

DARKNETS AND HIDDEN SERVERS: LOCATING I2P SERVICES VIA LEAKS ON THE APPLICATION LAYER

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
- ▣ (ir)Regular on the ISDPodcast
<http://www.isd-podcast.com/>
- ▣ Researcher for Tenacity Institute
<http://www.tenacitysolutions.com/>



Goals

- ▣ Find items on the application layer that may give away the identity of the operator, or at least reduce their anonymity set
- ▣ The information above can be used for:
 - Making suggestions so as to increase the anonymity of some I do like...
 - ...And to identify those I don't
- ▣ Yes, I know those points are at odds

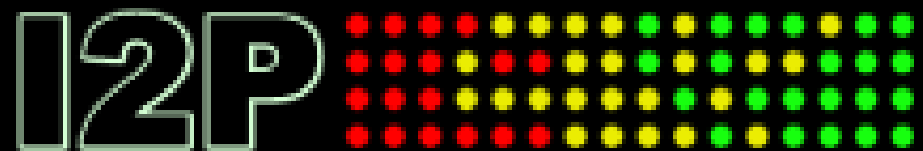


A little background...

Darknets

- ▣ There are many definitions, but mine is “anonymizing private networks”
- ▣ Use of encryption and proxies (some times other peers) to obfuscate who is communicating to whom





I2P

Invisible Internet Project
(in a nutshell)
Especially as compared to Tor



Overview

▣ Who?

I2P developers, started by Jrandom.

<http://www.i2p2.de/>

▣ Why?

To act as an anonymizing layer on top of the Internet

▣ What?

Mostly other web sites on I2P (eepSites), but the protocol allows for P2P (iMule, i2psnark), anonymous email and public Internet via out proxies.

▣ How?

Locally ran proxies that you can connect to and control via a web browser. These connect other I2P routers via tunnels. Network information is distributed via a DHT know as NetDB.



Layout

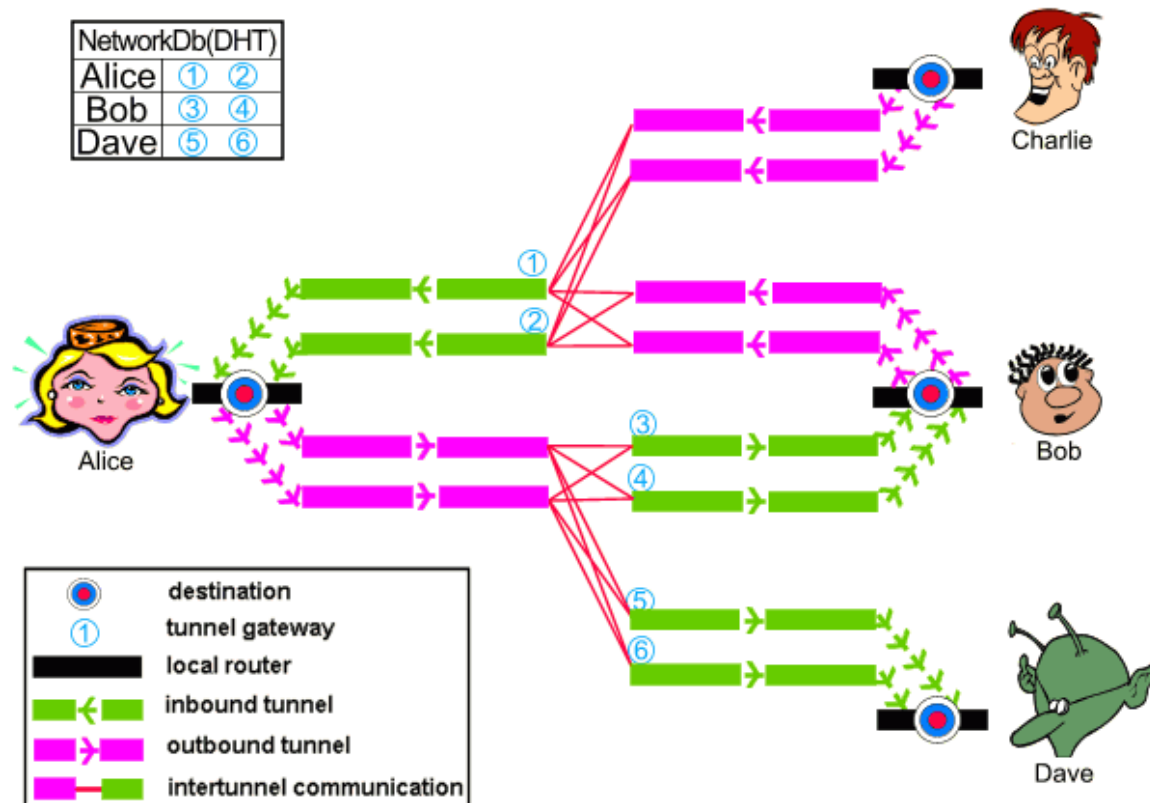


Image from http://www.i2p2.de/how_intro

<http://Irongeek.com>



Encryption Layers



- ❑ ElGamal/SessionTag+AES from A to H
- ❑ Private Key AES from A to D and E to H
- ❑ Diffie–Hellman/Station-To-Station protocol + AES

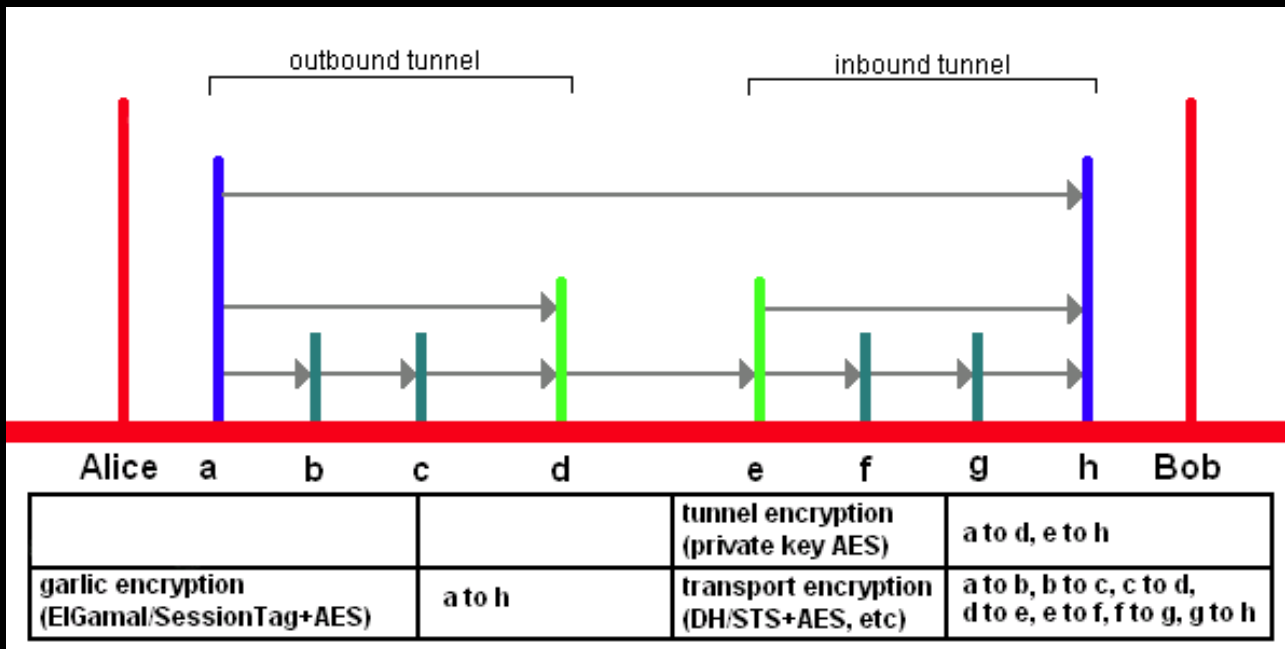
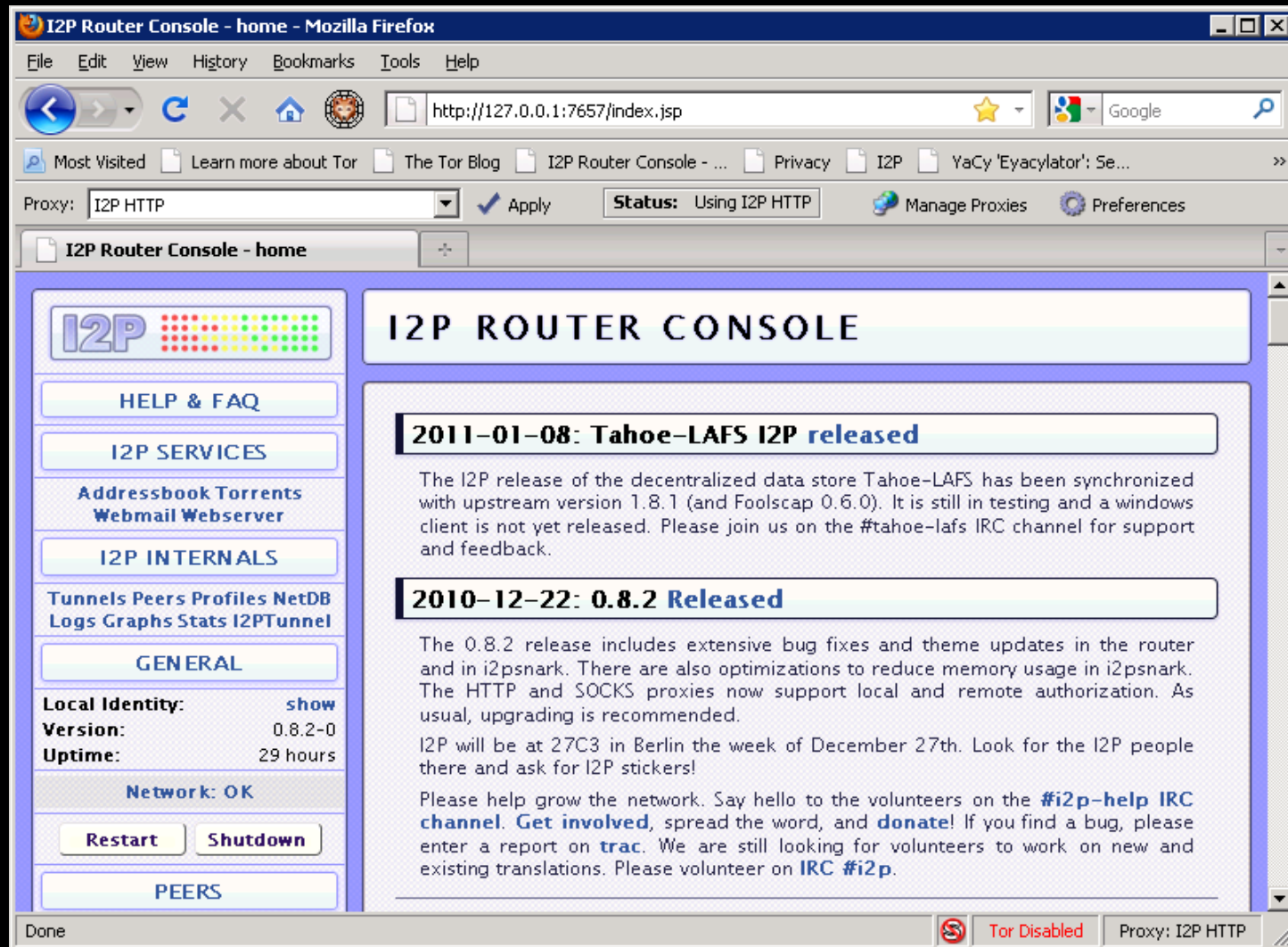


