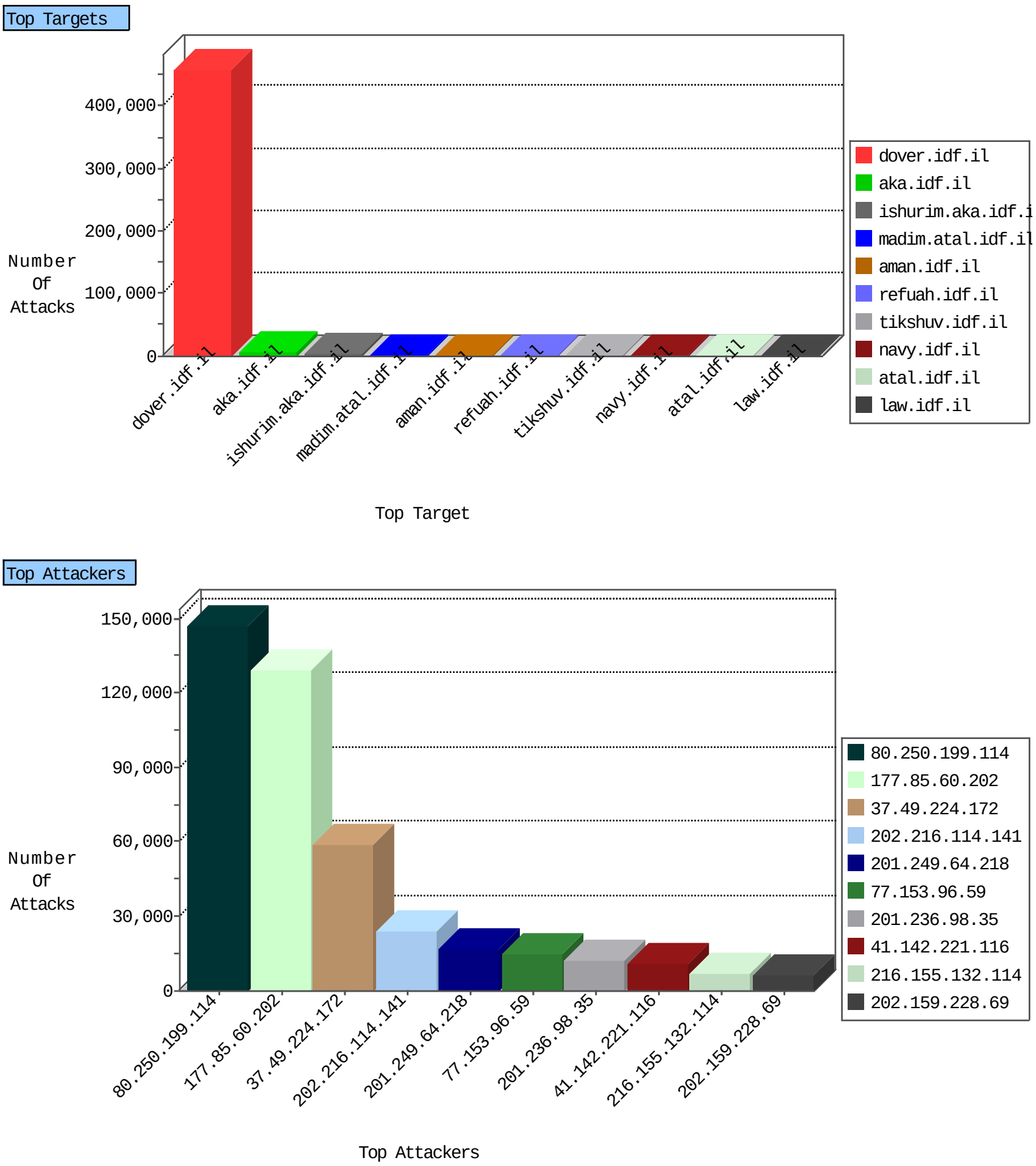
12-30-2014-00:00:08 to 12-31-2014-00:00:08

IDF Under Attack Daily Report



12-30-2014-00:00:08 to 12-31-2014-00:00:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
201.249.64.218	Venezuela	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	16389
201.249.64.218	Venezuela	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Tcp	drop	12705
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	8951
202.216.114.141	Japan	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3673
80.250.199.114	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3672
177.85.60.202	Brazil	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	2582
177.85.60.202	Brazil	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Tcp	drop	2024
202.216.114.141	Japan	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1709
77.153.96.59	France	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	1439
201.236.98.35	Chile	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	1342
216.155.132.114	United States	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	868
202.159.228.69	India	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	820
80.250.199.114	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Tcp	drop	784
77.126.251.251	Israel	147.237.77.233	atal.idf.il	HTTP-POST-Segmented-DoS	dest-reset	707
41.230.219.45	Tunisia	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	611
213.57.137.77	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	543
77.153.96.59	France	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Tcp	drop	539
79.177.151.176	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	516
2.54.29.86	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	499
85.64.210.184	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	495
216.155.132.114	United States	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Tcp	drop	396
201.236.98.35	Chile	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Tcp	drop	375
109.64.12.131	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	310
202.159.228.69	India	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Tcp	drop	309
5.29.117.52	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	250
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	232
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	227
180.182.76.11	Korea, Republic of	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	213
212.117.143.250	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	210
79.181.202.210	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	186
79.181.2.208	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	181
85.65.222.105	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	179
46.117.137.117	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	175
77.127.132.250	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	173
77.125.76.55	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	171
46.116.252.135	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	166
5.29.38.219	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	148
85.65.0.230	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	138
2.54.36.81	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	133
46.120.18.25	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	132
79.177.9.202	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	132
79.178.150.62	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	128
87.68.121.127	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	125
85.65.112.71	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	121
149.78.176.94	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	120
85.64.57.37	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	118
93.172.20.158	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	111
79.179.20.213	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	106
192.116.232.69	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	105
109.66.15.183	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	103

12-30-2014-00:00:08 to 12-31-2014-00:00:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
