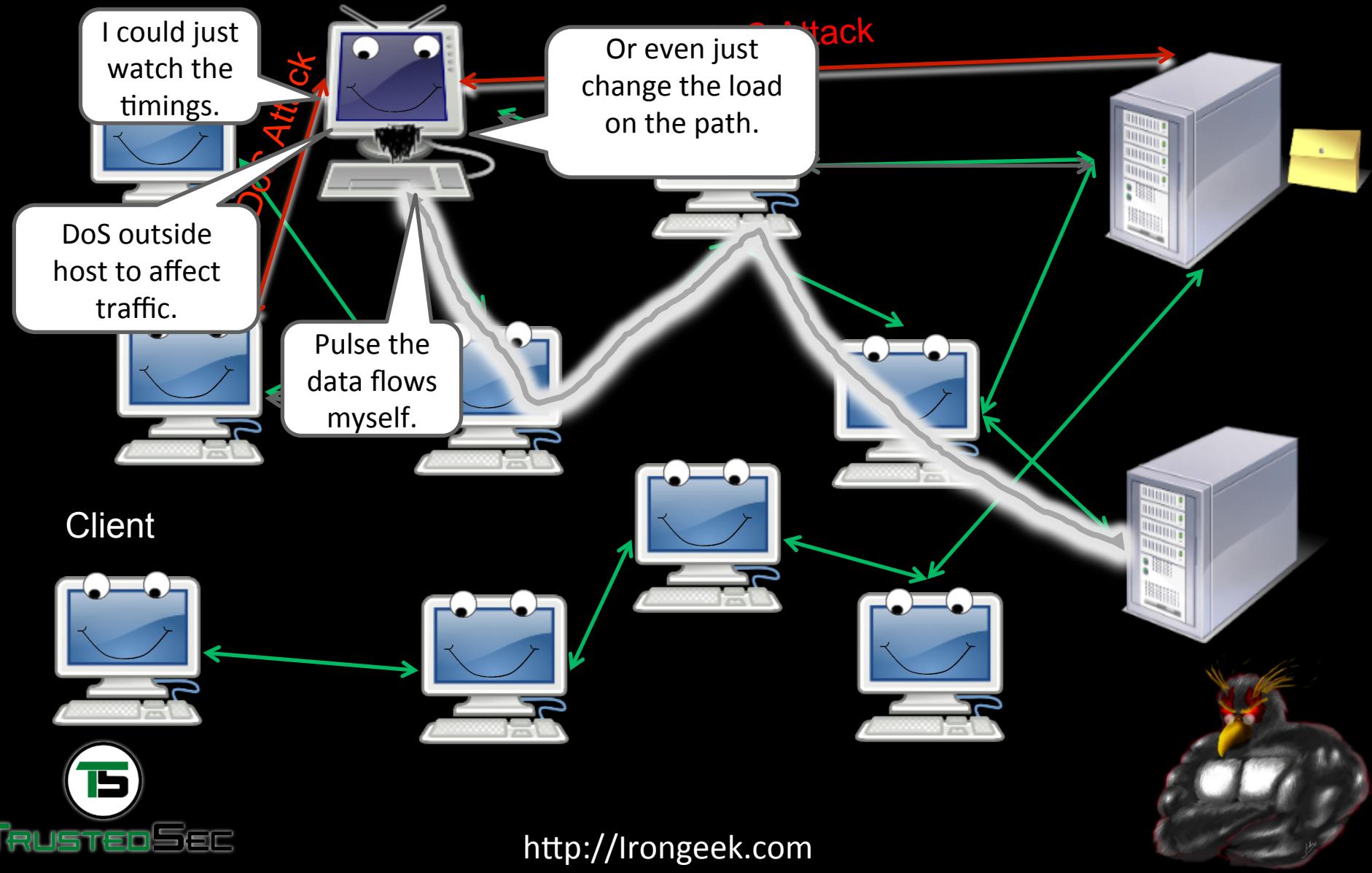
- ❑ Don't be the only person using Tor on a monitored network at a given time
- ❑ Use a bridge?
- ❑ Don't admit anything
- ❑ Correlation attacks are a bitch