Image from <http://www.i2p2.de/>
<http://Irongeek.com>



What does it look like to the user?



Naming and Addresses

- ▣ Details

<http://www.i2p2.de/naming.html>

- ▣ 516 Character Address

-KR6qyfPWxON~F3UzzYSMIsaRy4udcRkHu2Dx9syXSzUQXQdi2Af1TV2UMH3PpPuNu-GwrqihwmLSkPFg4fv4yQQY3E10VeQVuI67dn5vlan3NGMsjqxoXTSHHt7C3nX3szXK90JSO~tRMD11xyqtKm94-RpIyNcLXofd0H6b02683CQIjb-7JiCpDD0zharm6SU54rhdisIUVXp1lxYgg2pKVpssL~KCp7RAGzpt2rSgz~RHFsecqGBefwJdiko-6CYW~tcBcigM8ea57LK7JjCFVhOoYTqgk95AG04-hfehnmbtuAFHWklFyFh88x6mS9sbVPvi-am4La0G0jvUJw9a3wQ67jMr6KWQ~w~bFe~FDqoZqVXl8t88qHPivXelvWw2Y8EMSF5PJhWw~AZfoWOA5VQVYvcmGzZIEKtFGE7bgQf3rFtJ2FAtig9XXBsoLisHbJgeVb29Ew5E7bkwxvEe9NYkIqvrKvUAt1i55we0Nkt6xlEdhBqg6xXOyIAAAA

- ▣ SusiDNS Names

something.i2p

- ▣ Hosts.txt and Jump Services

- ▣ Base32 Address

{52 chars}.b32.i2p

rjxwbsw4zjhv4zsplma6jmf5nr24e4ymvvbycd3swgiinbvg7oga.b32.i2p



I2P Pros and Cons

Pros

- ▣ Lots of supported applications
- ▣ Can create just about any hidden service if you use SOCKS5 as the client tunnel
- ▣ Eepsites somewhat faster compared to Tor Hidden Services (Subjective, I know)
- ▣ No central point of failure
(Example: What happened to Tor when China blocked access to the core directory servers on September 25th 2009)

Cons

- ▣ Limited out proxies
- ▣ Sybil attacks a little more likely



Previous Attacks

- ▣ Clock based attacks
- ▣ Traffic flow analysis
- ▣ Sybil/infrastructure attacks
- ▣ Many more...

http://www.i2p2.de/how_threatmodel.html



Approach

“Specific exploits are temporary, bad configuration mistakes are forever”.

1. Banner grabs of both eepSites inside of I2P, and against know IPs participating in the Darknet, to reduce the anonymity set of the servers.
2. Reverse DNS and who is lookups to find out more information concerning the IPs of the I2P nodes.
3. TCP/IP stack OS finger printing.
4. Testing I2P virtual host names on the public facing IP of I2P nodes.
5. Compare the clock of the remote I2P site, and suspected IP hosts on the public Internet, to our own system's clock. We did this via the HTTP protocols “Date:” header.
6. Command injection attacks.
7. Web bugs to attempt to de-anonymize eepSite administrators or users. (This turned out more problematic than we originally thought)



Challenges

1. Communications with the eepSites is normally done via an HTTP proxy. This restricts our attack options somewhat. Where DNS queries went made a huge difference.
2. Perhaps because of point one, many of the tools I have experimented with so far have a tendency to give false results or hang while working on spidering an eepSite.
3. Filtering of client requests makes it somewhat harder to attack the administrator of an eepSite via web bugs, or odd XSS attacks put into the logs.
4. While spidering I needed to be careful not to download contraband onto my own system.



Improvements/Deliverables

1. Clearer examples of how leaked information can be found.
2. A concentration on I2P instead of Tor.
3. A concentration on the application layer instead of the network or transport layers.
4. Real world tests on systems that have been implemented for more than just academic purposes.
5. Less reliance on esoteric attack vectors.



PROBING I2P

Data collection and tools



Collecting eepSites

- ▣ Spider some of the popular portal eepSites like forum.i2p or ugha.i2p for URLs ending in .i2p, then continue spidering from there recursively.
- ▣ Another option is to parse though the host.txt file I2P uses for name to cryptographic identifier mappings, and check each i2p service for availability.
- ▣ Or both



Scripts

- ▣ [I2PMassGrabber-headers.py](#)
Checks the status of each I2P host listed in an I2P host.txt file to see if it's up, and then generates CSV and HTML formatted output with the hostname, status, and server banner. Input file and proxies will have to be changed based on user settings. This script also collects page scrapes that can be reviewed.
- ▣ [real-IP-banner.py](#)
Grabs HTTP banners from an Internet facing IP so we can compare, sort and filter later.
- ▣ [dump-and-sort-i2p-router-ips.py](#)
NetDB scraping code used to obtain a list of IPs from our local NetDB cache. The RegEX needs some work as some invalid IPs work their way into the resulting output text. Generates or adds to a file named all-sorted-uniq.txt, so this script can be ran by a scheduler to collect the IPs of I2P nodes over time.
- ▣ [time-stamp-server.py](#)
Compares times stamps found in the HTTP headers of both Internet IPs and I2P sites to the local clock, along with retrieval times, generating a CSV file and a synopsis in HTML.
- ▣ [virtual-server-test.py](#)
I2P Virtual Host checking script. This script uses a large CSV file to try specific I2P host names on a given public IP to see if a different page is returned. It saves scrapes of these pages to a time stamped directory.
- ▣ Download:
<http://www.irongeek.com/host/i2p-probe-scripts.zip>



