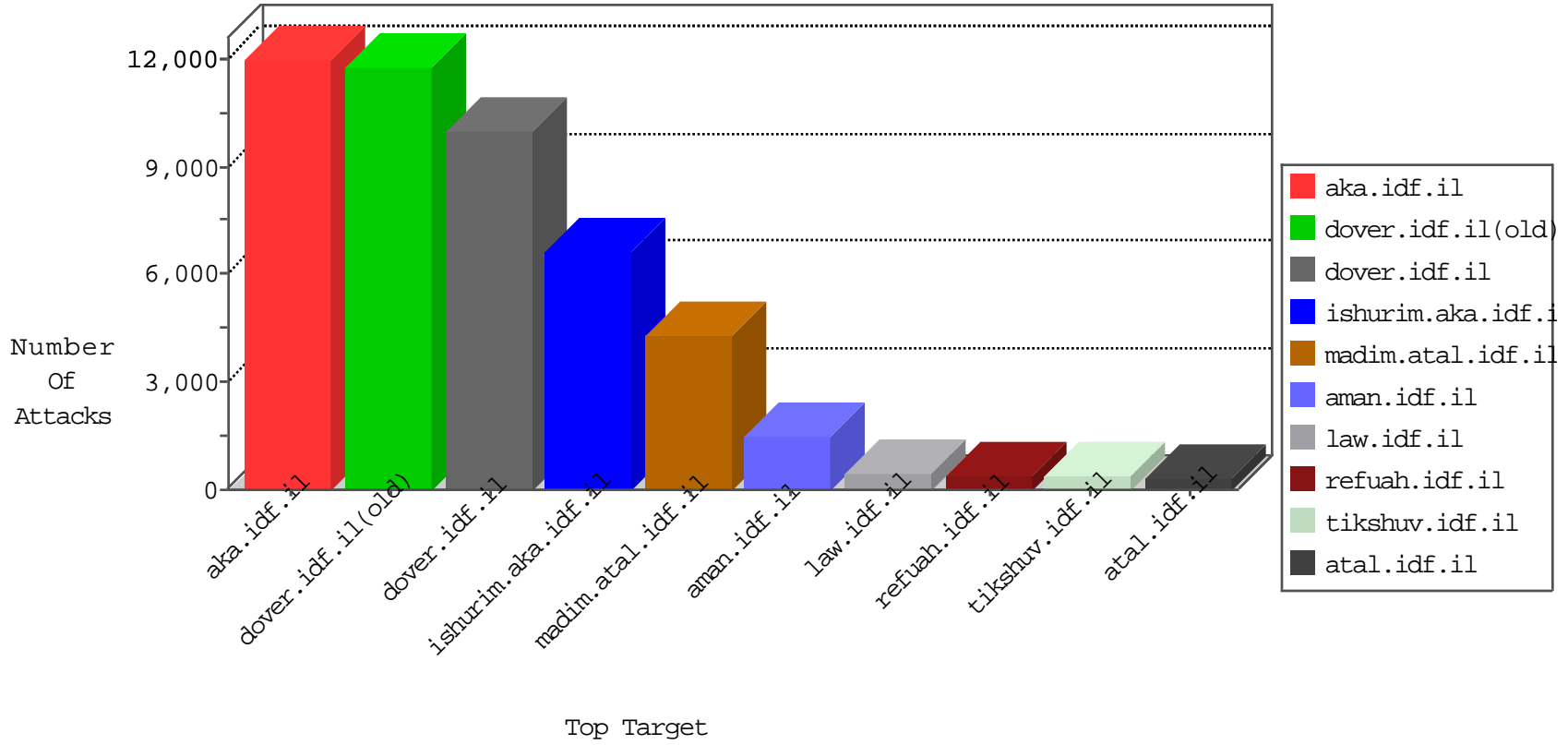


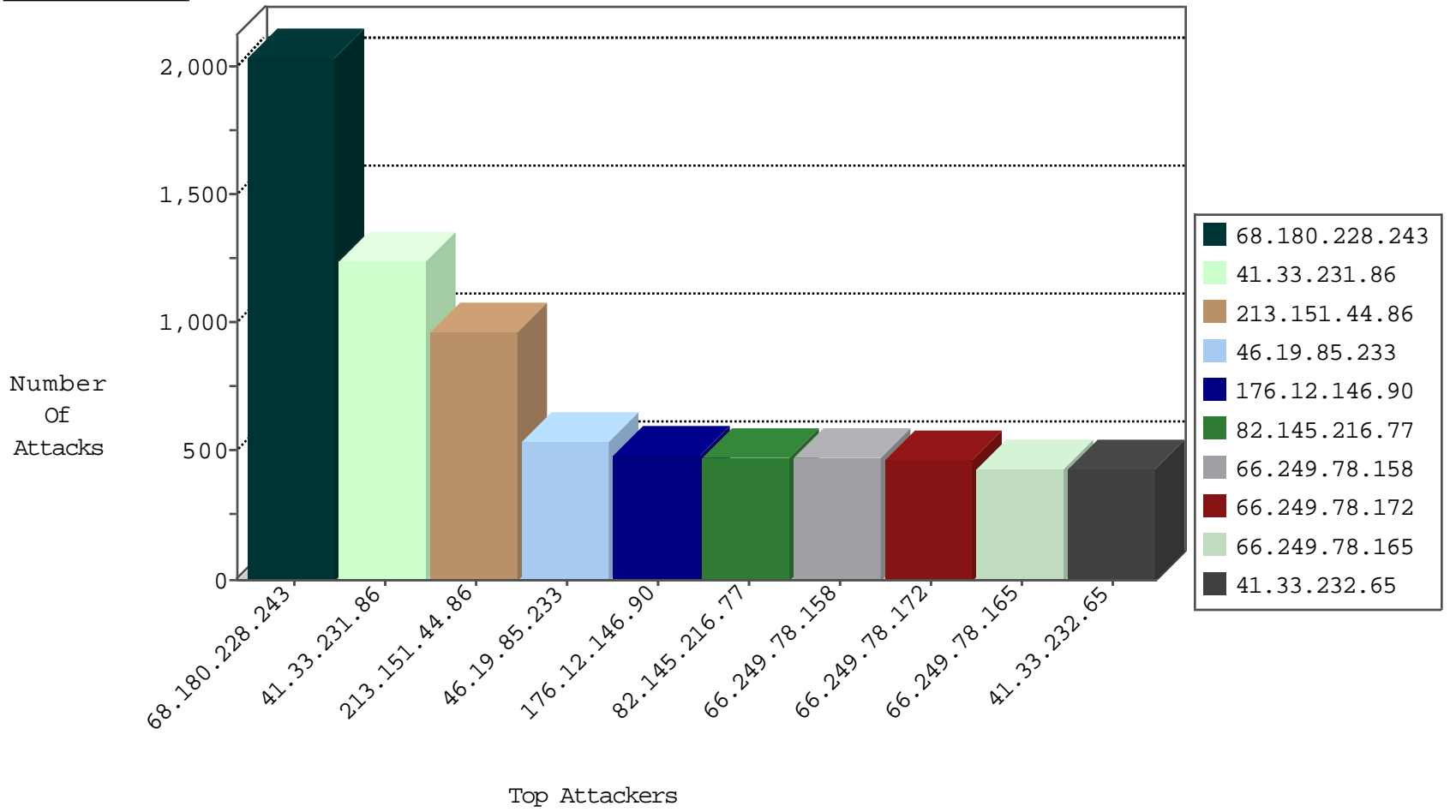
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.78.92	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	6281
66.249.78.103	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3339
66.249.78.59	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	3156
66.249.78.159	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	804
71.160.73.154	United States	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	547
192.116.232.69	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	drop	130
5.29.38.219	Israel	147.237.72.156	aman.idf.il	Anomaly-SSL-renegotiation-Cli	drop	127
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	111
132.64.67.11	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	drop	77
82.102.141.221	Israel	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	63
82.102.141.201	Israel	147.237.0.19	medim.atal.idf.il	Invalid TCP Flags	drop	39
82.102.141.211	Israel	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	35
82.102.141.197	Israel	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	26
82.102.141.194	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	21
82.102.141.216	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	18
82.102.141.193	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	16
82.102.141.217	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	14
82.102.141.209	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	14
82.145.218.82	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	14
82.102.141.200	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	13
114.79.1.126	Indonesia	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	12
82.102.141.255	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	10
82.102.141.212	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	9
125.64.35.67	China	147.237.0.34	tikshuv.idf.il	TCP Scan (vertical)	drop	9
82.102.141.222	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	9
82.102.141.204	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	9
82.102.141.195	Israel	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	9
82.102.141.253	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	8
82.102.141.206	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	8
66.249.78.165	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
82.102.141.218	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	7
82.102.141.202	Israel	147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	7
82.102.141.207	Israel	147.237.76.42	refuah.idf.il	Invalid TCP Flags	drop	6
82.102.141.213	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	6
82.102.141.251	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	6
82.102.141.197	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	6
82.102.141.248	Israel	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	6
82.102.141.207	Israel	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	6
82.102.141.202	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	6
82.102.141.250	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	5
82.102.141.198	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	5
82.102.141.211	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	5
82.102.141.207	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	5
81.218.151.130	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
82.102.141.221	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	5
172.12.56.29	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	4
82.102.141.215	Israel	147.237.76.42	refuah.idf.il	Invalid TCP Flags	drop	4
82.102.141.195	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	4
82.102.141.202	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid TCP Flags	drop	4