# Correlation of end point and exit point

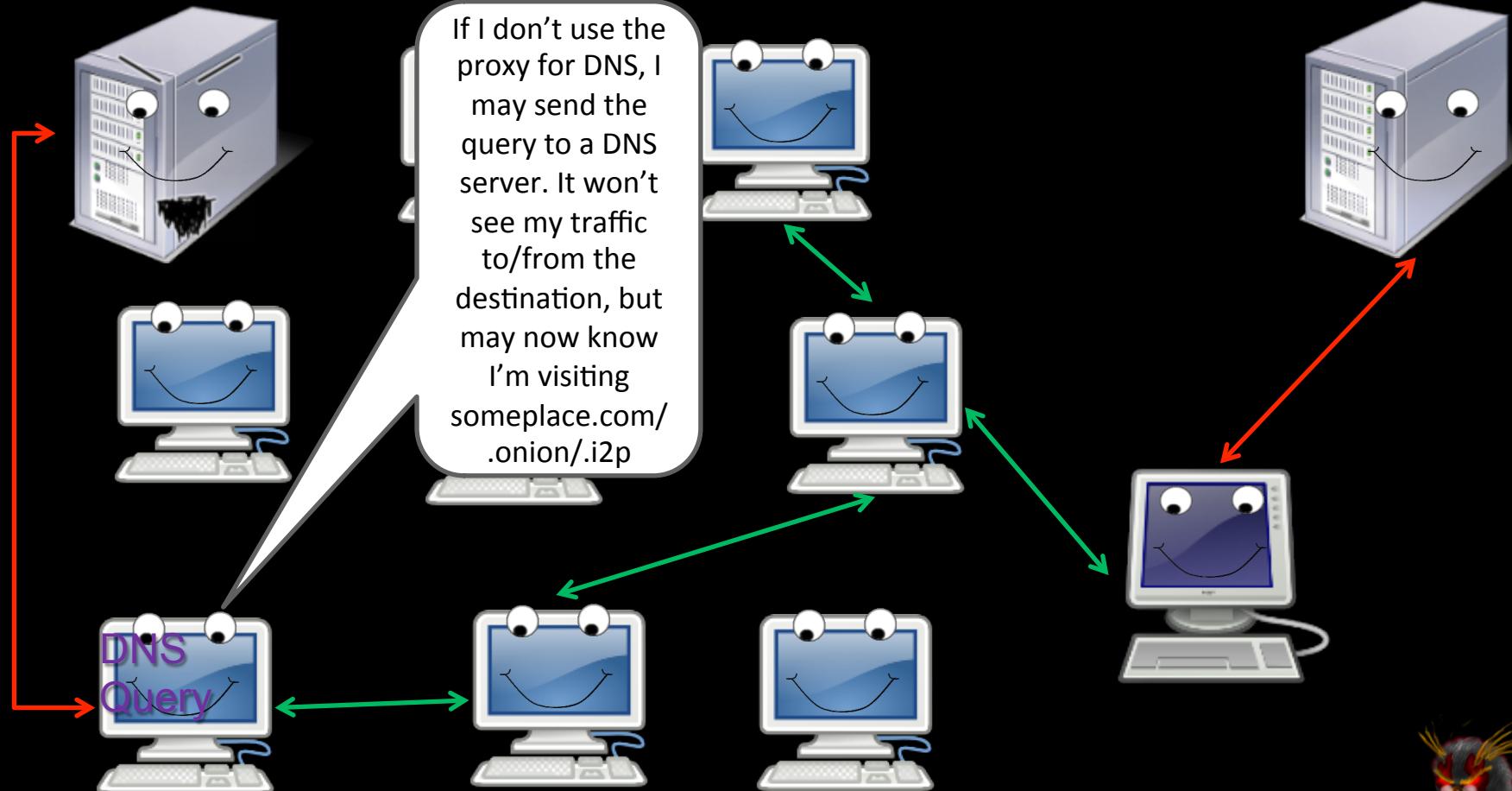


# Timing Correlation



# DNS Leaks

Monitored DNS Server



# Case 1: LulzSec

- ❑ Hector Xavier Monsegur (Sabu) normally used Tor for connecting to IRC but was caught not using it once and FBI found his home IP. After being caught, he started to collaborate.
- ❑ Hector spoke with Jeremy Hammond (sup\_g) on IRC, and Jeremy casually let slip where he had been arrested before and groups he was involved with.
- ❑ This narrowed the suspect pool, so the FBI got a court order to monitor his Internet access.



# Case 1: LulzSec

- Hammond used Tor, and while the crypto was never busted, FBI correlated times sup\_g was talking to Subu on IRC with when Hammond was at home using his computer.
- More Details:  
<http://arstechnica.com/tech-policy/2012/03/stakeout-how-the-fbi-tracked-and-busted-a-chicago-anon/>



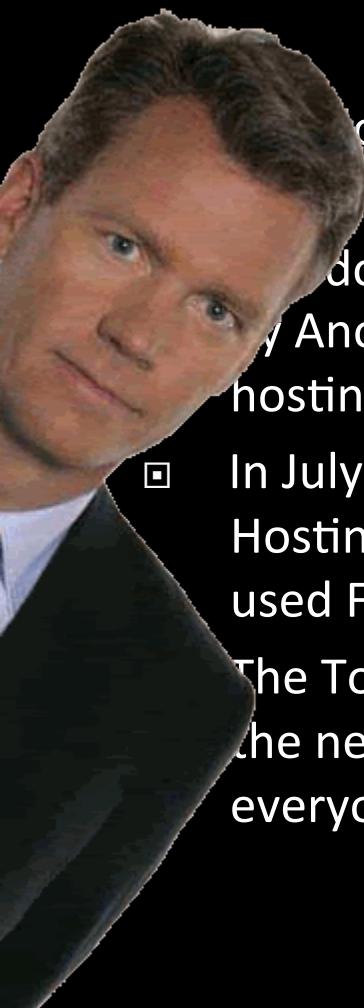
# Case 1: LulzSec

## Lessons Learned:

- ❑ Use Tor consistently
- ❑ Don't give personal information
- ❑ Correlation attacks are still a bitch!



