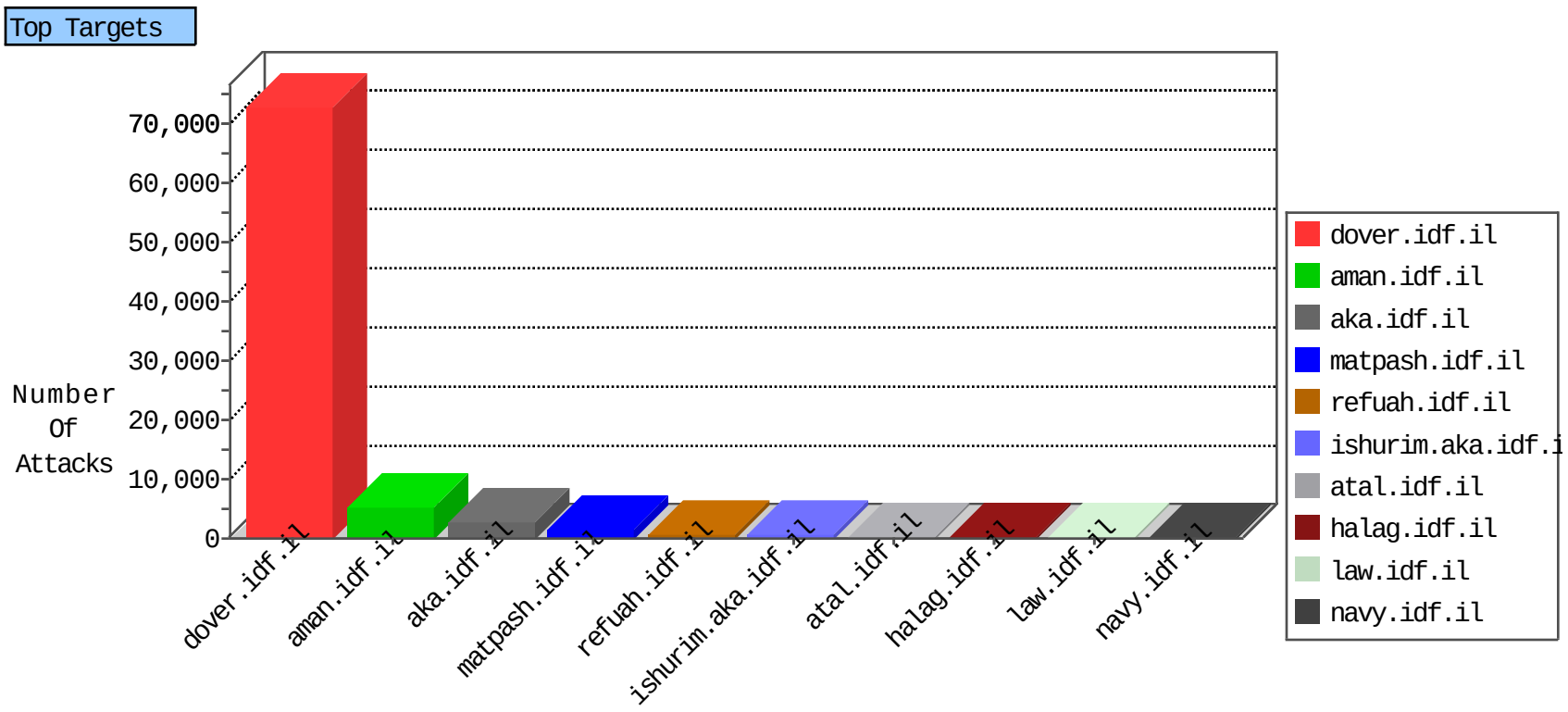
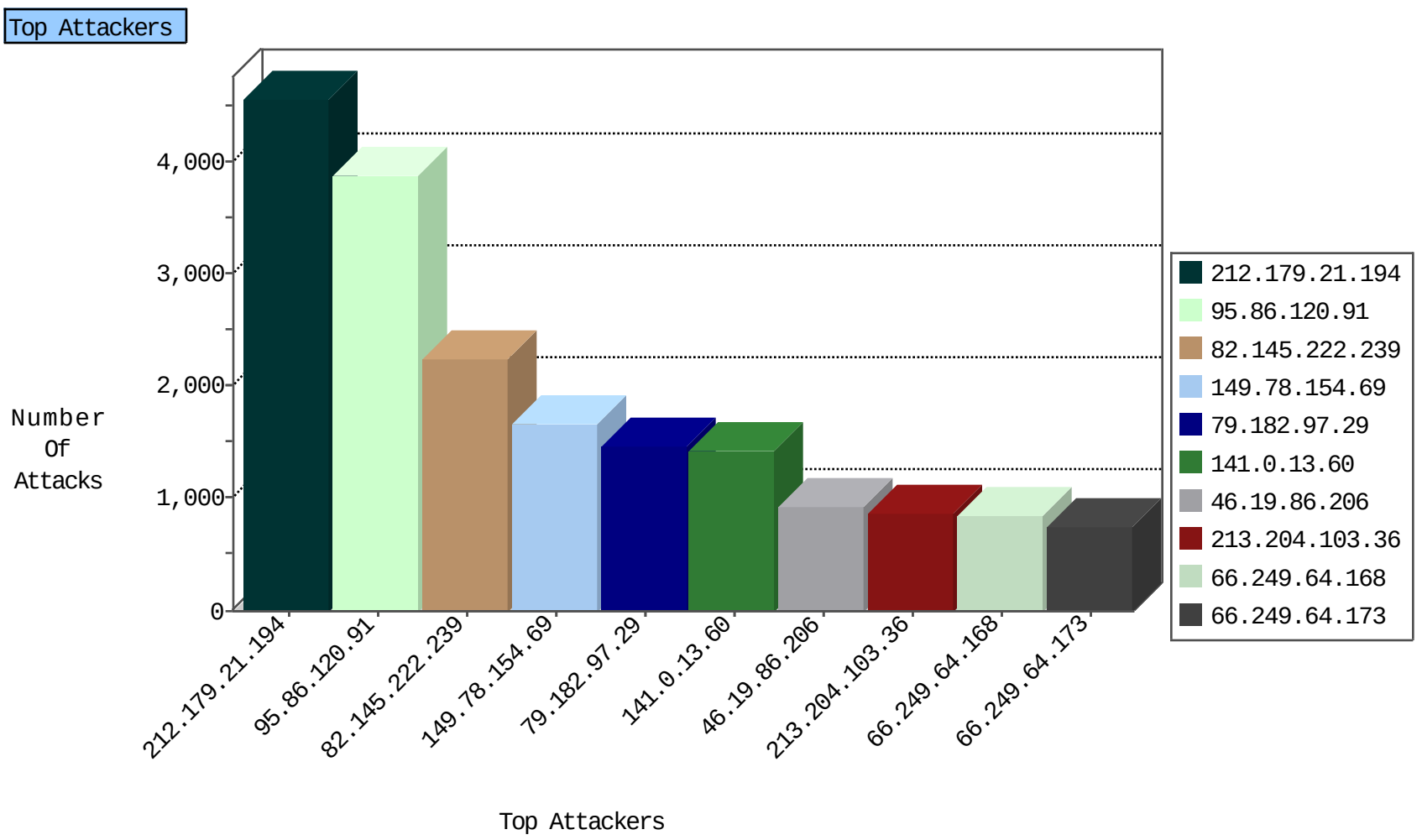
07-22-2015-00:00:05 to 07-23-2015-00:00:05