82.102.141.198	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
162.255.180.208		147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
81.218.70.243	Israel	147.237.76.31	nakchal.idf.il	C004: HTTP: options method	Block	16
88.185.131.138	France	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	14
81.218.118.126	Israel	147.237.77.216	dover.idf.il	C004: HTTP: options method	Block	8
176.12.156.142	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
71.75.65.167	United States	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
123.151.149.222	China	147.237.0.34	tikshuv.idf.il	C098: Block - dns poisoning	Block	6
194.90.222.130	Israel	147.237.77.216	dover.idf.il	C004: HTTP: options method	Block	5
87.69.22.184	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
212.179.46.21	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.19.86.4	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.19.85.216	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
82.139.151.181	Poland	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
84.94.181.145	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
213.57.244.254	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
81.218.78.66	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	4
152.133.6.196	United States	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
82.102.141.197	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
84.108.61.217	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
82.139.151.181	Poland	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
93.173.137.24	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
109.65.16.230	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.120	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.0	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
174.101.73.138	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.21	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
37.142.163.217	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
109.65.167.1	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.137	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
212.199.132.57	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.182.54.136	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
109.66.99.79	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
176.12.146.71	Israel	147.237.77.170	maarachot.idf.il	C004: HTTP: options method	Block	3
5.28.132.71	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
193.43.176.21	Italy	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
24.187.205.131	United States	147.237.72.166	aka.idf.il	C041: HTTP: Access to - index.php?option=com_jce	Block	2
82.102.141.212	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.86	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
49.236.200.176	Malaysia	147.237.77.74	law.idf.il	C041: HTTP: Access to - index.php?option=com_jce	Block	2
87.68.96.94	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
82.139.151.181	Poland	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
213.8.59.105	Israel	147.237.77.216	dover.idf.il	C004: HTTP: options method	Block	2
134.220.183.150	United Kingdom	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.120.25.34	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.178.141.67	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.188	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
93.173.151.207	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.90	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
149.88.88.252	United States	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
188.165.220.108	France	147.237.77.176	matpash.idf.il	C041: HTTP: Access to - index.php?option=com_jce	Block	2