# Case 2: Freedom Hosting



Freedom Hosting hosted, amongst other things, child porn related hidden service websites.

Freedom Hosting had previously come under attack by Anonymous during Op Darknet because of it hosting CP.

- In July of 2013, the FBI compromised Freedom Hosting, and inserted malicious Java Script that used Firefox bug CVE-2013-1690 in version 17 ESR.

The Tor Browser Bundle is based on Firefox, and the newest version was already patched, but not everyone updates in a timely fashion.



# Case 2: Freedom Hosting

- The payload was “Magneto”, which phoned home to servers in Virginia using the host’s public IP.  
<http://ghowen.me/fbi-tor-malware-analysis>
- It also reported back the computer’s:
  - MAC address
  - Windows host name
  - unique serial number to tie a user to a site
- May be same as EgotisticalGiraffe.
- See also:
  - Magic Lantern
  - FOXACID
  - Computer and Internet Protocol Address Verifier (CIPAV)
- Thanks to Joe Cicero for "Privacy In a Surveillance State, Evading Detection" (P.I.S.S.E.D.) talk.



I am the best Giraffe  
EVAR!!! Bow to my  
Giraffey goodness!

# Case 2: Freedom Hosting

- An Irish man, Eric Eoin Marques, is alleged to be the operator of Freedom Hosting. The servers hosting Freedom Hosting were tied to him because of payment records.
- Marques was said to have dived for his laptop to shut it down when police raided him.
- More Details:  
[http://www.wired.com/threatlevel/2013/09/  
freedom-hosting-fbi/](http://www.wired.com/threatlevel/2013/09/freedom-hosting-fbi/)



