DROPPING DOCS ON DARKNETS: HOW PEOPLE GOT CAUGHT

Adrian Crenshaw

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

TrustedSec

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

Twitter: @Irongeek_ADC

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

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)

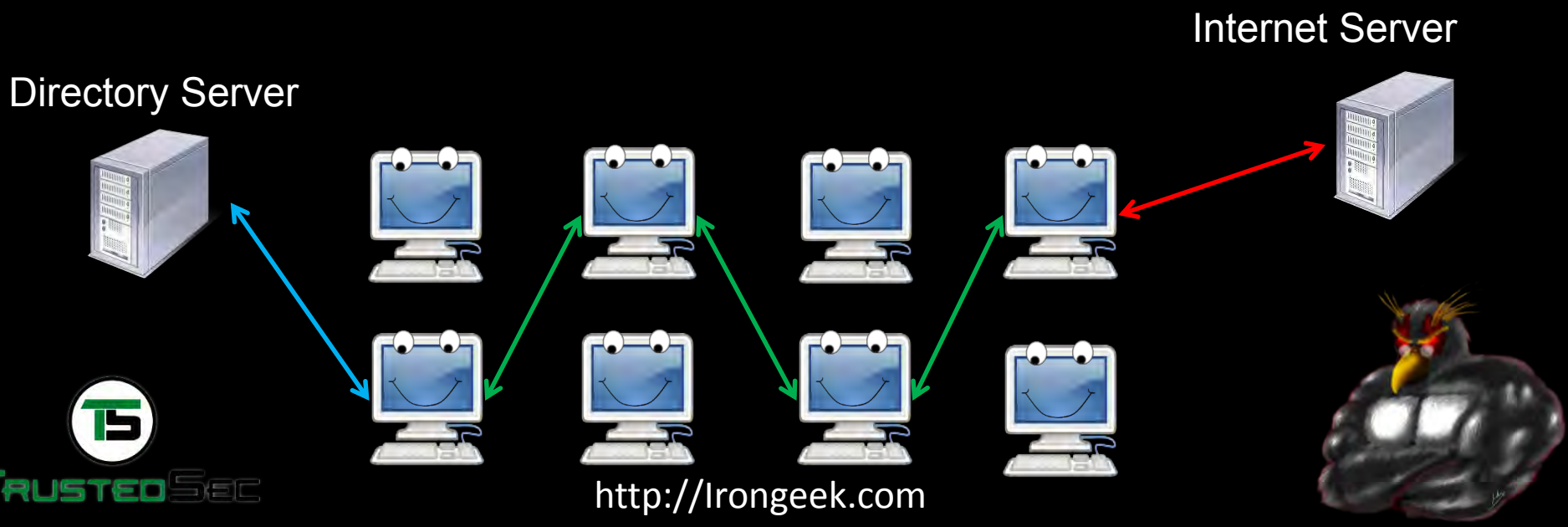
The Onion Router

Overview

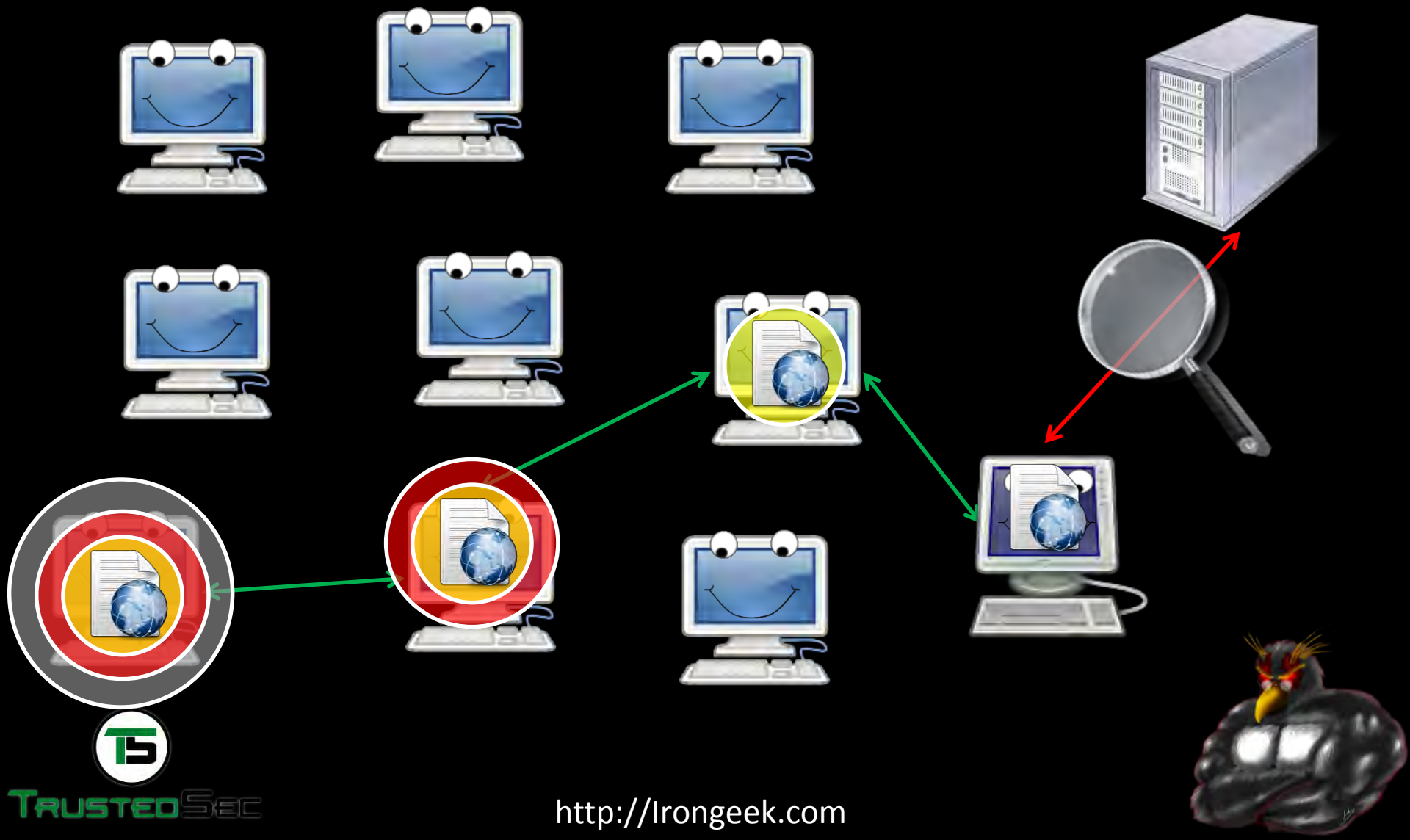
- **Who?**
  First the US Naval Research Laboratory, then the EFF and now the Tor Project (501c3 non-profit).
  http://www.torproject.org/
- **Why?**
  "Tor is free software and an open network that helps you defend against a form of network surveillance that threatens personal freedom and privacy, confidential 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