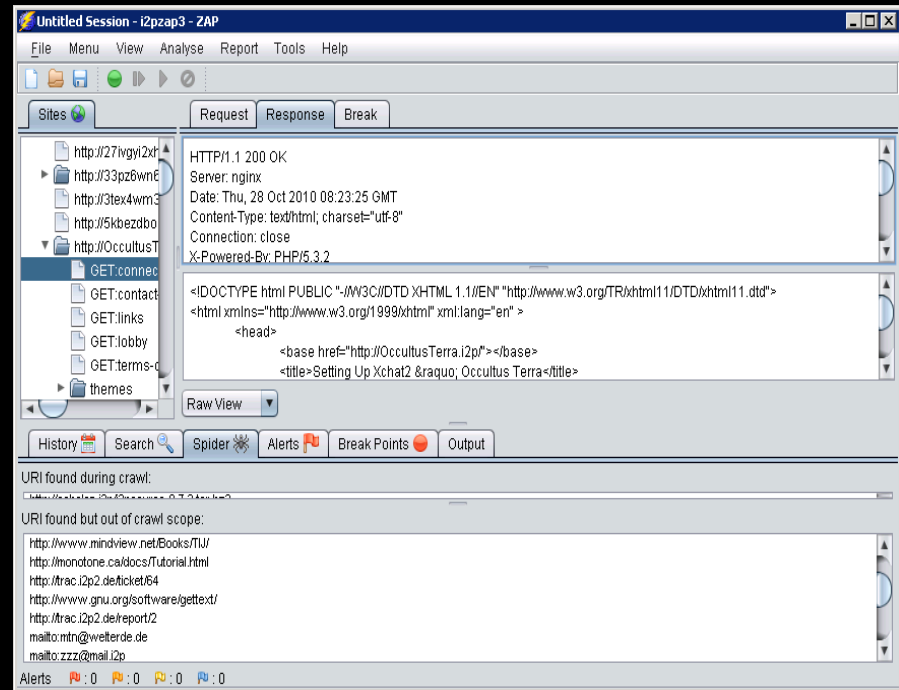
Output Format

- ▣ CSV, since we can import it just about anywhere
- ▣ `"bitcoin4cash.i2p","200","Apache"`
`"shpargalko.i2p","200","Apache/2.2.15 (Win32) PHP/5.3.2"`
`"darrob.i2p","200",""`
`"ufm.i2p","200","Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.12 with Suhosin-Patch"`
- ▣ Page scraps and headers so we can see the pages incase they are offline later.



Other Tools:ZAP

- ❑ ZAP
(ZED Attack Proxy)
- ❑ Has spidering, file/directory brute-forcing and scanning features



- ❑ Download:
[http://www.owasp.org/index.php/OWASP Zed Attack Proxy Project](http://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project)



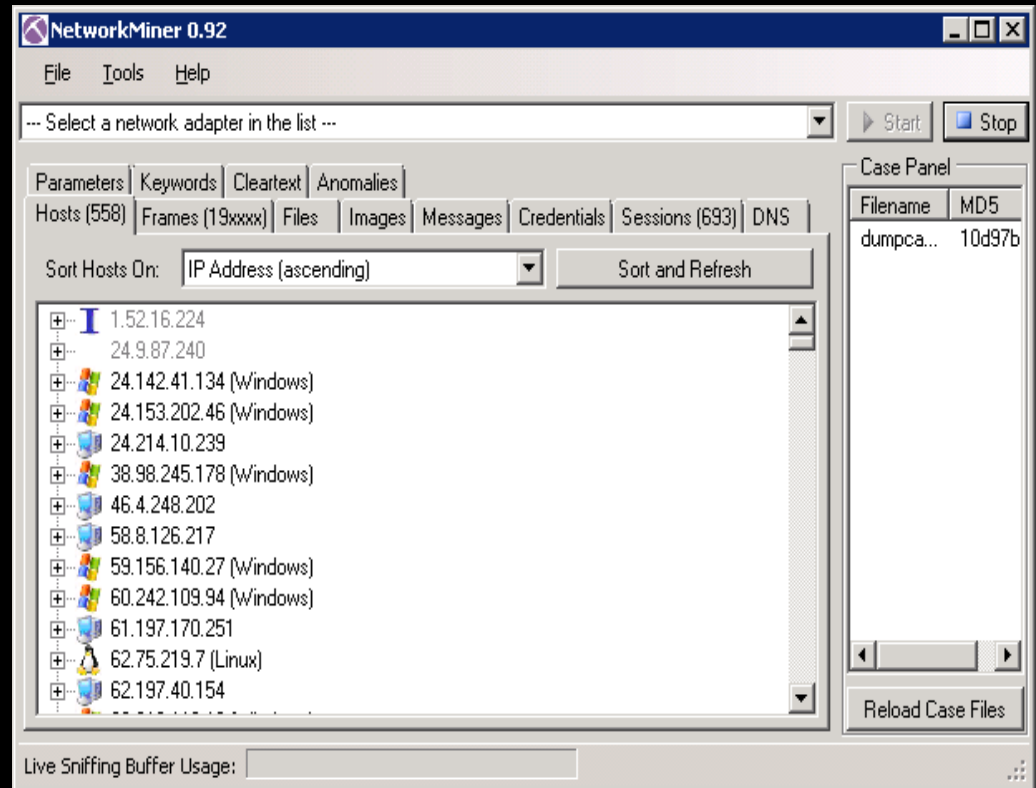
Other Tools: Wireshark/Dumpcap

- ▣ `dumpcap -i \Device\NPF_{E97777A0-5863-4741-AA42-FD3E02B2BD4C} -s 0 -f "port 12668" -w g:\dumpcap.pcap -a duration:3600`
- ▣ -i to tell dumpcap which network interface to use (if you are not sure which of your local interfaces to use, see the local interfaces options by using the `-D` flag)
 - s to set the snap length so that we capture the whole packet
 - f specifies the capture filter to use, thus emanating packets we may not care about
 - w locates the pcap file to output
 - a tells dumpcap to stop capturing under certain circumstances (in this case after one hour)
- ▣ Download:
<http://www.wireshark.org/>



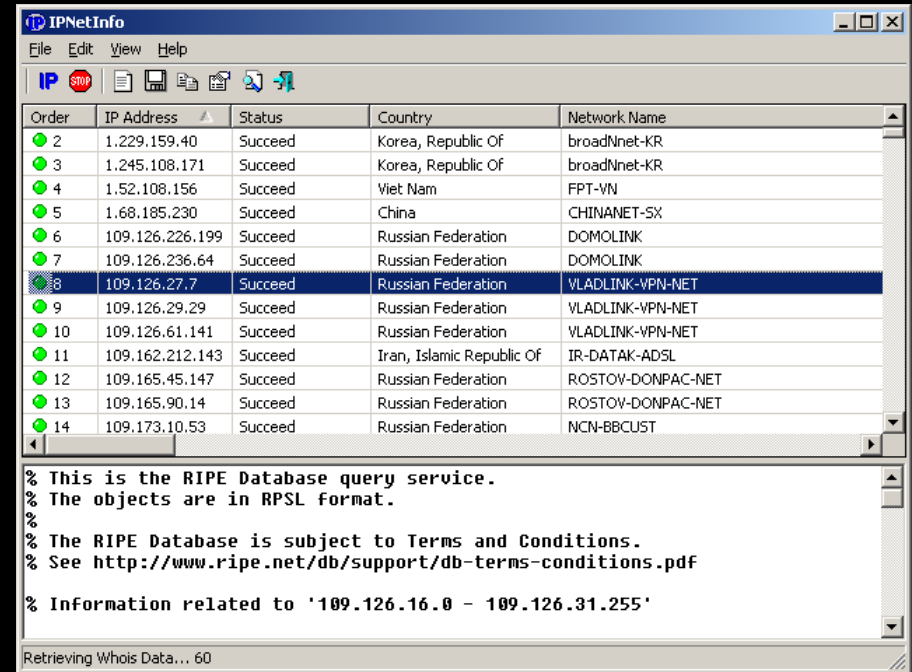
Other Tools: NetworkMiner

- ▣ NetworkMiner was used for OS fingerprinting
- ▣ Can extract needed data from a pcap file
- ▣ Download:
<http://networkminer.sourceforge.net/>



Other Tools: IPNetInfo

- ▣ Takes output from `dump-and-sort-i2p-router-ips.py`
- ▣ Does a Whois to recover owner, IP range, contact information, country, etc.



