

DROPPING DOCS ON DARKNETS: HOW PEOPLE GOT CAUGHT

Adrian Crenshaw



TRUSTED SEC

<http://Irongeek.com>



About Adrian

- ▣ I run Irongeek.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: @Irongeek_ADC



TRUSTEDSEC

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



TRUSTEDSEC

<http://Irongeek.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



TRUSTEDSEC

<http://lrongeek.com>



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.



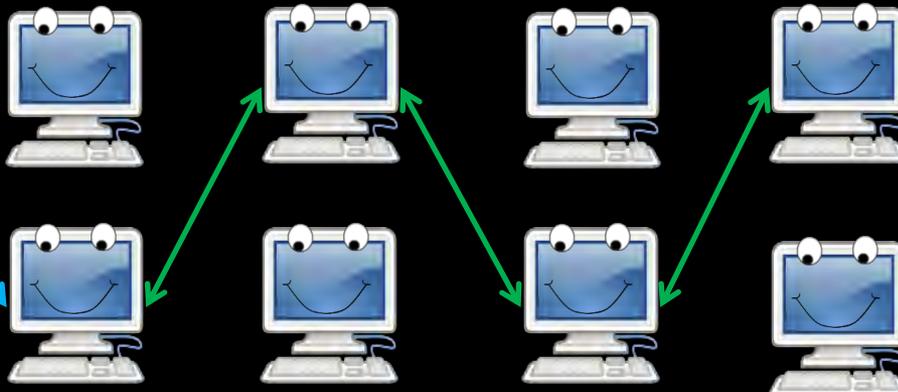
Tor: The Onion Router



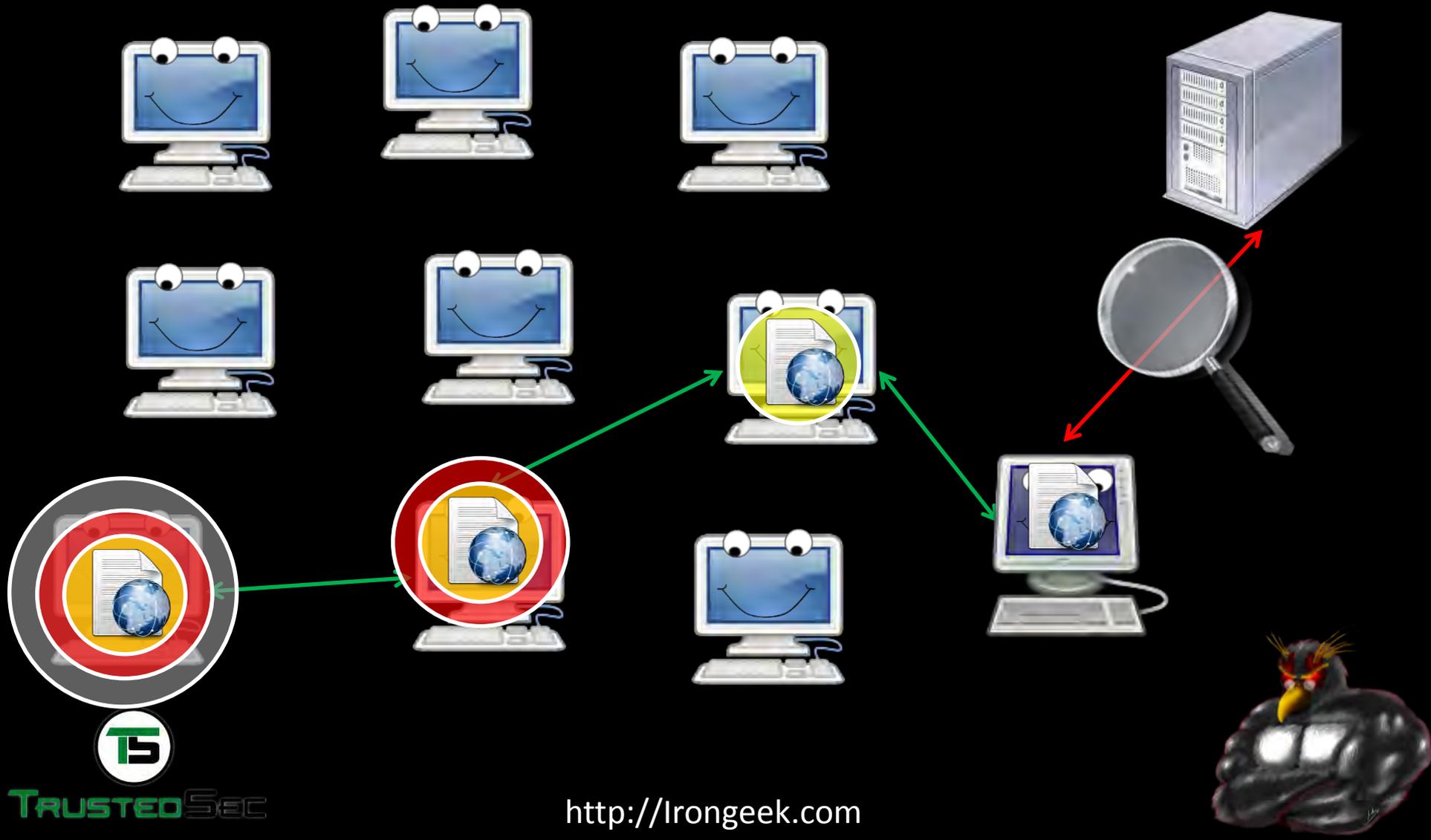
- ▣ Layered encryption
- ▣ Bi-directional tunnels
- ▣ Has directory servers
- ▣ Mostly focused on out proxying to the Internet
- ▣ More info at <https://www.torproject.org>

Directory Server

Internet Server



Layers like an Ogre



Layout to connect to Hidden Service

Tor Hidden Services: 1

Step 1: Bob picks some introduction points and builds circuits to them.



