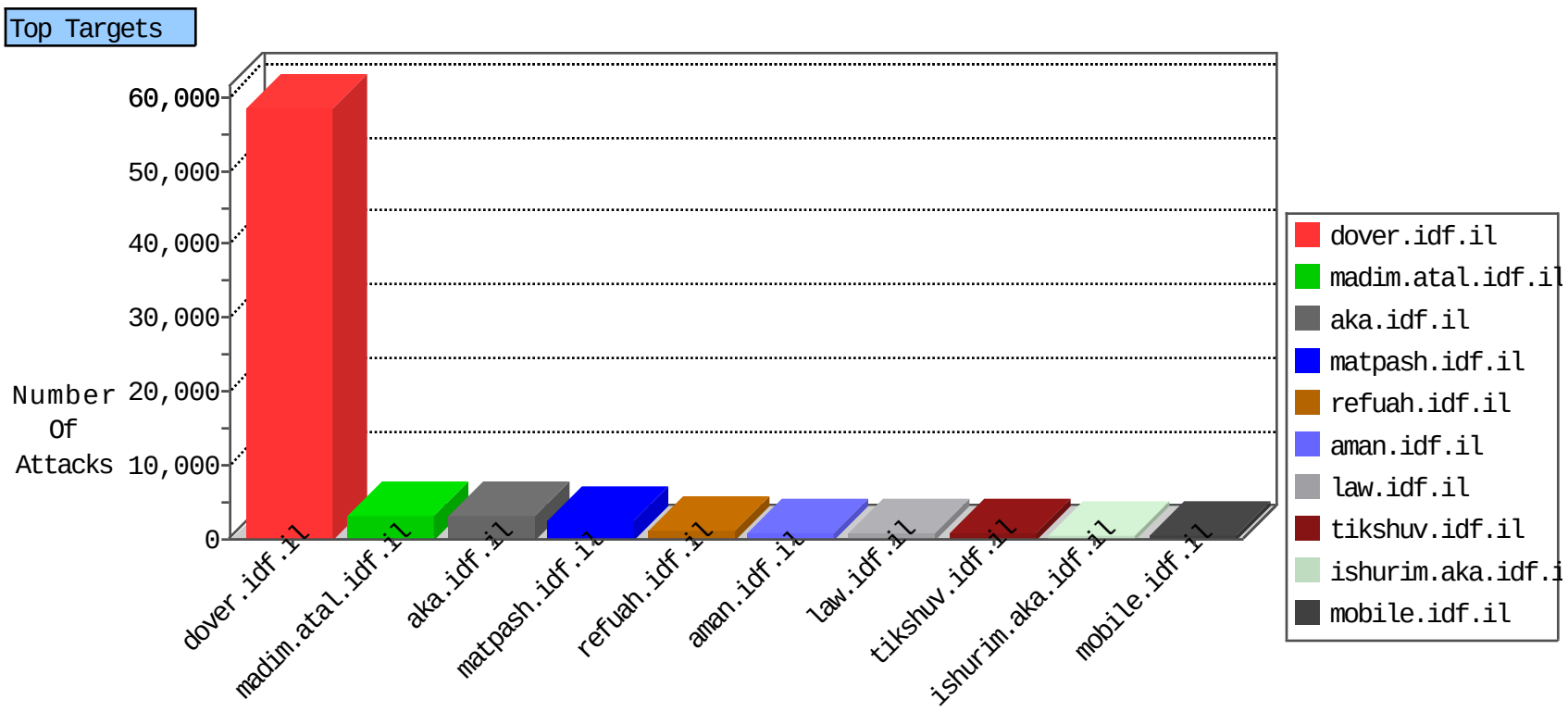
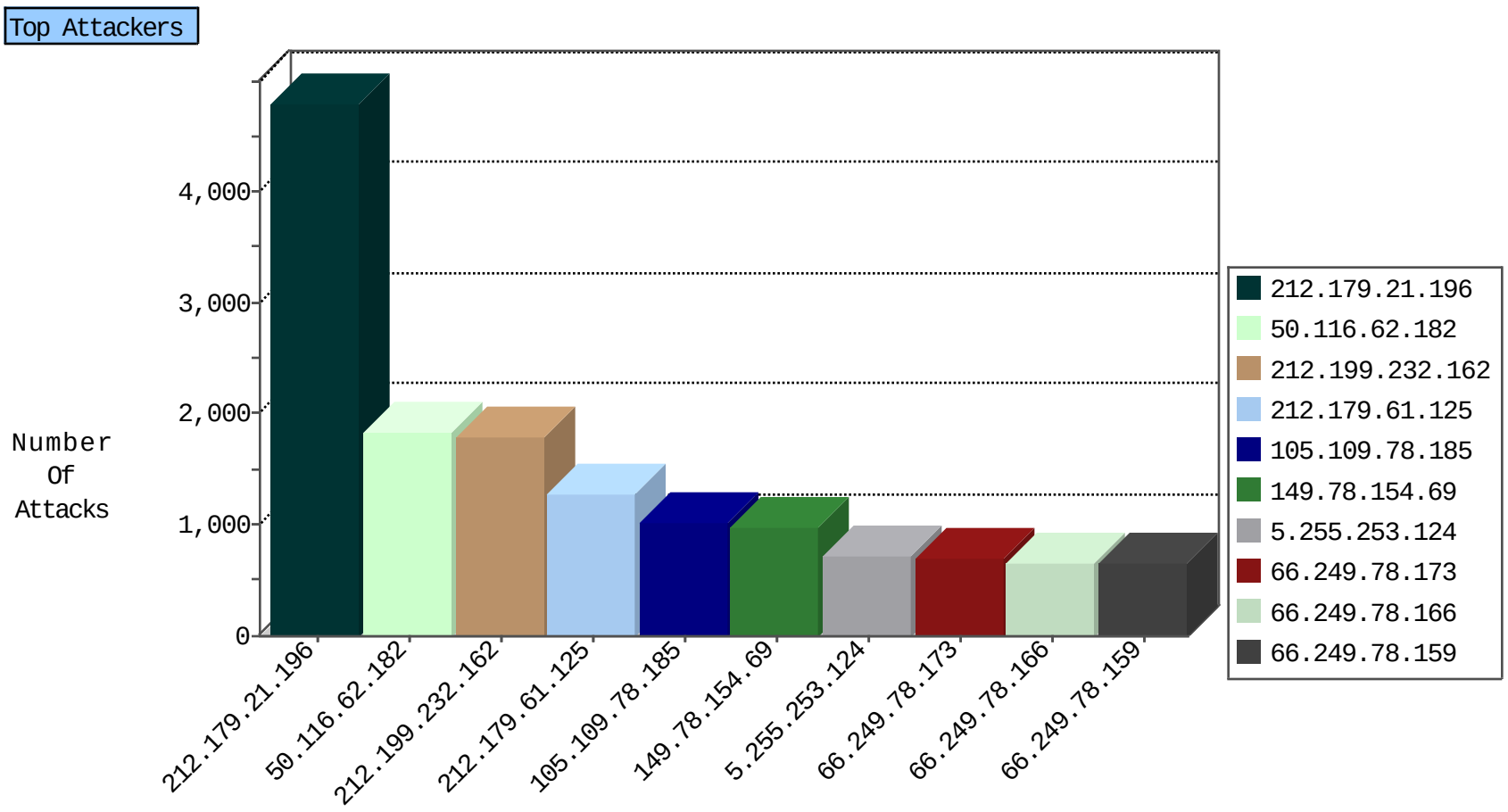
05-06-2015-00:00:05 to 05-07-2015-00:00:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



