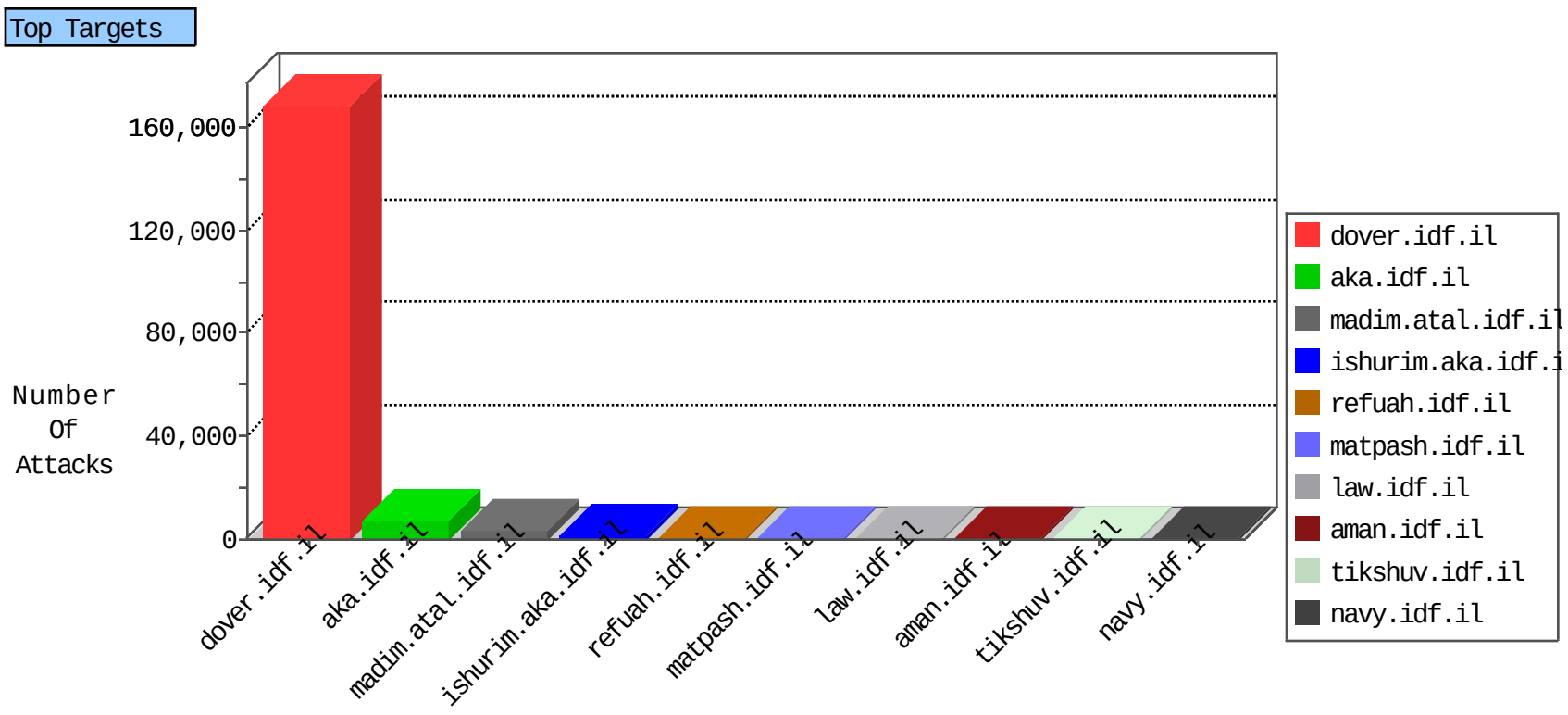
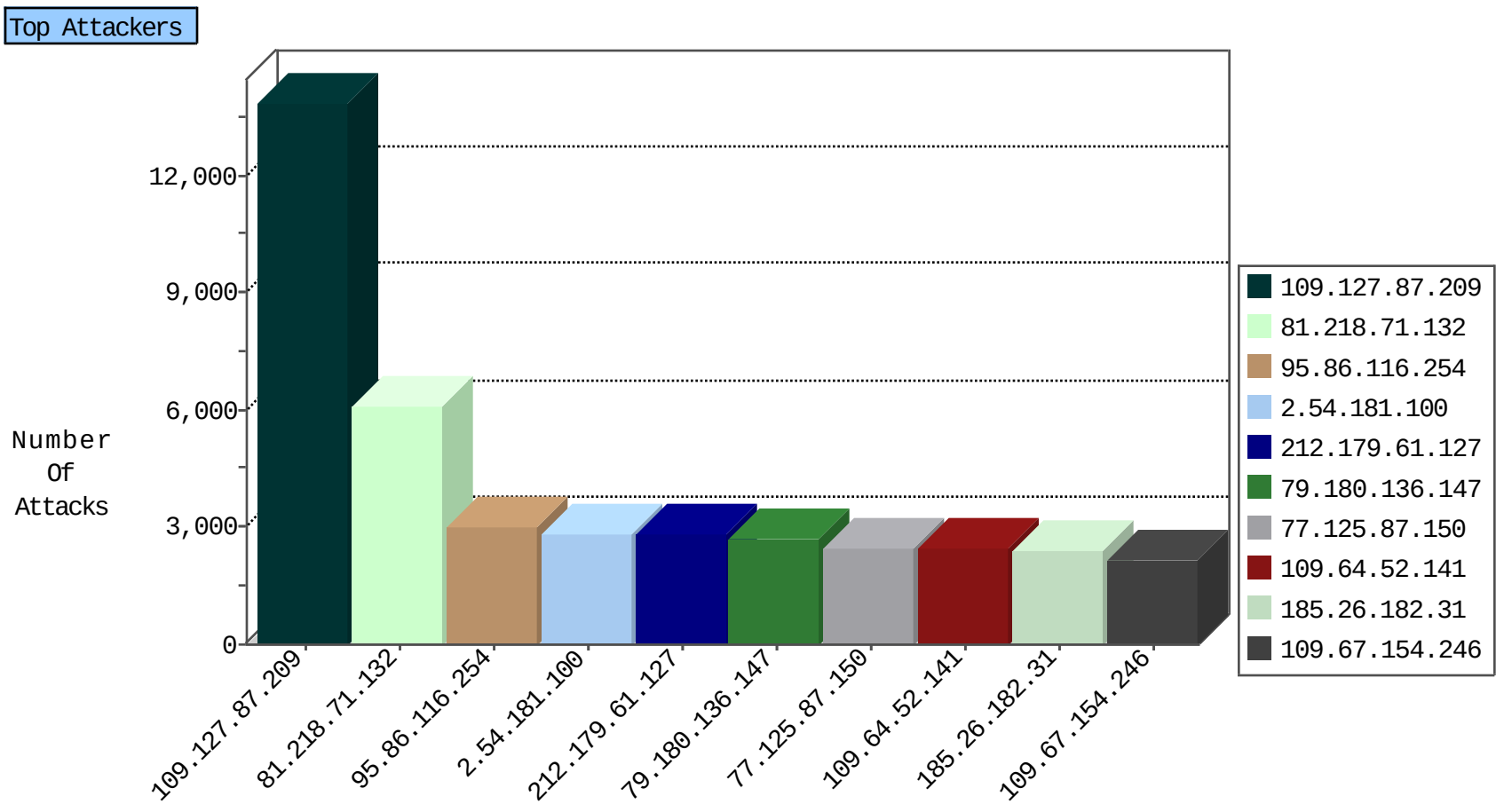
04-28-2015-00:00:05 to 04-29-2015-00:00:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-28-2015-00:00:05 to 04-29-2015-00:00:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.64.68	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	12252
109.127.87.209	Iraq	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4482
85.250.228.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3385
66.249.64.4	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3259
46.19.85.201	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2934
66.249.64.64	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	2834
66.249.78.109	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1991
220.181.108.97	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	1751
66.249.64.64	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1437
192.116.232.69	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1344
179.216.137.222	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1173
66.249.64.98	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1095
66.249.67.116	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1057
66.249.64.66	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	890
66.249.64.2	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	871
91.200.12.11	Ukraine	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	761
132.64.210.14	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	701
220.181.108.94	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	652
66.249.67.76	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	592
66.249.67.92	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	564
90.177.100.129	Czech Republic	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	530
85.250.223.65	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	482
109.253.133.15	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	466
109.67.127.154	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	426
94.159.142.243	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	419
84.111.244.139	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	410
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	405
84.229.196.85	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	387
66.249.67.84	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	385
220.181.108.186	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	380
220.181.108.105	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	380
220.181.108.171	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	377
220.181.108.111	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	322
66.249.64.66	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	265
213.8.71.26	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	261
220.181.108.95	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	256
79.178.165.108	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	231
37.142.237.40	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	230
220.181.108.155	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	226
66.249.67.108	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	223
192.115.116.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	221
91.231.193.150	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	214
79.183.140.147	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	206
220.181.108.119	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	202
93.173.244.169	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	199
79.183.148.174	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	197
46.117.20.86	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	189
81.218.37.2	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	180
37.142.162.212	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	174
84.110.60.199	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	167

04-28-2015-00:00:05 to 04-29-2015-00:00:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.64.52.141	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	2427
77.125.87.150	Israel	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	2426
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	237
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	137
180.76.5.193	China	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	132
180.76.5.193	China	147.237.77.74	law.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	85
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	21
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	20
117.131.78.26	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	14
37.142.100.150	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	11
