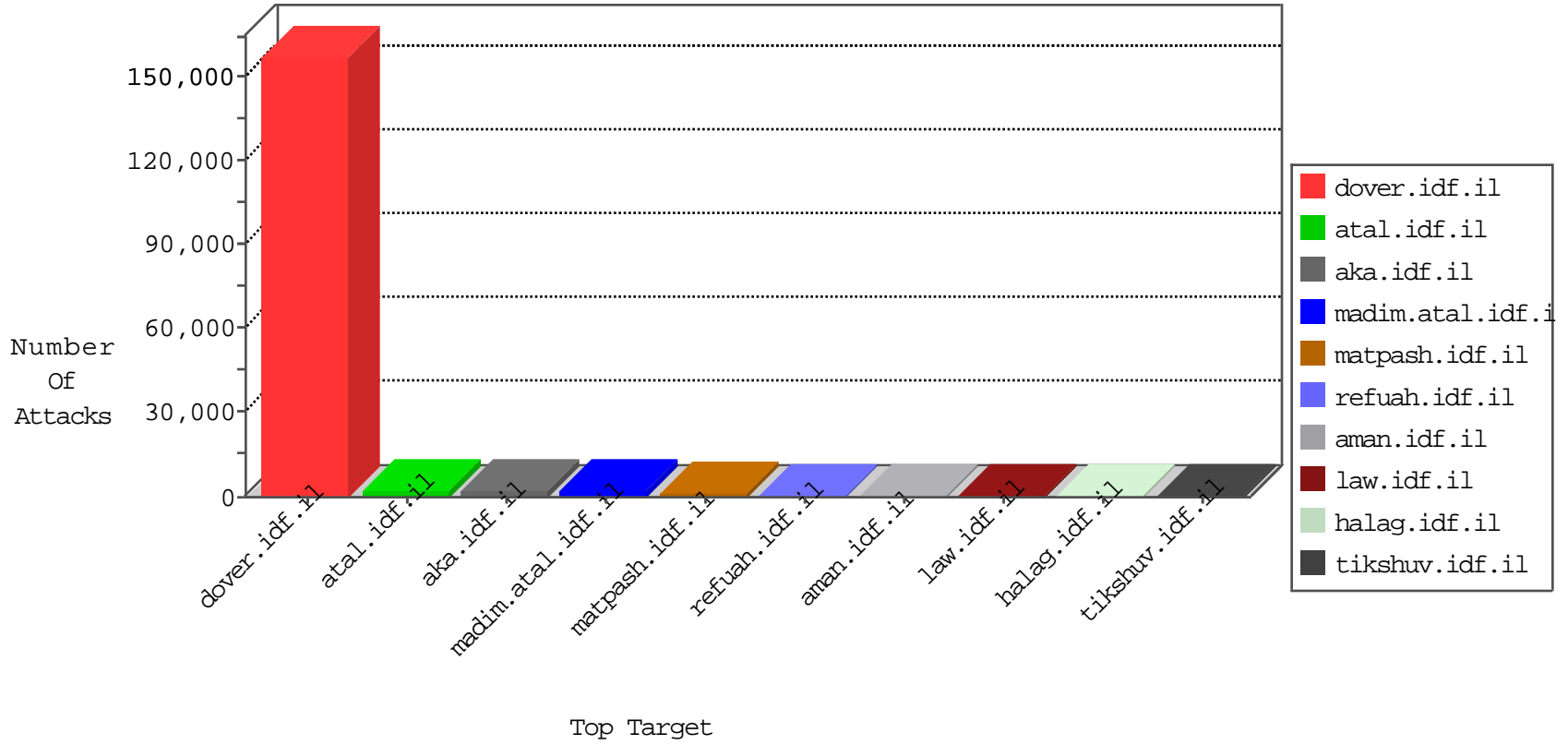


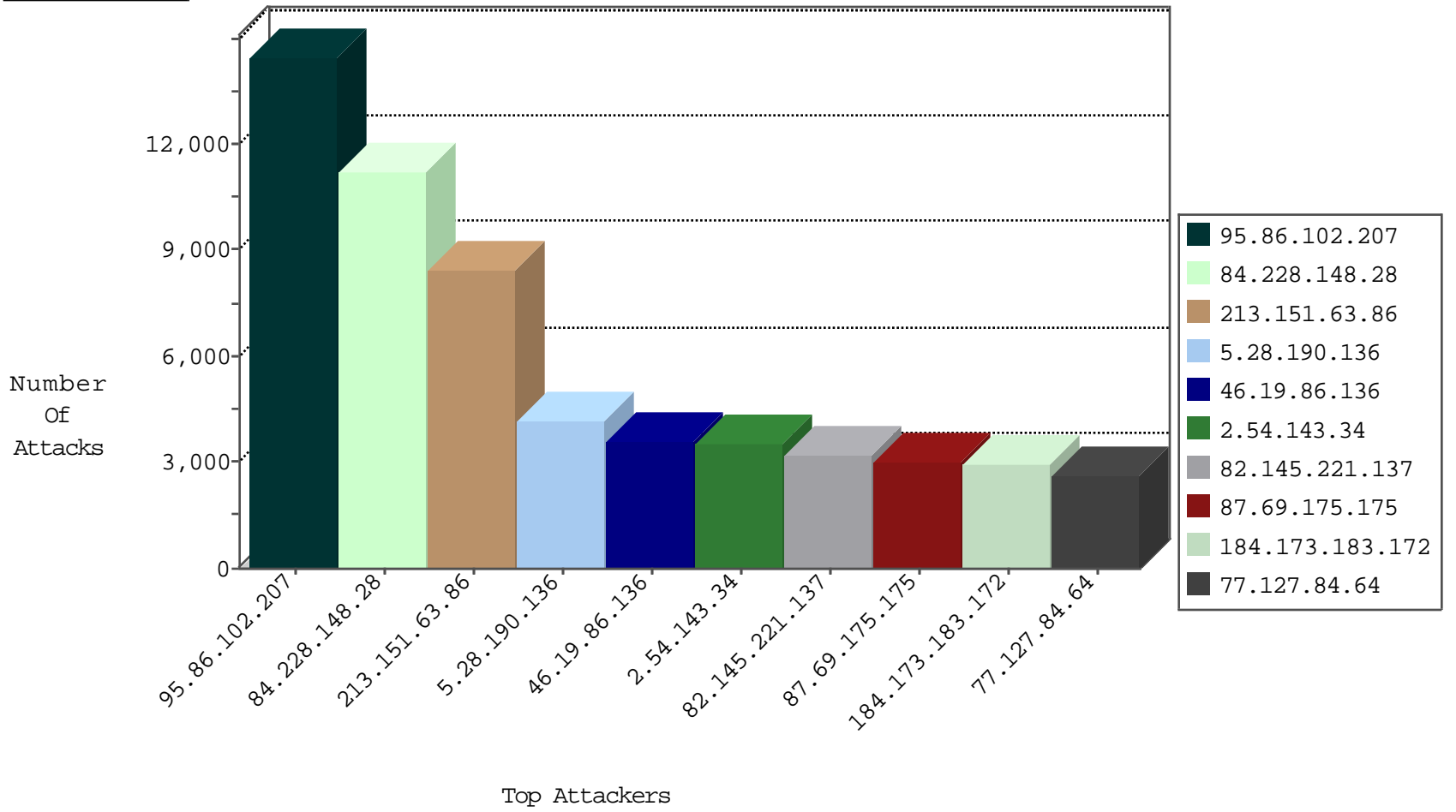
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
37.26.147.213	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5801
66.249.67.24	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	4727
66.249.67.32	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	4356
66.249.67.31	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3661
220.181.108.187	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	3522
220.181.108.101	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	3071
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	2745
2.52.172.178	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2552
66.249.67.40	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1151
66.249.67.23	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	997
84.110.86.111	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	581
66.249.93.160	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	573
220.181.108.168	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	573
84.111.5.40	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	450
37.60.40.149	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	386
94.159.236.166	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	377
79.179.139.123	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	368
66.249.78.166	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	345
85.65.0.225	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	315
77.125.74.8	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	313
149.78.31.147	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	287
84.228.148.28	Israel	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	266
84.110.60.59	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	258
79.183.126.221	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	244
5.29.38.219	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	232
220.181.108.142	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	205
82.145.221.137	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	201
79.182.196.48	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	172
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	170
89.139.11.174	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	169
5.29.163.91	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	169
2.54.60.19	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	146
87.68.151.205	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	145
149.78.6.214	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	144
31.210.187.193	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	118
46.116.154.43	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	117
77.127.203.21	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	113
93.173.233.64	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	112
80.246.140.246	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	88
46.120.169.21	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	87
79.179.107.228	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	86
84.228.121.162	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	85
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85
176.12.137.49	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	80
213.57.144.41	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76