05-06-2015-00:00:05 to 05-07-2015-00:00:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.81.212	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5975
66.249.64.151	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5095
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5018
66.249.64.161	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4492
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2555
176.106.46.74	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2539
66.249.64.156	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2219
66.249.78.22	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1461
66.249.78.254	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1136
66.249.78.166	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1039
79.180.198.28	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	858
84.228.102.102	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	790
66.249.64.153	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	767
66.249.64.143	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	732
105.109.78.185	Algeria	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	640
85.250.146.233	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	609
84.108.138.39	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	553
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	528
157.55.39.204	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	523
220.181.108.114	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	471
80.230.95.242	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	469
220.181.108.122	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	423
220.181.108.103	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	376
109.160.245.252	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	363
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	339
84.111.172.101	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	334
66.249.78.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	292
85.250.228.53	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	265
52.16.5.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	222
220.181.108.174	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	212
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	201
213.57.106.188	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	196
85.65.245.148	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	188
157.55.39.191	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	175
212.179.212.6	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	174
220.181.108.113	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	170
105.109.78.185	Algeria	147.237.77.216	dover.idf.il	HTTP-MISC-DoS-GoodBye-30	dest-reset	168
2.54.44.23	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	162
220.181.108.100	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	161
46.116.152.130	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	147
2.54.168.214	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	142
80.74.105.107	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	135
81.218.212.11	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	117
220.181.108.82	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	101
220.181.108.88	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	95
37.142.129.150	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	91
37.26.147.210	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
37.142.224.198	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
213.57.90.154	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	88
46.117.240.178	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	83

05-06-2015-00:00:05 to 05-07-2015-00:00:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
50.116.62.182	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	1831
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	330
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	189
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	167
180.76.5.193	China	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	66
14.47.125.204	Korea, Republic of	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
194.114.146.227	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	28
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
112.111.189.8	China	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	13
62.219.231.231	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	9
62.219.65.138	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
71.6.167.142	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	6
89.139.23.28	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
85.250.65.51	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
46.116.37.131	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.116.210.130	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
89.139.23.28	Israel	147.237.77.234	halag.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.167.142	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	5
84.109.106.45	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.167.142	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	5
62.219.231.231	Israel	147.237.77.234	halag.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
188.138.9.50	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.76.196	e.sviva.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
46.19.85.244	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
85.25.43.94	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	4
46.116.234.181	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
89.138.40.16	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
66.240.192.138	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	4
36.231.145.10	Taiwan	147.237.72.166	aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
188.138.9.50	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	4
85.25.103.50	Germany	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	3
71.6.167.142	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	3
198.20.69.98	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	3
79.177.184.68	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
188.138.9.50	Germany	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	3
198.20.69.98	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	3
66.240.192.138	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	3
66.240.192.138	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	3
129.79.222.178	United States	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.120.226.23	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
188.138.9.50	Germany	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	3
71.6.167.142	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	3
71.6.167.142	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	3
66.240.192.138	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	3
71.6.167.142	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	3
198.20.70.114	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	3