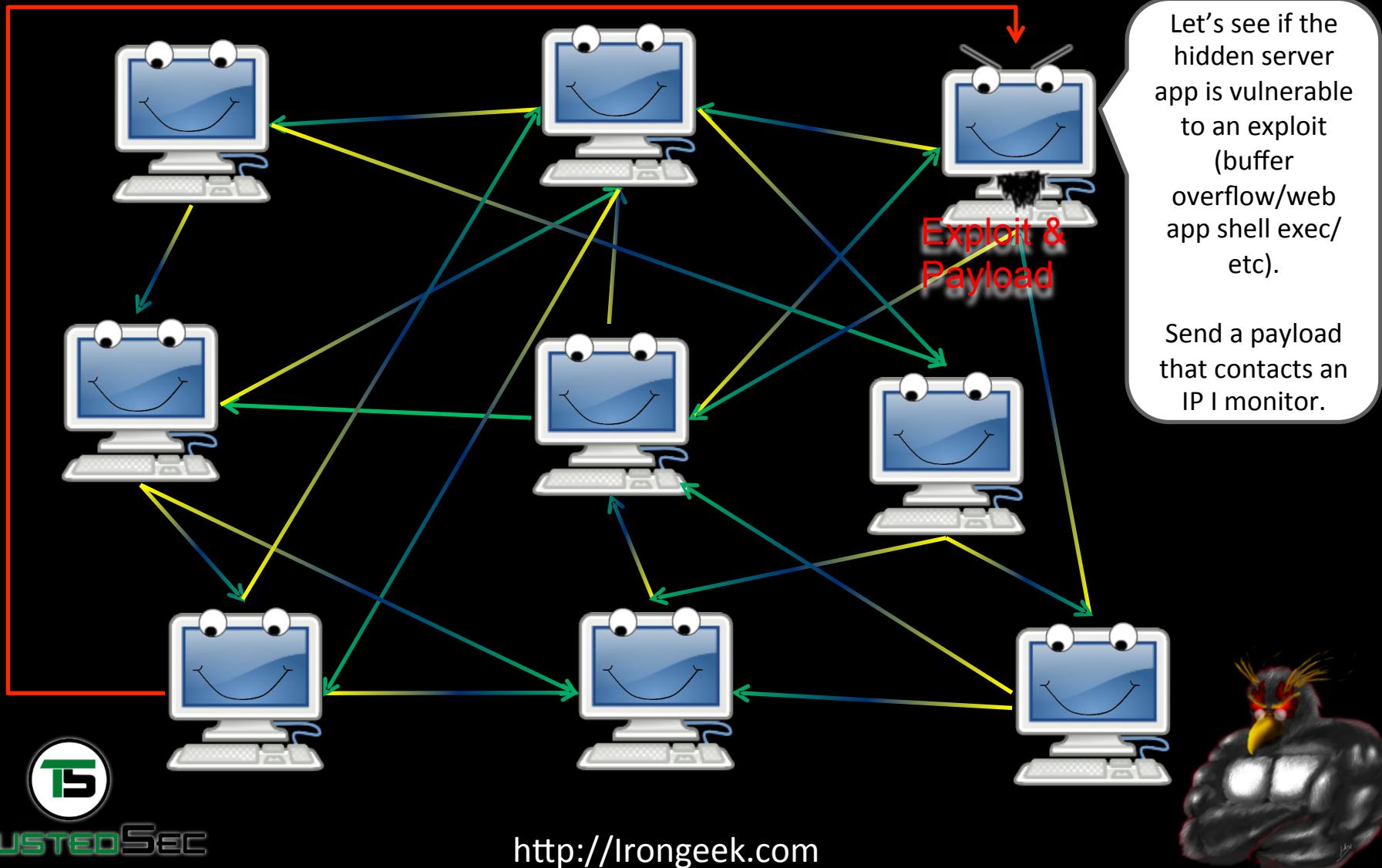
# Case 2: Freedom Hosting

## Lessons Learned:

- ❑ Don't host Captain Picard or Julian Bashir
- ❑ Patch, patch, patch
- ❑ Follow the money
- ❑ Leave encrypted laptops in a powered down state when not in use!



# Make hidden server contact you over public Internet



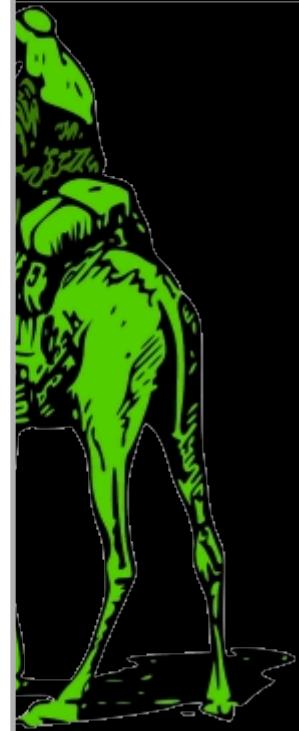
- ❑ Some services were offered for hire, such as "Robots," which allowed users to hire "legally prohibited services." <http://www.onionr.com>
- ❑ Within the same section, the FBI was quoted as saying:
- ❑ They also found that the site had a "Services" section.

### From court documents:

"As of September 23, 2013, there were nearly 13,000 listings for controlled substances on the website, listed under the categories "Cannabis," "Dissociatives," "Ecstasy," "Intoxicants," "Opioids," "Precursors," "Prescription," "Psychedelics," and "Stimulants," among others."

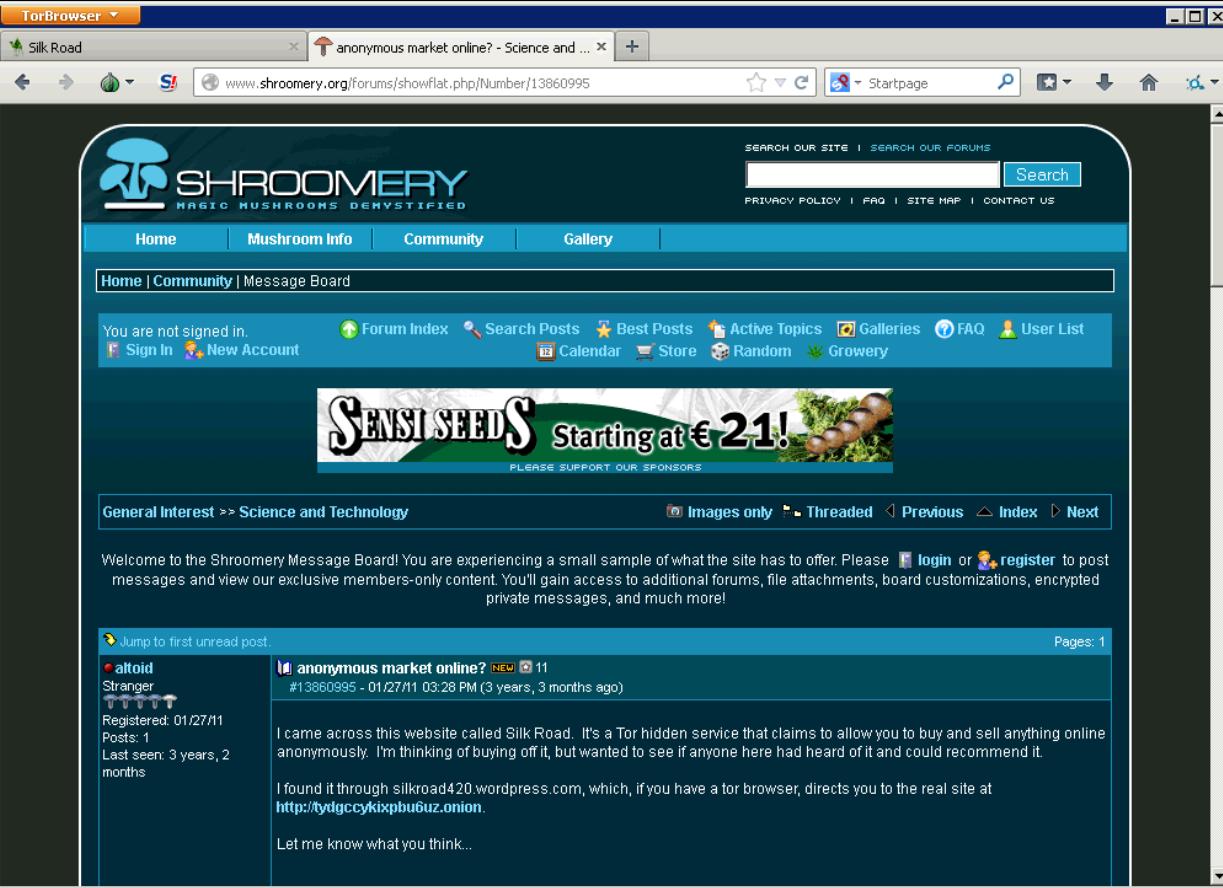
"There were 159 listings on the site under the category "Services." Most concerned computer-hacking services: for example, one listing was by a vendor offering to hack into Facebook, Twitter, and other social networking accounts of the customer's choosing, so that "You can Read, Write, Upload, Delete, View All Personal Info"; another listing offered tutorials on "22 different methods" for hacking ATM machines. Other listings offered services that were likewise criminal in nature. For example, one listing was for a "HUGE Blackmarket Contact List," described as a list of "connects" for "services" such as "Anonymous Bank Accounts," "Counterfeit Bills (CAD/GBP/EUR/USD) ,," "Firearms +Ammunition," "Stolen Info (CC [credit card], Paypal) ,," and "Hitmen (10+ countries)." "