The screenshot shows the IPNetInfo application window. It has a menu bar (File, Edit, View, Help) and a toolbar with icons for IP, Stop, Print, Save, Open, Find, and Help. Below the toolbar is a table with the following data:

Order	IP Address	Status	Country	Network Name
2	1.229.159.40	Succeed	Korea, Republic Of	broadNnet-KR
3	1.245.108.171	Succeed	Korea, Republic Of	broadNnet-KR
4	1.52.108.156	Succeed	Viet Nam	FPT-VN
5	1.68.185.230	Succeed	China	CHINANET-SX
6	109.126.226.199	Succeed	Russian Federation	DOMOLINK
7	109.126.236.64	Succeed	Russian Federation	DOMOLINK
8	109.126.27.7	Succeed	Russian Federation	VLADLINK-VPN-NET
9	109.126.29.29	Succeed	Russian Federation	VLADLINK-VPN-NET
10	109.126.61.141	Succeed	Russian Federation	VLADLINK-VPN-NET
11	109.162.212.143	Succeed	Iran, Islamic Republic Of	IR-DATAK-ADSL
12	109.165.45.147	Succeed	Russian Federation	ROSTOV-DONPAC-NET
13	109.165.90.14	Succeed	Russian Federation	ROSTOV-DONPAC-NET
14	109.173.10.53	Succeed	Russian Federation	NCN-BBCUST

Below the table is a text area containing the following text:

```
% This is the RIPE Database query service.  
% The objects are in RPSL format.  
%  
% The RIPE Database is subject to Terms and Conditions.  
% See http://www.ripe.net/db/support/db-terms-conditions.pdf  
% Information related to '109.126.16.0 - 109.126.31.255'
```

At the bottom of the window, it says "Retrieving Whois Data... 60".

- ▣ Download:
<http://www.nirsoft.net/utis/ipnetinfo.html>



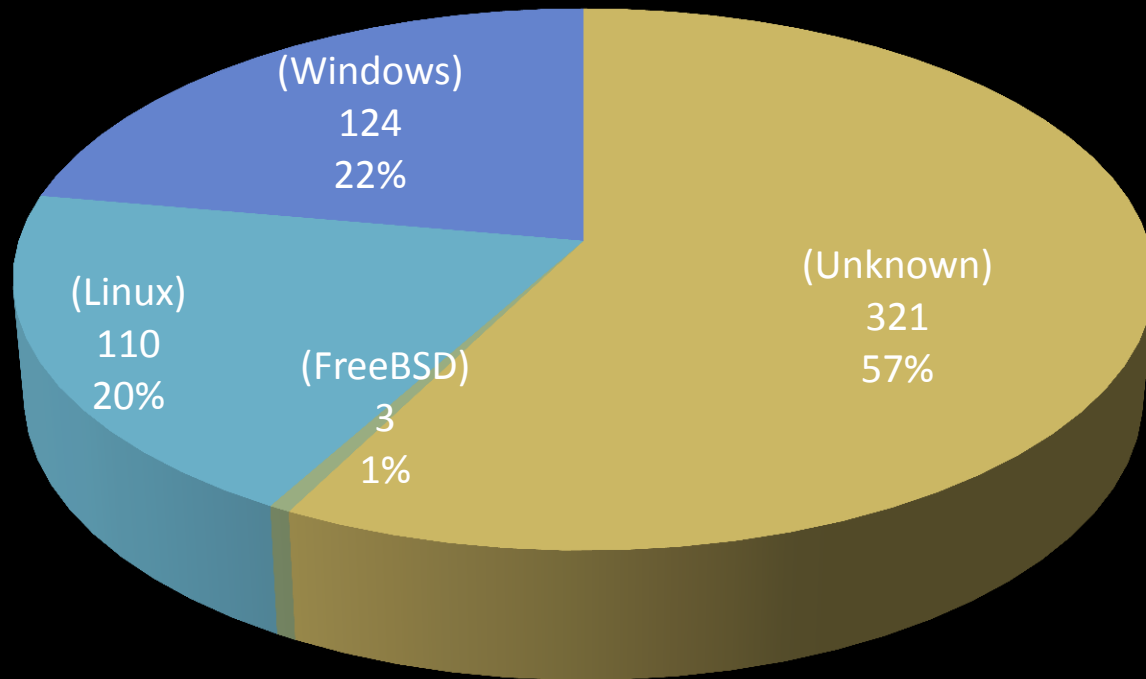
SOME GENERAL ANALYSIS

Items that may not be that anonymity threatening, but are still useful or interesting



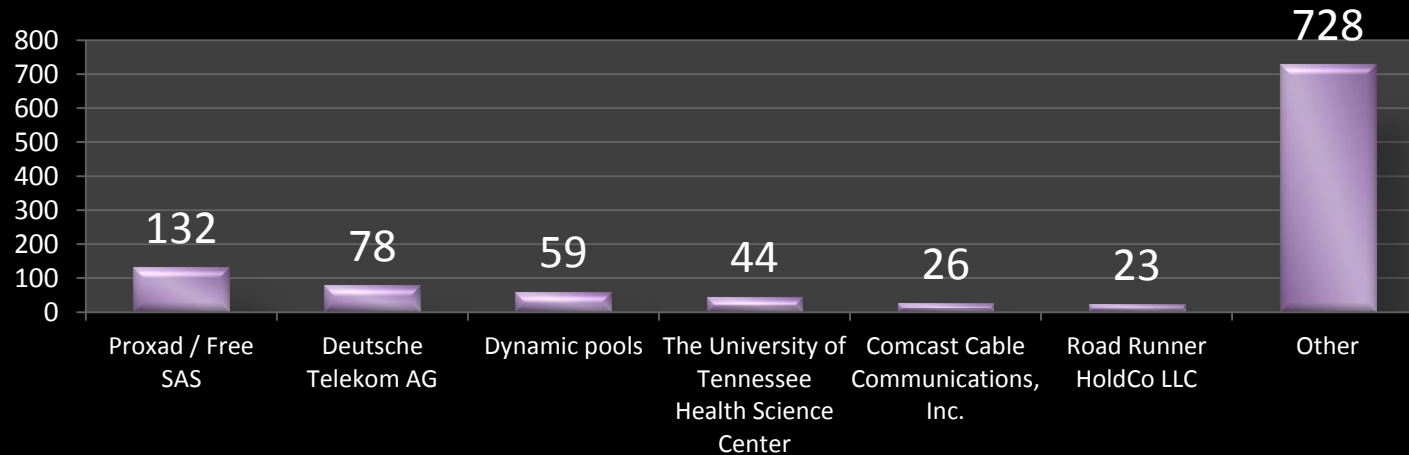
OS stats based on an hour long packet capture

NetworkMinor OS Detection by IP Stack

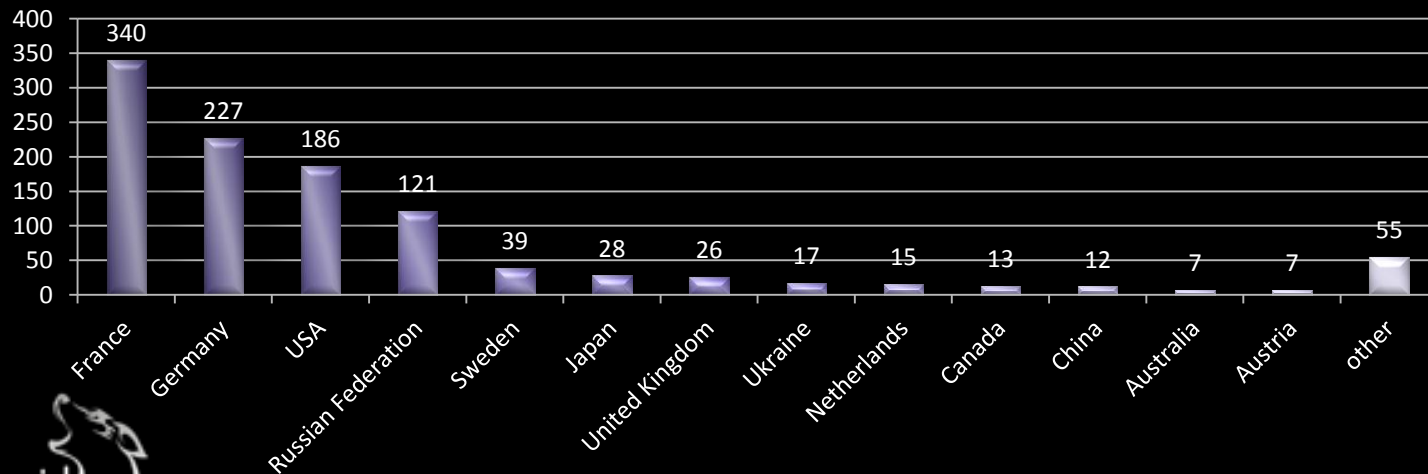


Organization and Country information

I2P Nodes By Organization



I2P Nodes By Country



What is in a name?

