

Web Use Profile Report

Powered by Congruity Technologies'



Network Quality Assurance Software

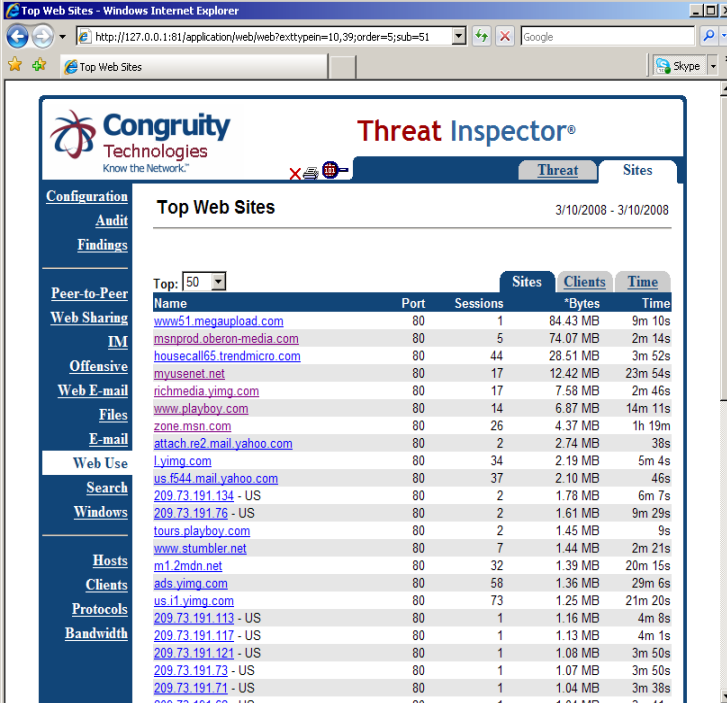
Documents all Web-related usage statistics for stakeholder planning and management activities

Prepared for: Sample Compliance Report

Contents:

Introduction	3
General use	4
Top HTTP Servers	5
Top RTSP Servers	7
Top HTTPS Servers	8
Top Users	10
SurfTime	11
Popular Search Engines	14
Common File Downloads	16
Web-based File Sharing	19
Microsft Updates	25
Spyware / Adware	29
Web-based E-mail	32
Web-based IM Services	37

The Threat Inspector interactive report interface enables drill-down review and data manipulation to investigate and troubleshoot with ease



The screenshot shows the Threat Inspector web interface in a browser window. The page title is "Top Web Sites" and the date range is "3/10/2008 - 3/10/2008". A sidebar on the left contains navigation links for various categories like Configuration, Audit, Findings, Peer-to-Peer, Web Sharing, IM, Offensive, Web E-mail, Files, E-mail, Web Use, Search, Windows, Hosts, Clients, Protocols, and Bandwidth. The main content area displays a table with columns for Name, Port, Sessions, Bytes, and Time. The table lists various websites and their associated metrics.

Name	Port	Sessions	Bytes	Time
www51.megaupload.com	80	1	84.43 MB	9m 10s
msnprod.oberon-media.com	80	5	74.07 MB	2m 14s
housecall65.trendmicro.com	80	44	28.51 MB	3m 52s
myusenet.net	80	17	12.42 MB	23m 54s
richmedia.yimg.com	80	17	7.58 MB	2m 46s
www.playboy.com	80	14	6.87 MB	14m 11s
zone.msn.com	80	26	4.37 MB	1h 19m
attach.re2.mail.yahoo.com	80	2	2.74 MB	38s
l.yimg.com	80	34	2.19 MB	5m 4s
us.f544.mail.yahoo.com	80	37	2.10 MB	46s
209.73.191.134 - US	80	2	1.78 MB	6m 7s
209.73.191.76 - US	80	2	1.61 MB	9m 29s
tours.playboy.com	80	2	1.45 MB	9s
www.stumble.net	80	7	1.44 MB	2m 21s
m1.2mdn.net	80	32	1.39 MB	20m 15s
ads.yimg.com	80	58	1.36 MB	29m 6s
us.i1.yimg.com	80	73	1.25 MB	21m 20s
209.73.191.113 - US	80	1	1.16 MB	4m 8s
209.73.191.117 - US	80	1	1.13 MB	4m 1s
209.73.191.121 - US	80	1	1.08 MB	3m 50s
209.73.191.73 - US	80	1	1.07 MB	3m 50s
209.73.191.71 - US	80	1	1.04 MB	3m 38s

Users can easily move through the data and determine which Web sites were accessed most heavily and had the greatest impact on bandwidth, productivity and compliance

Introduction

Today, the Internet plays a critical role in many businesses. It can be used for ordering supplies, tracking deliveries, making reservations, researching information or online training. Executives like it because it enables employees to easily access a wide range of information and services very quickly, making them more productive. Desktop Web browsers also enable users to send e-mail and Instant Messenger text messages, post opinions on bulletin boards, share files and download software. From modest beginnings, the Web has grown from an easy way to consume information into a powerful communications resource with global reach.

In a typical organization, approximately 80% of overall network bandwidth is consumed by various forms of Web browsing.

Because of its popularity and prevalence in business, Web use is becoming the primary means by which hackers and advertisers infiltrate the network. Attacks are shifting away from the heavily secured network perimeter to easier, more numerous, and more profitable attacks against individual users. A successful network attack or exploit can occur by getting just one user to visit a compromised web site or to download and install a "cool" piece of software. These social attacks often require the help of users, which, unfortunately, often occurs.

"The primary cause of security breaches - human error - is not being adequately addressed. The person behind the PC continues to be the primary area where weaknesses are exposed."

"Human error was responsible for nearly 60 percent of information security breaches."

**-Brian McCarthy, COO
CompTIA**

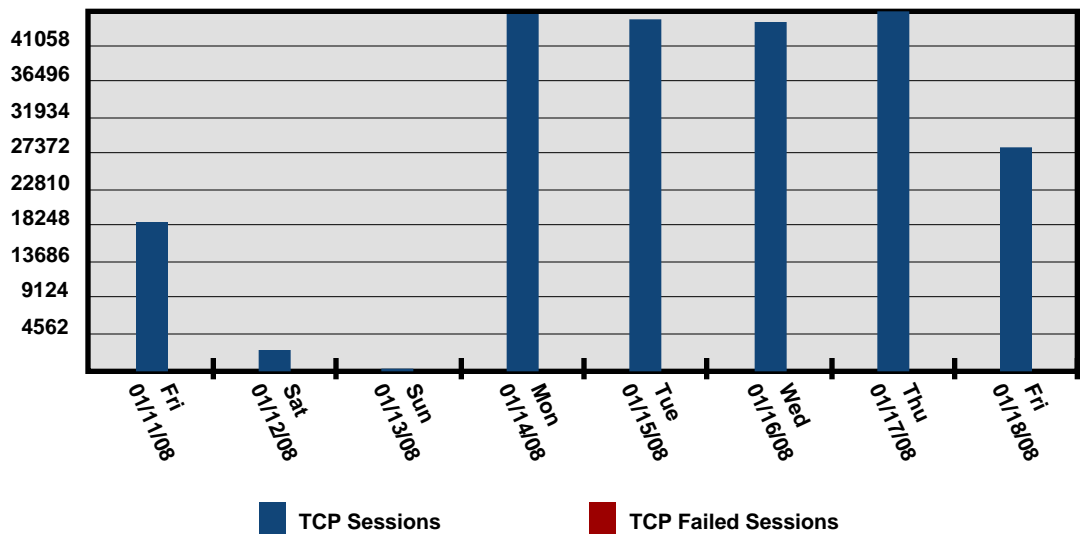
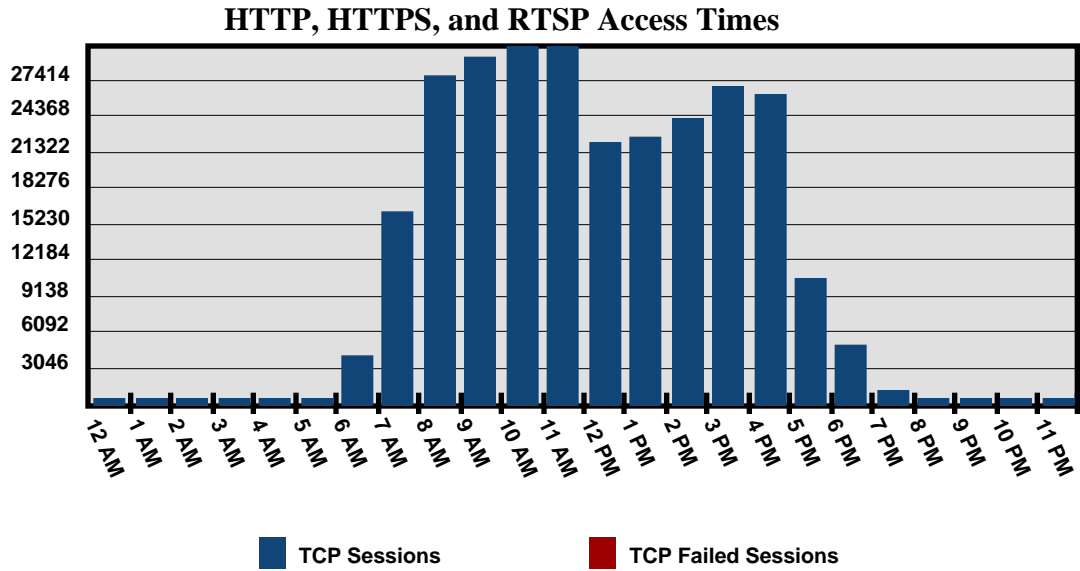
Proactive network management coupled with strong security policy and effective user training are your best defense and are recommended for maintaining a secure, compliant and productive network.

Use this report to:

- Evaluate the effectiveness of and compliance to your internet usage policy.
- Document the time and bandwidth impact of web browsing on your IT operations.
- Identify web-based services that reduce the effectiveness of or circumvent installed security measures.
- Understand how your organization is using and consuming its internet resources.

General use

The three primary web browsing protocols HTTP, HTTPS and RTSP consumed **70.59%** of the network's bandwidth.



Access time graphs show the time of day and the day of the week when web activity occurred.

Top HTTP Servers

Web access over HTTP (Hypertext Transfer Protocol) accounted for **63.95%** of total bandwidth consumption.

- 12,291 individual HTTP servers were accessed by 63 users.

Top site in terms of data downloaded, 7 sessions and over 700MB of data: suspicious!