"Sellers may not list forgeries of any privately issued documents such as diplomas/certifications, tickets or receipts. Also, listings for counterfeit currency are still not allowed in the money section."



# Case 3: The Silk Road

- The earliest they could find was from “altoid” on the Shroomery.org forums on 01/27/11.  
<http://www.shroomery.org/forums/showflat.php/Number/13860995>



A screenshot of a computer screen displaying a web browser window titled "Silk Road". The browser is identified as "TorBrowser". The URL in the address bar is "www.shroomery.org/forums/showflat.php/Number/13860995". The page itself is the Shroomery.org forums, specifically the "Message Board" section. The header features the Shroomery logo and navigation links for Home, Mushroom Info, Community, and Gallery. Below the header, there are links for Sign In, New Account, Forum Index, Search Posts, Best Posts, Active Topics, Galleries, FAQ, User List, Calendar, Store, Random, and Growery. A prominent banner for "SENSI SEEDS" is displayed, advertising seeds starting at €21. The main content area shows a post by user "altoid" under the category "Science and Technology". The post title is "anonymous market online? [NEW]". The post content discusses the Silk Road website, stating: "I came across this website called Silk Road. It's a Tor hidden service that claims to allow you to buy and sell anything online anonymously. I'm thinking of buying off it, but wanted to see if anyone here had heard of it and could recommend it." The post also mentions finding it through silkroad420.wordpress.com and provides the URL <http://fydgccykixpbu6uz.onion>. The post has 11 replies. The footer of the page includes links for General Interest, Science and Technology, Images only, Threaded, Previous, Index, and Next.

<http://Irongeek.com>



# Case 3: The Silk Road

- BitCoinTalk.org Post

- "Quote from: altoid on January 29, 2011, 07:44:51 PM"

The screenshot shows a web browser window displaying a forum post on BitCoinTalk.org. The post is titled "Re: A Heroin Store" by "ShadowOfHarbringer". The post content discusses the popularity of forest sightseeing and mentions the Silk Road as an anonymous marketplace. The user "grondilu" replies with a warning about forced fees and a link to a Bitcoin Client fork. The browser's address bar shows the URL <https://bitcointalk.org/index.php?topic=175.msg42479#msg42479>.

A Heroin Store

GLBSE.com

ShadowOfHarbringer Hero Member

Activity: 1260

Re: A Heroin Store

January 30, 2011, 08:09:37 PM

Quote from: Nefario on January 30, 2011, 06:30:07 AM

(probably berried in the desert or in a forest)

Somewhat, I'm seeing tremendous increase of popularity of forest sightseeing 😊

Quote from: altoid on January 29, 2011, 07:44:51 PM

What an awesome thread! You guys have a ton of great ideas. Has anyone seen Silk Road yet? It's kind of like an anonymous amazon.com. I don't think they have heroin on there, but they are selling other stuff. They basically use bitcoin and tor to broker anonymous transactions. It's at <http://tydgccykixbu6uz.onion>. Those not familiar with Tor can go to [silkroad420.wordpress.com](http://silkroad420.wordpress.com) for instructions on how to access the .onion site.

Let me know what you guys think

So here we go, first Bitcoin drug store.  
We're going into deep water faster than i thought then.