178.115.129.48	Austria	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
143.225.229.236	Italy	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	8
37.142.128.208	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
95.86.70.19	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
46.19.85.97	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
46.120.229.69	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
31.44.135.77	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
211.81.48.100	China	147.237.0.15	kosher-kravi.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	5
85.25.103.50	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	5
85.250.117.249	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
79.177.132.192	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.167.142	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	5
82.80.196.44	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
198.20.69.98	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	5
2.54.13.46	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
46.116.211.238	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
198.20.69.98	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	5
84.109.101.201	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
211.81.48.100	China	147.237.0.17	m.my-kosher-kravi.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	5
188.120.141.4	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.165.200	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	5
46.19.85.36	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
211.81.48.100	China	147.237.0.19	madim.atal.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	5
109.66.23.109	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
77.125.6.192	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
5.22.135.245	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.17	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.167.142	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	4
211.81.48.100	China	147.237.0.34	tikshuv.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	4
71.6.167.142	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	4
79.182.38.131	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
85.25.103.50	Germany	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	4
46.19.85.139	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.167.142	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	4
46.19.85.235	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.21	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.167.142	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	4
198.20.70.114	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	4

04-28-2015-00:00:05 to 04-29-2015-00:00:05

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	79
66.249.67.84	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	35
46.117.221.59	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	23
46.19.86.44	Israel	147.237.77.216	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	17
199.203.51.242	Israel	147.237.77.216	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	7
66.249.64.66	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	6
185.32.179.20	Israel	147.237.72.167	ishurim.aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	5
91.195.154.34	Sweden	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
66.249.64.4	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
190.106.66.54	Costa Rica	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
37.26.148.154	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
66.249.64.68	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
66.249.67.108	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.67.30	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	4
66.249.64.78	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	4
43.255.191.165	Japan	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	3
5.22.130.59	Israel	147.237.72.167	ishurim.aka.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	3
43.255.191.165	Japan	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	3
66.249.64.64	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	3
66.249.78.109	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	3
73.11.61.110	United States	147.237.77.74	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	3
199.119.180.110	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
43.255.191.165	Japan	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.95	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