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
80.74.98.102	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	294
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	143
2.54.179.217	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	42
54.188.240.68	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	31
54.184.86.214	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	29
83.15.143.50	Poland	147.237.72.156	aman.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	8
193.110.55.14	Netherlands	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
79.181.223.181	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
176.12.146.90	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	3
70.208.148.226	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	3
213.57.152.247	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	3
212.143.112.85	Israel	147.237.72.166	aka.idf.il	ET SCAN NMAP -f -sS	2
87.68.96.94	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
213.8.52.149	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
77.126.193.111	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.179.243.144	Israel	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 3072	2
103.10.186.70	Indonesia	147.237.72.166	aka.idf.il	SQL url ending in comment characters - possible sql injection attempt	2
46.19.85.204	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.186.191.63	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.179.243.144	Israel	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	2
138.134.102.18	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.177.154.28	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.183.223.185	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.186.146.131	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
5.29.202.12	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
91.123.201.179	Sweden	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	2
115.28.48.188	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
212.179.61.120	Israel	147.237.76.177	ncore.idf.il	ET DOS SSL Bomb DoS Attempt	2
109.66.80.105	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
91.123.201.179	Sweden	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	2
93.173.179.38	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
194.90.134.225	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.181.33.3	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
213.57.237.37	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.143.112.85	Israel	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 2048	2
54.86.184.22	United States	147.237.77.176	matpash.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
2.54.168.46	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
95.86.68.19	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.108.41.51	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
176.12.149.255	Israel	147.237.72.167	ishurim.aka.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
46.121.109.95	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
2.54.147.187	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.177.200.116	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.120.75.140	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
2.54.20.49	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.179.243.144	Israel	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 2048	2
82.102.141.250	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.19.85.171	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.179.243.144	Israel	147.237.72.166	aka.idf.il	ET SCAN NMAP -f -sS	2
79.176.107.180	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
68.180.228.243	United States	147.237.72.14	dover.idf.il(old)		drop	drop	1678