	Tor cloud
	Tor circuit
	Introduction points
	Public key
	One-time secret
	Rendezvous point

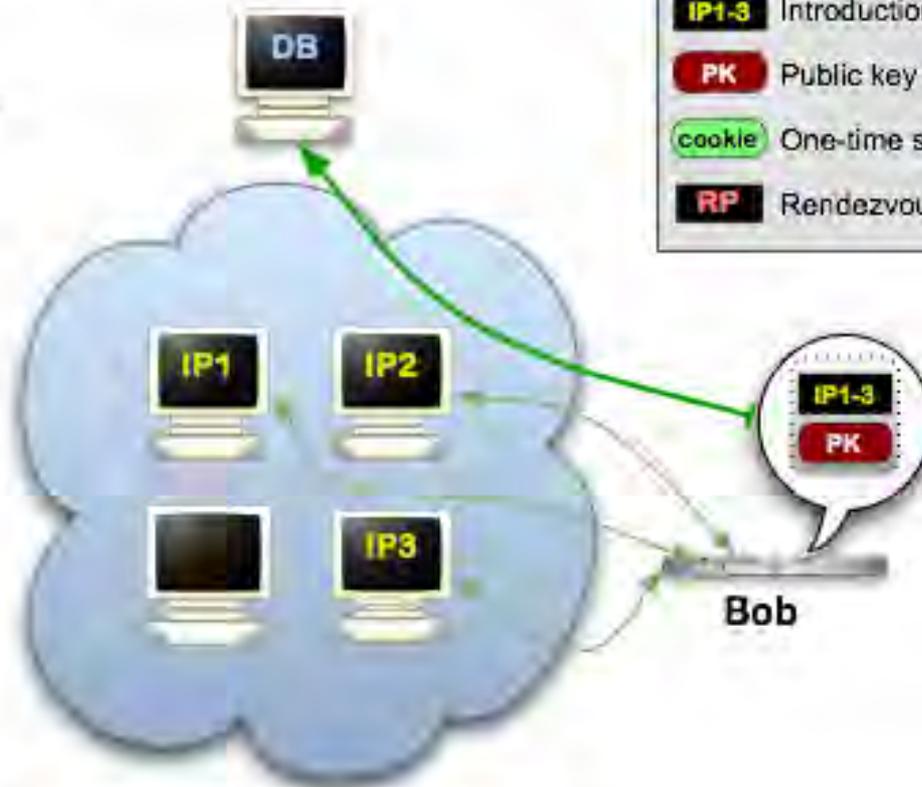
Image from <http://www.torproject.org/hidden-services.html.en>
<http://lrongeek.com>



Layout to connect to Hidden Service

Tor Hidden Services: 2

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



-  Tor cloud
-  Tor circuit
-  Introduction points
-  Public key
-  One-time secret
-  Rendezvous point

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

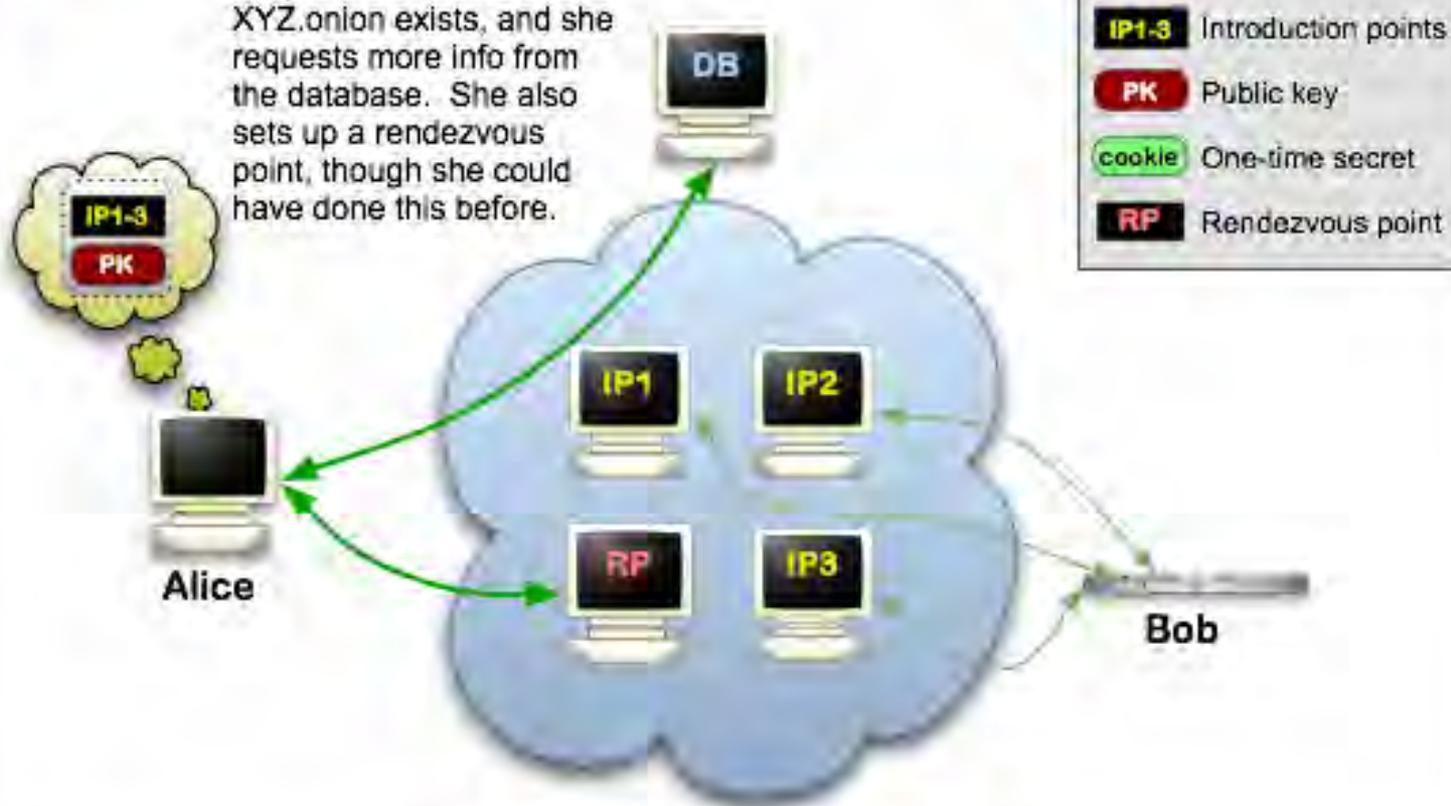


Image from <http://www.torproject.org/hidden-services.html.en>
<http://lrongeek.com>