Top HTTP Servers

Name	Port	Sessions	*Bytes	Time
dl-ak.solidworks.com	80	7	734.37 MB	2h 30m
www.damuxu.de	80	7	588.86 MB	30m 10s
serien-otr.bhnw.net	80	9	536.62 MB	30m 55s
liveupdate.symantecliveupdate.com	80	104	319.32 MB	43m 13s
livedocs.adobe.com	80	328	271.98 MB	3h 49m
au.download.windowsupdate.com	80	91	195.78 MB	27m 47s
www.naswug.com	80	49	166.90 MB	8m 33s
lh3.google.com	80	1430	155.58 MB	1h 13m
www0.pafnet.de	80	16935	111.24 MB	4h 41m
rs222tl.rapidshare.com	80	43	107.94 MB	1h 58m
rs277132.rapidshare.com	80	69	99.88 MB	1h 19m
rs28cg.rapidshare.com	80	102	96.29 MB	5m 58s
69.131.237.23 - US	80	6	57.92 MB	25m 17s
content.newsfilter.org	80	8	57.15 MB	3m 11s
www.google.com	80	1695	55.51 MB	4h 29m
rs12134.rapidshare.com	80	36	54.77 MB	42m 8s
msnbc.vo.llnwd.net	80	12	51.57 MB	2m 43s
m1.2msn.net	80	1468	51.49 MB	16h 36m
help.adobe.com	80	68	47.85 MB	32m 3s
www.businessplans.org	80	7	44.66 MB	8m 55s
w14.easy-share.com	80	4	40.83 MB	4m 33s
rs28gc2.rapidshare.com	80	48	39.80 MB	1h 7m
www.download.windowsupdate.com	80	31	39.55 MB	10m 37s
images.pafnet.de	80	4031	38.90 MB	7h 51m
us.i1.yimg.com	80	910	36.29 MB	13h 1m
www.bild.t-online.de	80	396	35.77 MB	30m 24s
spe.atdmt.com	80	777	31.88 MB	11h 0m
67.131.237.15 - US	80	6	31.36 MB	15m 27s
frog7.inkfrog.com	80	76	31.28 MB	3m 50s
63.250.197.57 - US	80	7	30.79 MB	47m 0s
content1.skillsoft.com	80	1217	29.71 MB	1h 24m
www.continental.com	80	449	28.92 MB	1h 1m
kh.google.com	80	75	27.60 MB	43m 59s
media.bei-uns.de	80	6388	26.01 MB	2h 48m
pagead2.google syndication.com	80	2021	25.01 MB	9h 29m
content.movies.myspace.com	80	1	24.45 MB	1m 15s
Wm-eon.vitalstreamcdn.com	80	1	23.81 MB	1h 33m
upload.wikimedia.org	80	219	23.39 MB	1h 8m
images.google.com	80	733	22.36 MB	36m 41s
rs15cg.rapidshare.com	80	31	21.93 MB	14m 34s

Note: over 16000 sessions, heavy resource use: German Social Networking site: Trouble

Name	Port	Sessions	*Bytes	Time
rss.msnbc.msn.com	80	242	21.79 MB	36m 52s
media01.crackle.com	80	6	21.47 MB	6m 2s
cache.opt.fimserve.com	80	221	21.46 MB	5h 19m
213.61.13.87 - GB	80	3	21.32 MB	9m 40s
rs73cg.rapidshare.com	80	27	20.43 MB	15m 13s
www.hiclip.de	80	5728	20.40 MB	1h 5m
largeassets.myspacecdn.com	80	20	20.25 MB	1m 40s
entimg.msn.com	80	113	20.08 MB	53m 54s
bannerfarm.ace.advertising.com	80	342	20.00 MB	13h 28m
69.250.197.135 - US	80	3	19.65 MB	19m 17s
albums.pafnet.de	80	630	19.18 MB	1h 18m
rs160132.rapidshare.com	80	32	18.99 MB	14m 1s
thumbs.ebaystatic.com	80	185	18.54 MB	2h 43m
www.vw.com	80	31	18.40 MB	31m 41s
ads.yimg.com	80	489	18.36 MB	6h 42m
l.yimg.com	80	390	18.35 MB	59m 8s
a2047.v1412b.c1412.g.vq.akamaistream.net	80	3	17.68 MB	6m 56s
rs95gc2.rapidshare.com	80	28	17.67 MB	13m 25s
vid6.stileproject.com	80	8	17.50 MB	1m 24s
www.coolpick.com	80	1427	16.86 MB	5m 47s
adserver.adtech.de	80	4207	16.79 MB	2h 29m
flash.sonypictures.com	80	3	16.45 MB	46s
rs7cg.rapidshare.com	80	18	16.08 MB	8m 18s
sb.google.com	80	365	16.03 MB	1h 44m
69.250.192.52 - US	80	2	15.84 MB	15m 42s
Sub Totals: 65		54,418	4.77 GB	
Percent: 1%		24%	53%	
Totals: 12,291		229,182	9.06 GB	

Reviewing this information provides insights into how the Internet resources are being used: Legitimate business purposes, acceptable entertainment or threats

Top RTSP Servers

RTSP (Real-Time Streaming Protocol) is used for playing audio/video data from a streaming media server. Some examples include Internet radio, pod casts, news and movies.

- Web access over RTSP accounted for **.06%** of total bandwidth consumption.
- 6 individual RTSP servers were accessed by 4 (6.35%) users.

Top RTSP Servers

Name	Port	Sessions	*Bytes	Time
a468.m.akastream.net	554	1	4.03 MB	1m 35s
a89.m.akastream.net	554	2	1.95 MB	2m 30s
a1246.m.akastream.net	554	1	1.72 MB	32s
dalwml010.bcst.yahoo.com	554	2	1.16 MB	6s
a2047.v1412b.c1412.g.vq.akamaistream.net	554	1	80.78 KB	2m 4s
a1494.v141765.c14176.g.vm.akamaistream.net	554	2	36.93 KB	9s
Sub Totals: 6		9	8.97 MB	
Percent: 100%		100%	100%	
Totals: 6		9	8.97 MB	

Top HTTPS Servers

HTTPS (Hypertext-Transport-Protocol over Secure Socket Layer) is primarily used for on-line commercial exchanges such as on-line banking; however, it can also be used to hide a user's activities from Web filtering and monitoring software. Data exchanged between the Web server and client (workstation) is encrypted.

- Web access over HTTPS accounted for **6.58%** of total bandwidth consumption.
- 737 individual HTTPS servers were accessed by 64 (101.59%) users.

Top HTTPS Servers

Name	Port	Sessions	*Bytes	Time
171.146.231.208 - US	443	603	253.05 MB	13h 35m
86.154.26.171 - DE	443	25888	174.69 MB	5h 45m
welcome.baxel.de	443	131	61.33 MB	1h 2m
81.154.26.183 - DE	443	99	33.49 MB	34h 23m
176.146.231.167 - US	443	3321	22.06 MB	1h 4m
www.continental.com	443	263	21.90 MB	1h 17m
www.update.microsoft.com	443	222	20.75 MB	55m 34s
227.72.199.55 - DE	443	878	18.97 MB	21m 43s
globaloffice.baxel.de	443	36	17.51 MB	19h 26m
81.154.26.170 - DE	443	143	17.39 MB	1h 39m
81.154.26.175 - DE	46629	98	16.81 MB	1h 48m
resource.adp.com	443	3309	15.19 MB	19m 28s
img.web.de	443	1092	13.88 MB	1h 18m
mail.yahoo.com	443	292	8.70 MB	4m 7s
229.73.168.74 - US	443	301	7.97 MB	2m 25s
226.115.222.32 - US	443	3	7.56 MB	25m 38s
69.163.169.186 - US	443	262	7.53 MB	2m 28s
124.103.32.50 - EU	443	57	6.82 MB	2h 15m
69.246.16.68 - US	443	109	6.07 MB	11m 17s
www22.verizon.com	443	66	5.41 MB	29m 43s
my.t-mobile.com	443	23	5.38 MB	15m 0s
ading.uimserv.net	443	230	5.28 MB	27m 3s
66.77.22.60 - US	443	40	3.85 MB	14m 26s
webmail.lattich.edu	443	1642	3.72 MB	7m 45s
227.72.199.54 - DE	443	649	3.54 MB	17m 37s
69.153.158.211 - DE	443	512	3.46 MB	5m 39s
216.175.122.186 - US	443	44	3.27 MB	21m 44s
69.98.129.46 - US	443	88	2.99 MB	7m 18s
61.150.120.29 - US	443	23	2.83 MB	9m 8s
236.252.124.207 - US	443	113	2.75 MB	1m 3s
portal.mxlogic.com	443	440	2.67 MB	6m 0s
81.154.26.179 - DE	443	62	2.64 MB	44m 9s
69.245.209.31 - US	443	57	2.60 MB	56m 35s
169.53.60.54 - US	443	17	2.32 MB	8m 53s
www.wireless.att.com	443	57	2.24 MB	56m 2s
66.55.184.61 - US	443	13	2.23 MB	1m 44s

Name	Port	Sessions	*Bytes	Time
login.yahoo.com	443	104	2.19 MB	1m 2s
227.72.199.57 - DE	443	347	2.07 MB	8m 8s
196.243.113.205 - CA	443	27	2.07 MB	8m 37s
219.184.80.20 - US	443	25	2.00 MB	24m 59s
66.161.188.147 - US	443	8	1.97 MB	6m 24s
124.103.72.4 - EU	443	17	1.95 MB	18m 5s
66.39.38.135 - US	443	14	1.89 MB	13m 31s
64.55.157.60 - US	443	272	1.85 MB	2m 17s
www.exglorehumdno.com	443	6	1.82 MB	2m 38s
217.46.211.124 - US	443	19	1.80 MB	1m 27s
www.innovateads.com	443	8	1.80 MB	6s
226.213.211.173 - US	443	19	1.79 MB	10m 35s
66.129.160.88 - US	443	242	1.70 MB	57s
227.72.199.58 - DE	443	317	1.70 MB	8m 17s
229.85.133.83 - US	443	16	1.70 MB	6m 39s
226.9.242.88 - CA	443	305	1.69 MB	59h 11m
179.146.231.146 - US	443	92	1.60 MB	10m 49s
229.66.240.15 - US	443	196	1.58 MB	2m 33s
adclient.uimserv.net	443	284	1.48 MB	10m 22s
224.187.87.88 - CA	443	277	1.44 MB	64h 36m
10.47.204.61 - US	443	11	1.40 MB	7m 16s
Darkfenceportal.elader.com	443	89	1.36 MB	6m 12s
wwwapps.ups.com	443	41	1.32 MB	7m 8s
226.115.210.202 - US	443	15	1.31 MB	2m 33s
228.65.147.160 - US	443	200	1.29 MB	1m 0s
161.159.66.159 - US	443	4	1.29 MB	5m 17s
69.61.160.244 - US	443	5	1.22 MB	49m 29s
219.62.177.57 - US	443	93	1.17 MB	1m 25s
69.55.157.61 - US	443	173	1.17 MB	1m 25s
Sub Totals: 65		44,409	836.47 MB	
Percent: 9%		81%	88%	
Totals: 737		54,594	954.18 MB	

Top Users

The following users had the largest impact on bandwidth consumption.