5.254.97.109	Romania	147.237.77.216	dover.idf.il	12132: HTTP: BOIC DoS Tool	Block	232
192.117.113.18	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	18
109.160.223.175	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	14
91.227.164.5	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	10
212.227.52.97	Germany	147.237.77.74	law.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	10
218.77.79.43	China	147.237.76.177	ncore.idf.il	Block_Level_70_100	Block	10
218.77.79.43	China	147.237.76.86	navy.idf.il	Block_Level_70_100	Block	10
218.77.79.43	China	147.237.76.201	e.atal.idf.il	Block_Level_70_100	Block	9
185.23.124.23	Saudi Arabia	147.237.77.216	dover.idf.il	C023: HTTP: administrator in URI	Permit	9
197.9.134.199	Tunisia	147.237.77.216	dover.idf.il	12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	9
218.77.79.43	China	147.237.76.42	refuah.idf.il	Block_Level_70_100	Block	9
218.77.79.43	China	147.237.76.31	nakchal.idf.il	Block_Level_70_100	Block	9
14.14.145.13	Japan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
218.77.79.43	China	147.237.76.147	chinuch.aka.idf.il	Block_Level_70_100	Block	8
36.79.240.209	Indonesia	147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	Block	8
218.77.79.43	China	147.237.76.148	gqcenter.aka.idf.il	Block_Level_70_100	Block	8
218.77.79.43	China	147.237.76.176	test.ncore.idf.il	Block_Level_70_100	Block	8
218.77.79.43	China	147.237.76.196	e.sviva.idf.il	Block_Level_70_100	Block	8
218.77.79.43	China	147.237.76.38	e.e.meitav.idf.il	Block_Level_70_100	Block	8
218.77.79.43	China	147.237.76.197	e.himush.idf.il	Block_Level_70_100	Block	7
218.77.79.43	China	147.237.76.39	mobile.meitav.idf.il	Block_Level_70_100	Block	7
218.77.79.43	China	147.237.76.202	e.halag.idf.il	Block_Level_70_100	Block	7
109.67.167.137	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
218.77.79.43	China	147.237.76.199	e.nakchal.idf.il	Block_Level_70_100	Block	7
218.77.79.43	China	147.237.76.44	e.refuah.idf.il	Block_Level_70_100	Block	7
109.64.189.45	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
218.77.79.43	China	147.237.76.30	himush.idf.il	Block_Level_70_100	Block	6
192.118.11.124	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
218.77.79.43	China	147.237.76.198	e.yohalan.idf.il	Block_Level_70_100	Block	6
104.143.12.42		147.237.77.216	dover.idf.il	Block_Level_70_100	Block	6
218.77.79.43	China	147.237.76.200	eitan.aka.idf.il	Block_Level_70_100	Block	6
10.0.0.2		147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
109.64.168.61	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
188.120.148.115	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
218.77.79.43	China	147.237.77.216	dover.idf.il	Block_Level_70_100	Block	5
218.77.79.43	China	147.237.77.178	e.matpash.idf.il	Block_Level_70_100	Block	5
212.34.12.154	Jordan	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
66.240.192.138	United States	147.237.77.235	sviva.idf.il	Block_Level_70_100	Block	5
218.77.79.43	China	147.237.76.34	yohalan.idf.il	Block_Level_70_100	Block	5
212.34.12.154	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.167.142	United States	147.237.77.176	matpash.idf.il	Block_Level_70_100	Block	4
71.6.167.142	United States	147.237.72.166	aka.idf.il	Block_Level_70_100	Block	4
71.6.167.142	United States	147.237.0.15	kosher-kravi.idf.il	Block_Level_70_100	Block	4
71.6.135.131	United States	147.237.77.19	law-forum.idf.il	Block_Level_70_100	Block	4
218.77.79.43	China	147.237.8.45	e.eitan.idf.il	Block_Level_70_100	Block	4
71.6.167.142	United States	147.237.77.61	e.cogat.idf.il	Block_Level_70_100	Block	4
71.6.135.131	United States	147.237.76.177	ncore.idf.il	Block_Level_70_100	Block	4
185.5.153.116	Saudi Arabia	147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	Block	4
71.6.135.131	United States	147.237.77.205	prisha.idf.il	Block_Level_70_100	Block	4
84.109.115.97	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4

12-30-2014-00:00:08 to 12-31-2014-00:00:08

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	125
80.74.98.102	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	101
