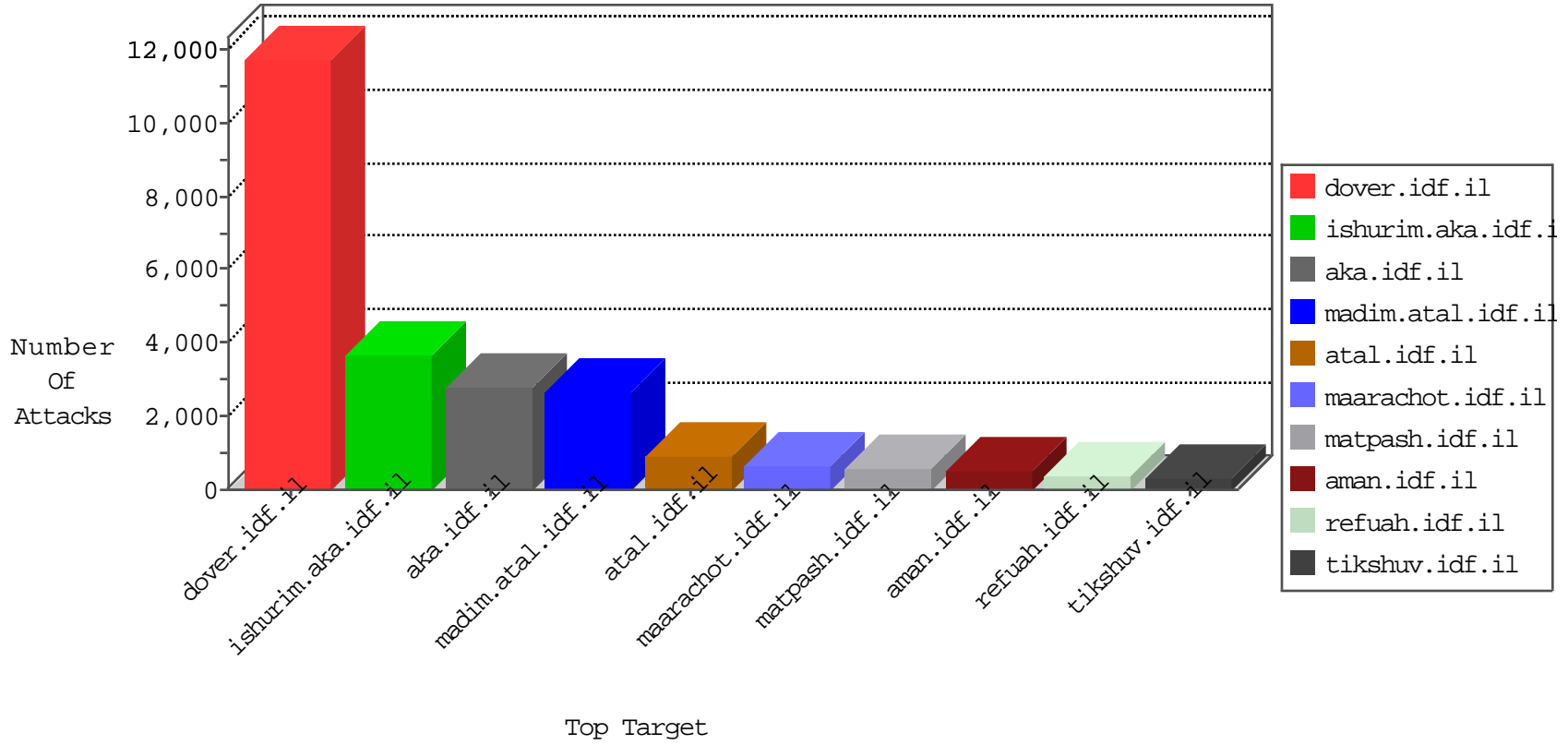


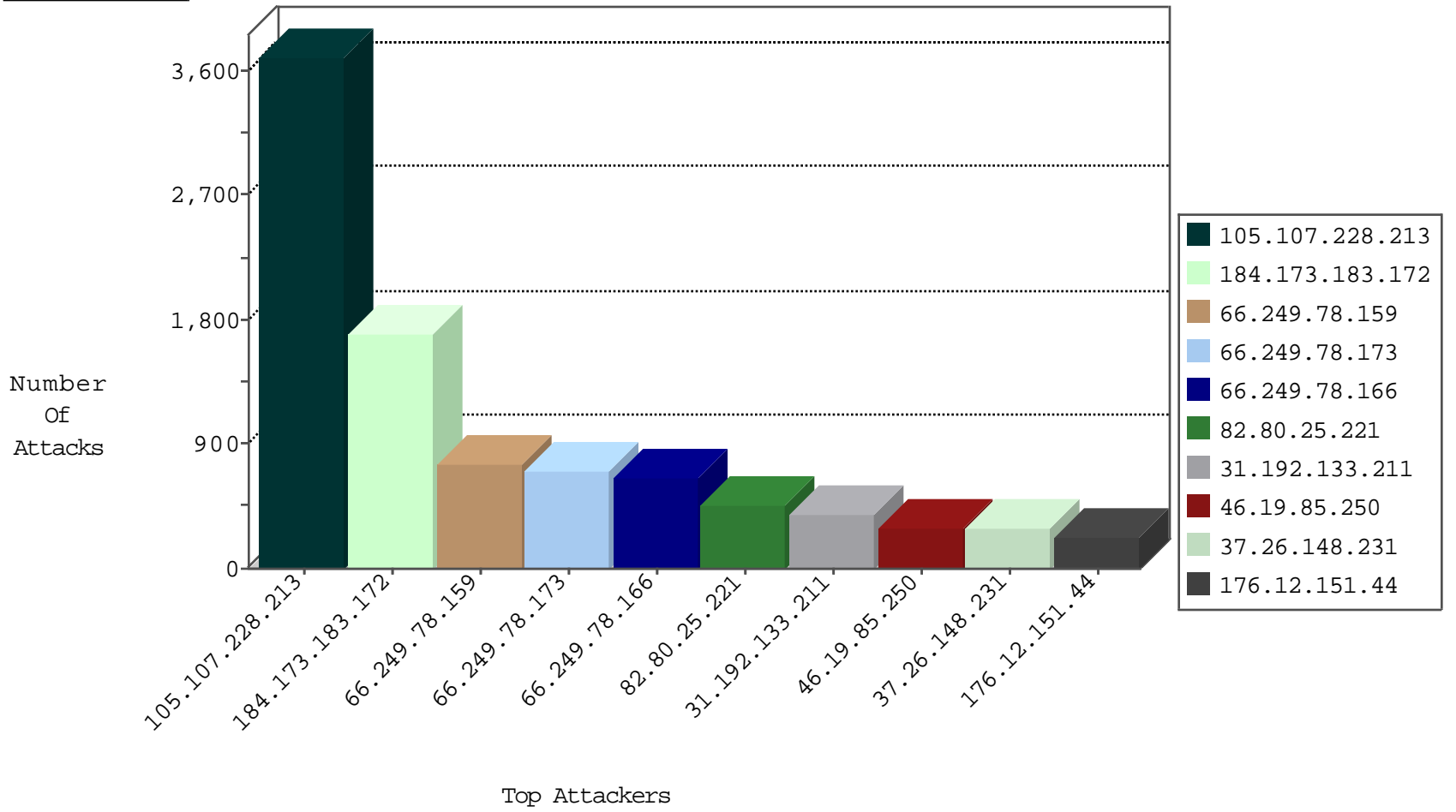
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
31.192.133.211	Russian Federation	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	45457
105.107.228.213	Algeria	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	15361
66.249.64.132	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	10252
89.138.55.202	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	1390
66.249.78.96	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	894
89.139.185.111	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	838
109.67.31.238	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	565
192.116.142.154	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	510
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	439
79.180.58.16	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	417
79.179.71.129	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	362
83.130.100.142	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	318
185.13.193.57	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	314
84.94.200.130	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	266
212.143.44.5	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	218
5.29.166.144	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	183
149.78.137.28	United States	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	175
109.66.120.46	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	175
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	168
84.110.8.75	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	157
213.8.71.26	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	154
85.64.79.159	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	151
212.179.239.194	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	132
46.19.85.48	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	120
2.54.44.149	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	118
87.69.165.138	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	115
79.180.169.89	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	110
80.246.136.214	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	109
85.64.52.203	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	108
79.182.101.92	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	108
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	100
149.78.204.93	United States	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	93
2.54.63.92	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	92
87.69.72.227	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
217.132.93.191	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	89
79.183.10.233	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85
109.253.134.56	Israel	147.237.72.156	aman.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	83
84.94.47.94	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	80
109.67.61.191	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	80
149.78.137.28	United States	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	79
109.66.138.246	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	78
2.52.151.35	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	77
2.52.150.174	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	77
2.52.181.217	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	75
2.52.51.107	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	73
109.253.159.7	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	73
82.80.216.12	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	67
37.26.146.190	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	63
109.253.132.216	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	61
46.19.85.189	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	61

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.233	atal.idf.il	DVRep_P-N_40-59	Permit	665
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	562
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	388
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	169
216.170.126.185		147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	148
180.76.5.193	China	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	88
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	87
85.250.180.53	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	52
81.218.251.252	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
71.6.135.131	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	6
80.179.122.253	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