41.33.231.86	Egypt	147.237.77.216	dover.idf.il		drop	drop	1244
213.151.44.86	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	964
82.145.216.77	Europe	147.237.77.216	dover.idf.il		drop	drop	480
41.33.232.65	Egypt	147.237.77.216	dover.idf.il		drop	drop	429
207.241.226.113	United States	147.237.72.166	aka.idf.il	SAM rule	drop	drop	320
62.219.239.207	Israel	147.237.72.14	dover.idf.il(old)		drop	drop	233
38.111.147.86	United States	147.237.72.14	dover.idf.il(old)		drop	drop	221
170.252.248.201	United States	147.237.77.216	dover.idf.il		drop	drop	211
65.49.2.181	Anonymous Proxy	147.237.77.216	dover.idf.il		drop	drop	202
66.249.78.158	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission		186
66.249.78.158	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	186
66.249.78.172	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	185
66.249.78.172	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission		184
68.180.228.243	United States	147.237.72.14	dover.idf.il(old)	Invalid ACK number	Bad TCP sequence	monitor	180
68.180.228.243	United States	147.237.72.14	dover.idf.il(old)	Invalid ACK number	Bad TCP sequence		178
66.249.78.165	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	164
66.249.78.165	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission		163
157.55.39.55	United States	147.237.72.14	dover.idf.il(old)		drop	drop	151
207.46.13.45	United States	147.237.72.14	dover.idf.il(old)		drop	drop	129
66.249.78.115	United States	147.237.72.14	dover.idf.il(old)		drop	drop	126
207.46.13.4	United States	147.237.72.14	dover.idf.il(old)		drop	drop	121
66.249.78.101	United States	147.237.72.14	dover.idf.il(old)		drop	drop	118
66.249.78.108	United States	147.237.72.14	dover.idf.il(old)		drop	drop	118
71.75.65.167	United States	147.237.72.14	dover.idf.il(old)		drop	drop	109
46.118.112.49	Ukraine	147.237.72.14	dover.idf.il(old)		drop	drop	108
95.211.140.221	Netherlands	147.237.77.216	dover.idf.il		drop	drop	94
95.86.109.128	Israel	147.237.72.14	dover.idf.il(old)		drop	drop	93
46.117.220.250	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	92
108.59.253.71	United States	147.237.77.216	dover.idf.il		drop	drop	91
192.114.87.2	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	90
91.199.69.254	Israel	147.237.72.14	dover.idf.il(old)		drop	drop	75
203.13.146.51	India	147.237.77.216	dover.idf.il		drop	drop	70
212.76.116.59	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	70
74.81.89.139	United States	147.237.72.14	dover.idf.il(old)		drop	drop	68
109.186.154.185	Israel	147.237.72.14	dover.idf.il(old)		drop	drop	68
54.72.73.168	United States	147.237.77.216	dover.idf.il		drop	drop	66
108.212.224.169	United States	147.237.77.216	dover.idf.il		drop	drop	65
109.253.143.61	Israel	147.237.72.167	ishurim.aka.idf.i		drop	drop	64
74.73.251.184	United States	147.237.77.216	dover.idf.il		drop	drop	60
109.253.158.55	Israel	147.237.72.156	aman.idf.il		drop	drop	57
157.55.39.12	United States	147.237.72.14	dover.idf.il(old)		drop	drop	57
207.46.13.55	United States	147.237.72.14	dover.idf.il(old)		drop	drop	55
91.97.95.44	Germany	147.237.72.14	dover.idf.il(old)		drop	drop	54
54.72.0.55	United States	147.237.77.216	dover.idf.il		drop	drop	52
66.249.93.205	United States	147.237.72.14	dover.idf.il(old)		drop	drop	51
194.90.122.217	Israel	147.237.72.14	dover.idf.il(old)		drop	drop	51
109.66.182.169	Israel	147.237.72.14	dover.idf.il(old)		drop	drop	50
194.90.105.94	Israel	147.237.72.14	dover.idf.il(old)		drop	drop	49
80.188.207.10	Czech Republic	147.237.72.14	dover.idf.il(old)		drop	drop	48

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.85.233	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.233	Block	537
176.12.146.90	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	486
