shadowserver

Chas Tomlin

Systems Administrator/Programmer
School of Electronics and Computer Science
University of Southampton

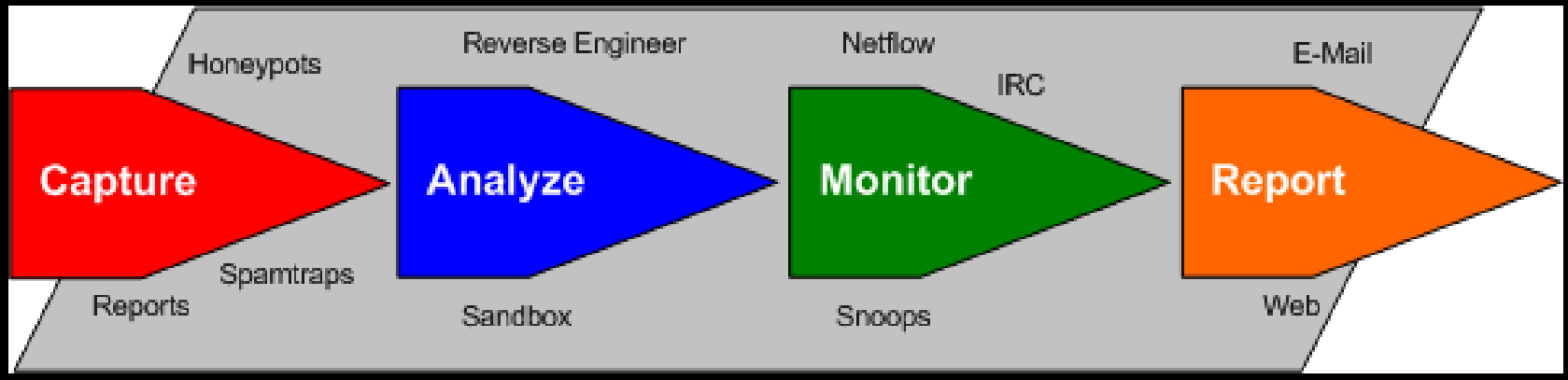
Who is Shadowserver?

- Shadowserver is an all volunteer watchdog group of security professionals.
- 15 Permanent members from five different countries
  - Everyone has day jobs (System Administrators, Network Technicians, Researchers at Universities, State Government offices, working in Small to Large Corporations)
- Shadowserver is non commercial, vendor neutral.

What does Shadowserver do?

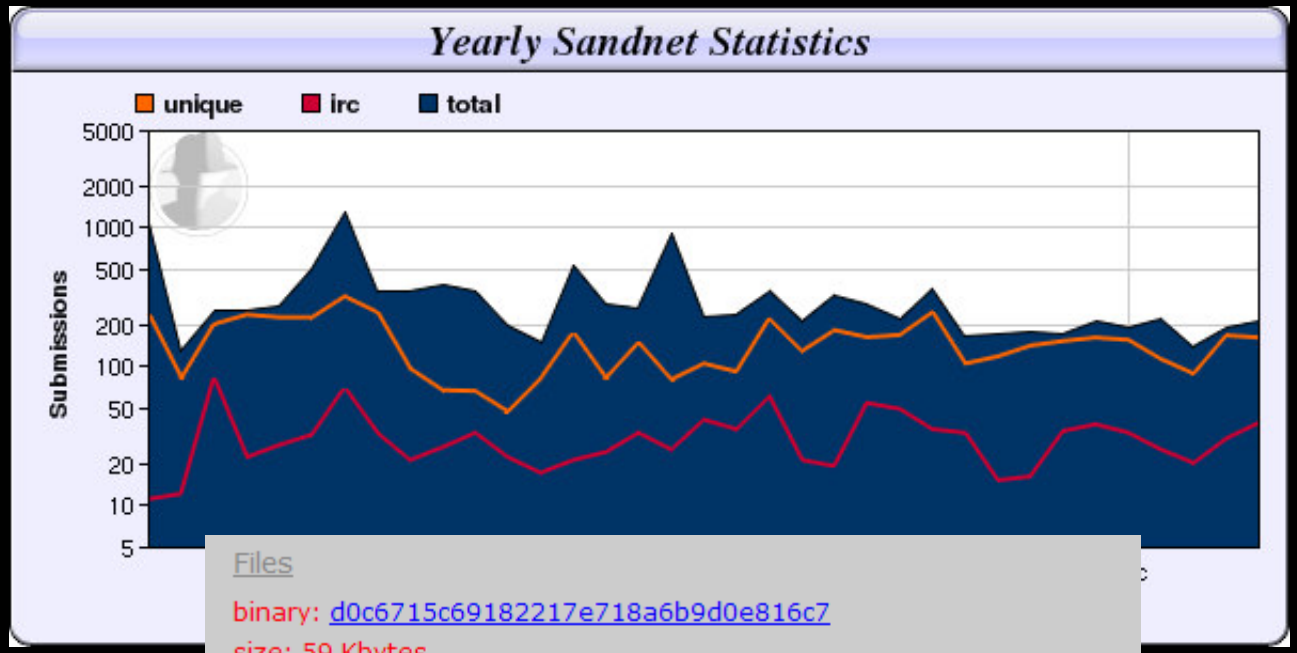
Primary focus is to track and monitor botnet activity