- ▣ What does a name like thor.schmelz.com tell you?
- ▣ NIMBIOS had 44 nodes in I2P on 11/9/2010
- ▣ Detecting possible Sybil attacks?



ATTACKS THAT WORKED...

...and mitigations



Main Attacks We Focused On

1. Correlating server banners grabbed from inside of I2P and off of the public Internet
2. Clock Differences
3. Command Injection attack



Summary before the details

Caveats:

- ▣ Exact statistics on the reliability of attacks are not easy
- ▣ Churn can be somewhat compensated for by collecting data over a longer period of time

Results:

- ▣ Correlating server banners grabbed from inside of I2P and off of the public Internet
 - Out of 119 I2P hostnames we have in our set we found 21 IP/I2P correlations
 - See paper for more details
- ▣ Clock Differences
 - Found only 1 new likely IP/I2P correlation
 - Helped confirm others
- ▣ Command Injection attack
 - Workable, but highly dependent on site

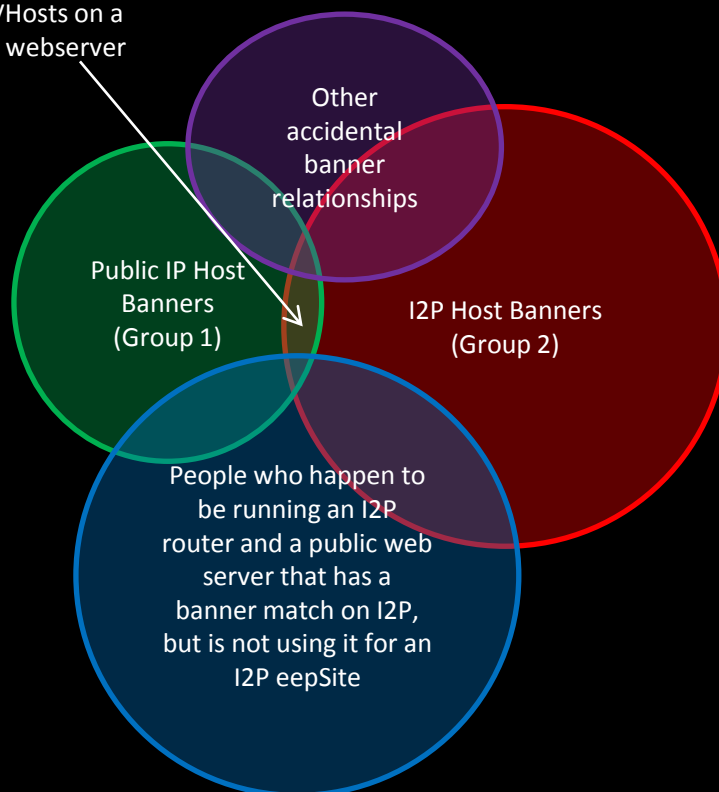


Correlating server banners grabbed from inside of I2P and off of the public Internet:

What we are looking for?

▣ Venn diagram

People running their eepSites as VHosts on a public facing webserver



What do I mean by HTTP headers?

Client example:

```
GET http://www.i2p2.i2p/ HTTP/1.1
Host: www.i2p2.i2p
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.12)
Gecko/20101026 Firefox/3.6.12
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Proxy-Connection: keep-alive
Referer: http://127.0.0.1:7657/index.jsp
```

Server response:

```
HTTP/1.1 200 OK
Server: nginx/0.6.32
Date: Wed, 08 Dec 2010 13:48:46 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Etag: "1b2a7b18a524b03f598944143fc7bd52"
Content-Length: 8701
Proxy-Connection: close
```

<http://Irongeek.com>



1 to 1 Banners

- Data from 11/09/2010, imported into MS Access and queried

1 to 1 IP to I2P Banners		
I2P hostname	IP	Banner
medosbor.i2p	89.31.112.91 (host-89-31-112-91.academ.org)	Apache/2.2.13 (Linux/SUSE)
ipredia.i2p	97.74.196.206 (ip-97-74-196-206.ip.secureserver.net)	Apache/2.2.3 (CentOS)
xorbot.i2p	178.77.75.23 (www.gernot-schulz.com)	Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny9 with Suhosin-Patch
trac.i2p2.i2p	46.4.248.202 (bilbo.srv.welterde.de)	nginx/0.6.32
lurker.i2p	178.63.47.16 (fleshless.org)	nginx/0.7.65

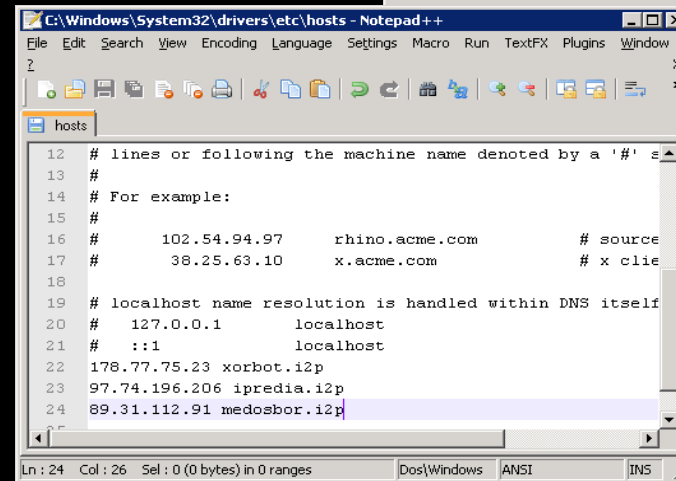
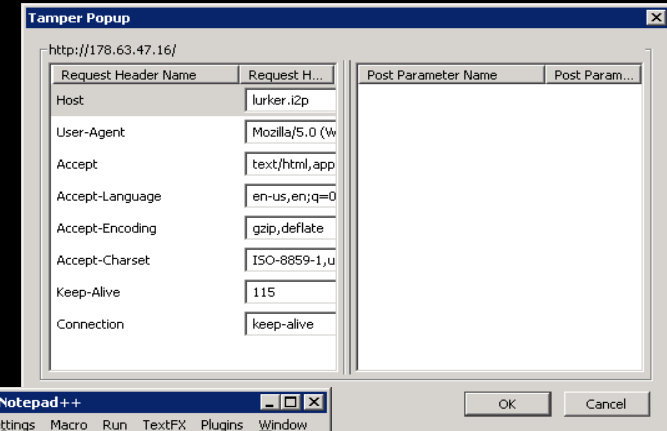
(although we later found ipredia.i2p on a different IP once we had collected more Internet facing hosts to test against)