85.250.203.37	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76
95.86.100.172	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	75
84.228.86.155	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
84.228.58.171	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
2.54.137.150	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69

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	2220
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	499
184.173.183.172	United States	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	236
180.76.5.193	China	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	109
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	87
180.76.5.193	China	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	52
90.61.124.227	France	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	22
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	20
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	20
182.114.223.61	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	12
188.138.9.50	Germany	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	11
188.138.9.50	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	9
79.181.198.139	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
85.25.103.50	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	7
37.48.74.42	Netherlands	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	6
205.134.224.235	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	6
71.6.165.200	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	5
176.228.158.5	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.165.200	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	5
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	5
66.240.192.138	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	5
198.20.69.98	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	5
79.176.30.122	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
188.138.9.50	Germany	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	5
188.138.9.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	5
188.138.9.50	Germany	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	5
188.138.9.50	Germany	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	5
93.172.180.143	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
188.138.9.50	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	4
188.138.9.50	Germany	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	4
198.20.70.114	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	4
198.20.70.114	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	4
85.25.103.50	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	4
109.186.132.136	Israel	147.237.77.234	halag.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.167.142	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	4
198.20.69.98	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	4
198.20.70.114	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	4
46.19.85.163	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
188.138.9.50	Germany	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	4
198.20.69.98	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	4
84.110.2.197	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
85.25.103.50	Germany	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	4