- Gather intelligence related to various forms of electronic fraud
- The analysis and collection of malware
- Provide data analysis and reporting on malicious activity to the security community



Malware analysis

Count	Bitdefender Output
1663	Trojan.Proxy.PPAgent.A
680	Win32.Virtob.C
449	Win32.Mydoom.M@mm
310	Backdoor.Perl.Shellbot.B
252	Win32.Worm.Korgo.U
201	Trojan.Downloader
154	Win32.Parite.B
137	Win32.Worm.Korgo.P
127	Backdoor.PoeBot.C
111	Backdoor.Poebot.AA
108	Backdoor.Gobot.S
106	Win32.SMTP-Mailer
87	Win32.Worm.Korgo.T
83	Backdoor.RBot.HES
75	Win32.Virtob.D
74	Backdoor.Poebot.O
72	Backdoor.Rbot.EZH
67	Backdoor.Rbot.FCE
67	Backdoor.Gobot.U
66	Win32.Bagle.FJ@mm



Files

binary: d0c6715c69182217e718a6b9d0e816c7

size: 59 Kbytes

pcap: d0c6715c69182217e718a6b9d0e816c7.pcap | tcpflow | DNS

pcap size: 218557 bytes

IRC

server ip: 216.218.213.197

server fqdn: new.antix.us

port: 1598

server password:

nick: [XP|1|DWyrag]

user: [XP|1|DWyrag] "XepPiYvw.com" "new.antix.us" :BILLY

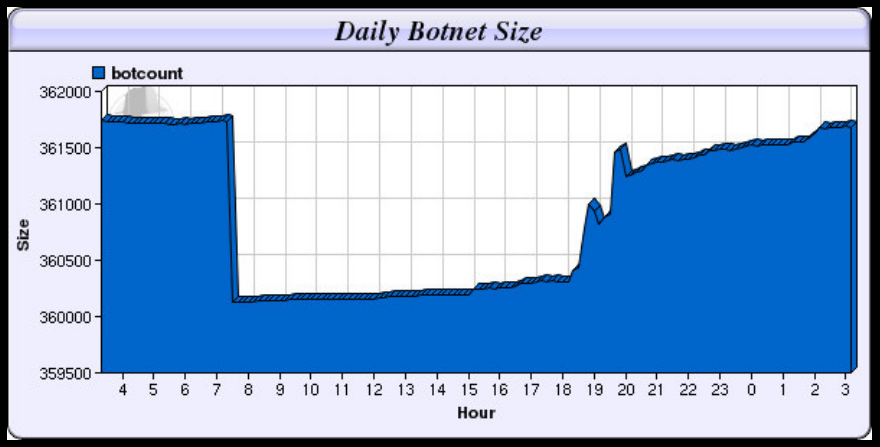
mode:

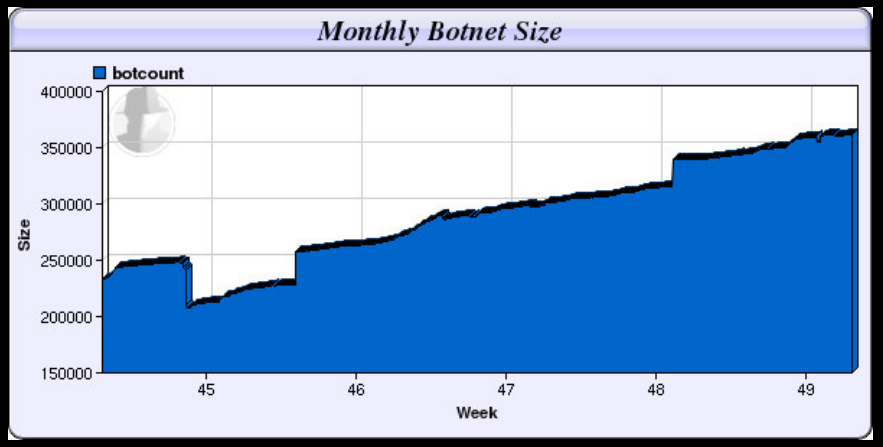
channel: #.heh

channel password: codyisleet

ctcp version:

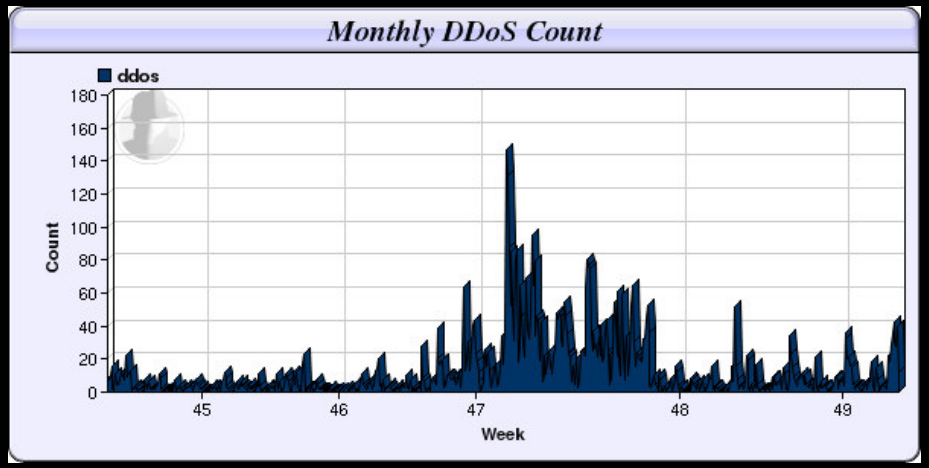
Monitoring botnets

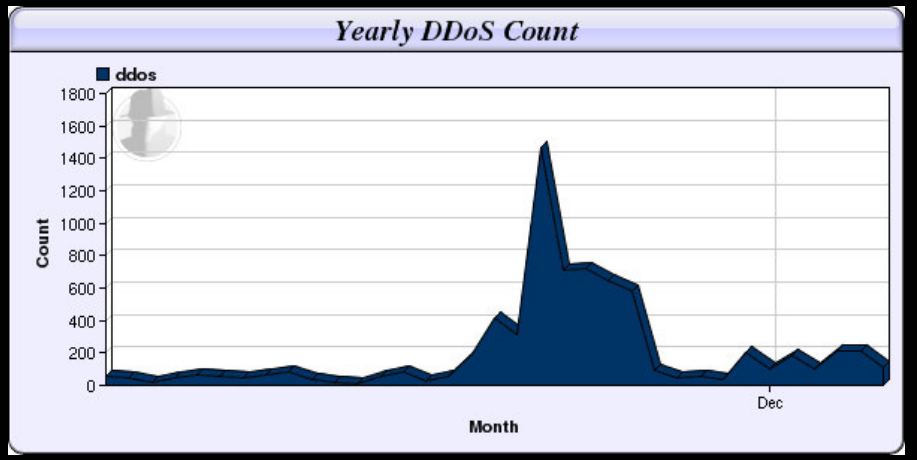





```
May 21 20:31:32 [EGY4WE] :scorTi!admin@admin.com PRIVMSG #A# :.asc asnlsmbnt 30 0 0 24.x.x.x -r -s
May 21 20:31:36 [EGY4WE] :scorTi!admin@admin.com PRIVMSG #A# :.asc lsass_445 50 0 0 24.x.x.x -r -s
May 21 20:51:23 [EGY4WE] :scorTi!admin@admin.com PRIVMSG #A# :.asc asnlsmbnt 30 0 0 77.x.x.x -r -s
May 21 20:51:27 [EGY4WE] :scorTi!admin@admin.com PRIVMSG #A# :.asc lsass_445 50 0 0 77.x.x.x -r -s
May 22 13:25:38 [EGY4WE] :scorTi!admin@admin.com PRIVMSG #A# :.asc asnlsmbnt 30 0 0 221.x.x.x -r -s
May 22 13:25:45 [EGY4WE] :scorTi!admin@admin.com PRIVMSG #A# :.asc lsass_445 30 0 0 221.x.x.x -r -s
May 22 13:45:41 [EGY4WE] :scorTi!admin@admin.com PRIVMSG #A# :.asc lsass_445 30 0 0 212.x.x.x -r -s
May 22 13:45:49 [EGY4WE] :scorTi!admin@admin.com PRIVMSG #A# :.asc asnlsmbnt 30 0 0 212.x.x.x -r -s
May 22 13:57:55 [EGY4WE] :scorTi!admin@admin.com PRIVMSG #A# :.asc asnlsmbnt 30 0 0 212.138.x.x -r -s
May 22 13:58:03 [EGY4WE] :scorTi!admin@admin.com PRIVMSG #A# :.asc lsass_445 30 0 0 212.138.x.x -r -s
May 22 14:59:21 [EGY4WE] :scorTi!admin@admin.com PRIVMSG #A# :.asc lsass_445 30 0 0 212.138.x.x -r -s
May 22 14:59:25 [EGY4WE] :scorTi!admin@admin.com PRIVMSG #A# :.asc asnlsmbnt 30 0 0 212.138.x.x -r -s
May 22 16:45:12 [EGY4WE] :scorTi!admin@admin.com PRIVMSG #A# :.asc asnlsmbnt 70 0 0 68.x.x.x -r -s
May 22 16:45:22 [EGY4WE] :scorTi!admin@admin.com PRIVMSG #A# :.asc lsass_445 30 0 0 68.x.x.x -r -s
May 22 17:19:32 [EGY4WE] :scorTi!admin@admin.com PRIVMSG #A# :.asc lsass_445 30 0 0 68.x.x.x -r -s
May 22 17:19:36 [EGY4WE] :scorTi!admin@admin.com PRIVMSG #A# :.asc asnlsmbnt 70 0 0 68.x.x.x -r -s
May 22 17:33:02 [EGY4WE] :scorTi!admin@admin.com PRIVMSG #A# :.asc asnlsmbnt 40 0 0 65.x.x.x -r -s
May 22 17:33:08 [EGY4WE] :scorTi!admin@admin.com PRIVMSG #A# :.asc lsass_445 30 0 0 65.x.x.x -r -s
```