Layers like an Ogre



TrustedSec

http://Irongeek.com

Layout to connect to Hidden Sevice

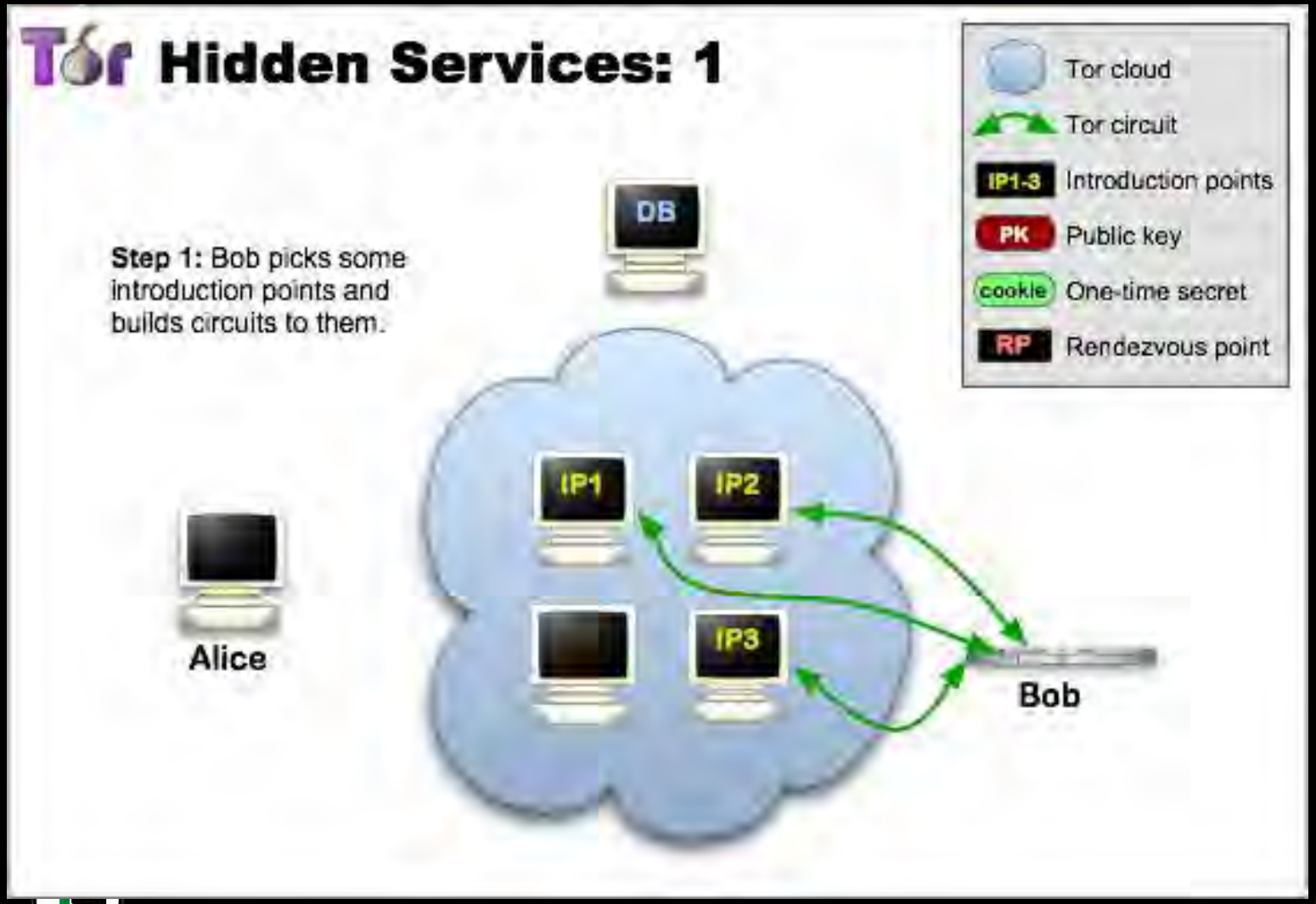


Image from http://www.torproject.org/hidden-services.html.en

Layout to connect to Hidden Sevice

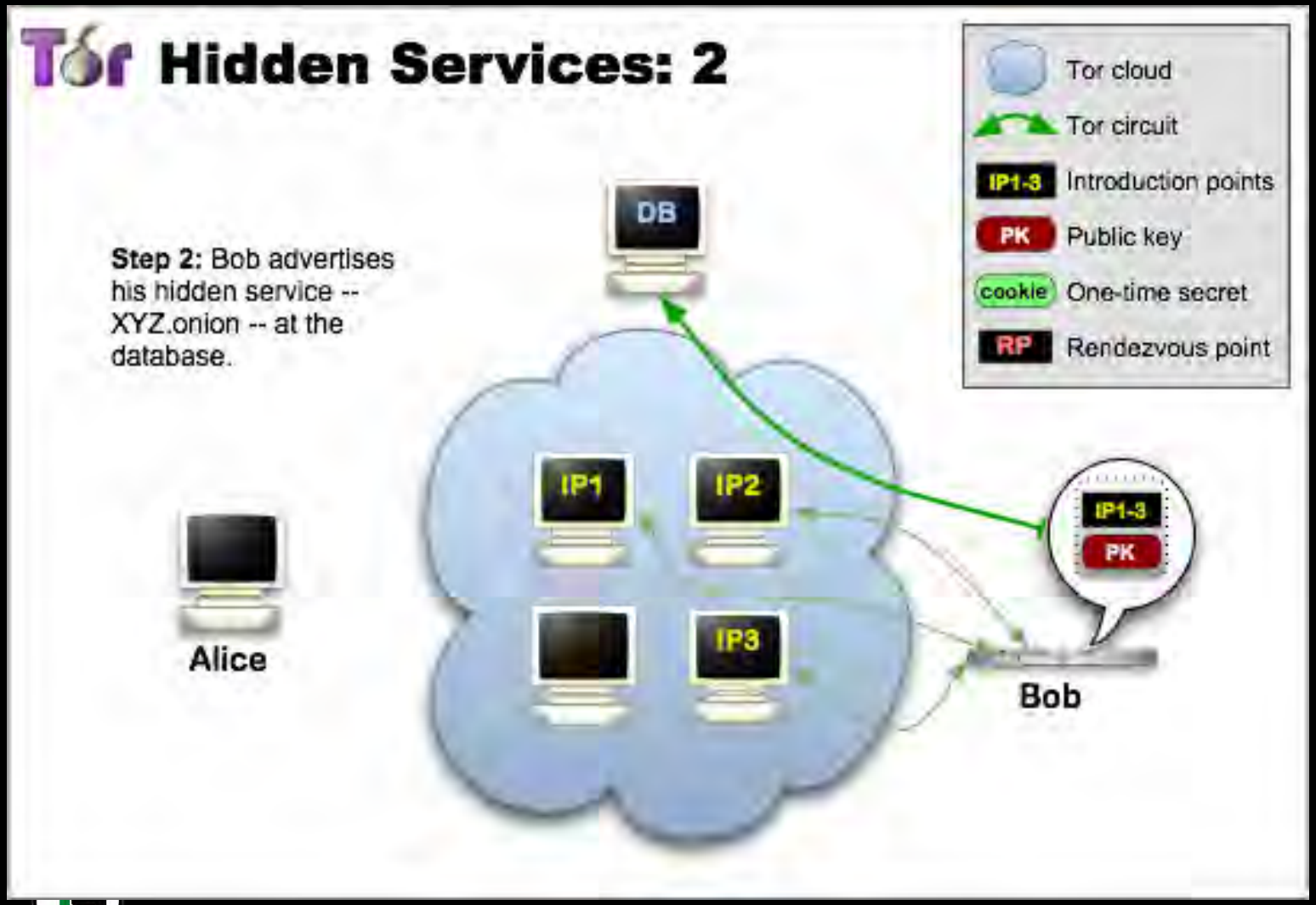


Image from http://www.torproject.org/hidden-services.html.en

http://Irongeek.com

Layout to connect to Hidden Sevice

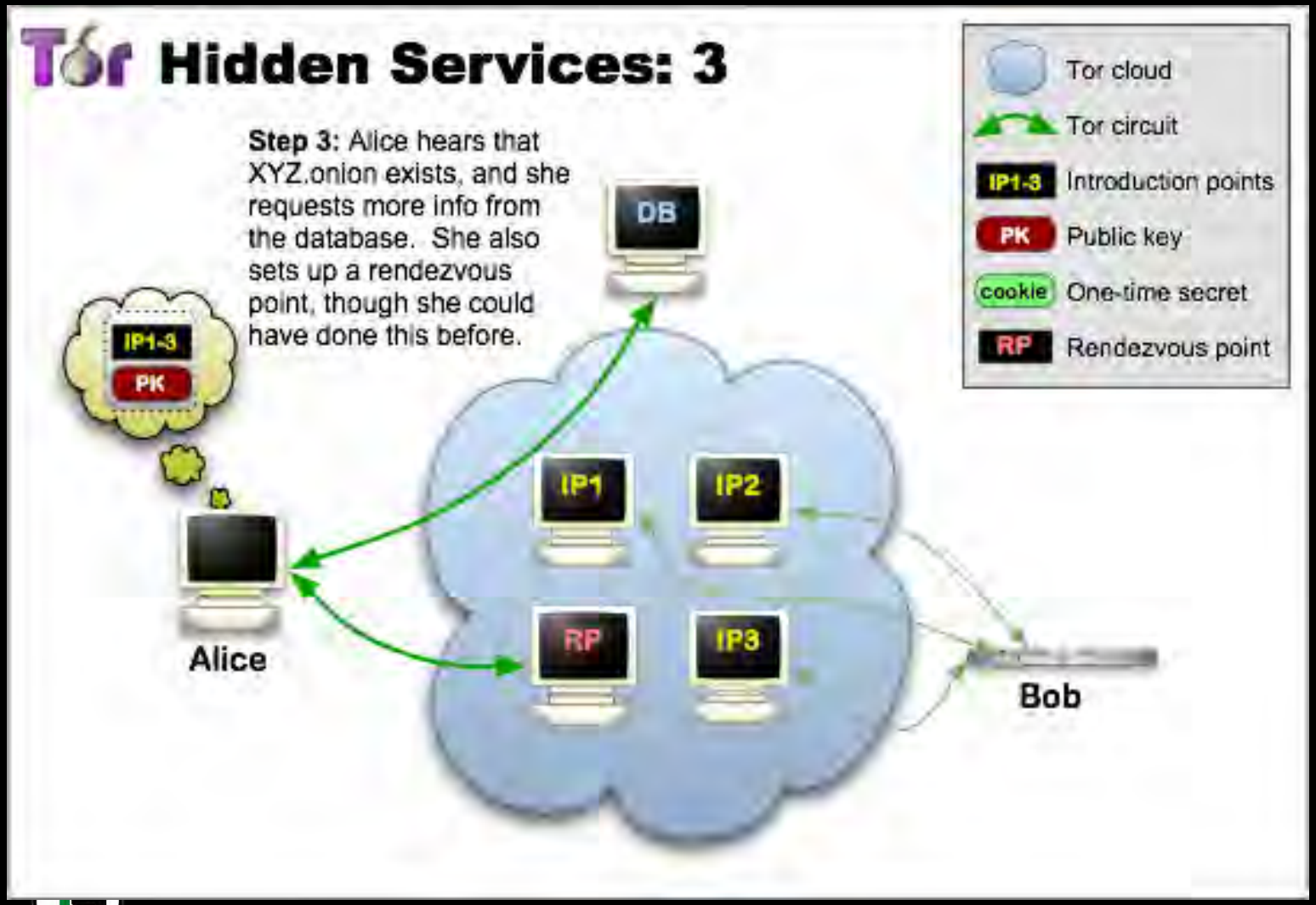


Image from http://www.torproject.org/hidden-services.html.en