201.249.64.218	Venezuela	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	83
180.182.76.11	Korea, Republic of	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	32
209.66.70.253	United States	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	31
212.227.52.97	Germany	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	30
202.159.228.69	India	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	28
201.236.98.35	Chile	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	28
37.49.224.172	Netherlands	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	17
77.153.96.59	France	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 2 Inbound	11
151.217.171.220		147.237.8.45	e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	6
77.153.96.59	France	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	6
151.217.171.220		147.237.76.42	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
202.216.114.141	Japan	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 2 Inbound	5
151.217.171.220		147.237.76.176	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
151.217.171.220		147.237.77.234	halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
151.217.171.220		147.237.77.216	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
216.155.132.114	United States	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 2 Inbound	4
202.216.114.141	Japan	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	4
185.23.124.23	Saudi Arabia	147.237.77.216	dover.idf.il	SQL Injection - Select From	4
151.217.171.220		147.237.0.35	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
151.217.171.220		147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
61.240.144.64	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	3
151.217.171.220		147.237.0.200	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
61.240.144.67	China	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 1024	3
151.217.171.220		147.237.76.30	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
61.240.144.65	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	3
151.217.171.220		147.237.72.156	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
151.217.171.220		147.237.76.177	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
151.217.171.220		147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
185.23.124.23	Saudi Arabia	147.237.77.216	dover.idf.il	SERVER-WEBAPP admin.php access	3
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	3
151.217.171.220		147.237.76.31	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
151.217.171.220		147.237.77.74	law.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
194.114.146.227	Israel	147.237.72.156	aman.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
151.217.171.220		147.237.72.166	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
151.217.171.220		147.237.72.14	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	3
151.217.171.220		147.237.76.196	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
151.217.171.220		147.237.8.46	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
208.80.155.189	United States	147.237.76.86	navy.idf.il	Tehila - Perl LWP with fake user agent	2
151.217.171.220		147.237.77.243	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
134.191.232.69	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
37.26.147.230	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
151.217.171.220		147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
85.65.28.99	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.183.17.75	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
151.217.171.220		147.237.77.179	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
151.217.171.220		147.237.77.121	e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
193.34.56.101	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2

12-30-2014-00:00:08 to 12-31-2014-00:00:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
80.250.199.114	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	SAM rule	drop	drop	137166
177.85.60.202	Brazil	147.237.77.216	dover.idf.il	SAM rule	drop	drop	108565