I wonder how long will it take for govs to start investigating Bitcoin.

{{{ Bitcoin.pl Elite Member, Bitcointalk Hero Member [1176] }}}  
1NLWBAD7ZD82fjDDawKfp5RAKSR8YWWYd3 | GPG/PGP Keys [3072D/F92EDBA4]  
Hate forced fees? Use "No Forced TX Fee" Bitcoin Client fork. **Now updated to v0.8.6 !** (use carefully !)

grondilu Hero Member

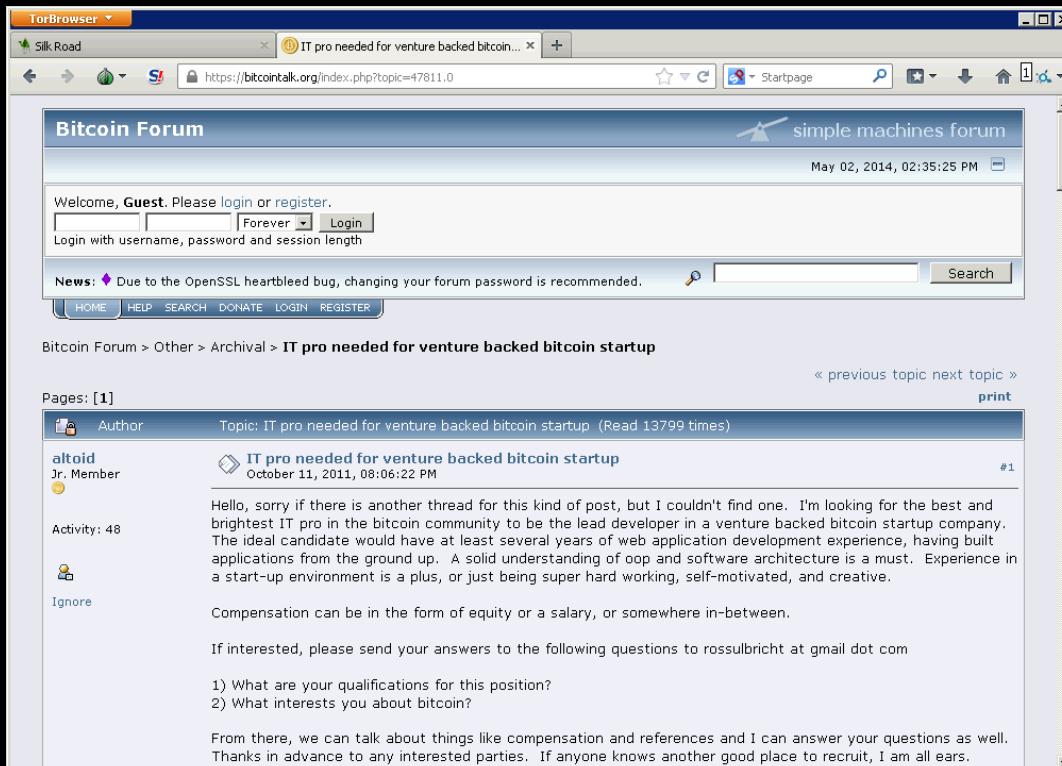
Re: A Heroin Store

January 30, 2011, 08:45:31 PM



# Case 3: The Silk Road

- An account named “altoid” also made a post on Bitcointalk.org about looking for an “IT pro in the bitcoin community” and asked interested parties to contact “[rossulbricht at gmail dot com](mailto:rossulbricht@gmail.com)” (10/11/11).  
<https://bitcointalk.org/index.php?topic=47811.0>



The screenshot shows a Tor Browser window displaying a post on the Bitcointalk.org forum. The title of the post is "IT pro needed for venture backed bitcoin startup". The post was made by a user named "altoid" on October 11, 2011, at 08:06:22 PM. The post content discusses the need for an IT pro in the bitcoin community to be the lead developer in a venture-backed bitcoin startup company. It specifies requirements such as several years of web application development experience, building applications from the ground up, and being self-motivated and creative. Compensation is mentioned as equity or salary. The post also asks interested parties to send answers to the email address rossulbricht at gmail dot com.

Bitcointalk.org - IT pro needed for venture backed bitcoin startup

Welcome, Guest. Please [login](#) or [register](#).

News: ♦ Due to the OpenSSL heartbleed bug, changing your forum password is recommended.

Author: altoid (Jr. Member)

Topic: IT pro needed for venture backed bitcoin startup (Read 13799 times)

October 11, 2011, 08:06:22 PM #1

Hello, sorry if there is another thread for this kind of post, but I couldn't find one. I'm looking for the best and brightest IT pro in the bitcoin community to be the lead developer in a venture backed bitcoin startup company. The ideal candidate would have at least several years of web application development experience, having built applications from the ground up. A solid understanding of oop and software architecture is a must. Experience in a start-up environment is a plus, or just being super hard working, self-motivated, and creative.

Compensation can be in the form of equity or a salary, or somewhere in-between.