Layout to connect to Hidden Service

Tor Hidden Services: 4

Step 4: Alice writes a message to Bob (encrypted to PK) listing the rendezvous point and a one-time secret, and asks an introduction point to deliver it to Bob.

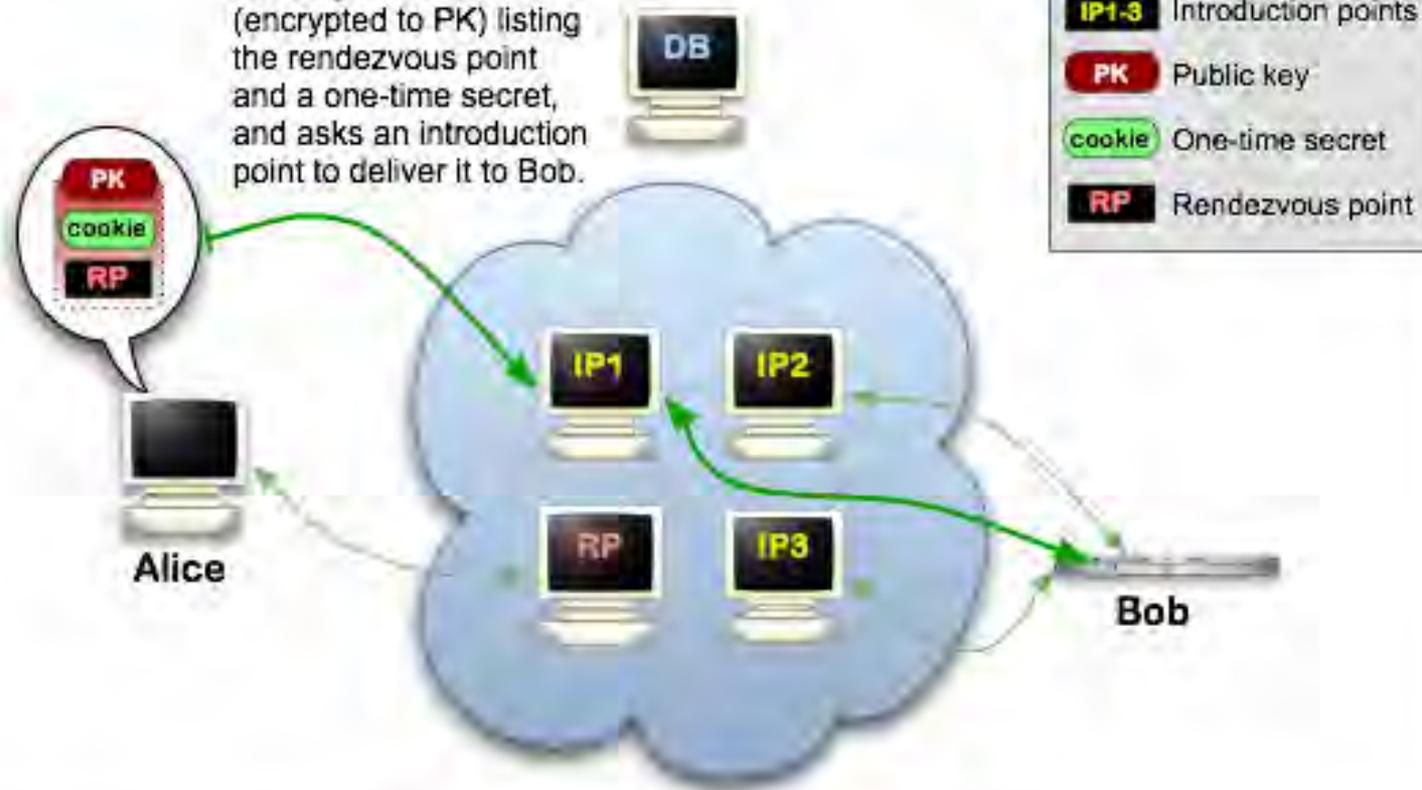


Image from <http://www.torproject.org/hidden-services.html.en>
<http://Irongeek.com>



Layout to connect to Hidden Service

Tor Hidden Services: 5

Step 5: Bob connects to the Alice's rendezvous point and provides her one-time secret.