IDF Under Attack Daily Report





07-22-2015-00:00:05 to 07-23-2015-00:00:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.93.168	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	5837
66.249.93.172	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	3439
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3432
141.0.13.60	Norway	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	3035
170.74.56.79	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2502
197.144.128.166	Morocco	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	1152
66.249.93.164	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	876
85.250.110.36	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	637
81.218.241.26	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	534
46.120.21.70	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	491
109.66.139.213	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	428
81.218.37.2	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	423
149.78.58.86	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	413
77.125.115.76	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	364
5.28.175.202	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	360
84.228.8.194	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	360
82.80.165.174	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	359
197.79.6.245	South Africa	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	358
79.181.118.114	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	349
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	340
79.177.51.176	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	323
149.88.106.58	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	312
93.173.146.21	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	303
89.139.170.58	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	275
84.228.226.91	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	266
37.142.64.169	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	252
46.120.114.77	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	231
213.57.214.96	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	229
79.183.26.143	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	228
77.126.203.79	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	215
79.181.148.115	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	214
87.69.89.8	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	211
87.68.24.42	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	202
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	187
79.181.60.33	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	173
85.64.94.58	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	169
109.67.81.44	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	168
220.181.108.160	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	168
50.87.144.145	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	164
85.65.20.244	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	157
37.26.149.184	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	156
79.179.3.254	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	155
85.65.25.74	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	154
79.178.164.58	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	140
213.57.180.137	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	137
109.67.123.228	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	136
213.151.37.182	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	130
79.176.179.247	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	128
109.67.51.70	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	125
93.173.139.101	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	118

07-22-2015-00:00:05 to 07-23-2015-00:00:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
138.134.102.15	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	18
37.142.64.169	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	15
105.210.89.93	South Africa	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	15
138.134.102.16	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
82.81.128.125	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	9
37.142.197.216	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
149.78.252.216	United States	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
149.78.252.216	United States	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
62.219.65.115	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
85.105.158.47	Turkey	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
31.154.92.139	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
62.219.131.7	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
213.57.153.73	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
217.55.189.254	Egypt	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
176.228.46.8	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
213.57.243.61	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
91.227.71.250	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
8.24.3.226	Canada	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
149.88.85.31	United States	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
78.62.194.131	Lithuania	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
62.219.54.250	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
79.181.21.71	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
79.183.140.10	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
109.66.180.35	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.103	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.120.248.19	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.103	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
82.166.22.217	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.34	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.147	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
80.179.54.68	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.182.27.53	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
46.19.85.223	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
94.188.248.70	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
197.202.191.249	Algeria	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.85.147	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.210.176.162	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
95.172.68.146	Germany	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
174.51.118.153	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
76.91.31.48	United States	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
31.154.91.151	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.85.67	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.176.223.57	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
192.114.23.18	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
5.29.208.128	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	2
46.19.85.142	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
188.161.67.227	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
109.65.198.15	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.85.83	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2

07-22-2015-00:00:05 to 07-23-2015-00:00:05

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
46.19.86.120	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	57
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	54
125.165.20.235	Indonesia	147.237.77.216	dover.idf.il	INDICATOR-SCAN sqlmap SQL injection scan attempt	43
125.165.20.235	Indonesia	147.237.77.216	dover.idf.il	ET SCAN w3af User Agent	28
2.54.187.28	Israel	147.237.77.216	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	24
66.249.81.140	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	16
125.165.20.235	Indonesia	147.237.77.216	dover.idf.il	SQL Injection - Select From	14
125.165.20.235	Indonesia	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM	13
125.165.20.235	Indonesia	147.237.77.216	dover.idf.il	ET SCAN Sqlmap SQL Injection Scan	13
125.165.20.235	Indonesia	147.237.77.216	dover.idf.il	SQL waitfor delay function - possible SQL injection attempt	7
66.249.78.153	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	6
125.165.20.235	Indonesia	147.237.77.216	dover.idf.il	ET WEB_SERVER MYSQL SELECT CONCAT SQL Injection Attempt	5
125.165.20.235	Indonesia	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible MySQL SQLi Attempt Information Schema Access	5
125.165.20.235	Indonesia	147.237.77.216	dover.idf.il	SQL use of concat function with select - likely SQL injection	5
125.165.20.235	Indonesia	147.237.77.216	dover.idf.il	SQL url ending in comment characters - possible sql injection attempt	4
125.165.20.235	Indonesia	147.237.77.216	dover.idf.il	INDICATOR-OBFUSCATION large number of calls to char function - possible sql injection obfuscation	3
218.65.30.107	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	3
221.203.3.117	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	3
125.165.20.235	Indonesia	147.237.77.216	dover.idf.il	ET WEB_SERVER SQL Injection Select Sleep Time Delay	3
218.65.30.107	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	3
125.165.20.235	Indonesia	147.237.77.216	dover.idf.il	SQL generic convert injection attempt - GET parameter	3
218.65.30.107	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	3
218.65.30.107	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	2
183.37.74.14	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
180.210.234.87	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
149.78.154.69	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
45.114.11.46		147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	2
66.249.81.204	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
45.114.11.46		147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	2
183.37.74.14	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	2
218.87.111.107	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	2
66.249.81.136	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
45.114.11.47		147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.49		147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	2
79.176.129.61	Israel	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
218.65.30.107	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.46		147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.146	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	2
45.114.11.47		147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.29	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
218.65.30.107	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	2
109.65.106.1	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	2
101.226.2.99	China	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	2
218.87.111.107	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
212.179.21.194	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
218.65.30.107	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
180.210.234.87	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.48		147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
218.87.111.107	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.47		147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	2