Monitoring botnets





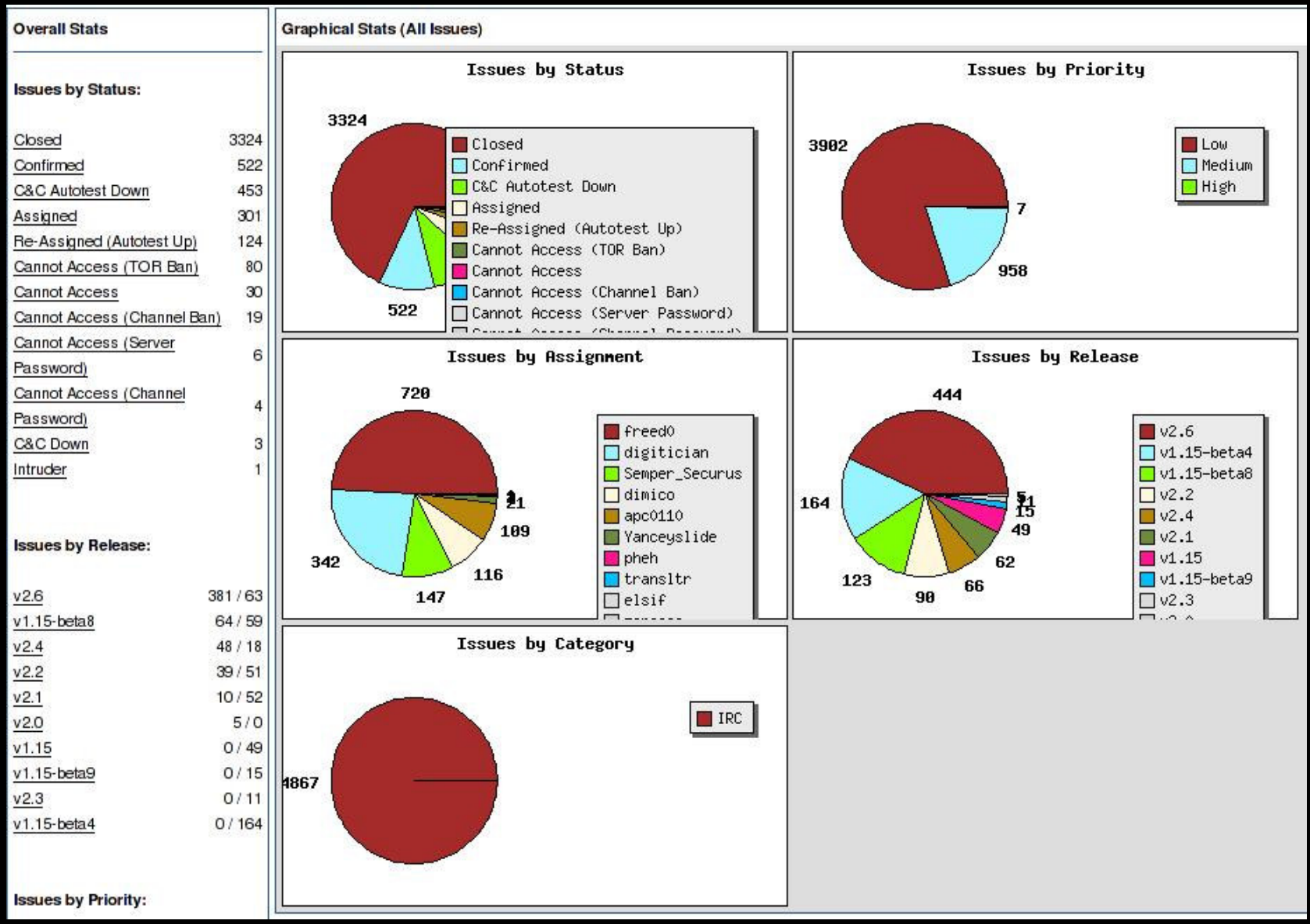
[DDoS Report: 2007-01-10]