37.49.224.172	Netherlands	147.237.77.216	dover.idf.il	SAM rule	drop	drop	53179
177.85.60.202	Brazil	147.237.77.216	dover.idf.il		drop	drop	20903
202.216.114.141	Japan	147.237.77.216	dover.idf.il	SAM rule	drop	drop	17173
201.249.64.218	Venezuela	147.237.77.216	dover.idf.il	SAM rule	drop	drop	15181
77.153.96.59	France	147.237.77.216	dover.idf.il	SAM rule	drop	drop	12546
201.236.98.35	Chile	147.237.77.216	dover.idf.il	SAM rule	drop	drop	12049
41.142.221.116	Morocco	147.237.77.216	dover.idf.il		drop	drop	11074
216.155.132.114	United States	147.237.77.216	dover.idf.il	SAM rule	drop	drop	6679
181.136.93.211	Colombia	147.237.77.216	dover.idf.il	SAM rule	drop	drop	5998
202.216.114.141	Japan	147.237.77.216	dover.idf.il		drop	drop	5971
202.159.228.69	India	147.237.77.216	dover.idf.il	SAM rule	drop	drop	5514
37.49.224.172	Netherlands	147.237.77.216	dover.idf.il		drop	drop	5377
80.250.199.114	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3834
80.250.199.114	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence		3816
180.182.76.11	Korea, Republic of	147.237.77.216	dover.idf.il	SAM rule	drop	drop	3284
41.143.5.36	Morocco	147.237.77.216	dover.idf.il		drop	drop	3124
77.153.96.59	France	147.237.77.216	dover.idf.il		drop	drop	1798
41.33.231.86	Egypt	147.237.77.216	dover.idf.il		drop	drop	1420
41.230.219.45	Tunisia	147.237.77.216	dover.idf.il		drop	drop	1264
80.250.199.114	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	1062
213.43.169.189	Turkey	147.237.77.216	dover.idf.il		drop	drop	472
41.33.232.65	Egypt	147.237.77.216	dover.idf.il		drop	drop	435
37.98.218.250	Poland	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	431
176.31.152.147	France	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	419
80.250.199.114	Iran, Islamic Republic of	147.237.77.216	dover.idf.il		drop	drop	411
202.159.228.69	India	147.237.77.216	dover.idf.il		drop	drop	410
37.98.218.250	Poland	147.237.77.216	dover.idf.il	SAM rule	drop	drop	409
104.216.126.162		147.237.77.216	dover.idf.il	SAM rule	drop	drop	360
216.155.132.114	United States	147.237.77.216	dover.idf.il		drop	drop	255
105.102.25.255	Algeria	147.237.77.216	dover.idf.il		drop	drop	246
201.249.64.218	Venezuela	147.237.77.216	dover.idf.il		drop	drop	231
84.17.226.69	Russian Federation	147.237.77.216	dover.idf.il	SAM rule	drop	drop	198
168.235.195.18		147.237.72.166	aka.idf.il		drop	drop	190
104.216.126.162		147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	153
201.249.64.218	Venezuela	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	105
104.131.93.139		147.237.72.166	aka.idf.il	SAM rule	drop	drop	98
84.17.226.69	Russian Federation	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	86
84.17.226.69	Russian Federation	147.237.77.216	dover.idf.il	illegal header format detected: Malformed HTTP format in request	Block HTTP Non Compliant	monitor	83
105.102.25.255	Algeria	147.237.77.216	dover.idf.il	SAM rule	drop	drop	81
104.216.126.162		147.237.77.216	dover.idf.il	illegal header format detected: Malformed HTTP format in request	Block HTTP Non Compliant	monitor	81
62.219.195.152	Israel	147.237.72.167	ishurim.aka.idf.i		drop	drop	78
104.216.126.162		147.237.77.216	dover.idf.il	illegal header format detected: Invalid HTTP End Of Line in request	Block HTTP Non Compliant	monitor	77
95.86.74.219	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	76
41.42.178.137	Egypt	147.237.77.216	dover.idf.il		drop	drop	74
104.216.126.162		147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	73
46.19.86.100	Israel	147.237.72.166	aka.idf.il	SAM rule	drop	drop	71
31.168.197.215	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	67
41.42.156.213	Egypt	147.237.77.216	dover.idf.il		drop	drop	66

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
185.23.124.23	Saudi Arabia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 185.23.124.23	Block	1628
105.102.25.255	Algeria	147.237.77.216	dover.idf.il	Multiple Malformed URL from 105.102.25.255	Block	407
109.253.132.99	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	244