http://Irongeek.com

Layout to connect to Hidden Sevice

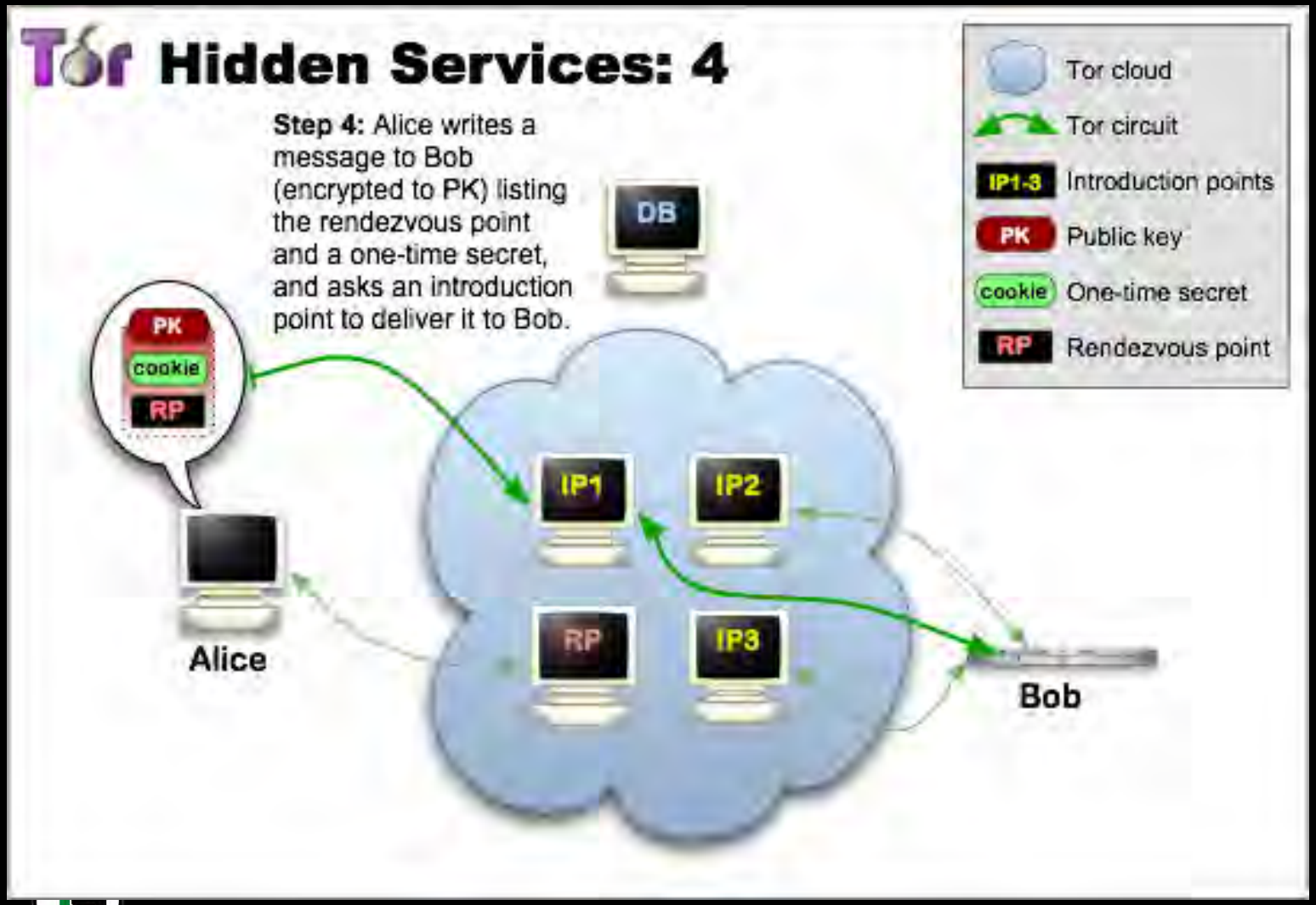


Image from http://www.torproject.org/hidden-services.html.en

Layout to connect to Hidden Sevice

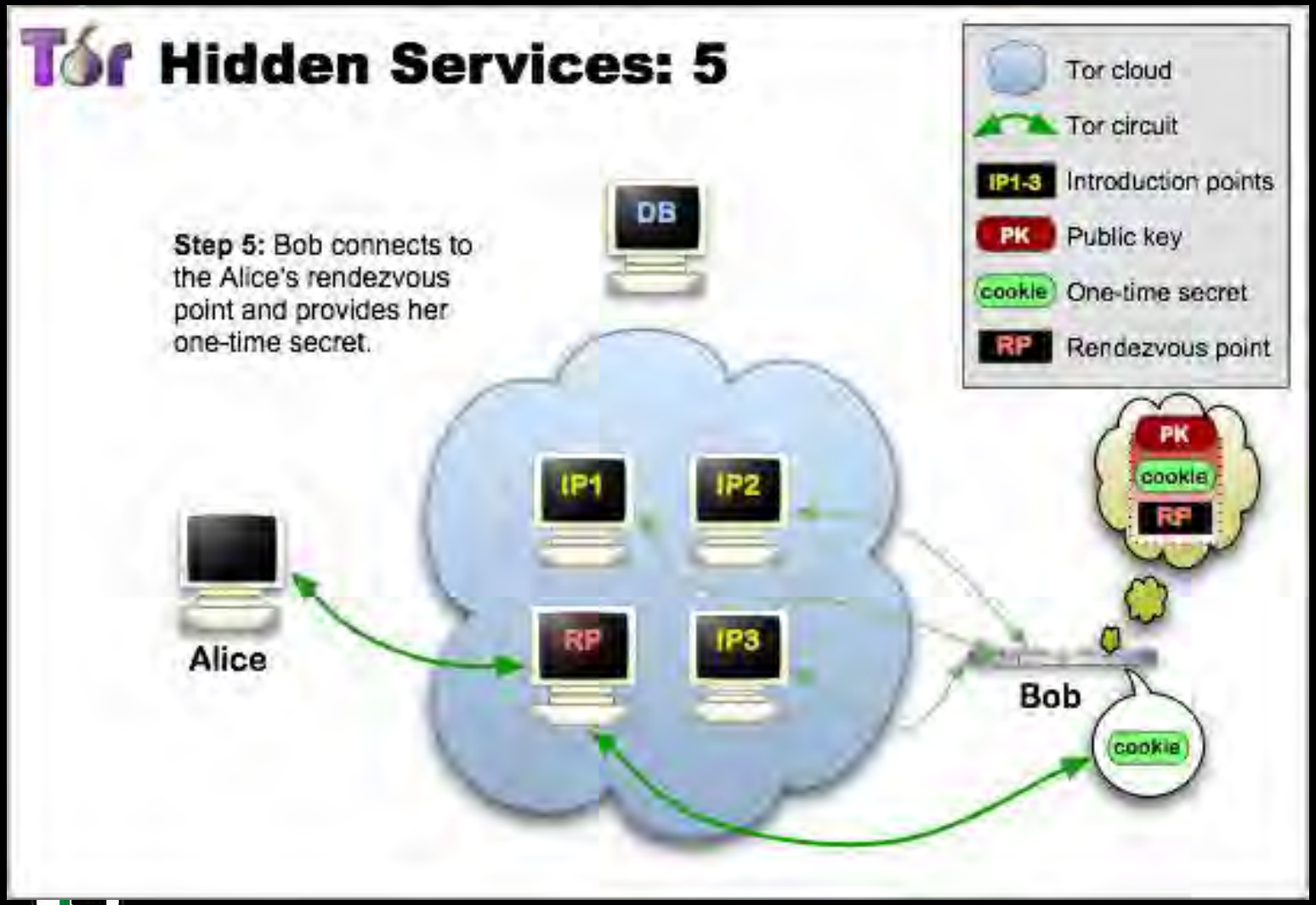


Image from http://www.torproject.org/hidden-services.html.en

http://Irongeek.com

Layout to connect to Hidden Sevice

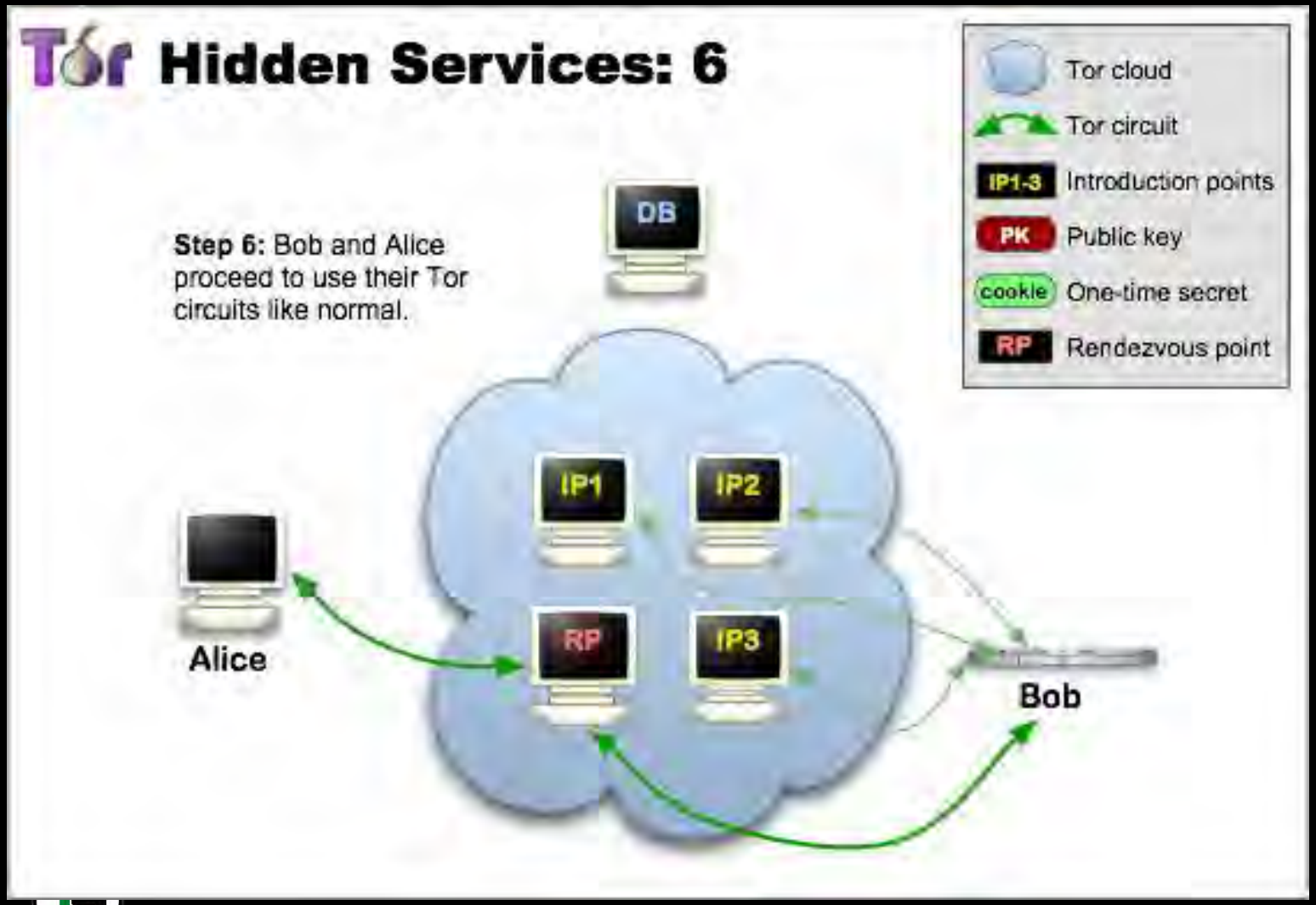


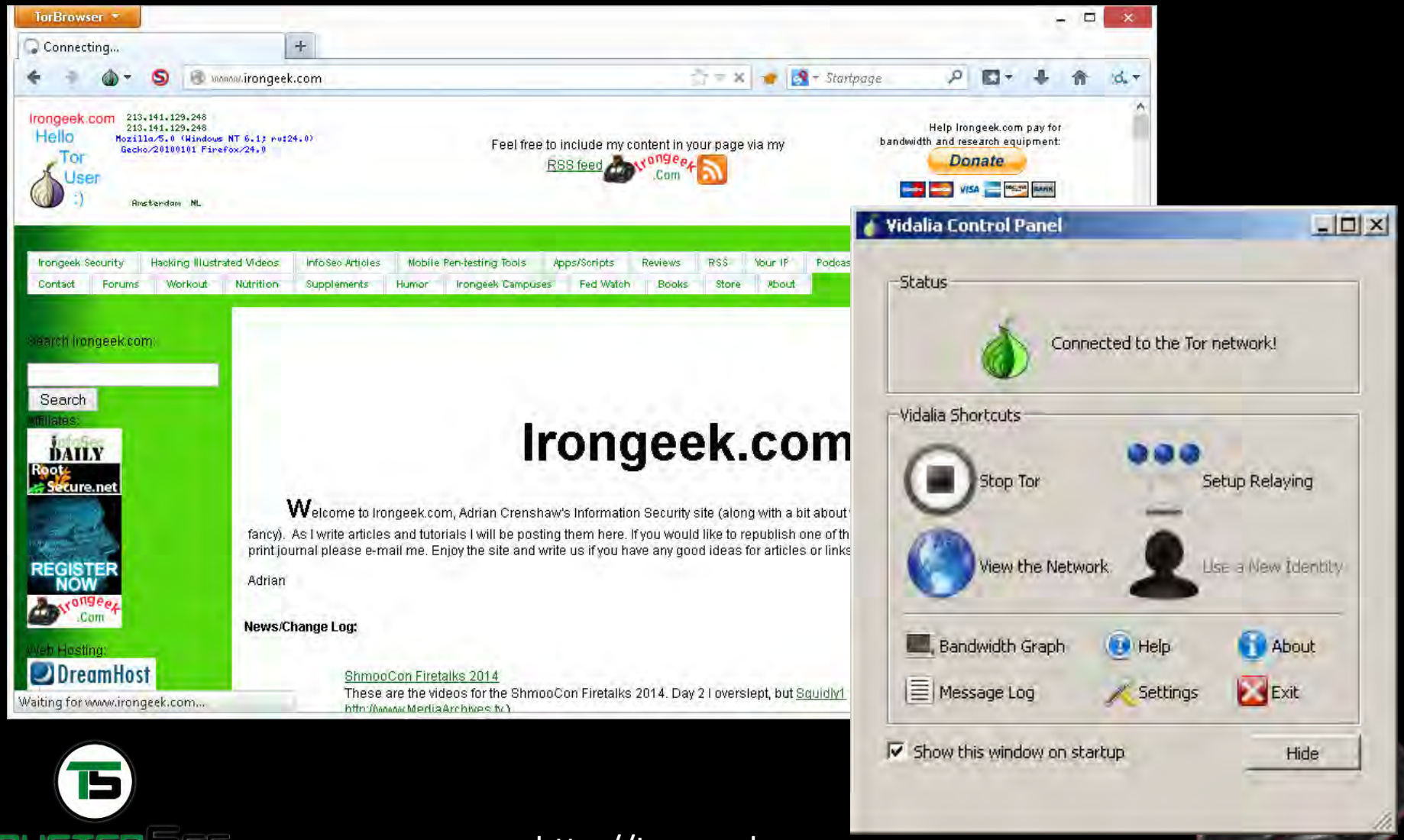