81.218.251.250	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
71.6.135.131	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	5
85.25.43.94	Germany	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	5
85.25.43.94	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	5
85.25.43.94	Germany	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	5
198.20.70.114	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	5
31.44.131.122	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
77.125.151.190	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
46.19.85.139	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
79.181.146.121	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.135.131	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	5
109.65.185.170	Israel	147.237.76.30	himush.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
84.108.161.155	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
85.25.43.94	Germany	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	4
46.19.85.154	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
62.90.235.246	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
46.19.85.157	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
213.57.108.165	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
198.20.70.114	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	4
85.25.43.94	Germany	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	4
85.25.43.94	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.76.198	e.ychalan.idf.il	DVRep_B-N_60_100	Block	4
37.142.254.97	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
197.37.187.45	Egypt	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
213.8.97.70	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
71.6.135.131	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	4
85.25.43.94	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	3
89.98.85.13	Netherlands	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
71.6.135.131	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	3
46.19.85.242	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
93.172.143.237	Israel	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	3
71.6.135.131	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	3
85.25.43.94	Germany	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	3
71.6.135.131	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	3
85.25.43.94	Germany	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	3
71.6.135.131	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	3
85.25.43.94	Germany	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	3
71.6.135.131	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	3

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	363
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	135
111.90.149.91	Malaysia	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	11
46.19.85.42	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	9
31.11.74.195	Macedonia, the Former Yugoslav Republic of	147.237.72.166	aka.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	7
82.145.216.138	Europe	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	3
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
207.241.237.166	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	3
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	3
122.228.207.193	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	3
122.228.207.193	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
46.120.38.35	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
77.125.94.2	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
62.48.49.78	Italy	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	2
37.26.147.204	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
2.54.139.218	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
213.57.165.12	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
186.120.99.242	Dominican Republic	147.237.0.33	idf.il	ET SCAN NMAP -sS window 2048	2
122.228.207.193	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
79.180.39.112	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
37.26.147.138	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.179.61.126	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
58.20.54.249	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
85.64.228.145	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
58.20.54.249	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
122.228.207.193	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
85.64.94.191	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.193	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	2