07-22-2015-00:00:05 to 07-23-2015-00:00:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4385
95.86.120.91	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3879
82.145.222.239	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2217
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1658
79.182.97.29	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	1475
141.0.13.60	Norway	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1399
46.19.86.206	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	925
213.204.103.36	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	858
38.111.147.88	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	753
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	743
94.159.158.214	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	722
197.79.6.245	South Africa	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	698
5.29.241.78	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	657
69.41.14.215	United States	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	642
68.180.228.176	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	586
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	575
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	575
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	543
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	540
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	534
66.249.64.168	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	504
66.249.64.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	470
66.249.64.178	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	464
132.183.13.252	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	442
85.250.247.37	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	438
69.41.14.151	United States	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	420
185.24.124.3	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	387
174.90.223.178	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	384
188.165.15.98	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	383
175.156.111.96	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	355
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	335
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	307
37.231.47.85	Kuwait	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	280
213.204.103.26	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	279
2.54.139.221	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	255
46.120.123.239	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	246
37.142.64.16	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	239
65.92.13.38	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	237
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	236
82.166.22.45	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	236
66.249.64.168	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	227
46.19.86.169	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	211
80.123.167.25	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	210
2.54.26.62	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	203
192.116.231.74	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	203
66.249.64.178	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	196
46.210.186.109	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	193
157.55.39.99	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	193
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	189
66.249.64.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	188

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
176.13.20.119	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.20.119	Block	38
31.168.103.115	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 31.168.103.115	Block	34
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.173	Block	31
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.168	Block	23
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.178	Block	22
176.12.140.145	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.140.145	Block	8
46.116.137.105	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
84.108.117.245	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/59452.swf	Block	3
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	3
37.26.147.144	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	3
79.182.134.37	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
79.180.174.123	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	3
66.249.65.83	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
68.180.229.217	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1117-he/nakhal.aspx	Block	2
37.26.146.207	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.65.12.78	Israel	147.237.72.156	aman.idf.il	Multiple Cross-site scripting from 109.65.12.78	Block	2
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	2
79.178.103.87	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
84.228.34.228	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
68.180.230.113	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1927-he/cogat.aspx	Block	2
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_text.asp	Block	2
79.181.161.16	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/giyus/general.aspx	Block	2
87.68.63.228	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
115.78.235.170	Vietnam	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	2
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	2
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
77.127.223.191	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
85.250.142.160	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
95.35.79.213	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
188.165.15.121	France	147.237.76.30	himush.idf.il	Unknown Parameter l in www.chimush.atal.idf.il/templates/sendtofriend/sendtofriend.aspx	None	2
46.19.85.59	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.176	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.176	Block	1
104.238.81.224		147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1
212.76.125.135	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/&sa=u&ved=0cagqfjaaahukewjlme6-3-7gahuctxqkhsjbbpa&usg=afqjcnhcvyyg7w1cq-yhd5_ammzoyodtwa	Block	1
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/090a.stm	Block	1
82.166.182.6	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
180.76.15.159	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	1
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/october/22.stm	Block	1
79.182.168.236	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
176.13.8.117	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
24.210.81.120	United States	147.237.76.86	navy.idf.il	Illegal HTTP Version	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/pratim/pirteykatava/	Block	1
91.227.71.250	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.110	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2004/march/25.stm	Block	1
87.68.16.84	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
192.187.108.58	United States	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1