<http://Irongeek.com>



Ways to modify the host header

- ❑ Tamperdata or a local proxy like ZED
- ❑ Modify your hosts file

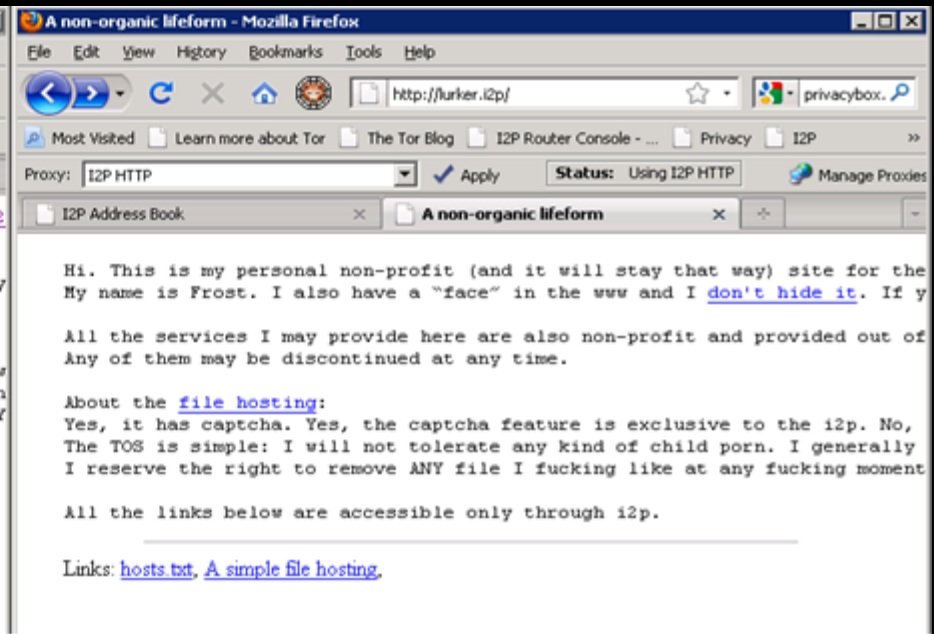
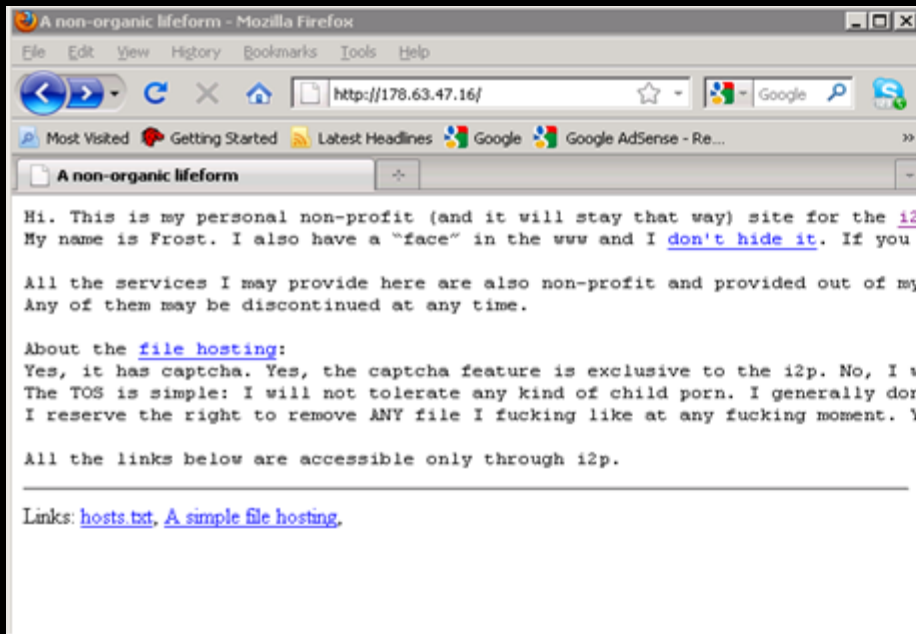


- ❑ Curl:
`curl 178.63.47.16`
`curl -H "Host: lurker.i2p" 178.63.47.16`



Results of modifying host header

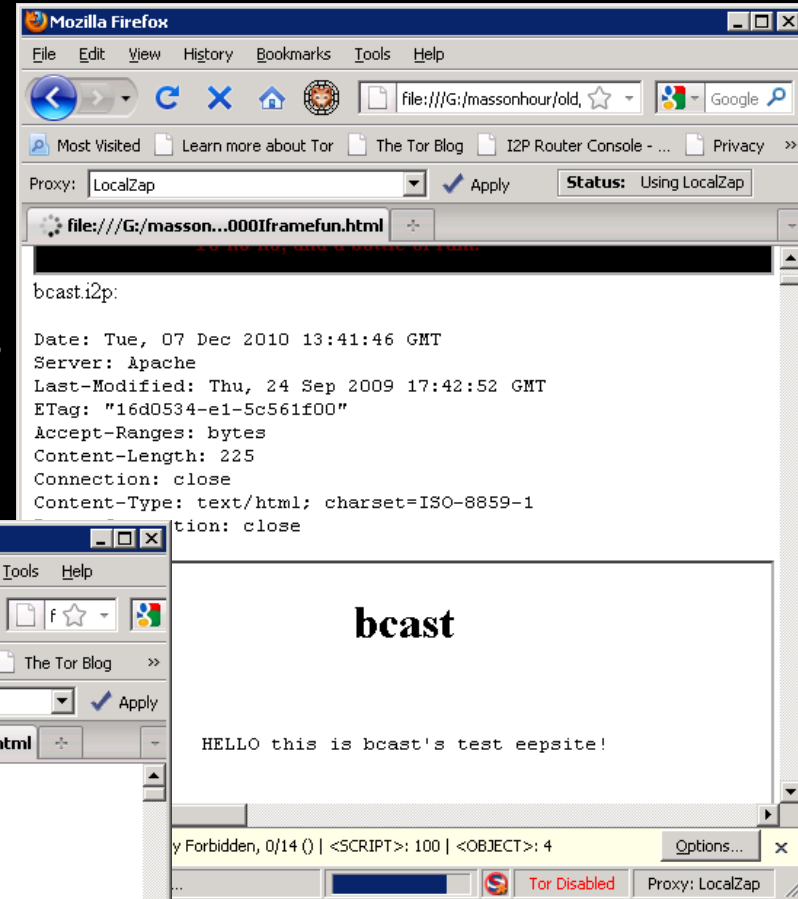
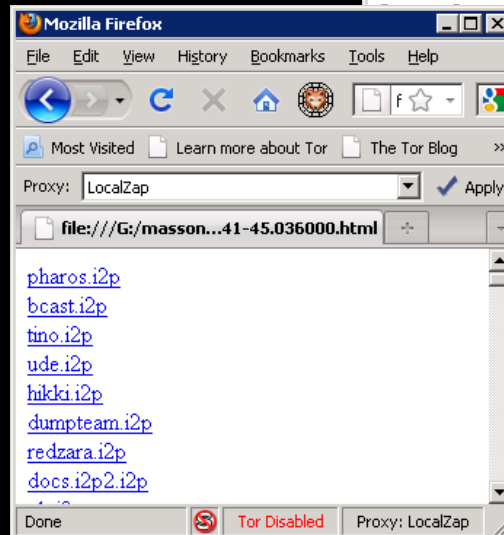
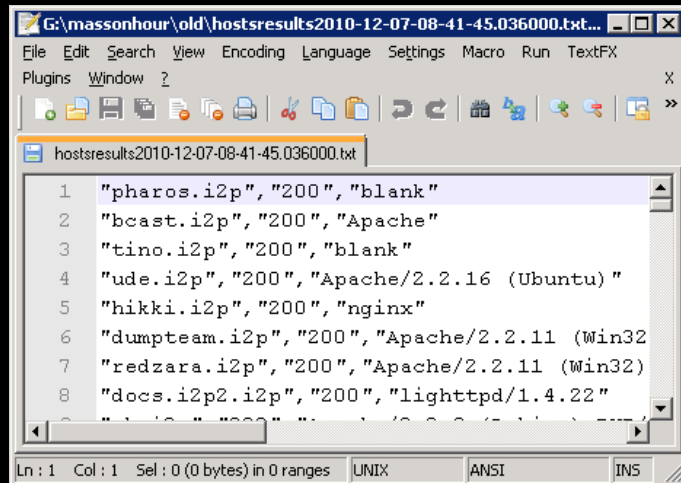
- ▣ Same site, found on IP and I2P



Automating

virtual-server-test.py

- ▣ Download and compare while changing host headers
- ▣ Multiple forms of output



Some Results

- Out of 119 I2P hostnames we have in our set we found 21 IP/I2P correlations

I2P Hostname	Likely Real IP
lurker.i2p	178.63.47.16
bzr.welterde.i2p	188.40.181.33
docs.i2p2.i2p	188.40.181.33
openmusic.i2p	188.40.181.33
paste.i2p2.i2p	188.40.181.33
syndie.welterde.i2p	188.40.181.33
www.i2p2.i2p	188.40.181.33
matterhorn.i2p	188.165.45.229
awxcnx.i2p	62.75.219.7
directedition.i2p	68.33.184.167
forum.i2p	82.103.134.192
ugha.i2p	82.103.134.192
bolobomb.i2p	83.222.124.19
ipredia.i2p	84.55.73.228
teknogods.i2p	84.234.26.123
jonatan.walck.i2p	85.229.85.244
medosbor.i2p	89.31.112.91
colombo-bt.i2p	< redacted >
www.i2p2.i2p (mirror?)	94.23.12.210, 94.23.46.106, 46.4.248.202
mathiasdm.i2p	94.23.52.151
privacybox.i2p	94.75.228.29



Mitigations for Vhost comparing

- ▣ Don't run the eepSite on a web server with a public facing IP, or to make sure that the virtual host for the I2P site is only set to respond to requests from the localhost .
- ▣ Configure HTTP service not to return a server banner or to just return a very non-distinctive banner such as the aforementioned "Server: Apache" (ServerTokens directive set to ProductOnly).
- ▣ Mathiasdm read a draft of this paper, and spurred a change in the I2P code base. Starting with I2P version 0.8.2 the server header is stripped.