115.231.218.23	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	2
84.109.10.137	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.253.142.183	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
188.165.214.208	France	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
122.228.207.193	China	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	2
46.121.101.194	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.160.225.131	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
58.20.54.249	China	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	2
109.66.4.176	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
62.90.235.246	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.193	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	2
46.120.2.204	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
186.120.99.242	Dominican Republic	147.237.0.33	idf.il	ET SCAN NMAP -sS window 3072	2
79.180.217.254	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.19.86.140	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
2.52.56.116	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.180.20.203	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
186.120.99.242	Dominican Republic	147.237.0.33	idf.il	ET SCAN NMAP -f -sS	2
89.248.162.228	Netherlands	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	2
122.228.207.193	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	2
79.177.32.109	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
176.12.137.242	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	360
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	306
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	304
207.241.237.166	United States	147.237.77.216	dover.idf.il	Web Servers Slow HTTP Denial of Service	Web Server Enforcement Violation	reject	184
90.16.143.238	France	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	160
66.249.81.218	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	80
109.242.209.163	Greece	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	78
194.255.185.50	Denmark	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	70
91.140.122.39	Greece	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	69
79.182.199.24	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	67
85.250.223.187	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	66
83.249.134.4	Sweden	147.237.77.170	maarachot.idf.il	First packet isn't SYN	drop	drop	66
190.107.176.148	Chile	147.237.77.216	dover.idf.il	TCP segment out of maximum allowed sequence. Packet dropped.	Streaming Engine: TCP Segment Limit Enforcement	drop	59
176.12.144.77	Israel	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	58
132.74.58.77	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	57
212.179.74.238	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	51
132.64.182.76	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	49
46.146.8.110	Russian Federation	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
176.12.140.51	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
66.249.78.44	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	46
176.12.138.109	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
108.27.92.243	United States	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	39
87.68.228.183	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	39
192.114.23.211	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
109.253.132.116	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
213.244.82.139	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	36
66.249.81.215	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
176.12.147.19	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
82.80.51.74	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	35
66.249.78.51	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
176.12.150.30	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
66.249.81.212	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
199.30.24.186	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
79.176.50.55	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	29
189.27.160.25	Brazil	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
109.253.146.17	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
66.249.64.150	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
109.253.135.94	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
195.110.40.7	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
212.25.102.57	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	25