Image from http://www.torproject.org/hidden-services.html.en

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

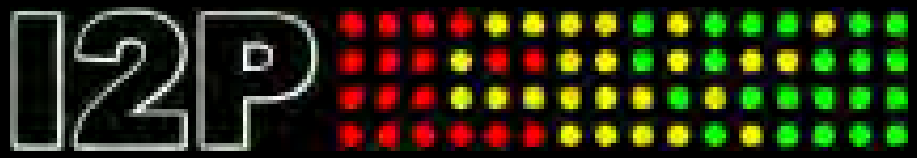
TrustedSec

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

TrustedSec



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
- Guerrilla M
  marked wh nt

To: "irongeek
From: <e9jnc
Subject: Hey
X-Originating
Content-Typ

shrapnel bombs placed in:
science center
sever hall
emerson hall
thayer hall
2/4.
guess correctly.
be quick for they will go off soon

Case 0:
Harvard Bomb Threat

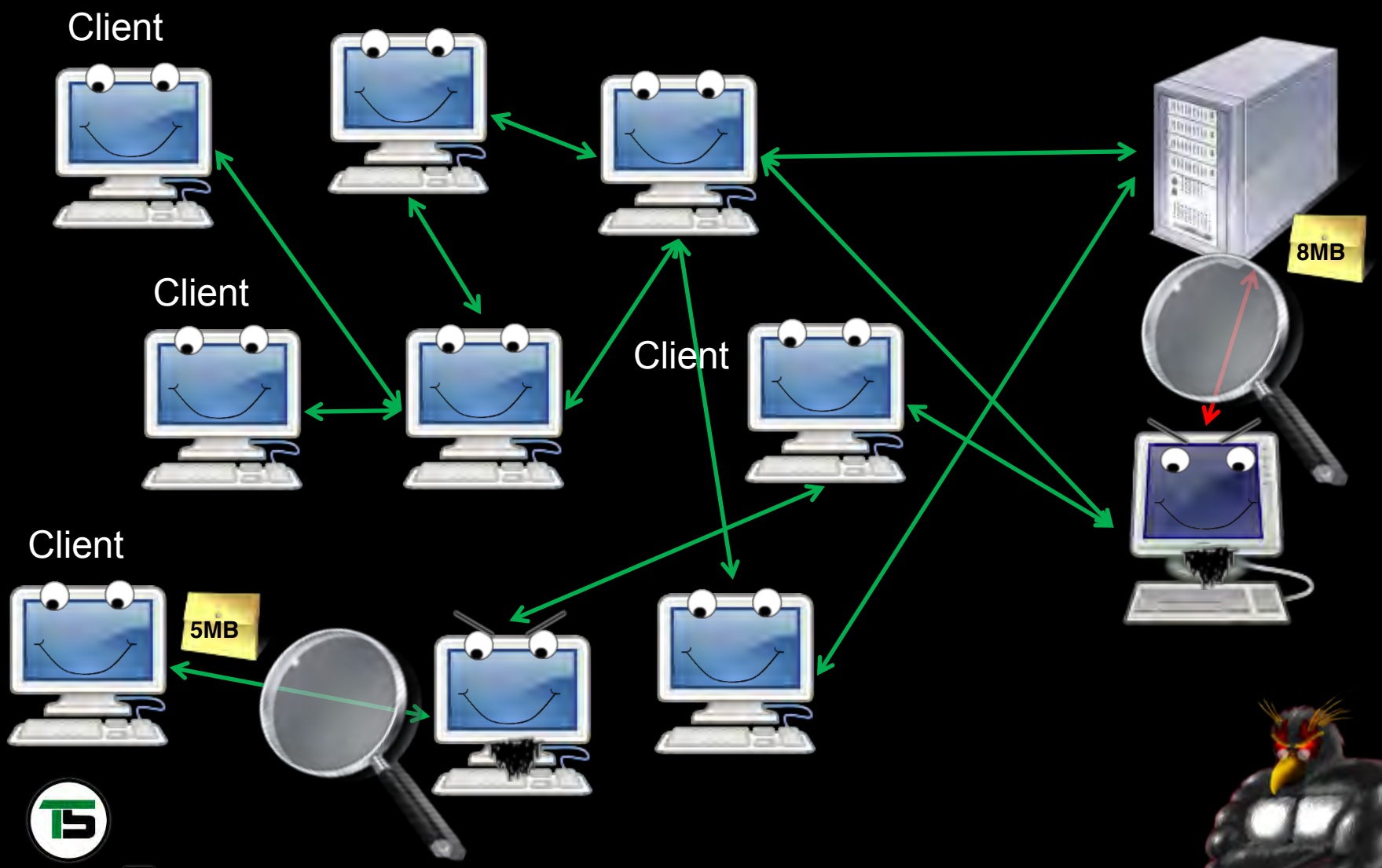
- All Tor nodes are publicly known (except bridges): http://torstatus.blutmagie.de
- Easy to correlate who was attached to Harvard network and using Tor at the same time the email was sent (unless you use a bridge).
- Eldo Kim was connected to the Tor network around that time.
- Suspect Eldo Kim wanted 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