If interested, please send your answers to the following questions to rossulbricht at gmail dot com

1) What are your qualifications for this position?  
2) What interests you about bitcoin?

From there, we can talk about things like compensation and references and I can answer your questions as well. Thanks in advance to any interested parties. If anyone knows another good place to recruit, I am all ears.



# Case 3: The Silk Road

- Ulbricht's Google+ profile show an interest in the "Mises Institute" a "world center of the Austrian School of economics."
- Dread Pirate Roberts' signature on the Silk Road forums had a link to the Mises Institute. Austrian Economic theory was also stated by Dread Pirate Roberts to be influential to the the Silk Road's philosophy.

Ludwig von Mises Institute : The Austrian School Is Advancing Liberty

mises.org

Ludwig von Mises Institute  
Advancing Austrian Economics, Liberty, and Peace

Help Us Rebuild Mises.org  
GIVE TODAY ▶

Search:

Daily | About | Blog | Literature | Audio / Video | Events | Donate | Store | Academy | Wiki

**The Future of Libertarianism**

May 5 • Llewellyn H. Rockwell Jr.

The “thin” libertarian believes in the nonaggression principle, that one may not initiate physical force against anyone else. The thin libertarian thinks of himself simply as a libertarian, without labels. Others mistakenly contend that libertarians must be committed to a slate of other views as well.

New Mises.org Coming Soon!  
Rebuilt • Expanded  
• Mobile Device Friendly

PLEASE HELP TODAY

Democracy, War, and the Myth of the Neutral State

May 3 • Luigi Marco Bassani and Carlo Lottieri

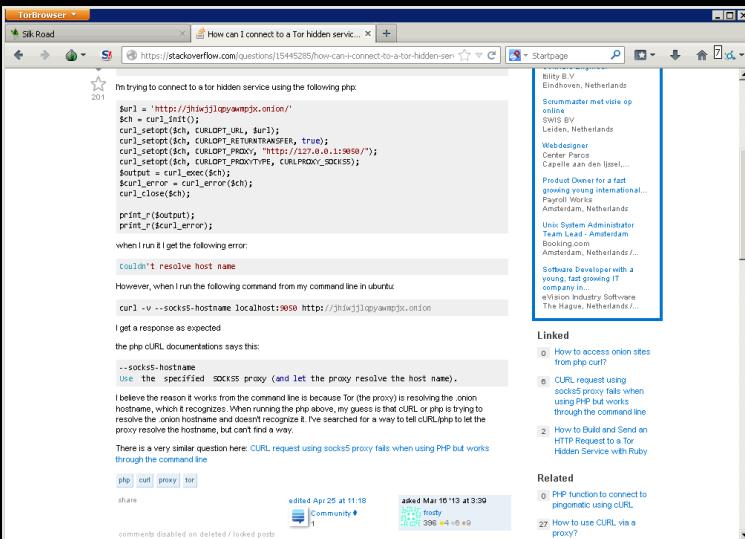
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Reset Firefox... ×



# Case 3: The Silk Road

- "Ross Ulbricht." account also posted on StackOverflow asking for help with PHP code to connect to a Tor hidden service. The username was quickly changed to "frosty" (03/16/12).  
<http://stackoverflow.com/questions/15445285/how-can-i-connect-to-a-tor-hidden-service-using-curl-in-php>



A screenshot of a Stack Overflow question page titled "How can I connect to a Tor Hidden service...". The question asks how to connect to a Tor hidden service using curl in PHP. It includes a code snippet:

```
$url = "http://jhix31jwpxmpjx.onion/";
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $url);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
curl_setopt($ch, CURLOPT_PROXY, "http://127.0.0.1:9050/");
curl_setopt($ch, CURLOPT_PROXYTYPE, CURLPROXY_SOCKS5);
curl_setopt($ch, CURLOPT_TIMEOUT, 30);
curl_error = curl_error($ch);
curl_close($ch);

print_r($output);
print_r($curl_error);
```

The question notes that running the code results in a "Couldn't resolve host name" error. It suggests using --socks5-hostname to resolve the host name. The user mentions that the proxy works fine from the command line in Ubuntu.

Below the question, there is a sidebar with user information and a related questions section.



- Guess who is now a suspect for being "Dread Pirate Roberts"? Ross William Ulbricht.



# Case 3: The Silk Road

- Someone was connecting to a server that hosts the Silk Road from an Internet café near where Ross lived in San Francisco. Private messages on Silk Road make it seem Dread Pirate Roberts lived in the Pacific time zone.
- IP of a Silk Road server was attached to via a VPN server that was connected to by an IP belonging to an Internet cafe on Laguna Street in San Francisco from which Ulbricht had also connected to his Gmail account with (both on June 3, 2013).
- PM to Dread Pirate Roberts from a user said the site was leaking "some sort of external IP address" belonging to the VPN.
- FBI starts taking down SilkRoad servers, though I'm not sure how they were found. Could have been money trail to aliases, or as Nicholas Weaver conjectured, they hacked SilkRoad and made it contact an outside server without using Tor so it revealed its real IP. Once located, FBI was able to get a copy of one of the servers.