77.109.139.27	Switzerland	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 77.109.139.27	Block	214
105.102.25.255	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	213
46.19.86.209	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	191
82.102.141.221	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 82.102.141.221	Block	179
185.32.177.180	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 185.32.177.180	Block	157
84.17.226.69	Russian Federation	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Method	Block	151
176.12.156.175	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	140
46.19.86.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	131
104.216.126.162		147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Method	Block	129
109.253.134.38	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	125
84.17.226.69	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	121
207.241.226.120	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	120
80.246.141.1	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	115
80.246.138.114	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	111
84.17.226.69	Russian Federation	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	110
84.17.226.69	Russian Federation	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	108
104.216.126.162		147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	100
104.216.126.162		147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	93
104.216.126.162		147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	83
84.17.226.69	Russian Federation	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Header Name	Block	77
176.228.43.89	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	75
84.17.226.69	Russian Federation	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	70
104.216.126.162		147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Header Name	Block	63
162.248.48.39	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/994-8613-he/navy.aspx.aspx	Block	62
104.216.126.162		147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	61
46.19.86.209	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.209	Block	57
149.78.251.11	United States	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 149.78.251.11	Block	56
37.77.55.87	Iraq	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	55
46.19.86.154	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.154	Block	54
37.77.55.87	Iraq	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 37.77.55.87	Block	54
80.246.138.26	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	53
84.17.226.69	Russian Federation	147.237.77.216	dover.idf.il	Distributed Abnormally Long Header Line	Block	43
84.228.173.141	Israel	147.237.72.166	aka.idf.il	Multiple Double URL Encoding from 84.228.173.141	Block	41
80.246.141.144	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	39
84.17.226.69	Russian Federation	147.237.77.216	dover.idf.il	Distributed Malformed HTTP Header Line	Block	38
84.17.226.69	Russian Federation	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Header Value	Block	38
46.19.86.154	Israel	147.237.77.233	atal.idf.il	Distributed Suspicious Response Code	Block	37
104.216.126.162		147.237.77.216	dover.idf.il	Distributed Abnormally Long Header Line	Block	37
185.23.124.23	Saudi Arabia	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 185.23.124.23	Block	36
104.216.126.162		147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Header Value	Block	36
82.102.141.201	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	35
104.216.126.162		147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	34
84.17.226.69	Russian Federation	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	34
31.168.197.215	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	32
104.216.126.162		147.237.77.216	dover.idf.il	Distributed Malformed HTTP Header Line	Block	32
37.98.218.250	Poland	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Method	Block	28
185.23.124.23	Saudi Arabia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	27

12-30-2014-00:00:08 to 12-31-2014-00:00:08