Top users of HTTP, HTTPS and RTSP by bandwidth consumption

Client	Outbound		*Total	Bytes	
	Sessions	Failed		Inbound	Outbound
192.168.10.101	23350	0	2.26 GB	2.16 GB	100.36 MB
192.168.10.106	9537	0	1.25 GB	1.20 GB	51.02 MB
192.168.10.91	10525	0	1.03 GB	1006.90 MB	49.54 MB
192.168.10.98	5356	0	462.29 MB	433.73 MB	28.56 MB
192.168.10.112	12672	0	434.78 MB	381.65 MB	53.13 MB
192.168.10.129	52922	0	417.93 MB	329.53 MB	88.40 MB
192.168.10.108	17155	0	278.13 MB	231.85 MB	46.28 MB
192.168.10.7	135	0	219.48 MB	213.22 MB	6.26 MB
192.168.10.81	1955	0	217.17 MB	207.98 MB	9.19 MB
192.168.10.142	22037	0	216.15 MB	178.63 MB	37.52 MB
192.168.10.116	5867	0	206.54 MB	185.42 MB	21.12 MB
192.168.10.82	6581	0	192.78 MB	171.42 MB	21.37 MB
192.168.10.97	8266	0	192.66 MB	146.78 MB	45.88 MB
192.168.10.99	3597	0	191.12 MB	180.63 MB	10.49 MB
192.168.10.94	5729	0	171.23 MB	143.25 MB	27.98 MB
192.168.10.131	3365	0	162.39 MB	149.72 MB	12.67 MB
192.168.10.105	6312	0	155.10 MB	138.47 MB	16.63 MB
192.168.10.83	4929	0	151.09 MB	112.62 MB	38.46 MB
192.168.10.130	4360	0	143.25 MB	125.53 MB	17.73 MB
192.168.10.92	5872	0	133.51 MB	117.73 MB	15.78 MB
192.168.10.103	8673	0	122.61 MB	106.71 MB	15.90 MB
192.168.10.95	3858	0	115.41 MB	103.83 MB	11.59 MB
192.168.10.141	7931	0	108.95 MB	94.87 MB	14.08 MB
192.168.10.140	3621	0	108.72 MB	89.31 MB	19.41 MB
192.168.10.123	4375	0	82.67 MB	70.16 MB	12.51 MB
192.168.10.6	358	0	81.79 MB	75.81 MB	5.98 MB
192.168.10.119	2584	0	70.96 MB	62.12 MB	8.84 MB
192.168.10.93	875	0	60.64 MB	57.19 MB	3.45 MB
192.168.10.134	3211	0	59.95 MB	52.14 MB	7.81 MB
192.168.10.136	1328	0	58.86 MB	50.45 MB	8.41 MB
192.168.10.126	3774	0	58.83 MB	49.67 MB	9.17 MB
192.168.10.120	2645	0	55.89 MB	50.04 MB	5.84 MB
192.168.10.127	1251	0	53.23 MB	48.74 MB	4.49 MB
192.168.10.88	2020	0	46.01 MB	37.73 MB	8.28 MB
192.168.10.109	2499	0	45.04 MB	38.12 MB	6.92 MB
Sub-total: 35	259,525		9.5 GB	8.68 GB	841.04 MB
Percent: 54%	91%	NaN	95%	95%	90%
Totals: 65	283,785		10 GB	9.09 GB	933.67 MB

SurfTime

SurfTime is an estimate of the total amount of time a user spends surfing the Internet and provides a way to quantify Internet use. Estimates are based on the assumption that as long as a user is Web surfing, clicking link after link, he is adding to his SurfTime. Acceptable amounts of SurfTime vary widely depending on company culture, type of business, applications in use and job functions. This report lists all clients (workstations) that have a daily SurfTime averaging more than 30 minutes, and is a good tool to understand how heavily the Internet is being used.

Note: Some clients may report suspiciously high SurfTimes. These occurrences may be caused by Internet applications that maintain a constant connection to an Internet site or which make frequent update requests for new data. Applications may include Spyware, web-based remote desktop control, real time stock quotes, Instant Messaging, Internet radio and Peer-to-Peer applications. In most cases, any application exhibiting constant or high levels of traffic activity should be investigated. Anything not directly supporting a legitimate business purpose should be eliminated.

Note: All SurfTime is in an Hours:Minutes:Seconds format (HH:MM:SS)

Summary:

- A total of 65 web surfing clients were discovered.
- On average each client visited 342.55 unique web sites.
- On average each client has a daily SurfTime of 01:31:01
- 44 (68%) clients had a daily average SurfTime over 30 minutes.
- Total accumulated SurfTime for all clients over the audit period was 574:49:02

Clients with a daily average SurfTime greater than 30 minutes.

Client	*Daily Avg	Total	#Days	#Sites
192.168.10.97	20:46:13	166:09:45	8	295
192.168.10.108	06:59:27	41:56:45	6	247
192.168.10.85	05:56:58	23:47:52	4	154
192.168.10.129	05:00:23	30:02:22	6	724
192.168.10.103	04:55:52	39:27:03	8	924
192.168.10.123	04:24:53	26:29:19	6	273
192.168.10.142			5	455
192.168.10.87			1	101
192.168.10.101			8	5555
192.168.10.112			8	869
192.168.10.117			5	171
192.168.10.84			1	82
192.168.10.98			5	443
192.168.10.140	01:50:55	07:54:29	5	243
192.168.10.88	01:27:37	02:55:14	2	225
192.168.10.91	01:26:15	08:37:33	6	1878
192.168.10.86	01:23:04	02:46:09	2	31
192.168.10.82	01:18:44	06:33:43	5	550
192.168.10.83	01:17:36	05:10:27	4	525
192.168.10.130	01:16:06	07:36:37	6	526
192.168.10.95	01:10:16	04:41:05	4	332
192.168.10.92	01:10:04	07:00:29	6	419
192.168.10.141	01:09:06	04:36:24	4	89
192.168.10.106	01:05:34	05:27:51	5	377
192.168.10.119	00:59:53	05:59:19	6	123
192.168.10.116	00:59:00	05:54:03	6	562
192.168.10.136	00:56:46	05:40:37	6	96
192.168.10.128	00:54:23	07:15:10	8	585
192.168.10.94	00:53:04	05:18:24	6	1090
192.168.10.132	00:50:31	05:03:07	6	98
192.168.10.89	00:48:11	00:48:11	1	80
192.168.10.113	00:47:56	02:23:50	3	64
192.168.10.139	00:47:04	04:42:24	6	78
192.168.10.131	00:45:00	04:30:02	6	384
192.168.10.105	00:44:15	05:09:48	7	419
192.168.10.90	00:39:28	01:58:24	3	173
192.168.10.96	00:37:23	04:59:10	8	193
192.168.10.99	00:36:33	03:39:19	6	306
192.168.10.134	00:36:31	03:39:09	6	354
192.168.10.145	00:33:53	01:41:40	3	45
192.168.10.120	00:33:52	03:23:12	6	208
192.168.10.126	00:33:30	03:21:01	6	177
192.168.10.81	00:32:53	03:17:20	6	242
192.168.10.111	00:30:47	03:04:46	6	119

The # of sites users access equates to risk. The more sites the greater the possibility for exploit via malicious software, viruses or offensive content. Anytime you note more than 500 sites accessed, this is a red flag for potential problems (policy breach, productivity issues, abuse and misuse)

Sub-Total: 44
Percent: 68%
Total: 65

Client	*Daily Avg	Total	#Days	#Sites
--------	------------	-------	-------	--------

Popular Search Engines

Use of popular search engines presents a unique snapshot of Internet use. While not directly a security threat, search engines are powerful tools that can be misused to purposely or accidentally subvert policy and security measures.

If your organization relies on web filtering, realize that the number of sites indexed, the technology used and the investment in keeping current by any of the popular search engines far exceeds the investments of web filtering companies to block or classify content. It is not uncommon to use search engines to find unblocked sites, proxies, or even software that will evade detection by web filters.

Popular Search engines in use

Types	Clients	Sites	Sessions	Failed	*Bytes
google.com	40	5	2901	0	81.84 MB
yahoo.com	22	7	447	0	3.11 MB
msn.com	19	2	272	0	1.50 MB
ask.com	1	1	4	0	44.29 KB
altavista.com	2	1	2	0	4.89 KB
Totals: 5		16	3,626		86.49 MB

Top search queries

Rank	Query	*Hits	Percent
1.	type:gpick	60	4.3%
2.	planet	55	4%
3.	WiFi	55	4%
4.	world	55	4%
5.	NFL	55	4%
6.	moon	55	4%
7.	Packers	55	4%
8.	earth	55	4%
9.	Chargers	55	4%
10.	globe	55	4%
11.	Giants	55	4%
12.	Super Bowl	55	4%
13.	Patriots	53	3.8%
14.	cloverfield	20	1.4%
15.	run	20	1.4%
16.	myspace	19	1.4%
17.	cozumel	18	1.3%
18.	projection screen installer	13	.9%
19.	dallas cowboys cheerleaders	13	.9%
20.	katie clarke	11	.8%
21.	devilish fetish ball 2008	9	.6%

**Want to know how the Internet is used?
Here's what the user base may be
searching for using Google, Yahoo or MSN
and so forth. If you note searches for
"hacking tools" or "New Jobs" it may be a
signal of pending problems.**

Rank	Query	*Hits	Percent
22.	galveston cruises	8	.6%
23.	starwars monsters	8	.6%
24.	progreso mexico	8	.6%
25.	adjustable beds	7	.5%
26.	performance manual transmission for 2003 mustang gt	6	.4%
27.	FRAM DONALDSON DYNAFLEX	6	.4%
28.	improper contact line/surface	5	.4%
29.	John Winters	5	.4%
30.	www.bader.de.	5	.4%
31.	Diagram walls AND stop pins	5	.4%
32.	chicago	5	.4%
33.	Diagragm walls AND stop pins	4	.3%
34.	COSMIC DRIP TEST linear/surface	4	.3%
35.	Entertech INSTRUMENTS	4	.3%
Sub Total: 35 (9.2%)		921	66.5%
Totals:382		1385	100%

Common File Downloads

A significant portion of Web traffic is not simply the viewing of text and graphics on Web pages, but the downloading of files that are themselves executable or data that is passed onto helper applications. File types such as .cab, .class, .zip and .exe often represent programs that are being downloaded either to be installed on the local machine or to run within the web browser and file types such as wmv, asf, rm, mp3 and ram represent video and audio feeds. A large number of .pdf, .doc and .ps files can be an indication of users conducting research activities. Regardless of how common they are or which company produces them, all software can contain known and unknown flaws creating an undocumented vector for attack and compromise. Therefore, it is important to understand what types of common file downloads are typically associated with user Web surfing activities.