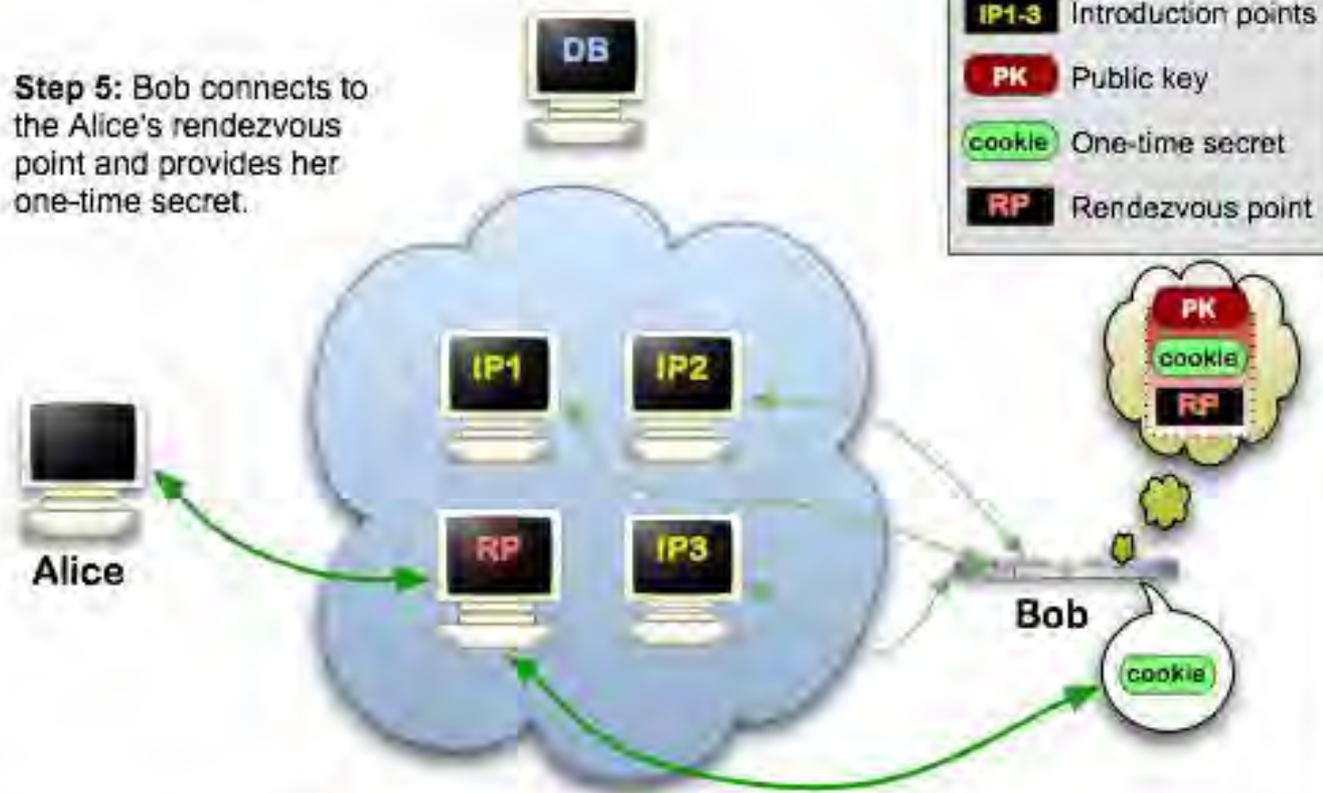


Image from <http://www.torproject.org/hidden-services.html.en>
<http://Irongeek.com>



Layout to connect to Hidden Service

Tor Hidden Services: 6

Step 6: Bob and Alice proceed to use their Tor circuits like normal.

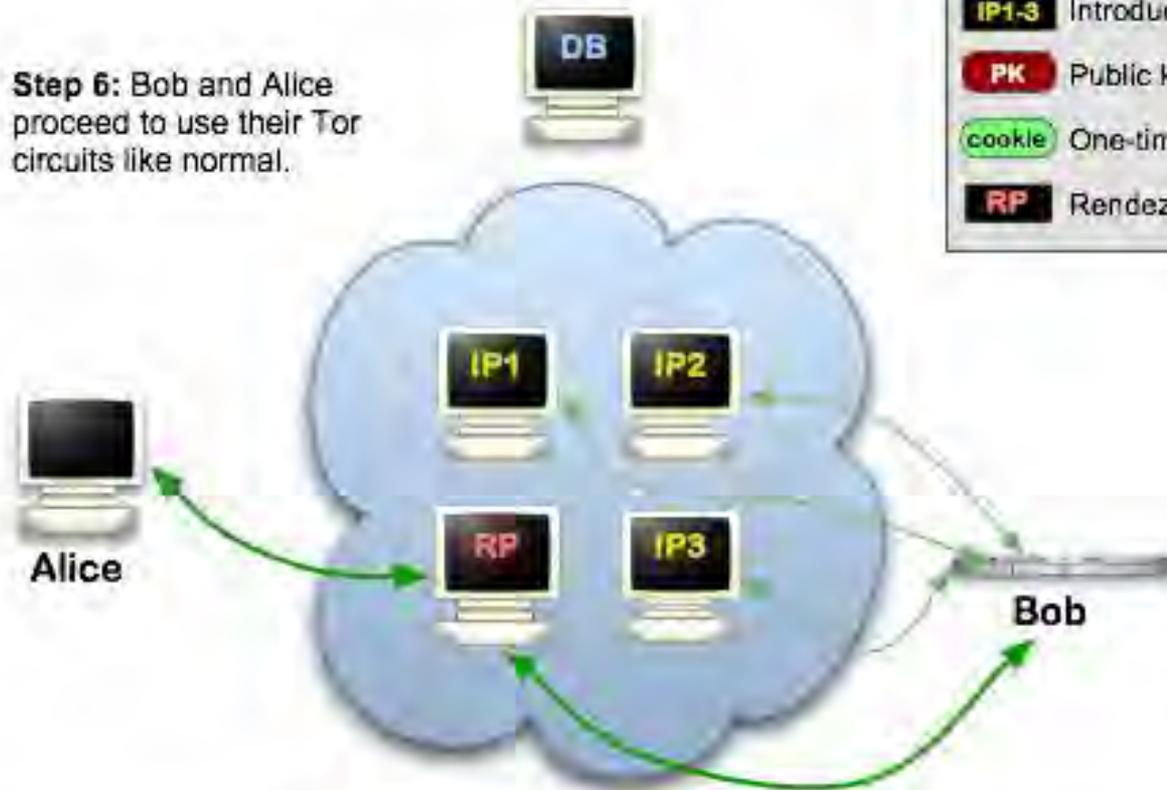


Image from <http://www.torproject.org/hidden-services.html.en>
<http://Irongeek.com>



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?