Related

- ▣ X-Powered-By headers can also give away information:

Date: Wed, 01 Dec 2010 21:02:21 GMT

Server: Apache

X-Powered-By: PHP/5.2.13-pl0-gentoo

- ▣ Want to see historical records of headers?

<http://i2p.to/frame.php?page=info&host=somesite.i2p>

- ▣ Public header search engine:

<http://www.shodanhq.com/>

- ▣ Bing and the IP: search parameter



Clock Differences

- ▣ We are not really looking a skew here, more total clock differences.
- ▣ For skew, see: Steven J. Murdoch, "Hot or Not: Revealing Hidden Services by their Clock Skew," University of Cambridge, Cambridge, 2006
- ▣ Some of these techniques may work better in I2P than Tor.



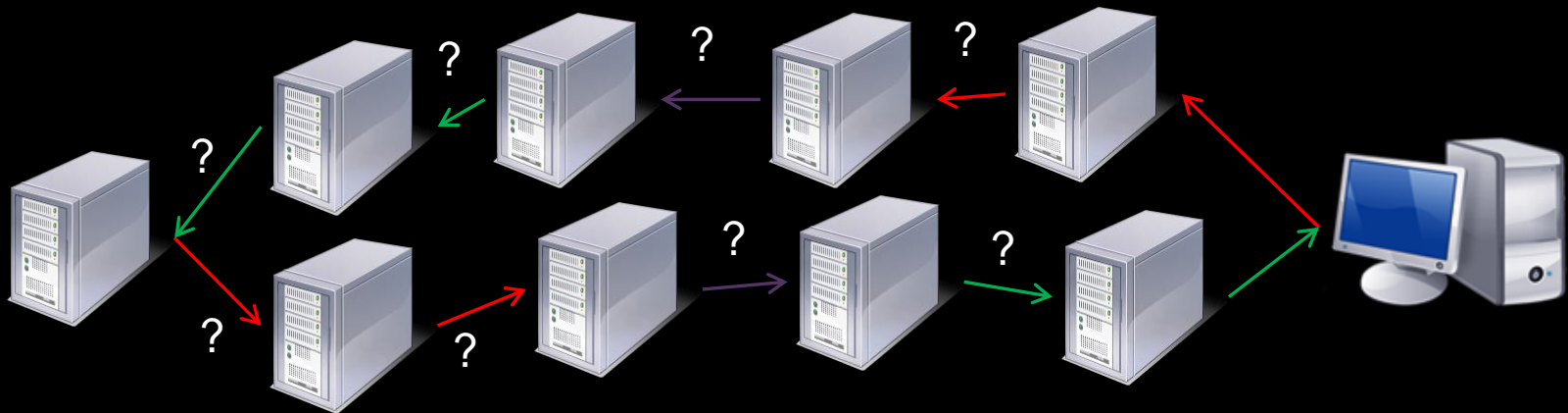
Clock Differences

Time Difference	Retrieval Time	Host	Header
40.417	0.436	89.31.112.91	Apache/2.2.13 (Linux/SUSE)
50.294	10.549	medosbor.i2p	Apache/2.2.13 (Linux/SUSE)
3.418	0.35	85.229.85.244	Apache/2.2.15 (Debian)
4.325	5.059	jonatan.walck.i2p	Apache/2.2.15 (Debian)
-4325.58	0.353	84.55.73.228	Apache/2.2.3 (CentOS)
-4321.66	8.946	ipredia.i2p	Apache/2.2.3 (CentOS)
4488.434	0.702	130.241.45.216	Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny8 with Suhosin-Patch
4490.365	4.894	error.i2p	Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny8 with Suhosin-Patch
2.407	4.89	bolobomb.i2p	Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny9 with Suhosin-Patch mod_ssl/2.2.9 OpenSSL/0.9.8g
2.421	0.091	83.222.124.19	Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny9 with Suhosin-Patch mod_ssl/2.2.9 OpenSSL/0.9.8g
3.43	0.282	188.40.181.33	lighttpd/1.4.22
5.366	2.901	docs.i2p2.i2p	lighttpd/1.4.22
6.274	3.673	zzz.i2p	lighttpd/1.4.22
53.415	0.26	93.174.93.93	Microsoft-IIS/6.0
54.404	3.92	colombo-bt.i2p	Microsoft-IIS/6.0
3.287	0.531	www.i2p2.i2p	nginx/0.6.32
3.429	0.285	46.4.248.202	nginx/0.6.32
11.323	8.989	lurker.i2p	nginx/0.7.65
12.433	8.882	178.63.47.16	nginx/0.7.65



Why not split the difference?

How do you know which tunnel or node caused which percentage of the delay?



Mitigations for clock differences

- ❑ Don't run the eepSite on a web server with a public facing IP, or to make sure that the virtual host for the I2P site is only set to respond to requests from the localhost .
- ❑ Making sure that the time is properly synchronized with a reliable and widely used NTP server and the time zone is set correctly would help.
- ❑ The reason we specify a widely used and reliable NTP server is that synchronizing against an NTP system that is significantly off may also reduce the anonymity set.



Command Injection attack

- ▣ Command injection

Vulnerability occurs when improperly sanitized input, be it from a web form, get request, cookie or header, is fed into an application that then uses the input as part of a command that is to be issued at a shell.

- ▣ Related attacks:

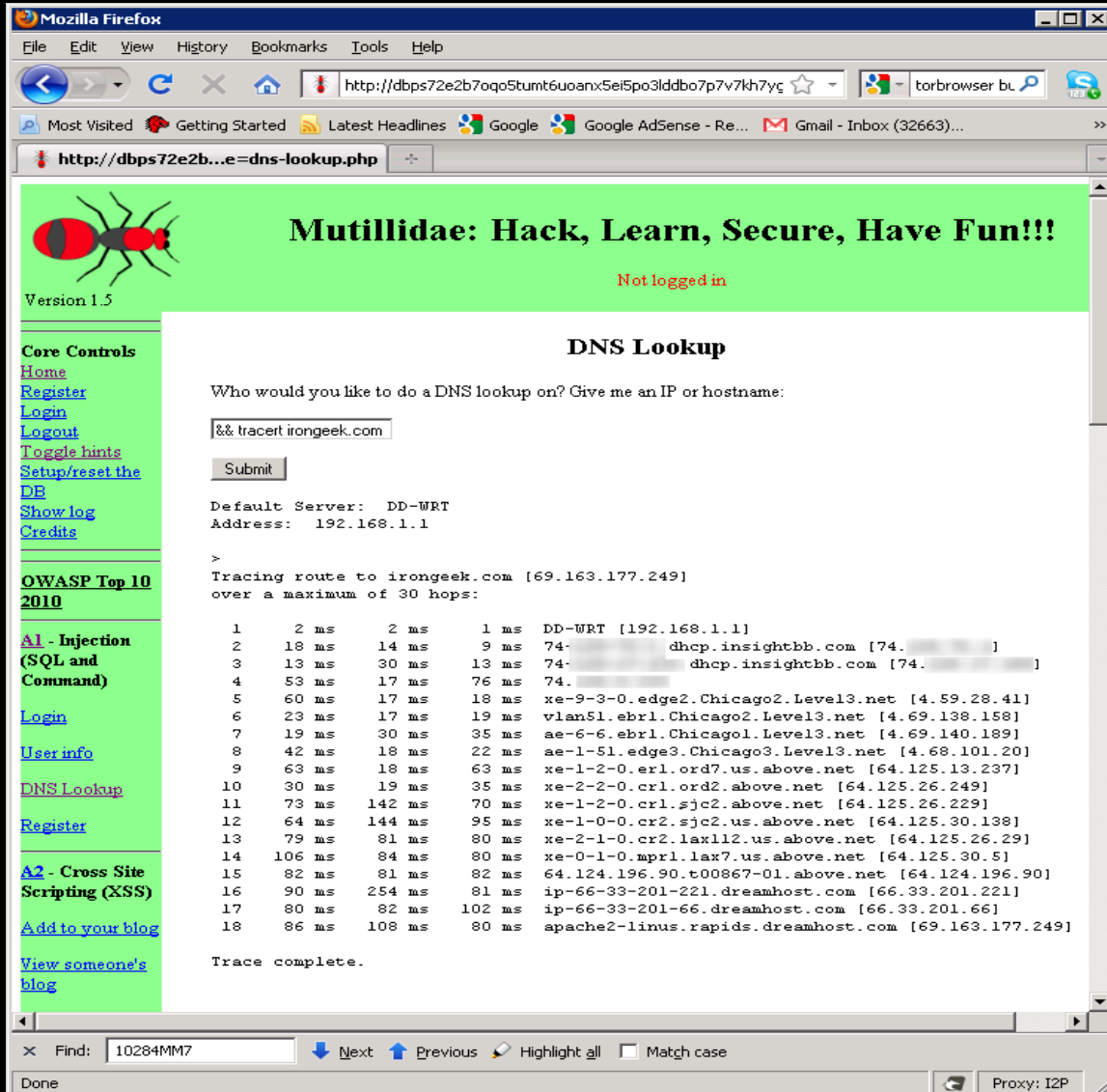
Code Injection attack

SQL Injection (xp_cmdShell)?