Common types of files downloaded

File Ext	Requests	Clients	Servers	Bytes
.exe	536	19	14	870.69 MB
.rar	984	1	68	647.01 MB
.jpg	862	30	545	442.04 MB
.pdf	509	18	43	306.55 MB
.flv	100	26	37	266.87 MB
.swf	140	32	71	235.95 MB
.mov	27	2	7	107.79 MB
.cab	1830	58	10	85.36 MB
.gif	163	22	106	83.05 MB
.zip	498	14	9	79.94 MB
.mp3	94	15	39	55.16 MB
.wmv	52	7	10	46.81 MB
.png	77	9	55	35.29 MB
.bmp	14	5	14	7.33 MB
.asf	11	1	3	7.23 MB
.gz	23	2	3	3.20 MB
.mpg	3	1	1	3.06 MB
.jar	22	6	7	550.25 KB
.jpeg	1	1	1	329.01 KB
.doc	1	1	1	272.00 KB
.wav	6	2	2	193.21 KB
.class	22	8	8	49.77 KB
.mid	2	1	1	28.25 KB
Totals: 23	5977			3.21 GB

Top 35 downloads

Web Site	Mime Type	Bytes
Filename		
dl-ak.solidworks.com	octet-stream	
swexplorer.exe		379.31 MB
dl-ak.solidworks.com	octet-stream	
dwgeditor.exe		144.49 MB
dl-ak.solidworks.com	octet-stream	
sw2008-0.1-2.0-i.exe		120.35 MB
rs222tl.rapidshare.com	octet-stream	
3300Icons_www.softarchive.net.part1.rar		100.31 MB
rs277132.rapidshare.com	octet-stream	
-www.softarchive.net-Nude_Fun-12.rar		92.51 MB
rs28cg.rapidshare.com	octet-stream	
www.softarchive.net.bts5.part7.rar		89.97 MB
www.naswug.com	x-shockwave-flash	
single_sketch.swf		71.10 MB
67.131.237.23	x-rtsp-tunnelled	
972345688g_1_350.mov		51.70 MB
rs12134.rapidshare.com	octet-stream	
EZ.Photo.Calendar.Creator.Plus.v907.rar		50.91 MB
www.naswug.com	x-shockwave-flash	
unabsorb_sketches.swf		50.91 MB
livedocs.adobe.com	pdf	
indesign_cs3_help.pdf		45.75 MB
au.download.windowsupdate.com	octet-stream	
officesbmesp3-kb920115-fullfile-enu_47026dbd94a489641f0d9ea18266fbfa416fa209.cab		44.55 MB
livedocs.adobe.com	pdf	
photoshop_cs3_help.pdf		43.49 MB
www.businessplans.org	octet-stream	
pwe10hereto.exe		41.75 MB
livedocs.adobe.com	pdf	
illustrator_cs3_help.pdf		38.91 MB
w14.easy-share.com	octet-stream	
StormPredator.Full.v3.2.2.0.rar		38.16 MB
rs28gc2.rapidshare.com	octet-stream	
3300Icons_www.softarchive.net.part2.rar		36.96 MB
help.adobe.com	pdf	
pselements_6_help.pdf		35.75 MB
dl-ak.solidworks.com	octet-stream	
eDrawings.exe		32.78 MB
67.131.237.15	x-rtsp-tunnelled	
972345688g_1_350.mov		27.99 MB
www.download.windowsupdate.com	octet-stream	
wmp11-windowsxp-x86-enu_0581874009280c186f856f079594d1ccc7a851f4.exe		24.56 MB
content.movies.myspace.com	octet-stream	
2085707266.flv		22.69 MB
livedocs.adobe.com	pdf	

Web Site	Mime Type	Bytes
Filename		
dreamweaver_cs3_help.pdf		21.55 MB
www.naswug.com	x-shockwave-flash	
filletxpert08.swf		21.47 MB
rs15cg.rapidshare.com	octet-stream	
FarfalleWalls_www.softarchive.net.rar		20.39 MB
livedocs.adobe.com	pdf	
incopy_cs3_help.pdf		19.54 MB
rs73cg.rapidshare.com	octet-stream	
Google.Earth.Pro.v4.1.7087.rar		18.98 MB
content.newsfilter.org	octet-stream	
47519.flv		18.49 MB
livedocs.adobe.com	pdf	
flash_cs3_help.pdf		18.08 MB
rs160132.rapidshare.com	octet-stream	
GoogleEarth.rar		17.65 MB
223.61.13.87	x-flv	
sex-lehrerin,property=Video.flv		16.95 MB
rs95gc2.rapidshare.com	octet-stream	
HarmonyDesktop_08__WP_Pack_www.softarchive.net.zip		16.42 MB
vid6.stileproject.com	x-ms-wmv	
tay7.wmv		16.21 MB
a2047.v1412b.c1412.g.vq.akamaistream.net	x-rtsp-tunnelled	
972345688g_1_350.mov		15.72 MB
rs7cg.rapidshare.com	octet-stream	
www.softarchive.net_google-earth4.2.rar		14.96 MB
Totals: 35		1.78 GB
Percent: 2%		55%
Totals: 2,037		3.21 GB

Web-based File Sharing

Web-based file sharing sites represent a growing phenomenon that allows users to exchange large files through special hosted web servers. Many of these sites offer users free storage for 30 days or more for individual files less than 50 MB in size. Users that subscribe to the service can store larger files for longer periods of time. When a user uploads a file it is assigned a unique URL that can be used by anyone to access the information. File sharers then distribute these URLs by posting them to blogs, news groups, bulletin boards and e-mail lists. These sites effectively perform the same function as peer-to-peer file sharing but are less obvious and more difficult to identify. Like Peer-to-peer file sharing, Web-based file sharing represents a mechanism for exporting internal confidential data or potentially creating an undocumented vector for attack. These services illustrate how the market continuously evolves to create new ways to evade network monitoring and filtering tools and gain access to a large user population. Any use should be investigated.

Things to consider:

- Use of this service creates an undocumented vector for attack and conduit through which confidential information and Intellectual property can be exported out of the network.
- File sharing represents a huge liability for businesses when it is used to share pirated software, songs, videos and other copyrighted or controlled materials.
- These services are harder to detect than Peer-to-peer and offer the use anonymity and are becoming a preferred resource among aggressive file sharers.
- If there is a legitimate use of Web-based file sharing such as for file back-up, is it being used to circumvent other security controls? For example, is it being used to bypass the controls on the size or types of file attachments that are allowed to pass through e-mail?

Web-based File Sharing Clients

Client	Outbound		*Total	Bytes	
	Sessions	Failed		Inbound	Outbound
192.168.10.101	1275	0	672.86 MB	650.47 MB	22.38 MB
192.168.10.95	1	0	3.85 KB	3.05 KB	821.00 B
Totals: 2	1,276		672.86 MB	650.48 MB	22.39 MB

File Sharing Servers

Server	Outbound		*Total	Bytes	
	Sessions	Failed		Inbound	Outbound
rs222tl.rapidshare.com	45	0	107.94 MB	104.25 MB	3.70 MB
rs277l32.rapidshare.com	74	0	99.89 MB	96.52 MB	3.37 MB
rs28cg.rapidshare.com	103	0	96.29 MB	93.54 MB	2.75 MB
rs12l34.rapidshare.com	36	0	54.77 MB	52.91 MB	1.86 MB
rs28gc2.rapidshare.com	48	0	39.80 MB	38.41 MB	1.39 MB
rs15cg.rapidshare.com	31	0	21.93 MB	21.19 MB	763.53 KB
rs73cg.rapidshare.com	27	0	20.43 MB	19.73 MB	718.30 KB
rs160l32.rapidshare.com	32	0	18.99 MB	18.35 MB	658.61 KB
rs95gc2.rapidshare.com	28	0	17.67 MB	17.07 MB	616.08 KB
rs7cg.rapidshare.com	18	0	16.08 MB	15.55 MB	550.41 KB
rs57tl2.rapidshare.com	14	0	13.03 MB	12.60 MB	435.74 KB
rs259tg.rapidshare.com	22	0	12.37 MB	11.97 MB	412.88 KB
www100.megaupload.com	54	0	12.05 MB	11.69 MB	366.32 KB
rs133tl2.rapidshare.com	22	0	11.19 MB	10.81 MB	385.33 KB
rs228tg.rapidshare.com	25	0	11.17 MB	10.79 MB	388.66 KB
rs171tl.rapidshare.com	19	0	10.82 MB	10.46 MB	368.29 KB
rs11tl2.rapidshare.com	46	0	10.35 MB	9.97 MB	386.48 KB
rs227tl.rapidshare.com	11	0	10.26 MB	9.93 MB	333.37 KB
rs165gc.rapidshare.com	19	0	9.73 MB	9.41 MB	335.82 KB
rs164cg.rapidshare.com	22	0	8.20 MB	7.92 MB	280.33 KB
rs105tg.rapidshare.com	23	0	7.38 MB	7.14 MB	250.93 KB
rs288tl.rapidshare.com	13	0	6.41 MB	6.21 MB	202.94 KB
rs80l34.rapidshare.com	21	0	5.66 MB	5.46 MB	198.66 KB
rs268tg.rapidshare.com	17	0	5.09 MB	4.92 MB	177.91 KB
rs14gc2.rapidshare.com	20	0	5.00 MB	4.82 MB	181.47 KB
rs178l3.rapidshare.com	13	0	3.96 MB	3.83 MB	131.34 KB
rs102gc.rapidshare.com	18	0	3.89 MB	3.76 MB	129.99 KB
rs102tl2.rapidshare.com	12	0	3.53 MB	3.41 MB	122.60 KB
rs213tl2.rapidshare.com	9	0	2.64 MB	2.56 MB	83.86 KB
rs127tl2.rapidshare.com	13	0	1.96 MB	1.90 MB	65.20 KB
rs58gc.rapidshare.com	11	0	1.83 MB	1.77 MB	64.08 KB
rs12gc2.rapidshare.com	11	0	1.83 MB	1.76 MB	66.99 KB
rs256tl2.rapidshare.com	25	0	1.74 MB	1.67 MB	72.31 KB
rs263gc.rapidshare.com	9	0	1.73 MB	1.67 MB	58.91 KB
rs257cg.rapidshare.com	8	0	1.52 MB	1.47 MB	48.83 KB
rs208tl2.rapidshare.com	17	0	1.48 MB	1.43 MB	51.94 KB
rs142tg.rapidshare.com	8	0	1.33 MB	1.29 MB	41.50 KB
rs263l32.rapidshare.com	8	0	1.06 MB	1.02 MB	34.09 KB
rs246cg.rapidshare.com	4	0	878.42 KB	849.15 KB	29.27 KB
rs262tl2.rapidshare.com	4	0	687.87 KB	667.02 KB	20.85 KB
rs83gc2.rapidshare.com	4	0	679.96 KB	657.29 KB	22.66 KB
rs273tl.rapidshare.com	4	0	637.97 KB	618.08 KB	19.89 KB
rapidshare.com	188	0	604.00 KB	465.21 KB	138.79 KB
rs206cg.rapidshare.com	4	0	590.94 KB	571.87 KB	19.07 KB
rs172cg.rapidshare.com	4	0	529.28 KB	511.72 KB	17.57 KB
rs98l32.rapidshare.com	4	0	519.45 KB	503.17 KB	16.28 KB