Applications/Sites

- ▣ Tails: The Amnesic Incognito Live System
<https://tails.boum.org/>
- ▣ Tor2Web Proxy
<http://tor2web.org>
- ▣ Tor Hidden Wiki:
<http://kpvz7ki2v5agwt35.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>



I2P

SHOUT OUT TO I2P

<http://geti2p.net>



TRUSTEDSEC

<http://lrongeek.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
- Guerrilla Mail marked who sent the email.
 - To: "irongeek"
 - From: <e9jnc...>
 - Subject: Hey
 - X-Originating
 - Content-Type: text/html



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>



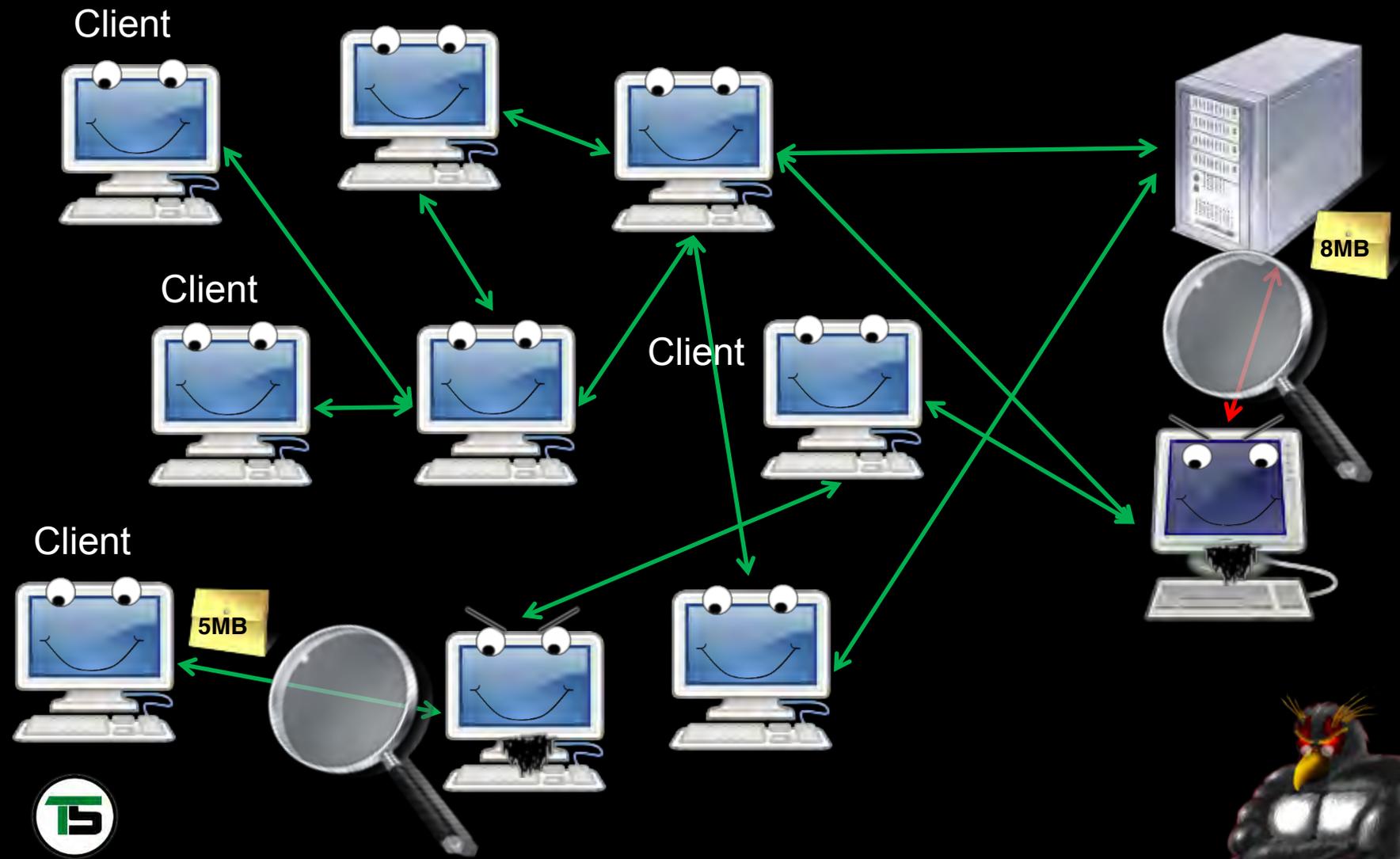
Case 0: Harvard Bomb Threat

Lessons Learned:

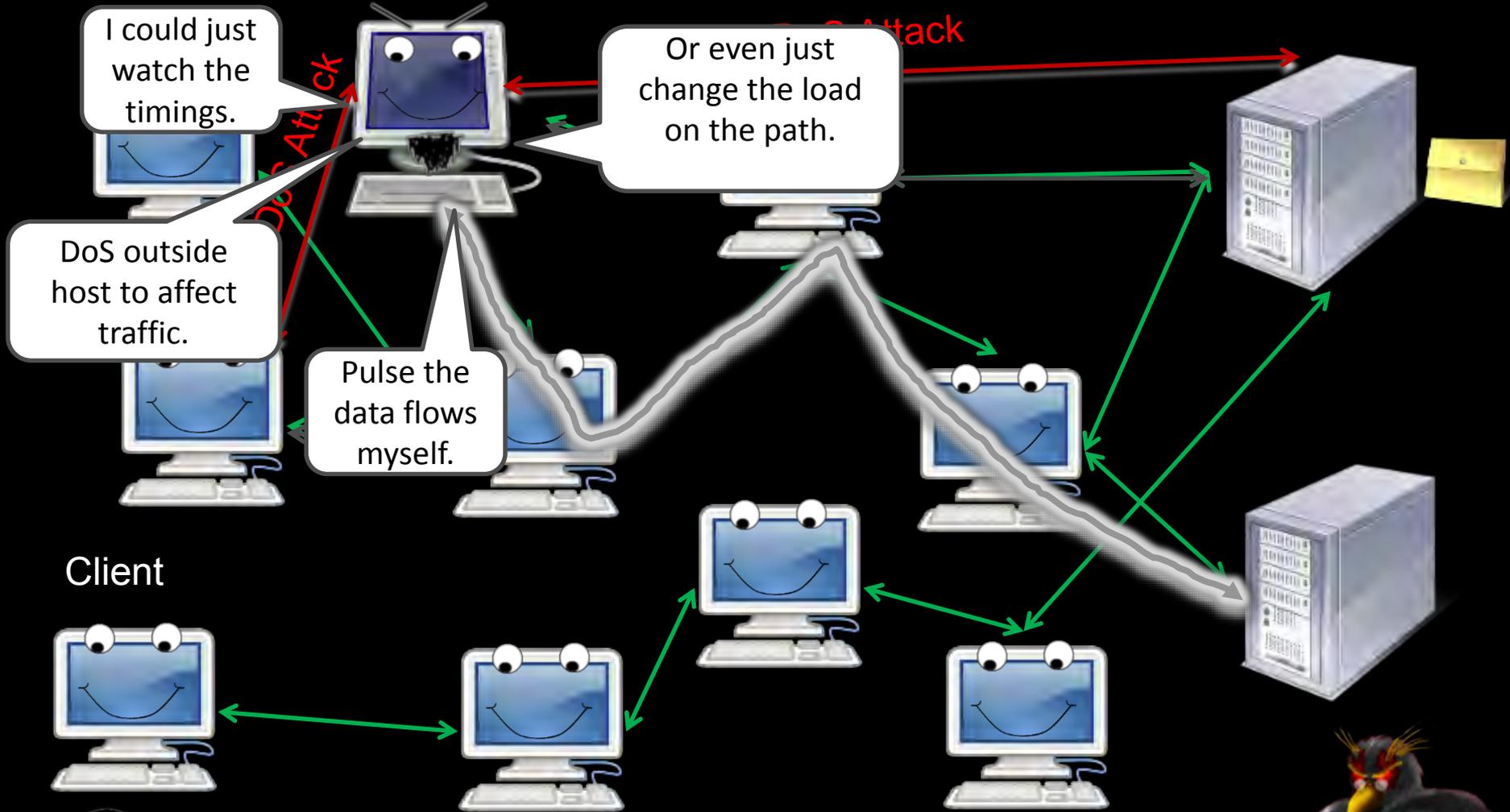
- ▣ Don't be the only person using Tor on a monitored network at a given time
- ▣ Use a bridge?
- ▣ Don't admit anything
- ▣ Correlation attacks are a bitch