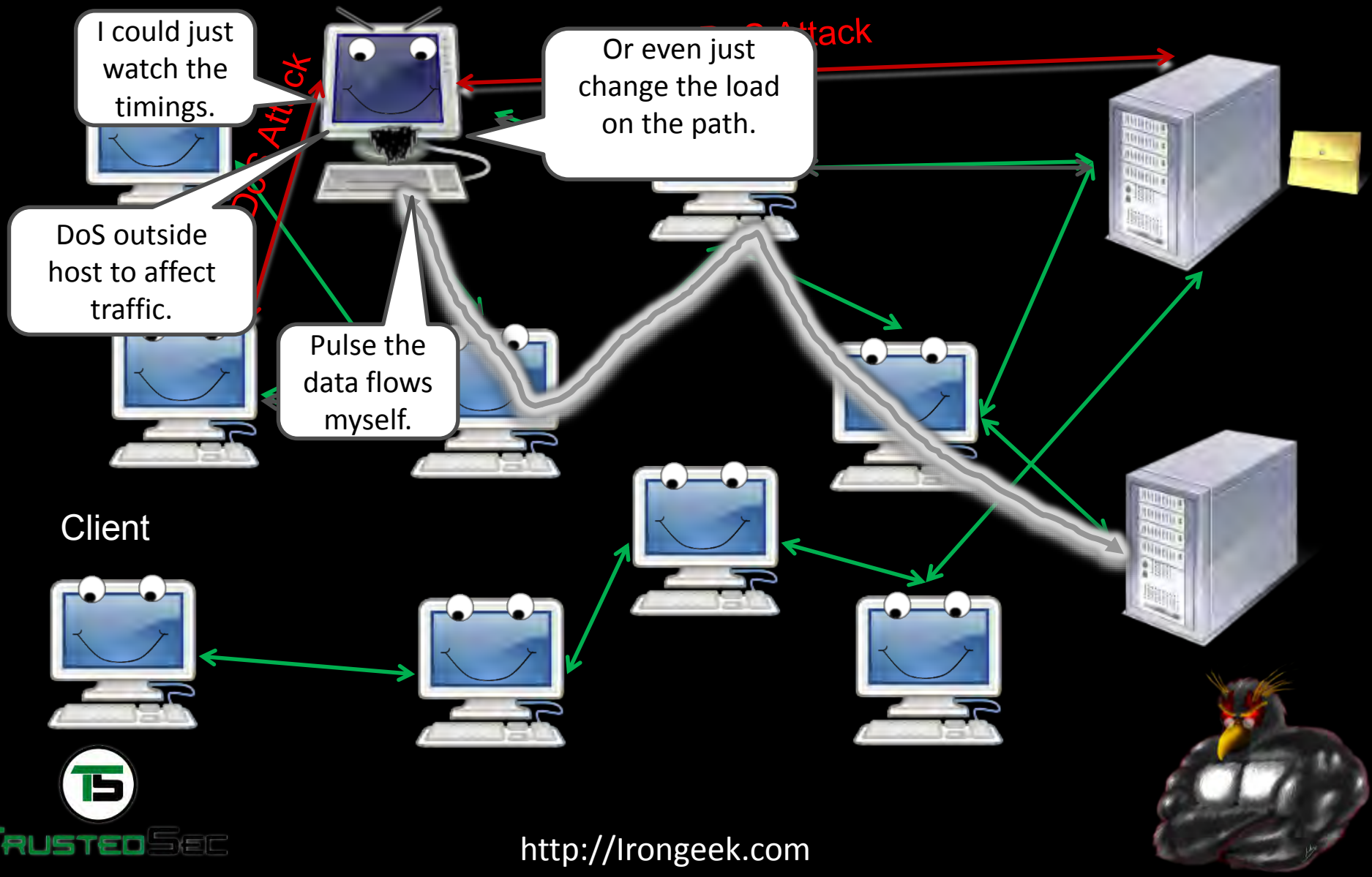
Lessons Learned:

- 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

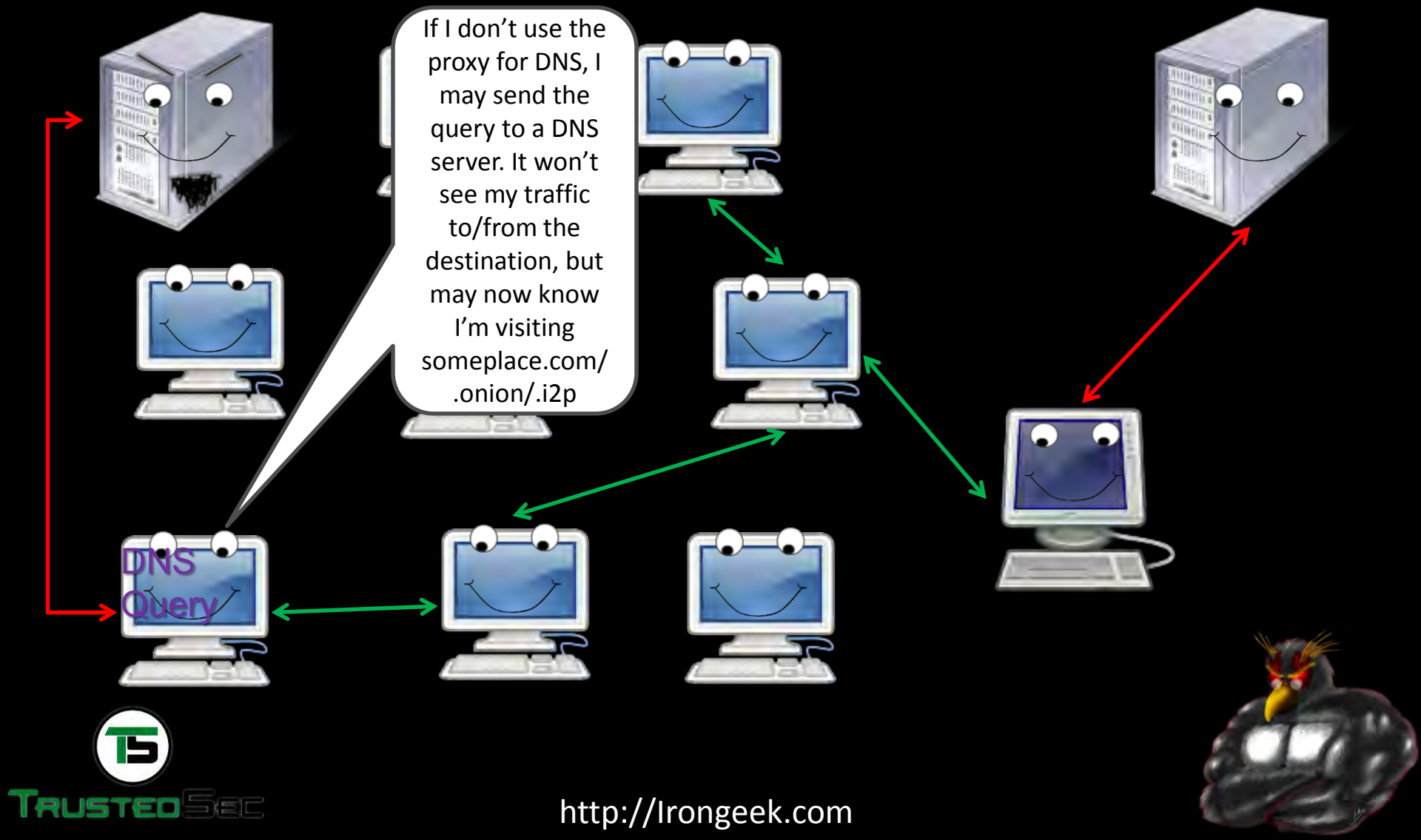


Timing Correlation



DNS Leaks

Monitored DNS Server



TrustedSec

http://Irongeek.com

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

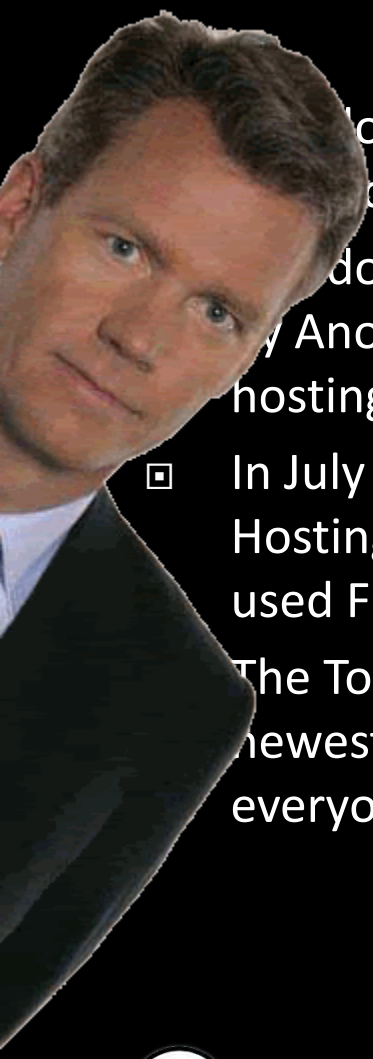
- Hammond used Tor, and while the crypto was never busted, FBI correlated times sup_g was talking to Subu on IRC with when Hammond was at home using his computer.
- More Details: http://arstechnica.com/tech-policy/2012/03/stakeout-how-the-fbi-tracked-and-busted-a-chicago-anon/

Case 1: LulzSec

Lessons Learned:

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

Case 2: Freedom Hosting



- dom Hosting hosted, amongst other things, child porn related hidden service websites.
- dom Hosting had previously come under attack y 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.

TrustedSec

http://Irongeek.com

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.

Case 2: Freedom Hosting

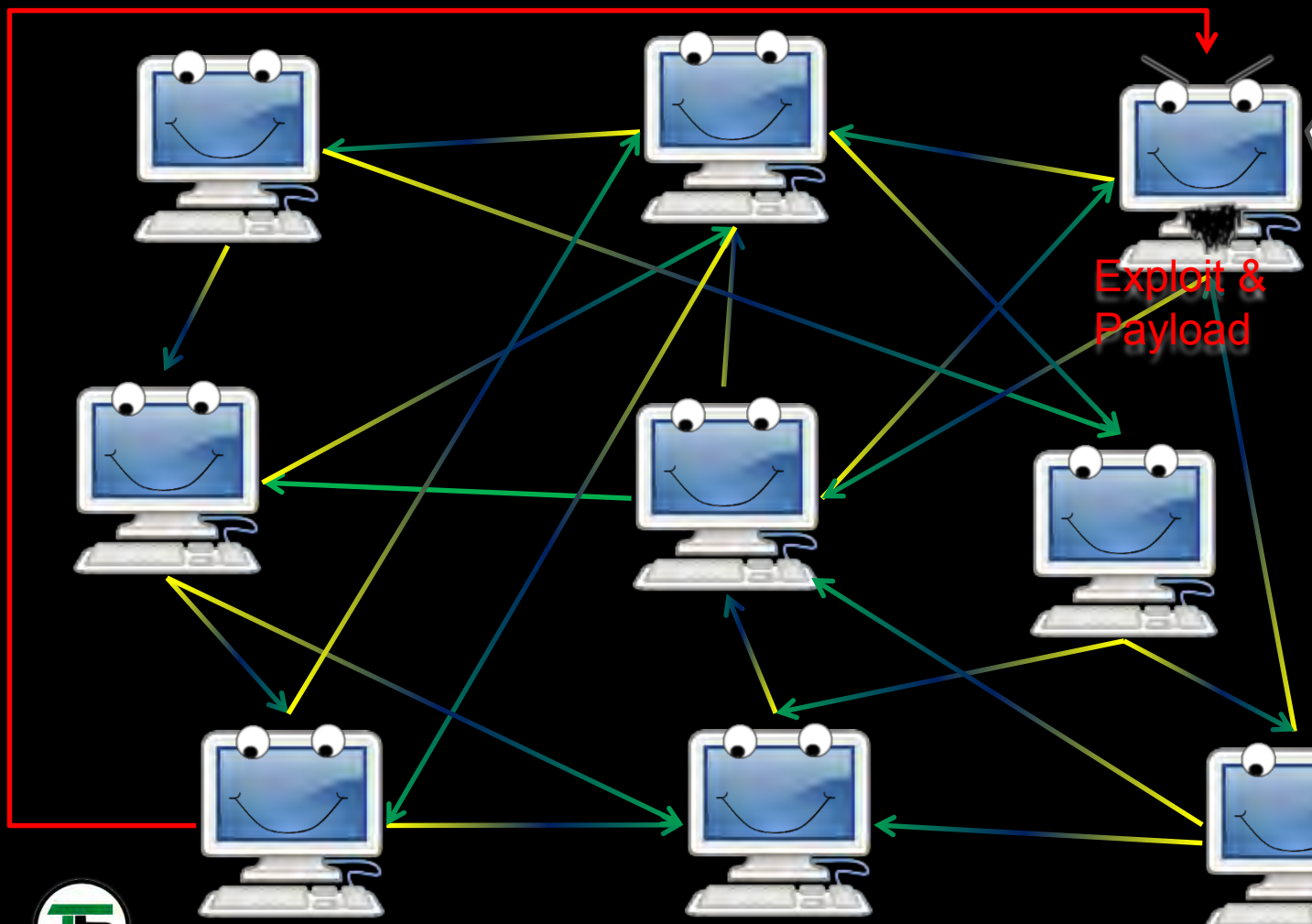
- An Irish man, Eric Eoin Marques, is alleged to be the operator of Freedom Hosting. The servers hosting Freedom Hosting were tied to him because of payment records.
- Marques was said to have dived for his laptop to shut it down when police raided him.
- More Details: http://www.wired.com/threatlevel/2013/09/freedom-hosting-fbi/

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.

http://Irongeek.com

- Som
  Rob
  allo
  lega
  http
- With
  FBI
- The
  the

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."