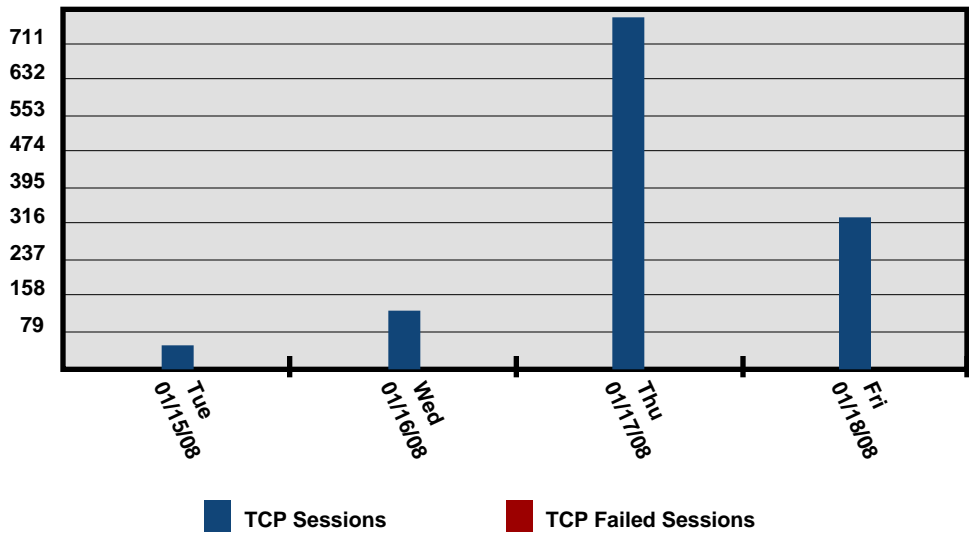
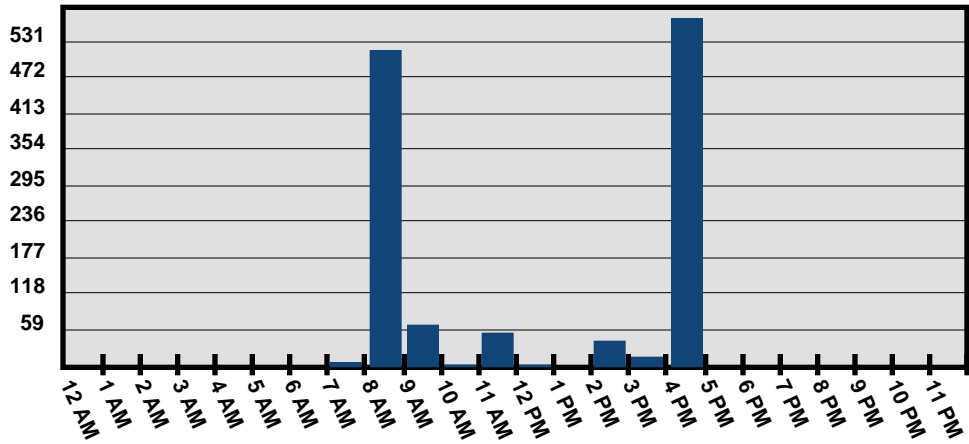
Server	Outbound		*Total	Bytes	
	Sessions	Failed		Inbound	Outbound
rs275cg.rapidshare.com	4	0	481.03 KB	465.36 KB	15.67 KB
rs211cg.rapidshare.com	4	0	439.33 KB	424.83 KB	14.50 KB
rs50132.rapidshare.com	4	0	405.83 KB	392.54 KB	13.29 KB
rs261132.rapidshare.com	4	0	387.67 KB	374.40 KB	13.28 KB
rs207132.rapidshare.com	4	0	383.20 KB	370.21 KB	12.98 KB
rs284132.rapidshare.com	4	0	382.91 KB	370.16 KB	12.76 KB
rs162gc2.rapidshare.com	4	0	355.59 KB	343.61 KB	11.98 KB
rs109cg2.rapidshare.com	4	0	349.64 KB	337.93 KB	11.71 KB
rs21013.rapidshare.com	4	0	345.25 KB	333.72 KB	11.53 KB
rs285132.rapidshare.com	4	0	336.73 KB	325.39 KB	11.34 KB
rs138gc.rapidshare.com	4	0	331.08 KB	319.80 KB	11.28 KB
rs136tg.rapidshare.com	4	0	327.93 KB	316.92 KB	11.00 KB
rs62132.rapidshare.com	4	0	313.57 KB	302.92 KB	10.65 KB
www.megaupload.com	2	0	310.10 KB	283.98 KB	26.12 KB
rs62tl2.rapidshare.com	4	0	303.20 KB	291.79 KB	11.41 KB
rs150gc.rapidshare.com	4	0	250.20 KB	241.30 KB	8.89 KB
rs246tl.rapidshare.com	4	0	248.97 KB	239.98 KB	8.99 KB
rs267gc.rapidshare.com	4	0	239.93 KB	230.18 KB	9.75 KB
rs78cg.rapidshare.com	4	0	205.84 KB	197.97 KB	7.88 KB
rs77tg.rapidshare.com	4	0	204.38 KB	196.57 KB	7.82 KB
rs179cg.rapidshare.com	4	0	147.96 KB	141.87 KB	6.08 KB
rs238tg.rapidshare.com	4	0	139.49 KB	133.47 KB	6.02 KB
rs28.rapidshare.com	5	0	39.68 KB	35.18 KB	4.50 KB
rs28132.rapidshare.com	5	0	27.76 KB	24.08 KB	3.68 KB
rs275gc.rapidshare.com	4	0	26.39 KB	23.60 KB	2.78 KB
rs21132.rapidshare.com	2	0	13.23 KB	11.81 KB	1.42 KB
rs26713.rapidshare.com	3	0	9.32 KB	6.60 KB	2.73 KB
rs18113.rapidshare.com	2	0	7.90 KB	6.02 KB	1.88 KB
www.fileden.com	1	0	3.85 KB	3.05 KB	821.00 B
Totals: 75	1,276		672.86 MB	650.48 MB	22.39 MB

Top 35 URL requests to Servers

Filename	Requests	Method	Status	*Total Bytes	Mime Type Avg. Bytes
3300Icons_www.softarchive.net.part1.rar	43	Get	Partial Content	100.31 MB	octet-stream 2.33 MB
-www.softarchive.net-Nude_Fun-12.rar	65	Get	Partial Content	92.51 MB	octet-stream 1.42 MB
www.softarchive.net.bts5.part7.rar	1	Post	OK	89.97 MB	octet-stream 89.97 MB
EZ.Photo.Calendar.Creator.Plus.v907.rar	36	Get	Partial Content	50.91 MB	octet-stream 1.41 MB
3300Icons_www.softarchive.net.part2.rar	47	Get	Partial Content	36.96 MB	octet-stream 805.16 KB
FarfalleWalls_www.softarchive.net.rar	31	Get	Partial Content	20.39 MB	octet-stream 673.37 KB
Google.Earth.Pro.v4.1.7087.rar	27	Get	Partial Content	18.98 MB	octet-stream 719.82 KB
GoogleEarth.rar	32	Get	Partial Content	17.65 MB	octet-stream 564.88 KB
HarmonyDesktop_08_WP_Pack_www.softarchive.net.zip	28	Get	Partial Content	16.42 MB	octet-stream 600.53 KB
www.softarchive.net_google-earth4.2.rar	18	Get	Partial Content	14.96 MB	octet-stream 851.01 KB
www.softarchive.netInternet.Business.Promoter.v9.7.1.Multilingual-ACME.rar	13	Get	Partial Content	12.13 MB	octet-stream 955.10 KB
business_concept_nice_images_Vol.1_www.softarchive.net.rar	22	Get	Partial Content	11.51 MB	octet-stream 535.84 KB
GFX-254.Icons.Collection_softarchive.net.rar	1	Get	Partial Content	11.23 MB	octet-stream 11.23 MB
incredimail.5.70.build.3317_www.softarchive.net.rar	22	Get	Partial Content	10.40 MB	octet-stream 484.26 KB
XnView.v1.92.Final.rar	25	Get	Partial Content	10.38 MB	octet-stream 425.33 KB
51_HTPJFTEG_www.softarchive.net.rar	19	Get	Partial Content	10.06 MB	octet-stream 542.39 KB
Avatars64x64_www.softarchive.net.rar	35	Get	Partial Content	9.59 MB	octet-stream 280.55 KB
IncrediMail_5.68_Build_3242.rar	11	Get	Partial Content	9.55 MB	octet-stream 889.42 KB
NetworkMagic4.2.7234.0_www.softarchive.net.rar	19	Get	Partial Content	9.05 MB	octet-stream 487.71 KB
11K_Recipes_www.softarchive.net.rar	22	Get	Partial Content	7.62 MB	octet-stream 354.71 KB
Hacking.Google.Maps.and.Google.Earth_DangerZone.rar	23	Get	Partial Content	6.87 MB	octet-stream 305.73 KB
MMWWW_www.softarchive.net.rar	11	Get	Partial Content	5.96 MB	octet-stream 554.95 KB
Folder.Marker.Pro.v3.0.rar	21	Get	Partial Content	5.25 MB	octet-stream 256.19 KB