Correlation of end point and exit point

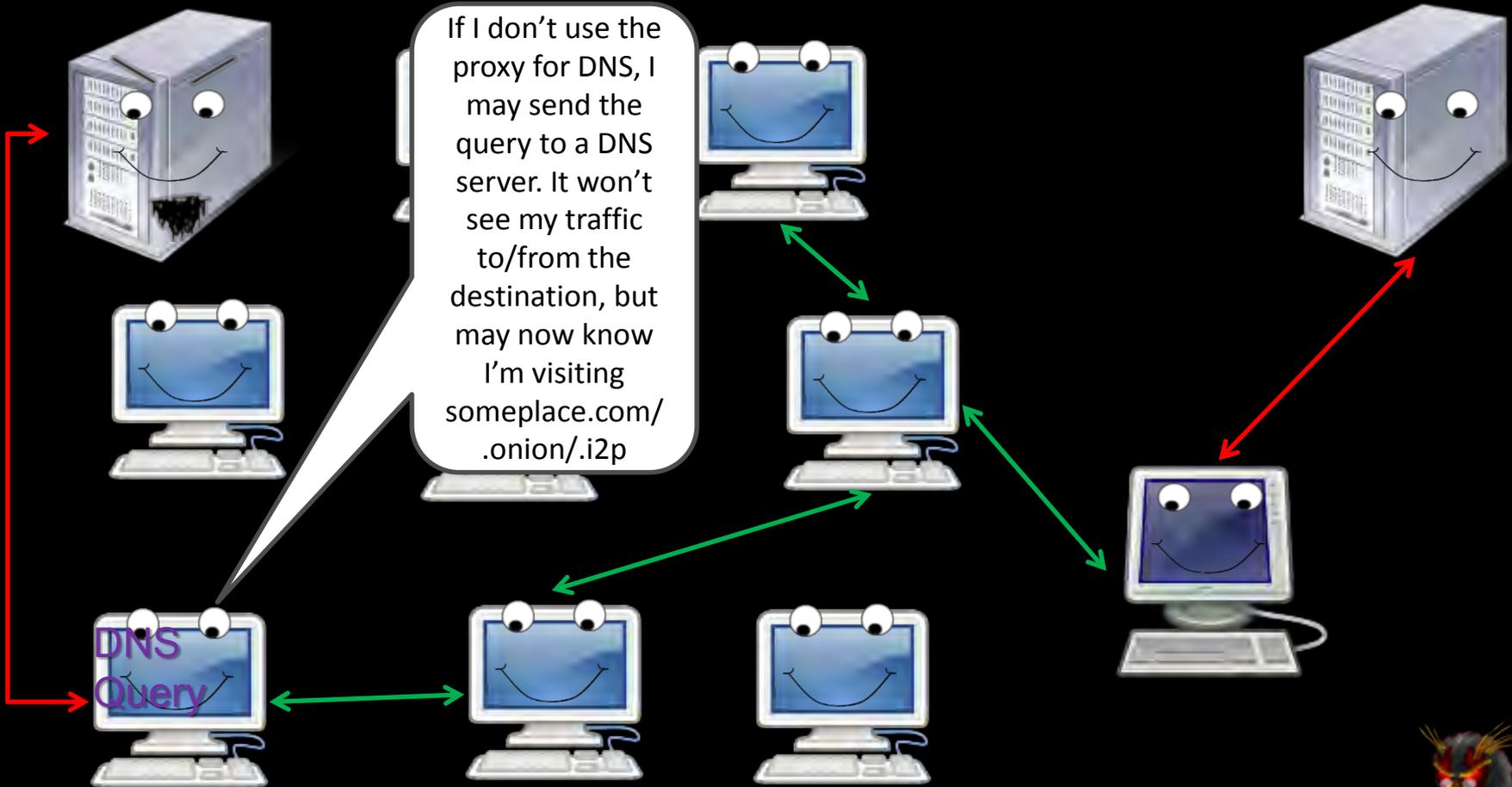


Timing Correlation



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/>



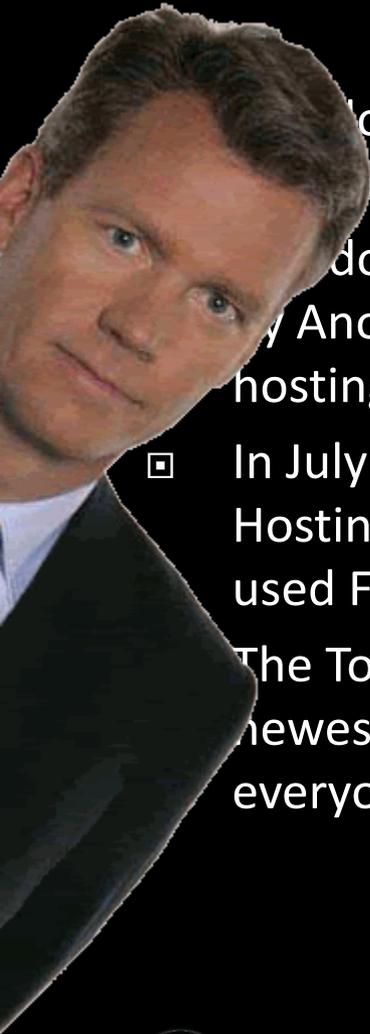
Case 1: LulzSec

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/>



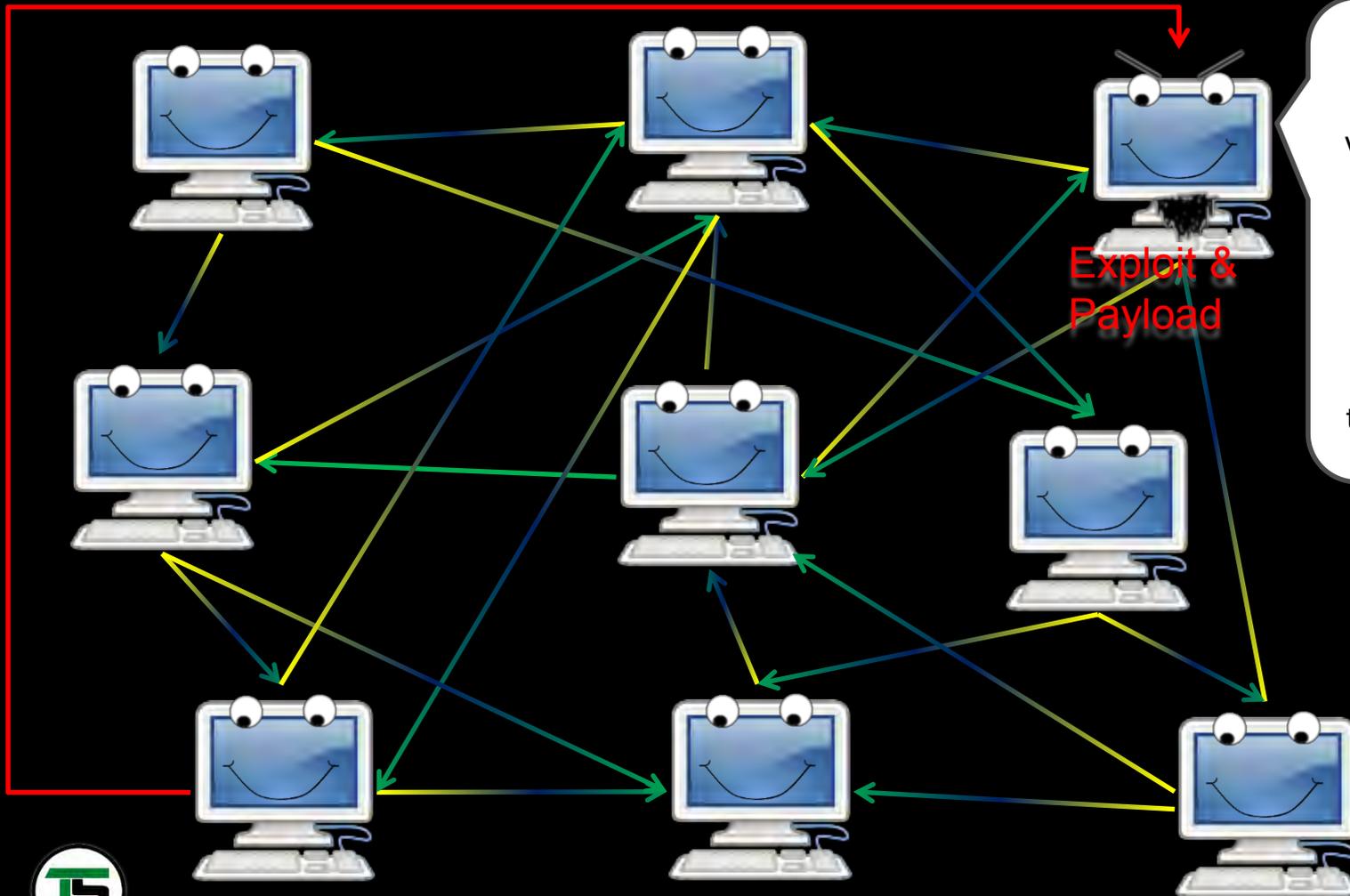
Case 2: Freedom Hosting

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



Let's see if the hidden server app is vulnerable to an exploit (buffer overflow/web app shell exec/etc).