79.177.152.193	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	25
109.253.141.18	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.253.141.123	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.253.139.252	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
157.55.39.119	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
79.176.202.109	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.253.156.19	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
84.94.114.92	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	23

03-01-2015-00:00:02 to 03-02-2015-00:00:02

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
192.118.27.253	Israel	147.237.72.167	ishurim.aka.idf.i	First packet isn't SYN	drop	drop	23

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.173	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	386
66.249.78.159	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	377
66.249.78.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	341
37.26.148.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	274
46.19.85.250	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.250	Block	244
176.12.151.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	222
2.52.151.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	219
46.19.85.242	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.242	Block	203
109.253.128.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	172
46.120.182.229	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.120.182.229	Block	170
176.12.141.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	126
82.102.141.248	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 82.102.141.248	Block	108
2.54.40.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	98
46.19.85.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	97
109.64.142.184	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 109.64.142.184	Block	78
185.32.179.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	77
37.142.221.241	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	72
66.249.64.142	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.142	Block	69
2.54.21.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	64
185.32.178.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	61
46.19.85.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	60
176.12.146.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	49
176.12.137.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	47
2.54.132.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	46
46.19.85.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	44
80.246.137.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	44
81.144.138.34	United Kingdom	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 81.144.138.34	Block	43
66.249.64.150	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.150	Block	41
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	40
2.54.164.231	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.164.231	Block	38
80.246.141.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	35
85.64.182.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	31
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	21
46.229.164.115	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.229.164.115	Block	18
46.229.164.114	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.229.164.114	Block	18
37.26.146.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	17
62.48.49.78	Italy	147.237.77.74	law.idf.il	Multiple Illegal Byte Code Character in Method from 62.48.49.78	Block	17
109.66.56.8	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.66.56.8	Block	16
46.120.80.151	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.120.80.151	Block	16
62.48.49.78	Italy	147.237.77.74	law.idf.il	Multiple NULL Character in Method from 62.48.49.78	Block	16
46.19.86.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15
195.160.240.11	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	15
81.218.251.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	14
176.12.147.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	12
37.142.98.104	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	12
178.214.73.197	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	11
66.96.183.45	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Method	Block	11
46.229.164.111	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.229.164.111	Block	11
176.12.151.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	10
93.172.70.97	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	None	10