109.253.134.104	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	362
82.102.141.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	336
46.19.86.253	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	301
84.109.92.2	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	300
38.111.147.84	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 38.111.147.84	Block	295
176.12.147.231	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	234
10.110.110.38		147.237.72.166	aka.idf.il	Distributed Suspicious Response Code	Block	230
46.19.85.185	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	224
46.19.85.52	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	223
176.12.149.241	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.149.241	Block	205
66.249.78.94	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.94	Block	164
85.65.189.38	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	149
176.12.156.73	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	148
66.249.78.101	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.101	Block	139
66.249.78.108	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.108	Block	134
94.230.89.29	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 94.230.89.29	Block	120
109.253.141.31	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.141.31	Block	112
46.120.175.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	101
157.55.39.88	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code	Block	96
176.12.142.167	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	95
207.46.13.11	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code	Block	84
176.12.148.207	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.148.207	Block	80
66.249.78.158	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.158	Block	77
176.12.142.16	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	73
66.249.78.172	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.172	Block	70
66.249.78.165	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.165	Block	70
5.29.214.215	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 5.29.214.215	Block	48
81.218.70.243	Israel	147.237.76.31	nakchal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	48
209.95.34.86	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/994-8613-he/navy.aspx.aspx	Block	47
79.181.141.89	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/undefined/	Block	39
88.185.131.138	France	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	37
46.120.25.34	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	36
46.19.86.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	36
68.180.228.121	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.121	Block	33
77.126.30.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	33
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	31
81.218.48.37	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	30
109.160.141.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code	Block	29
46.116.180.83	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	28
84.108.176.180	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	27
212.179.61.122	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	26
95.86.109.192	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	26
46.19.86.64	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	25
5.255.253.36	Russian Federation	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code	Block	22
212.117.151.70	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code	Block	21
89.139.10.42	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code	Block	20
109.65.127.52	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	19
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	18