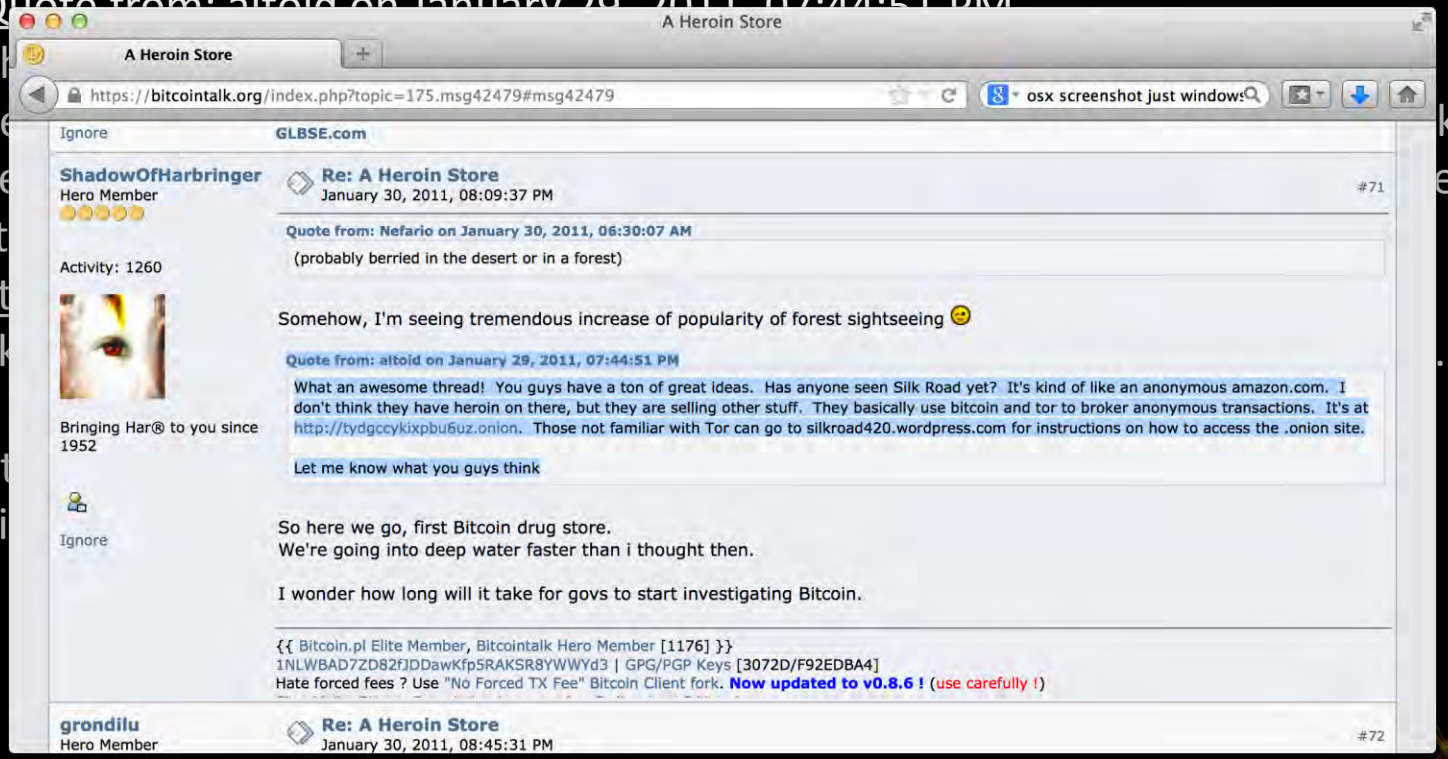
Case 3: The Silk Road

- 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

Case 3: The Silk Road

- BitCoinTalk.org Post
- "Quote from: altoid on January 29, 2011, 07:44:51 PM
  Wh
  see
  the
  bit
  htt
  silk

  Let
  thi

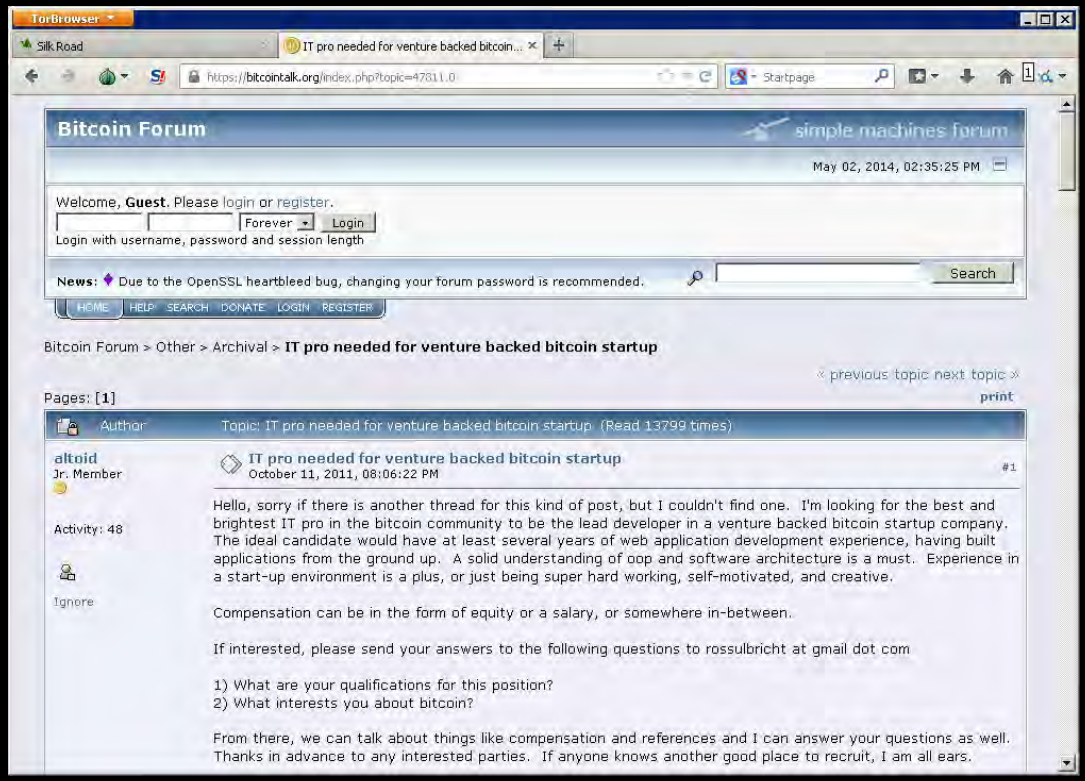


TrustedSec

http://Irongeek.com

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

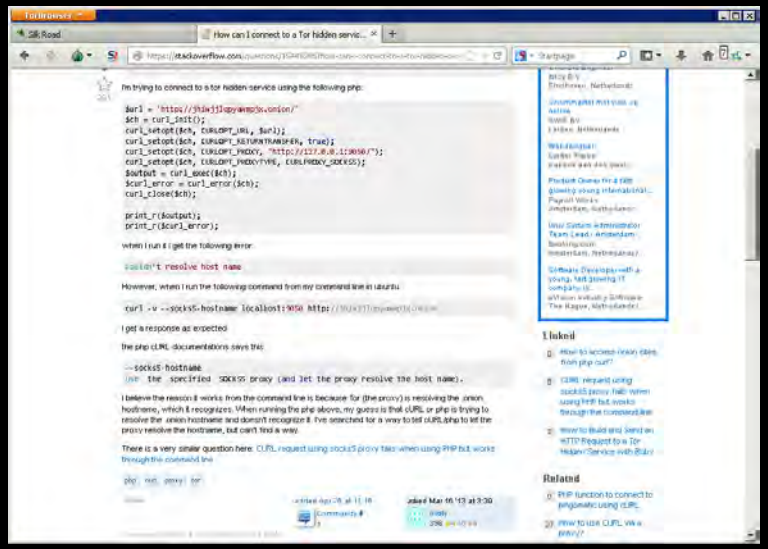


Case 3: The Silk Road

- 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.

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



- 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

TrustedSec

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?

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
- 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 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

TrustedSec

http://Irongeek.com

QUESTIONS?

42

Twitter: @Irongeek_ADC