C&C	C&C Port	C&C ASN	C&C Geo	Channel	Command	TGT	TGT ASN	TGT Geo
69.213.57.174	6667	7132	US	##r0x##	ack	82.153.159.60	12513	UK
69.213.57.174	6667	7132	US	##NzM##	ack	82.153.159.60	12513	UK
69.213.57.174	6667	7132	US	##b0tz##	ack	82.153.159.60	12513	UK
209.78.171.7	56213	7132	US	#retaliati0n#	:~ddos.random	82.47.128.23	5462	UK
209.78.171.7	56213	7132	US	#retaliati0n#	:~udp	82.47.128.23	5462	UK

Botnets and ASN's

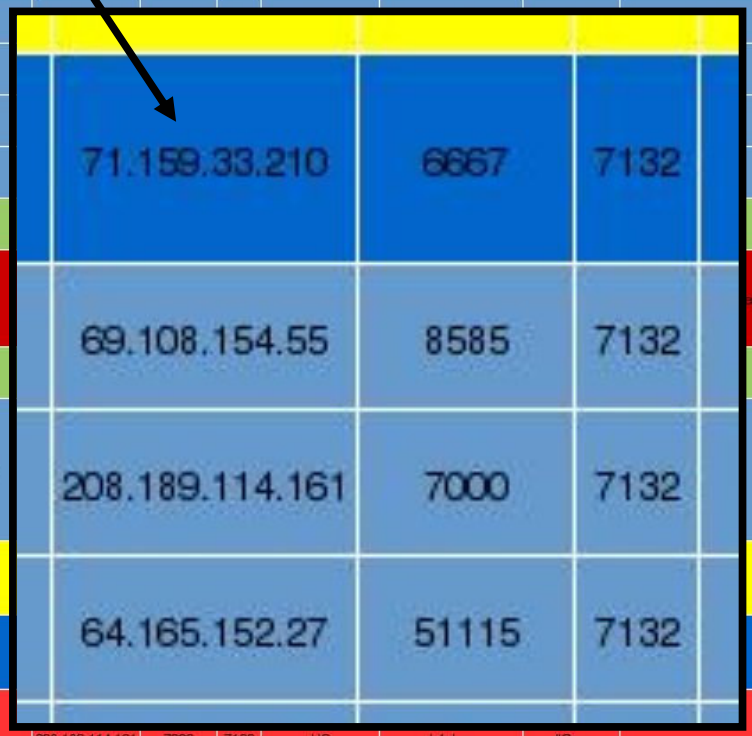
ASN	Number	Details	Closed
13301	220	UNITEDCOLO - AS Autonomous System of unitedcolo.de	48%
19318	194	NJIIX-AS-1 - NEW JERSEY INTERNATIONAL INTERNET EXCHANGE LLC	60%
30058	167	FDCSERVERS - FDC Servers.net, LLC	70%
25761	163	STAMINUS-COMM - Staminus Communications	58%
23522	128	IPNAP-ES - Ecomdevel, LLC	33%
16265	126		28%
3265	112	XS4ALL - NL XS4ALL	39%
12832	88	LYCOS - EUROPE Lycos Europe GmbH, Spray Network Services AB	60%
4766	71	KIXS-AS - KR Korea Telecom	73%
174	71		21%
7132	70	SBIS-AS - SBC Internet Services	62%
8560	69	SCHLUND - AS Schlund + Partner AG	33%
3786	63	ERX - DACOMNET DACOM Corporation	25%
8376	61	GO - JOR Autonomous System	72%
9318	57	HANARO - AS Hanaro Telecom Inc.	59%
19048	52	CORIO - Corio, Inc.	100%
4837	51	CHINA169 - BACKBONE CNCGROUP China169 Backbone	64%
15083	51	INFOLINK-MIA-US - Infolink Information Services Inc.	84%
25232	49	ROKSCOM - AS Rokscom Internet B.V. / Co-locate.nl Autonomous System	97%
31800	47	DALNET - DALnet	46%