# Case 3: The Silk Road

- On 07/10/13 US Customs intercepted 9 IDs with different names, but all having a picture of Ulbricht. Homeland Security interviewed Ulbricht, but he denied having ordered them.

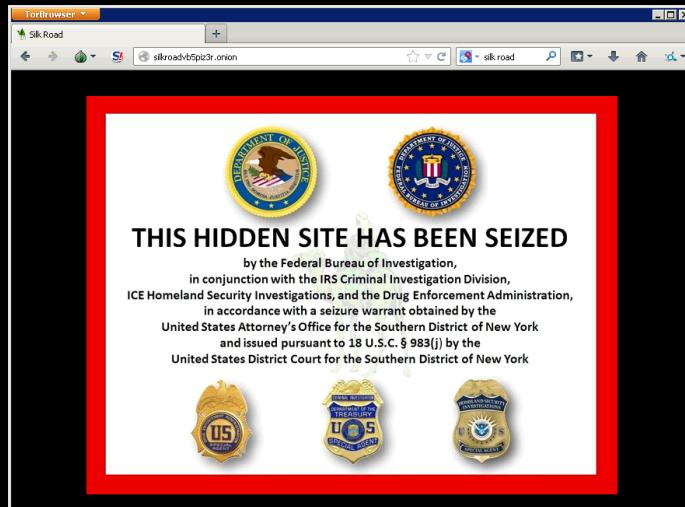


- Smart: "ULBRICHT generally refused to answer any questions pertaining to the purchase of this or other counterfeit identity documents."
- Stupid: "However, ULBRICHT volunteered that "hypothetically" anyone could go onto a website named "Silk Road" on "Tor" and purchase any drugs or fake identity documents the person wanted."
- Roommates knew him as "Josh". PMs show DPR was interested in getting fake IDs.



# Case 3: The Silk Road

- Server used SSH and a public key that ended in frosty@frosty. Server also had some of the same code posted on StackOverflow.
- Eventually, on 10/01/2013 the FBI Landed on him in a Library right after he entered the password for his laptop. More evidence was found on his laptop.
- More info (Big thanks to Nate Anderson for the original article and Agent Christopher Tarbell for court docs):  
<http://arstechnica.com/tech-policy/2013/10/how-the-feds-took-down-the-dread-pirate-roberts/>  
<https://www.cs.columbia.edu/~smb/UlbrichtCriminalComplaint.pdf>



<http://Irongeek.com>



# Case 3: The Silk Road

## Lessons Learned:

- ❑ Keep online identities separate
  - Keep different usernames
  - From different locations
- ❑ Have a consistent story
- ❑ Don't talk about interests
- ❑ Don't volunteer information!



# DEMOS

Maybe?



# Many More Links

- Talk on Darknets in general  
[http://www.irongeek.com/i.php?page=videos/aide-winter-2011#Cipherspace/Darknets:\\_anonymizing\\_private\\_networks](http://www.irongeek.com/i.php?page=videos/aide-winter-2011#Cipherspace/Darknets:_anonymizing_private_networks)
- I2P FAQ  
<http://www.i2p2.de/faq.html>
- Tor FAQ  
<https://trac.torproject.org/projects/tor/wiki/doc/TorFAQ>
- Tor Manual  
<https://www.torproject.org/docs/tor-manual.html.en>
- I2P Index to Technical Documentation  
<http://www.i2p2.de/how>



# Sites of Mine

- ❑ Intro to Darknets: Tor and I2P Workshop  
<http://www.irongeek.com/i.php?page=videos/intro-to-tor-i2p-darknets>
- ❑ My Tor/I2P Notes  
<http://www.irongeek.com/i.php?page=security/i2p-tor-workshop-notes>
- ❑ Cipherspaces/Darknets An Overview Of Attack Strategies  
<http://www.irongeek.com/i.php?page=videos/cipherspaces-darknets-an-overview-of-attack-strategies>
- ❑ Anonymous proxy to the normal web  
<http://www.irongeek.com/i.php?page=videos/tor-1>
- ❑ Hidden services  
Normally websites, but can be just about any TCP connection  
<http://www.irongeek.com/i.php?page=videos/tor-hidden-services>



# ADHD Linux

- ❑ Active Defense Harbinger Distribution (ADHD)  
<http://sourceforge.net/projects/adhd/>  
from Black Hills Information Security & Secureideas
- ❑ Metasploit Decloaker, web bugs, etc.



# Events



Sept 24th-28th, 2014

<http://www.derbycon.com>



Derbycon Art Credits to DigiP

Photo Credits to KC (devauto)

## Others

<http://www.louisvilleinfosec.com>

<http://skydogcon.com>

<http://hack3rcon.org>

<http://outerz0ne.org>

<http://phreaknic.info>

<http://notacon.org>



# QUESTIONS?

42

Twitter: @Irongeek\_ADC