Filename	Requests	Method	Status	*Total Bytes	Mime Type
					Avg. Bytes
SmartWhois_v4.3.212_www.softarchive.net.rar					octet-stream
17	Get	Partial Content	4.73 MB	284.84 KB	
megascopic_Wallpapers_www.softarchive.net.rar					octet-stream
20	Get	Partial Content	4.64 MB	237.42 KB	
Apolisoft.Font.Fitting.Room.Deluxe.v2.9.5.5.rar					octet-stream
13	Get	Partial Content	3.69 MB	290.44 KB	
WinWAP.for.Windows.v3.2.1.28.rar					octet-stream
18	Get	Partial Content	3.61 MB	205.58 KB	
LANview.v2.9.build.1229.rar					octet-stream
12	Get	Partial Content	3.28 MB	279.89 KB	
Soth.Web.Video.Downl.for.Firef.v3.6.build.71113_www.softarchive.net.rar					octet-stream
9	Get	Partial Content	2.46 MB	280.27 KB	
XmasIco2k8_www.softarchive.net.rar					octet-stream
13	Get	Partial Content	1.82 MB	143.60 KB	
Firefox_Secrets_www.softarchive.net.rar					octet-stream
9	Get	Partial Content	1.69 MB	192.25 KB	
Scan-to-PDF-3.2.0.6_www.softarchive.net.rar					octet-stream
9	Get	Partial Content	1.68 MB	191.35 KB	
Tracks_Eraser_Pro_7.0_www.softarchive.net.rar					octet-stream
25	Get	Partial Content	1.60 MB	65.70 KB	
Web.Dumper.v2.4.rar					octet-stream
9	Get	Partial Content	1.60 MB	182.49 KB	
www.softarchive.net_Mayoko110.rar					octet-stream
7	Get	Partial Content	1.41 MB	206.57 KB	
Sub-total: 733				610.9 MB	
Percent: 63%				98%	
Total: 1167				625.72 MB	

Sharing Access times



Microsoft Updates

Windows based workstations dominate most organizations and this fact makes them the preferred target of today's Internet hackers and thieves. The following data shows you what clients did and did not contact Microsoft's update servers. During a one week audit all of your Windows workstations should have contacted these servers at least once. With new patches available monthly and critical patches made available more frequently any workstation that is not updating, quickly becomes an easy target.

The audit discovered 77 total network clients. 22% of them did not contact known Microsoft update servers.

Issues to consider:

- Do you have an update / patch management policy in place?
- Do users have individual control over the update / patch process?
- Installed virus, spyware, firewalls and vulnerability scanning do not guarantee that un-patched systems are safe against known exploits and are not a substitute for poor patch management.
- How much of your bandwidth does getting updates from Microsoft consume? By default every machine will download an individual copy of an update. In larger networks this can lead to unexplained bandwidth spikes or performance problems. Microsoft's Windows Server Update Services (WSUS) is one solution that can be used to manage updates / patches and minimize bandwidth consumption.
- If 22% exposure to patched Microsoft vulnerabilities sounds too high then its time to review policies and procedures for ensuring that systems are patched in a timely fashion.

Potentially 22% of your network clients maybe exposed to known Microsoft vulnerabilities simply because they are not checking for updates.

If 22% of your organizations clients are not running the Microsoft operating system or if you have in place a centralized software distribution system that ensures timely installations of updates this may not be a problem.

Clients that did not contact Microsoft's servers. 17 (22%)

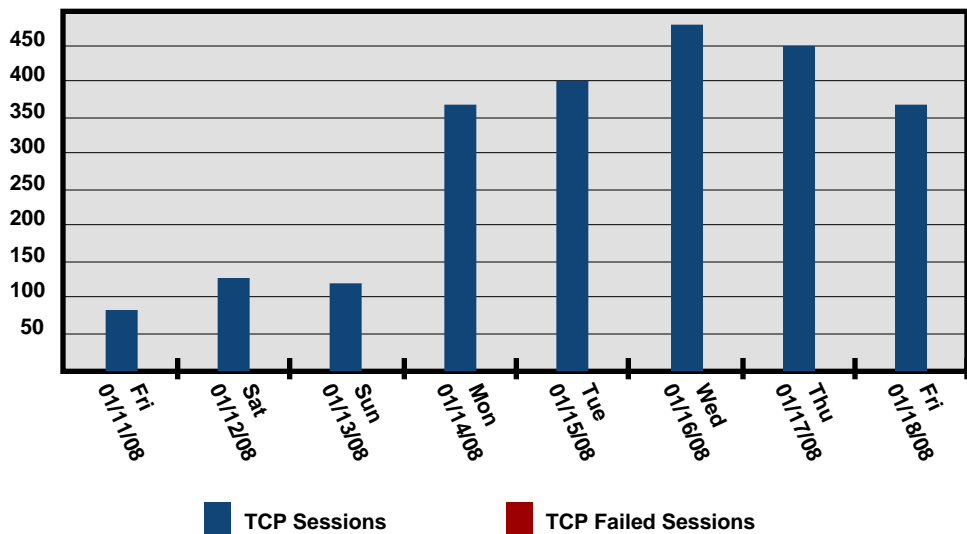
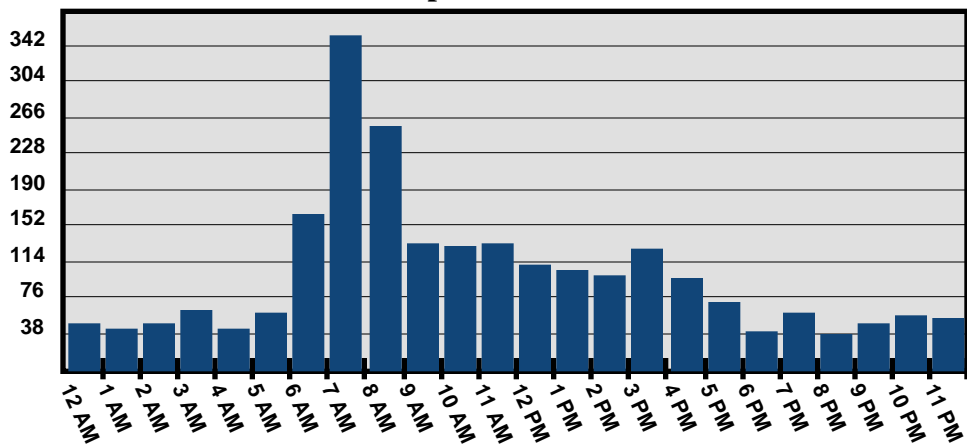
10.69.6.6	169.254.102.157	169.254.130.194
169.254.20.80	169.254.235.128	192.168.0.100
192.168.0.104	192.168.0.107	192.168.10.100
192.168.10.124	192.168.10.135	192.168.10.144
192.168.10.20	192.168.10.21	192.168.10.22
192.168.10.87	192.168.10.88	

Clients that did contact Microsoft's servers. 60 (78%)

Top clients shown by bandwidth.

Client	Outbound		*Total	Bytes	
	Sessions	Failed		Inbound	Outbound
192.168.10.131	79	0	106.00 MB	103.04 MB	2.97 MB
192.168.10.116	35	0	60.83 MB	58.04 MB	2.80 MB
192.168.10.81	16	0	35.29 MB	34.29 MB	1018.91 KB
192.168.10.129	64	0	11.66 MB	10.71 MB	965.38 KB
192.168.10.110	18	0	10.84 MB	10.35 MB	499.94 KB
192.168.10.127	44	0	9.03 MB	8.61 MB	430.29 KB
192.168.10.117	64	0	3.67 MB	3.05 MB	639.23 KB
192.168.10.5	23	0	3.28 MB	3.03 MB	259.21 KB
192.168.10.137	10	0	3.11 MB	3.01 MB	102.81 KB
192.168.10.113	21	0	2.99 MB	2.86 MB	140.46 KB
192.168.10.101	177	0	2.01 MB	760.88 KB	1.26 MB
192.168.10.7	131	0	1.51 MB	607.01 KB	944.12 KB
192.168.10.112	129	0	1.16 MB	563.34 KB	625.94 KB
192.168.10.132	90	0	1.10 MB	477.77 KB	648.56 KB
192.168.10.103	131	0	1.06 MB	560.09 KB	522.55 KB
192.168.10.96	127	0	1.05 MB	591.85 KB	481.76 KB
192.168.10.94	95	0	1.04 MB	485.49 KB	578.52 KB
192.168.10.105	106	0	1.03 MB	489.57 KB	563.58 KB
192.168.10.6	18	0	956.09 KB	433.13 KB	522.96 KB
192.168.10.123	87	0	949.92 KB	420.57 KB	529.36 KB
192.168.10.136	54	0	899.42 KB	342.59 KB	556.82 KB
192.168.10.85	64	0	860.91 KB	357.43 KB	503.49 KB
192.168.10.82	47	0	733.87 KB	320.03 KB	413.84 KB
192.168.10.134	59	0	733.83 KB	376.24 KB	357.59 KB
192.168.10.83	44	0	699.23 KB	272.85 KB	426.38 KB
192.168.10.97	19	0	689.45 KB	300.21 KB	389.24 KB
192.168.10.108	51	0	686.11 KB	322.10 KB	364.01 KB
192.168.10.98	40	0	683.96 KB	265.93 KB	418.02 KB
192.168.10.102	21	0	673.21 KB	298.39 KB	374.82 KB
192.168.10.130	44	0	663.96 KB	313.60 KB	350.35 KB
192.168.10.139	27	0	654.28 KB	199.77 KB	454.51 KB
192.168.10.138	50	0	644.10 KB	311.63 KB	332.47 KB
192.168.10.119	48	0	641.95 KB	312.78 KB	329.16 KB
192.168.10.92	51	0	635.35 KB	304.66 KB	330.69 KB
192.168.10.122	21	0	627.10 KB	220.38 KB	406.72 KB
192.168.10.8	25	0	620.57 KB	270.34 KB	350.23 KB
192.168.10.120	19	0	616.52 KB	226.08 KB	390.44 KB
192.168.10.91	20	0	613.03 KB	246.24 KB	366.79 KB
192.168.10.140	18	0	603.12 KB	319.04 KB	284.08 KB
192.168.10.121	15	0	508.61 KB	207.16 KB	301.45 KB
Sub-total: 40	2,202		271.7 MB	247.9 MB	23.8 MB
Percent: 67%	92%	NaN	98%	99%	90%
Totals: 60	2,403		276.48 MB	250.01 MB	26.47 MB

Access to Update Server times



■ TCP Sessions
 ■ TCP Failed Sessions

Spyware / Adware

Spyware / Adware programs are a tremendous resource drain for many IT departments. These programs are usually downloaded and installed by users unintentionally or bundled with other applications that profess to make the Internet experience easier or more fun. While many of these programs promise to benignly track user surfing habits, most quickly become more than an annoyance spawning pop-up advertisements, causing performance problems and system instability. These actions lead directly to loss of employee productivity, increased helpdesk calls, and increasing IT costs.