Botnets & Tracking



Botnets & Tracking

All	Priority	Issue ID	Reporter	Assigned	Category	Release	Status	Last Action Date	Bots #	Bots # (count)	Current IP	Server Port	ASN	GeoLoc (Country)	IRC Network Name	Channel Name	Channel Password	Source	Summary
	Medium	1010	Semper_Securus	Semper_Securus	IRC		C&C Autotest Down	Update: 4d 16h ago		21	71.132.224.174	6667	7132	US		#monkey			72.20.18.29 - #monkey
	Low	1633	Automated Process	apc0110	IRC		C&C Autotest Down	Closed: 1d 8h ago		0	71.159.33.210	7000	7132	US		##EviL##	oper		adsl-71-159-33-210.dsl.irvnca.sbcglobal.net:7000 ##EviL##
	Low	1922	Automated Process	apc0110	IRC		Re-Assigned (Autotest Up)	Update: 1d 4h ago		3	71.159.33.210	6667	7132	US		##leech##	qawsedrftg		adsl-71-159-33-210.dsl.irvnca.sbcglobal.net:6667 ##leech##
	Medium	2793	Automated Process	freed0	IRC	v2.6	Assigned	Update: 1d 23h ago		0								Norman	yourirc.justdied.com:8585 #linux
	Medium	2859	Automated Process	freed0	IRC	v2.6	Assigned	Update: 80d 19h ago		1								Norman	ness.d2g.biz:7000 #M
	Low	3191	Automated Process	dimico	IRC	v2.6	Assigned	Updated: 19d 6h ago		5									saudi.d2g.biz:51115 #cxx
	Medium	3408	Automated Process	freed0	IRC	v2.6	Assigned	Update: 17d 20h ago		0								Norman	saudi.d2g.biz:51115 #cxxx
	Low	3514	Automated Process		IRC		Confirmed	: 0d 20h ago		0									haniDone.dynu.com:6667 #nohani
	Medium	3617	Automated Process	freed0	IRC	v2.6	Cannot Access (Server Password)	Update: 3d 22h ago		0								Norman	fuck.syn-flood.us:1863 #NGEN
	Low	3856	Automated Process		IRC		Confirmed	: 0d 20h ago		0									hanidone.dynu.com:6667 #ncahmed
	Medium	4241	Yanceyslide	Yanceyslide	IRC		Assigned	Updated: 4d 3h ago		53									#1 @ 1.xshells.com.ar:4000 **[Private]**
	Medium	4577	Automated Process	digitician	IRC	v1.15-beta8	C&C Autotest Down	Closed: 5d 7h ago		31								Sandbox	s3cure.zapto.org:3625 ###VrX###
	Medium	4697	Automated Process	freed0	IRC	v2.6	Re-Assigned (Autotest Up)	Closed: 0d 4h ago		0								Sandbox	208.99.207.142mayday.proircd.net:5821 ##uber##
	Medium	4859	Automated Process	freed0	IRC	v2.6	Cannot Access (Channel Password)	Update: 3d 22h ago		0	208.189.114.161	7000	7132	US	h4cker	#Gxx		Norman	ness.d2g.biz:7000 #Gxx



The Future of Shadowserver

- Become an official non-profit in 2007
- Achieve a non-negative cash flow in 2007
- Expand relationships and influence with the Service Provider community and organizations
- Continue to expand our operations and expertise in Internet Threats and assist in the reduction of those threats

What does Shadowserver Need?

- Data – honeypots, malware, and anything from the systems taken down
- Access – Places to investigate from and connections to allow us to host services
- Contacts – Introductions and assistance in gaining access to other security efforts and organizations
- Funding – To support efforts and growth

Contact Us

- http://www.shadowserver.org
- http://www.shadowserver.org/eventum
- chas@shadowserver.org