05-06-2015-00:00:05 to 05-07-2015-00:00:05

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	98
46.19.86.107	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	46
66.249.67.147	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	38
84.108.9.218	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	8
64.233.172.214	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	8
109.253.157.64	Israel	147.237.76.30	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
66.249.67.121	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	5
66.249.64.161	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
221.235.189.244	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	3
212.179.61.125	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	3
66.249.64.148	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	3
109.186.185.133	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.180.204.117	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.22	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
2.54.0.175	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.64	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.66	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
221.235.189.245	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	2
79.179.109.167	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.64	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	2
221.235.189.245	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	2
221.235.189.245	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	2
46.116.166.166	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
87.81.208.80	United Kingdom	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	2
221.235.189.245	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	2
217.132.192.33	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.64.156	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
212.179.155.129	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
31.168.232.154	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.253.139.24	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.83.146	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
221.235.189.244	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
79.177.56.54	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.64.151	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
2.54.129.76	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
149.88.20.31	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.189.244	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.248	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
212.179.21.196	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
84.109.3.77	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.64.143	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
149.78.174.142	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
37.46.39.200	Israel	147.237.72.167	ishurim.aka.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
66.249.78.120	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.64	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
77.125.104.144	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.29	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
121.88.5.177	Korea, Republic of	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
84.95.110.108	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
183.136.216.3	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2

05-06-2015-00:00:05 to 05-07-2015-00:00:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.21.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4791
212.199.232.162	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1784
212.179.61.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1270
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	982
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	709
105.109.78.185	Algeria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	630
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	624
199.190.46.172	Satellite Provider	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	547
79.180.65.88	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	503
212.179.46.21	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	477
109.66.110.10	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	466
109.64.160.191	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	450
212.179.180.7	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	420
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	386
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	372
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	368
82.145.222.255	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	353
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	352
82.145.221.156	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	327
191.189.153.245	Brazil	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	298
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	289
82.205.31.157	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	285
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	268
38.99.190.240	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	259
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	253
82.145.211.21	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	245
205.132.119.8	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	245
2.54.45.62	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	244
46.19.86.254	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	230
148.177.129.213	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	227
78.40.232.82	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	221
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	215
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	214
46.19.85.252	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	204
213.151.53.59	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	204
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	200
31.168.90.18	Israel	147.237.76.42	refuah.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	195
130.253.186.47	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	191
81.218.251.251	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	191
157.55.39.191	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	189
141.0.9.118	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	187
157.55.39.136	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	179
105.46.38.239		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	176
5.108.19.25	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	170
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	169
23.27.248.92	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	168
213.8.96.180	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	164
212.45.46.36	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	162
131.137.245.208	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	161
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	156

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.160.189.124	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.160.189.124	Block	564
46.19.85.35	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	523
109.253.139.197	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.139.197	Block	436
212.29.220.163	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 212.29.220.163	Block	424
37.26.147.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	333
2.54.44.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	146
95.86.118.151	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	140
109.253.147.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	113
46.210.255.23	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	102
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	100
46.19.85.120	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	98
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	86
207.106.190.66	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.106.190.66	Block	75
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	74
176.12.146.11	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.146.11	Block	73
66.249.78.223	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.78.223	Block	58
176.12.151.166	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	53
109.253.143.132	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	50
176.12.136.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	45
66.249.78.216	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.78.216	Block	44
80.246.137.238	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	43
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	39
66.249.78.230	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.78.230	Block	36
157.55.39.248	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 157.55.39.248	Block	32
157.55.39.182	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il//captcha.ashx	Block	31
46.121.28.16	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	25
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	24
2.52.61.120	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.52.61.120	Block	23
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	20
80.246.137.35	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	19
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	19
157.55.39.183	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il//captcha.ashx	Block	18
207.106.190.66	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	18
62.81.85.102	Spain	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 62.81.85.102	Block	18
157.55.39.190	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il//captcha.ashx	Block	17
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	16
31.44.139.134	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	15
31.210.186.154	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	13
178.137.166.68	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/	Block	12
85.250.71.116	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.250.71.116	Block	11
212.76.97.173	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	10
2.54.132.215	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	10
66.249.64.248	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.64.248	Block	10
46.19.85.192	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	9
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	9
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	9
84.228.253.2	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	9
52.6.169.50	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.stm	Block	9
176.12.149.179	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.149.179	Block	9
157.55.39.182	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il//main/giyus/giyus/general.aspx	Block	9

05-06-2015-00:00:05 to 05-07-2015-00:00:05