From a practical standpoint, any workstation infected with a Spyware / Adware program is compromised. The reputation of Spyware / Adware programs to secretly install themselves on machines has become mythical. The truth is that most Spyware / Adware program are installed with the consent of the user, although often this consent is socially engineered. The important fact to understand is that a hacker with malicious intent can exploit the same social, network and technology conditions to install backdoors, key loggers and Trojans. The degree to which an organization is infected with Spyware / Adware is a fairly accurate barometer for how susceptible it is to attacks.

Note: More specific details are included in the standalone Spyware / Adware report.

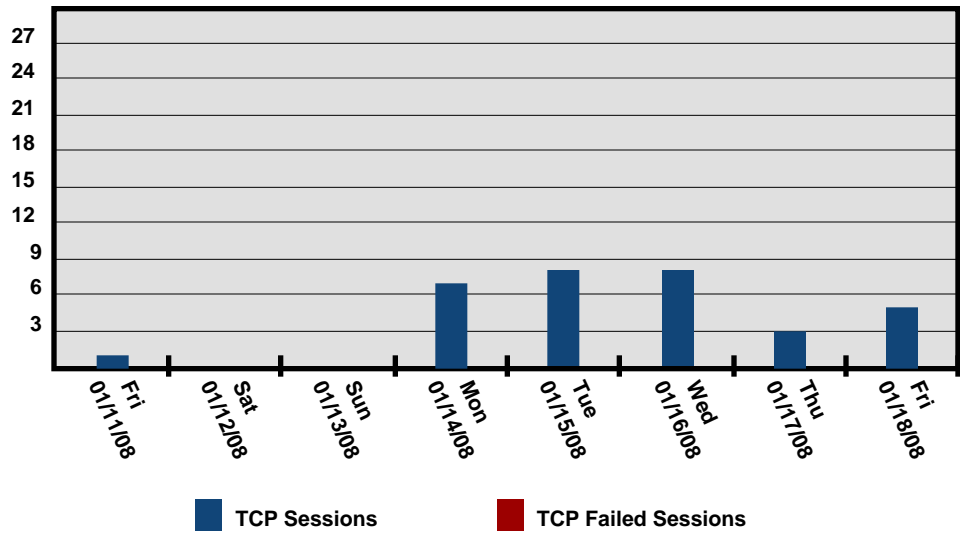
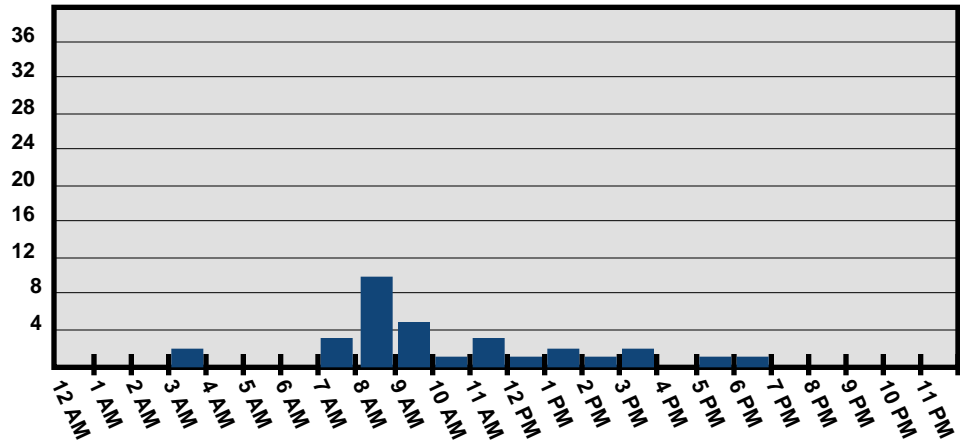
Discovered Spyware / Adware types

Types	Clients	Sites	Sessions	Failed	*Bytes
MyWebSearch	5	1	32	0	63.94 KB
Totals: 1		1	32		63.94 KB

Top Spyware / Adware Clients

Client	Outbound		*Total	Bytes	
	Sessions	Failed		Inbound	Outbound
192.168.10.111	13	0	24.88 KB	15.20 KB	9.67 KB
192.168.10.94	9	0	19.34 KB	11.38 KB	7.96 KB
192.168.10.85	4	0	8.88 KB	5.15 KB	3.73 KB
192.168.10.98	4	0	8.52 KB	5.44 KB	3.08 KB
192.168.10.123	2	0	2.32 KB	1.27 KB	1.04 KB
Sub-total: 5	32		63.94 KB	38.45 KB	25.49 KB
Percent: 100%	100%	NaN	100%	100%	100%
Totals: 5	32		63.94 KB	38.45 KB	25.49 KB

Access times



Web-based E-mail

Web-based e-mail offers a flexible and convenient way to view and send e-mails from any Internet-connected computer. Many of these services are free, anonymous, convenient for personal e-mail use and unmonitored.

Organizations that allow users to access personal Web-based accounts from work maybe seriously compromising their security. Web-based e-mail circumvents investment in SMTP e-mail security technologies such as anti-virus, anti-spam and content protection systems. As an undocumented information conduit it can be used to export confidential company information or exchange materials and views clearly against company or regulatory policy. Additionally, while web-based e-mail offers its users some degree of identity protection the same is not true for the organization. E-mails that contain web beacons, scripts, and executables can be used to identify the organization, internal workstations or compromise systems.

Threats:

- Represents an undocumented conduit for exporting confidential information out of the organization.
- Regulated industries that allow employees to use personal e-mail tools, without retaining those messages, could face serious legal and regulatory trouble related to Sarbanes-Oxley compliance.
- Regulated healthcare industries that allow employees to use external e-mail services to exchange patient records could face serious legal and regulatory trouble related to HIPAA by exposing confidential healthcare information in a readable format over the Internet.
- Each use represents an undocumented remotely exploitable vulnerability and vector for attack.

Web-based E-mail providers

Types	Clients	Sites	Sessions	Failed	*Bytes
Yahoo! Mail	23	33	3243	2	57.95 MB
Google	4	4	1153	0	14.88 MB
Hotmail	14	11	107	0	632.33 KB
AOL-Web-Mail	3	5	25	0	347.03 KB
Totals: 4		53	4,528	2	73.79 MB

Top Web-based E-mail Clients

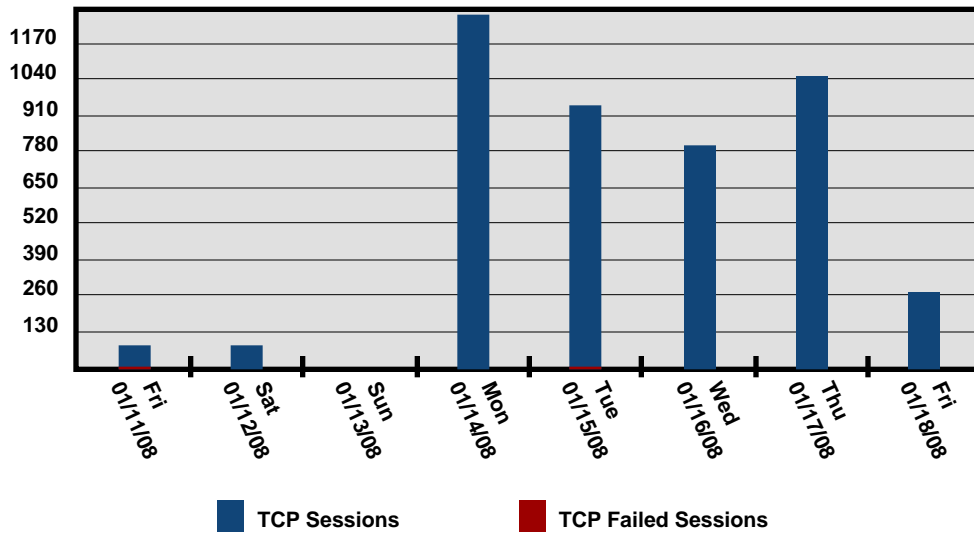
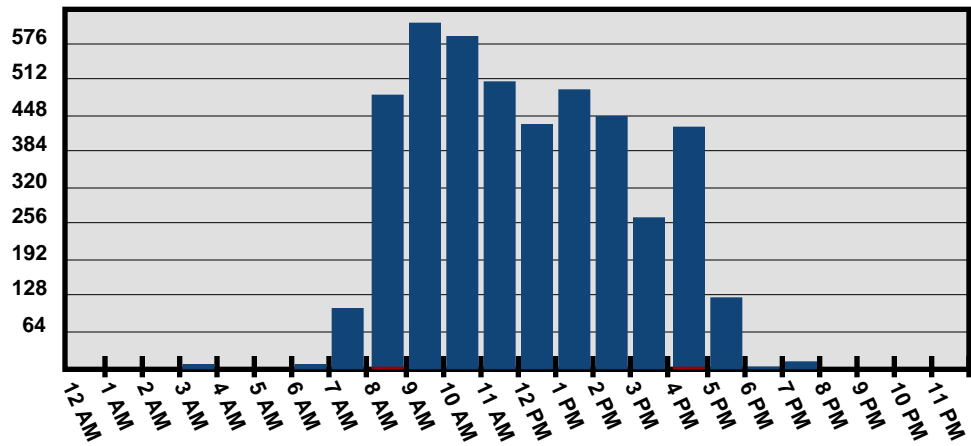
Client	Outbound		*Total	Bytes	
	Sessions	Failed		Inbound	Outbound
192.168.10.101	2154	0	22.23 MB	19.02 MB	3.21 MB
192.168.10.140	267	0	9.75 MB	8.81 MB	962.88 KB
192.168.10.112	629	0	9.06 MB	5.19 MB	3.86 MB
192.168.10.95	220	1	7.50 MB	6.79 MB	732.49 KB
192.168.10.116	162	0	3.59 MB	3.21 MB	392.30 KB
192.168.10.92	191	0	3.35 MB	2.83 MB	532.24 KB
192.168.10.105	134	0	3.00 MB	2.54 MB	466.79 KB
192.168.10.91	80	0	2.65 MB	2.02 MB	641.12 KB
192.168.10.97	91	0	2.30 MB	2.09 MB	211.98 KB
192.168.10.104	73	0	2.03 MB	1.80 MB	235.96 KB
192.168.10.98	120	0	2.02 MB	1.62 MB	406.69 KB
192.168.10.103	62	0	1.24 MB	1.10 MB	144.05 KB
192.168.10.134	68	0	879.77 KB	511.34 KB	368.43 KB
192.168.10.127	56	1	864.23 KB	741.42 KB	122.82 KB
192.168.10.130	57	0	827.97 KB	700.55 KB	127.42 KB
192.168.10.131	34	0	467.03 KB	390.34 KB	76.69 KB
192.168.10.85	21	0	450.19 KB	386.20 KB	64.00 KB
192.168.10.82	33	0	431.44 KB	362.89 KB	68.55 KB
192.168.10.90	21	0	416.73 KB	248.77 KB	167.96 KB
192.168.10.94	6	0	343.16 KB	210.30 KB	132.86 KB
192.168.10.88	15	0	306.31 KB	271.19 KB	35.12 KB
192.168.10.117	16	0	99.42 KB	71.28 KB	28.14 KB
192.168.10.128	5	0	80.01 KB	67.36 KB	12.66 KB
192.168.10.138	2	0	11.91 KB	3.22 KB	8.68 KB
192.168.10.110	7	0	9.00 KB	4.36 KB	4.64 KB
192.168.10.86	1	0	3.63 KB	2.32 KB	1.31 KB
192.168.10.123	1	0	3.36 KB	2.43 KB	954.00 B
192.168.10.83	1	0	1.51 KB	915.00 B	629.00 B
192.168.10.136	1	0	1.19 KB	531.00 B	689.00 B
Sub-total: 29	4,528	2	73.79 MB	60.91 MB	12.88 MB
Percent: 100%	100%	100%	100%	100%	100%
Totals: 29	4,528	2	73.79 MB	60.91 MB	12.88 MB