149.78.109.8	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.75.117	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	2
50.63.174.137	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
61.240.144.64	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	2
77.125.116.243	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.67	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.67.116	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
212.143.234.229	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
82.80.230.200	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
192.169.217.96	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
91.238.134.92	Poland	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	2
216.69.179.127	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.67.92	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
89.234.68.85	Ireland	147.237.77.216	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
87.68.147.174	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
178.19.107.114	Poland	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.191.165	Japan	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	2
194.114.146.227	Israel	147.237.77.216	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
66.249.67.76	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
46.116.211.238	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
89.139.23.28	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.67	China	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.67.3	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
199.116.250.199	United States	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	2
46.121.93.113	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
149.88.196.76	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2

04-28-2015-00:00:05 to 04-29-2015-00:00:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
109.127.87.209	Iraq	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13790
81.218.71.132	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6093
95.86.116.254	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2995
2.54.181.100	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2829
212.179.61.127	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2785
79.180.136.147	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2695
185.26.182.31	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2377
109.67.154.246	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2163
80.94.146.53	Switzerland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2117
212.179.46.21	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1945
2.54.133.89	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1867
212.179.61.120	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1626
82.145.221.48	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1594
2.54.2.7	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1394
212.179.61.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1377
212.76.97.111	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1281
5.102.227.120	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1261
79.177.172.178	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1259
79.181.124.21	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1172
84.228.157.56	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1157
37.26.147.236	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1155
46.116.180.190	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1070
46.19.85.156	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1048
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	988
176.12.146.123	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	973
213.57.57.94	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	972
46.19.85.217	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	963
32.97.110.58	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	952
79.180.35.253	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	848
213.151.48.77	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	828
66.249.78.109	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	766
66.249.78.102	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	765
66.249.78.95	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	758
2.54.144.38	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	753
109.64.4.28	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	715
46.19.85.90	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	675
109.186.18.234	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	670
213.57.190.144	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	655
46.19.85.189	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	643