Top Attackers In ID

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	287
66.249.65.26	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	184
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	139
66.249.67.40	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	24
66.249.78.204	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	18
66.249.78.197	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	14
66.249.67.24	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	14
66.249.78.190	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	14
79.178.119.159	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	13
66.249.67.32	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	10
66.249.65.28	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	8
66.249.65.30	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	8
66.249.73.211	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	6
66.249.67.81	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	6
66.249.67.31	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
66.249.78.166	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	4
66.249.73.203	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
60.208.72.139	China	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
84.108.76.174	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
61.240.144.67	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	3
221.235.188.210	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	3
5.101.156.43	Russian Federation	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
221.235.188.210	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	3
221.235.188.210	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	3
221.235.188.212	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	2
109.160.243.192	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
157.55.39.131	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.76	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	2
109.64.195.38	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.81.201	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
80.179.122.171	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.67.23	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.64	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	2
221.235.188.210	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
221.235.188.210	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	2
221.235.188.210	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.173	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.10	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
82.145.223.132	Europe	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
85.65.1.78	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.64.66	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
221.235.188.210	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	2
46.120.249.199	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
77.125.114.24	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.64.59	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.89	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
84.110.60.59	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.188.212	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
66.249.67.73	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
221.235.188.212	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	2

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
95.86.102.207	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14486
84.228.148.28	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10994
213.151.63.86	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8442
5.28.190.136	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4189
46.19.86.136	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3624
2.54.143.34	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3532
82.145.221.137	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3192
87.69.175.175	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3018
77.127.84.64	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2647
109.186.164.29	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2572
46.19.85.135	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2011
82.145.223.139	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1900
2.54.22.168	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1766
84.229.192.93	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1743
77.127.23.37	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1735
95.86.100.172	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1674
37.26.147.231	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1672
82.145.221.65	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1553
85.250.132.137	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1541
2.54.173.120	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1428
176.106.41.71	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1239
37.26.147.170	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1000
149.78.109.111	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	983
89.139.184.234	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	839
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	820
37.26.147.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	816
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	775
109.64.146.66	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	727
80.178.169.168	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	722
77.125.1.71	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	691
82.145.223.132	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	600
5.29.198.130	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	563
46.120.158.141	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	531
84.108.14.49	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	529
2.54.39.123	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	493
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	468
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	465
212.76.121.115	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	463
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	448
2.54.141.172	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	427
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	422
82.145.222.239	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	410
2.54.37.225	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	387
46.19.86.48	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	374
82.205.66.168	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	373
84.108.235.42	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	373
79.183.56.108	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	356
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	354
92.221.5.216	Norway	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	349
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	338

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
77.125.13.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	536
77.126.17.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	514
2.54.175.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	360
46.117.43.149	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.117.43.149	Block	136
109.253.129.198	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.129.198	Block	107
84.110.1.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	73
84.111.102.95	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 84.111.102.95	Block	72
176.12.149.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	69
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	63
176.12.138.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	51
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	46
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	44
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	41
207.46.13.104	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	17
66.249.73.211	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	17
157.55.39.130	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	16
77.126.7.253	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 77.126.7.253	Block	16
125.65.46.140	China	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 125.65.46.140	Block	15
157.55.39.178	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	11
66.249.73.219	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	11
188.120.148.244	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	11
66.249.73.203	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	11
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	10
77.127.250.212	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	10
176.12.141.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	10
93.173.133.83	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/login.aspx?xjx\$ xžx™x"xç x?x™x@x™n.aspx	Block	9
192.99.39.235	Canada	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
93.173.181.161	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	7
77.127.95.191	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
176.12.151.51	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.151.51	Block	7
66.249.64.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
149.78.105.4	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	7
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
2.52.33.99	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	7
136.243.36.88	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 136.243.36.88	Block	6
176.12.150.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
95.86.98.253	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
5.28.169.235	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 5.28.169.235	Block	6
207.46.13.104	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.104	Block	6
37.142.32.180	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
157.55.39.5	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
85.65.32.247	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
66.249.64.63	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
5.29.238.254	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	5
37.142.183.19	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.142.183.19	Block	5
134.249.53.8	Ukraine	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/901-11442-en/	Block	5
207.46.13.104	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.104	Block	5
66.249.78.87	Israel	147.237.0.17	m.ny-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	5
79.178.133.232	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	5
66.249.64.63	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.63	Block	5