Send a payload that contacts an IP I monitor.

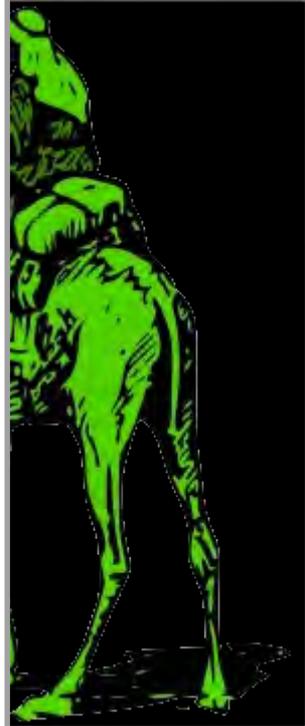


From court documents:

“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>

The screenshot shows a TorBrowser window with the following details:

- Browser: TorBrowser
- Address Bar: www.shroomery.org/forums/showflat.php/Number/13860995
- Page Title: anonymous market online? - Science and Technology
- Forum Name: SHROOMERY MAGIC MUSHROOMS DEMYSTIFIED
- Navigation: Home, Mushroom Info, Community, Gallery
- User Status: You are not signed in. Sign In, New Account
- Forum Post: anonymous market online? by altoid (Stranger, Registered: 01/27/11, Last seen: 3 years, 2 months)
- Post Content: 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. I found it through silkroad420.wordpress.com, which, if you have a tor browser, directs you to the real site at <http://tydgccykixpbu6uz.onion>. Let me know what you think...



Case 3: The Silk Road

- BitCoinTalk.org Post
- "Quote from: altoid on January 29, 2011, 07:44:51 PM"

When we see the bit http silk Let thi

The screenshot shows a forum post on BitCoinTalk.org. The browser address bar displays the URL: <https://bitcointalk.org/index.php?topic=175.msg42479#msg42479>. The post is titled "Re: A Heroin Store" and is posted by "ShadowOfHarbringer" on January 30, 2011, at 08:09:37 PM. The post includes a quote from "Nefario" and a quote from "altoid". The "altoid" quote contains the text: "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://tydgccykixpbu6uz.onion>. Those not familiar with Tor can go to silkroad420.wordpress.com for instructions on how to access the .onion site. Let me know what you guys think". Below the quote, the user "ShadowOfHarbringer" writes: "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." The post also includes a signature block with PGP keys and a note about a Bitcoin client update.



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 TorBrowser window with the title 'Silk Road'. The address bar contains the URL 'https://bitcointalk.org/index.php?topic=47811.0'. The page content is from the 'Bitcoin Forum' and displays a forum post. The post title is 'IT pro needed for venture backed bitcoin startup' and it was posted by user 'altoid' on October 11, 2011. The post text reads: '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

Ludwig von Mises Institute : Th...

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.

Non-aggression

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*

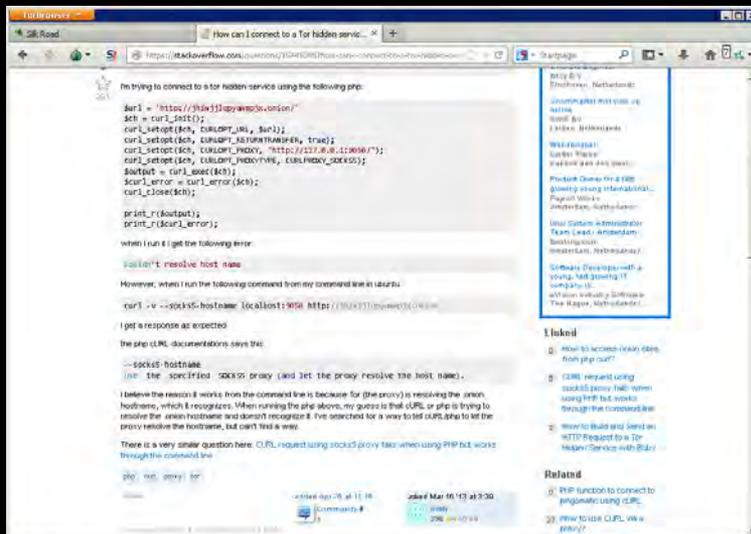
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back! Reset Firefox...



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>



The screenshot shows a StackOverflow question titled "How can I connect to a Tor hidden service...". The user asks for help with PHP code to connect to a Tor hidden service. The code provided is:

```
curl = "https://[socks]@[ip]:[port]/";
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $url);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
curl_setopt($ch, CURLOPT_PROXY, "https://127.0.0.1:8080/");
curl_setopt($ch, CURLOPT_PROXYUSERPWD, "user:passwd");
$output = curl_exec($ch);
$curl_error = curl_error($ch);
curl_close($ch);

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

The user reports an error: "curl() error: resolve: host name". They mention that the code works when run from a terminal but fails when run from a PHP script. The question is answered by another user, suggesting that the issue is related to the proxy settings in the PHP script.



- 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 are 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 outsides server without using Tor so it revealed it's 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://lrongeek.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?



TRUSTEDSEC

<http://Irongeek.com>



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:anonymizingprivatenetworks)
- ▣ 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>



Events

 **DERBYCON**

Sept 24th-28th, 2014

<http://www.derbycon.com>



Derbycon Art Credits to DgipP

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>



TRUSTEDSEC

<http://lrongeek.com>



QUESTIONS?

42

Twitter: @Irongeek_ADC



TRUSTEDSEC

<http://Irongeek.com>