Top Client requests

Filename	Requests	Method	Status	*Total Bytes	Mime Type Avg. Bytes
Directory Request					html
1511	Get	OK	20.27 MB	13.74 KB	
Directory Request					html
990	Post	OK	9.02 MB	9.33 KB	
login					html
318	Get	OK	5.56 MB	17.90 KB	
launch					html
206	Get	OK	4.27 MB	21.25 KB	
securedownload					octet-stream
2	Get	OK	2.64 MB	1.32 MB	
bind					html
132	Get	OK	2.63 MB	20.44 KB	
securedownload					jpeg
29	Get	OK	1.87 MB	66.17 KB	
Directory Request					javascript
505	Get	OK	1.82 MB	3.69 KB	
securedownload					gif
12	Get	OK	760.48 KB	63.37 KB	
Directory Request					html
1063	Get	Moved Temporarily	731.29 KB	704.46 B	
ShowLetter					html
22	Get	OK	584.72 KB	26.58 KB	
ShowFolder					html
18	Get	OK	359.27 KB	19.96 KB	
ShowLetter					html
110	Get	Moved Temporarily	276.69 KB	2.52 KB	
Directory Request					javascript
58	Post	OK	254.96 KB	4.40 KB	
Directory Request					jpeg
4	Get	OK	234.00 KB	58.50 KB	
Directory Request					plain
13	Get	OK	216.01 KB	16.62 KB	
_us.js					html
51	Get	Not Found	174.46 KB	3.42 KB	
securedownload					msword
3	Get	OK	162.05 KB	54.02 KB	
favicon.ico					x-icon
24	Get	OK	150.33 KB	6.26 KB	
toolbar1.gif					gif
1	Get	OK	144.67 KB	144.67 KB	
launch					html
206	Get	Moved Temporarily	138.45 KB	688.22 B	
Directory Request					html
1	Get	Not Modified	112.23 KB	112.23 KB	
rte.js					x-JavaScript
2	Get	OK	101.18 KB	50.59 KB	

Filename	Requests	Method	Status	*Total Bytes	Mime Type Avg. Bytes
test	41	Get	OK	91.65 KB	html 2.24 KB
RPC.aspx	19	Post	OK	81.16 KB	json 4.27 KB
bundle.js.aspx	2	Get	OK	72.56 KB	javascript 36.28 KB
Directory Request	8	Get	OK	63.98 KB	xml 8.00 KB
fc	11	Get	OK	57.61 KB	html 5.24 KB
Static	20	Get	OK	41.37 KB	html 2.07 KB
Directory Request	12	Post	OK	39.75 KB	xml 3.31 KB
Light.js	5	Get	OK	39.56 KB	x-JavaScript 7.91 KB
Header.js	5	Get	OK	32.95 KB	x-JavaScript 6.59 KB
login	23	Get	Moved Temporarily	31.66 KB	html 1.38 KB
formrpc	7	Get	OK	30.67 KB	xml 4.38 KB
load.html	13	Get	OK	26.63 KB	html 2.05 KB
Sub-total: 5447				52.99 MB	
Percent: 92%				98%	
Total: 5922				54.12 MB	

Access times



■ TCP Sessions ■ TCP Failed Sessions

Web-based IM Services

Web-based Instant Messaging services appear to be the next evolution of IM. Web-based IM offers many of the same user features as software based versions installed on a user's workstation, but utilize a Web browser for sending and receiving text messages and files. Web-based IM clients do not have the same issues as software clients but they are vulnerable to attacks against the browser itself. When users are logged in they are exposed to the IM network. A user's machine can be quickly compromised if the user clicks on a link that contains a browser exploit, an ActiveX control or some other rogue software.

Note: More specific details are included in the standalone Instant Messaging report.

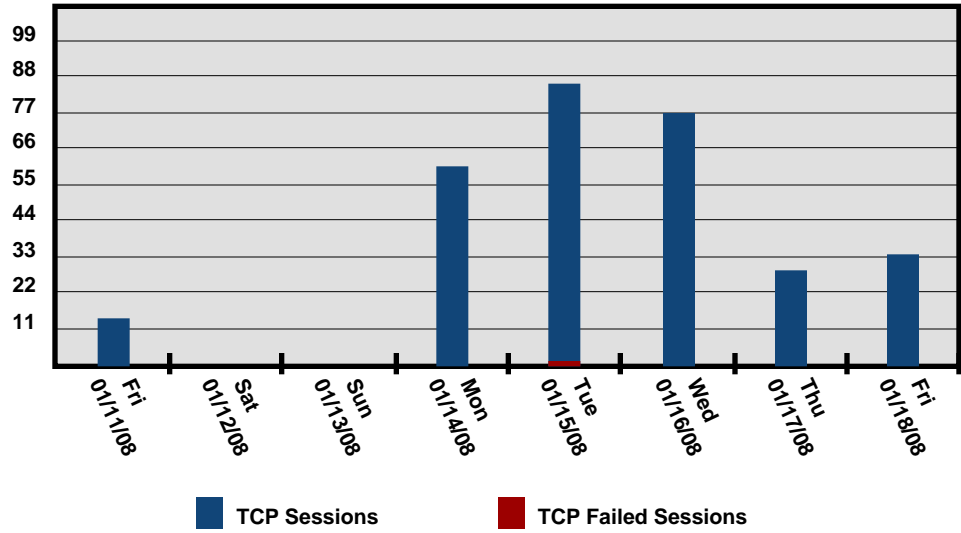
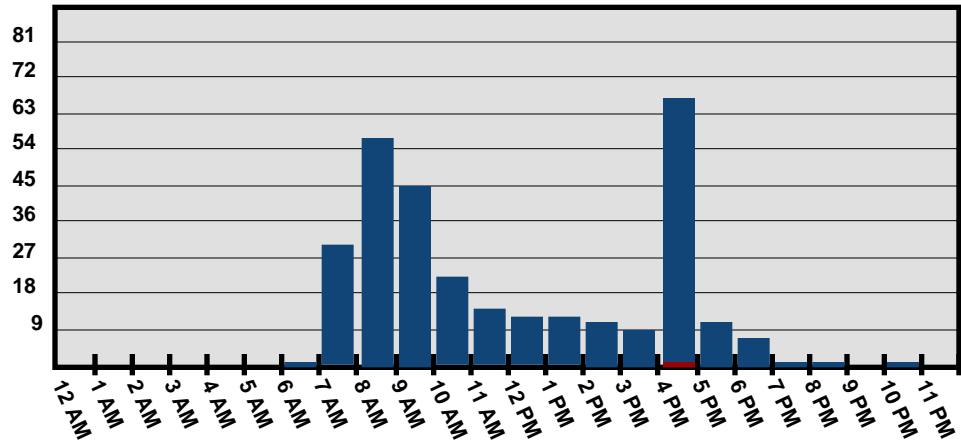
Web-based IM Services

Types	Clients	Sites	Sessions	Failed	*Bytes
Yahoo! Web-based Messenger	10	11	284	1	1.46 MB
MSN Web Messenger	5	2	16	0	425.42 KB
AOL Web-based AIM Express	1	1	1	0	3.93 KB
Totals: 3		14	301	1	1.88 MB

Top Web-based IM Clients

Client	Outbound		*Total	Bytes	
	Sessions	Failed		Inbound	Outbound
192.168.10.95	67	0	372.10 KB	260.57 KB	111.53 KB
192.168.10.98	47	0	342.57 KB	249.43 KB	93.15 KB
192.168.10.94	40	0	241.87 KB	158.64 KB	83.23 KB
192.168.10.91	29	0	203.48 KB	157.73 KB	45.76 KB
192.168.10.117	5	0	189.15 KB	175.15 KB	14.01 KB
192.168.10.97	46	1	184.78 KB	132.70 KB	52.08 KB
192.168.10.140	33	0	145.93 KB	103.94 KB	41.99 KB
192.168.10.85	10	0	81.76 KB	63.40 KB	18.36 KB
192.168.10.123	13	0	77.32 KB	59.73 KB	17.59 KB
192.168.10.128	2	0	39.31 KB	35.63 KB	3.68 KB
192.168.10.86	5	0	34.40 KB	8.02 KB	26.38 KB
192.168.10.101	1	0	8.20 KB	791.00 B	7.42 KB
192.168.10.134	2	0	3.96 KB	2.44 KB	1.51 KB
192.168.10.88	1	0	3.93 KB	1.89 KB	2.04 KB
Sub-total: 14	301	1	1.88 MB	1.38 MB	518.75 KB
Percent: 100%	100%	100%	100%	100%	100%
Totals: 14	301	1	1.88 MB	1.38 MB	518.75 KB

Web-based IM Access times



■ TCP Sessions ■ TCP Failed Sessions