46.116.118.155	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	604
212.179.61.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	576
79.179.164.28	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	571
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	538
62.90.202.179	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	530
176.12.144.162	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	529
66.249.78.95	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	500
79.177.116.184	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	495
46.116.211.238	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	481
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	473
66.249.78.109	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	454

04-28-2015-00:00:05 to 04-29-2015-00:00:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
77.125.151.243	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 77.125.151.243	Block	989
46.19.85.52	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.52	Block	442
46.19.85.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	394
85.64.39.184	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	309
46.19.86.125	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	249
37.26.146.129	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 37.26.146.129	Block	204
79.180.10.167	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 79.180.10.167	Block	181
176.12.139.105	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.139.105	Block	179
109.253.159.79	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	174
2.52.34.189	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.52.34.189	Block	77
192.114.163.27	Israel	147.237.76.42	refuah.idf.il	Too Many of the Same Response Code (404) in Session from 192.114.163.27	Block	63
109.253.140.51	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	50
46.19.86.33	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	45
37.142.68.209	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 37.142.68.209	Block	39
109.253.133.135	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	36
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	35
192.151.151.202	United States	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 192.151.151.202	Block	28
176.12.149.75	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	22
176.12.150.132	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	22
85.64.74.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	21
109.65.191.69	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	20
2.54.183.179	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	17
79.177.14.157	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.177.14.157	Block	16
79.176.25.122	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	16
109.253.140.79	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.140.79	Block	15
213.151.48.77	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	15
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	14
109.64.113.4	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	14
109.253.147.170	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	13
192.116.232.69	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
176.12.137.94	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	13
109.253.146.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	12
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	11
95.86.73.128	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	11
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	11
132.71.64.228	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	11
37.26.146.237	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	10
176.12.143.49	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	10
93.172.169.104	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	9
37.60.44.243	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	8
37.26.147.240	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	8
149.78.69.183	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
212.150.214.122	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	8
194.213.108.130	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
109.65.20.162	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	8
87.68.156.45	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
46.121.64.227	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
79.179.33.238	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	7
82.166.134.94	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 82.166.134.94	Block	7
212.76.100.114	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7

04-28-2015-00:00:05 to 04-29-2015-00:00:05