Injection attack example

- ❑ Set up Mutillidae
- ❑ Injected command to trace route
- ❑ Read the results




Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://dbps72e2b7oqo5tunt6uoanx5ei5po3lddb07p7v7kh7yç

Most Visited Getting Started Latest Headlines Google Google AdSense - Re... Gmail - Inbox (32663)...

http://dbps72e2b...e=dns-lookup.php

 **Mutillidae: Hack, Learn, Secure, Have Fun!!!**

Not logged in

Version 1.5

Core Controls

[Home](#)
[Register](#)
[Login](#)
[Logout](#)
[Toggle hints](#)
[Setup/reset the DB](#)
[Show log](#)
[Credits](#)

OWASP Top 10 2010

A1 - Injection (SQL and Command)

[Login](#)
[User info](#)
[DNS Lookup](#)
[Register](#)

A2 - Cross Site Scripting (XSS)

[Add to your blog](#)
[View someone's blog](#)

DNS Lookup

Who would you like to do a DNS lookup on? Give me an IP or hostname:

Default Server: DD-WRT
Address: 192.168.1.1

>

Tracing route to irongeek.com [69.163.177.249]
over a maximum of 30 hops:

	1	2 ms	2 ms	1 ms	DD-WRT [192.168.1.1]
2	18 ms	14 ms	9 ms	74-	dhcp.insightbb.com [74. ...]
3	13 ms	30 ms	13 ms	74-	dhcp.insightbb.com [74. ...]
4	53 ms	17 ms	76 ms	74.	74. ...
5	60 ms	17 ms	18 ms	xe-9-3-0.	edge2.Chicago2.Level3.net [4.59.28.41]
6	23 ms	17 ms	19 ms	vlan51.ebri1.	Chicago2.Level3.net [4.69.138.158]
7	19 ms	30 ms	35 ms	ae-6-6.ebri1.	Chicago1.Level3.net [4.69.140.189]
8	42 ms	18 ms	22 ms	ae-1-51.edge3.	Chicago3.Level3.net [4.68.101.20]
9	63 ms	18 ms	63 ms	xe-1-2-0.er1.	ord7.us.above.net [64.125.13.237]
10	30 ms	19 ms	35 ms	xe-2-2-0.cr1.	ord2.above.net [64.125.26.249]
11	73 ms	142 ms	70 ms	xe-1-2-0.cr1.	sjc2.above.net [64.125.26.229]
12	64 ms	144 ms	95 ms	xe-1-0-0.cr2.	sjc2.us.above.net [64.125.30.138]
13	79 ms	81 ms	80 ms	xe-2-1-0.cr2.	lax112.us.above.net [64.125.26.29]
14	106 ms	84 ms	80 ms	xe-0-1-0.mpr1.	lax7.us.above.net [64.125.30.5]
15	82 ms	81 ms	82 ms	64.124.196.90.	t00867-01.above.net [64.124.196.90]
16	90 ms	254 ms	81 ms	ip-66-33-201-221.	dreamhost.com [66.33.201.221]
17	80 ms	82 ms	102 ms	ip-66-33-201-66.	dreamhost.com [66.33.201.66]
18	86 ms	108 ms	80 ms	apache2-linus.	rapids.dreamhost.com [69.163.177.249]

Trace complete.

Find: 10284MM7

Next Previous Highlight all Match case

Done

Proxy: I2P

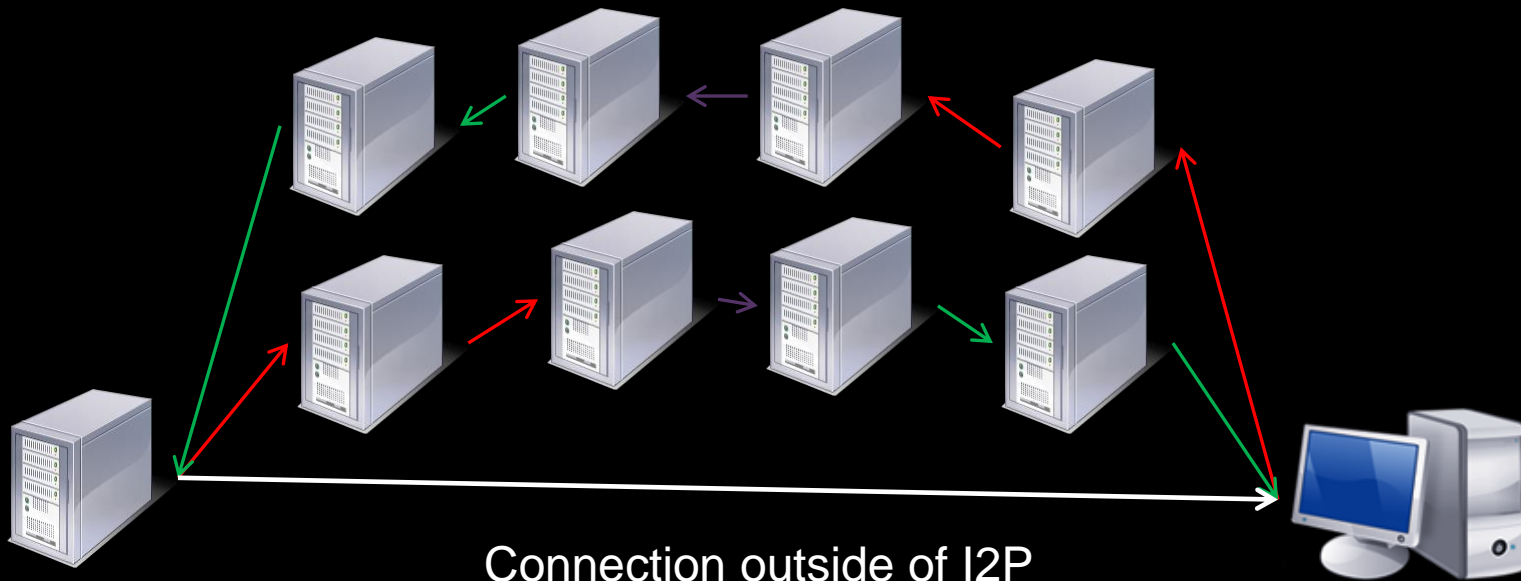
Mitigations for injection attacks

- ▣ Keep up to date with your software
- ▣ Do a code review
- ▣ Review the OWASP Top 10
http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- ▣ Another solution may be to massively lock down the eepSite's firewall rules not to allow any sort of egress to the outside Internet
- ▣ Look in Web Application Firewalls (bandaid)



You don't have to see the results on the page

- ▣ Make the server contact you outside of I2P
- ▣ Sniff for connection or expected traffic
- ▣ Ping/Netcat



Future

- ▣ Look at other protocols IRC, eMule and BitTorrent
- ▣ Targeting the administrators via whatever contact information they provide and enticing them to visit a site the attacker controls could be fruitful
 - Decloak.net (plugins like Flash)
- ▣ Metadata
- ▣ Look more into clock difference based attacks



Events

- ▣ Louisville Infosec
<http://www.louisvilleinfosec.com/>
- ▣ DerbyCon 2011, Louisville Ky
Sept 30 - Oct 2
<http://derbycon.com/>
- ▣ Skydogcon/Hack3rcon/Phreaknic/Notacon/Outerz0ne
<http://www.skydogcon.com/>
<http://www.hack3rcon.org/>
<http://phreaknic.info>
<http://notacon.org/>
<http://www.outerz0ne.org/>



QUESTIONS?

42

Project Page:

<http://www.irongeek.com/i.php?page=security/darknets-i2p-identifying-hidden-servers>

Installing:

<http://www.irongeek.com/i.php?page=videos/getting-started-with-the-i2p-darknet>

<http://www.irongeek.com/i.php?page=videos/i2p-darknet-software-in-linux>

