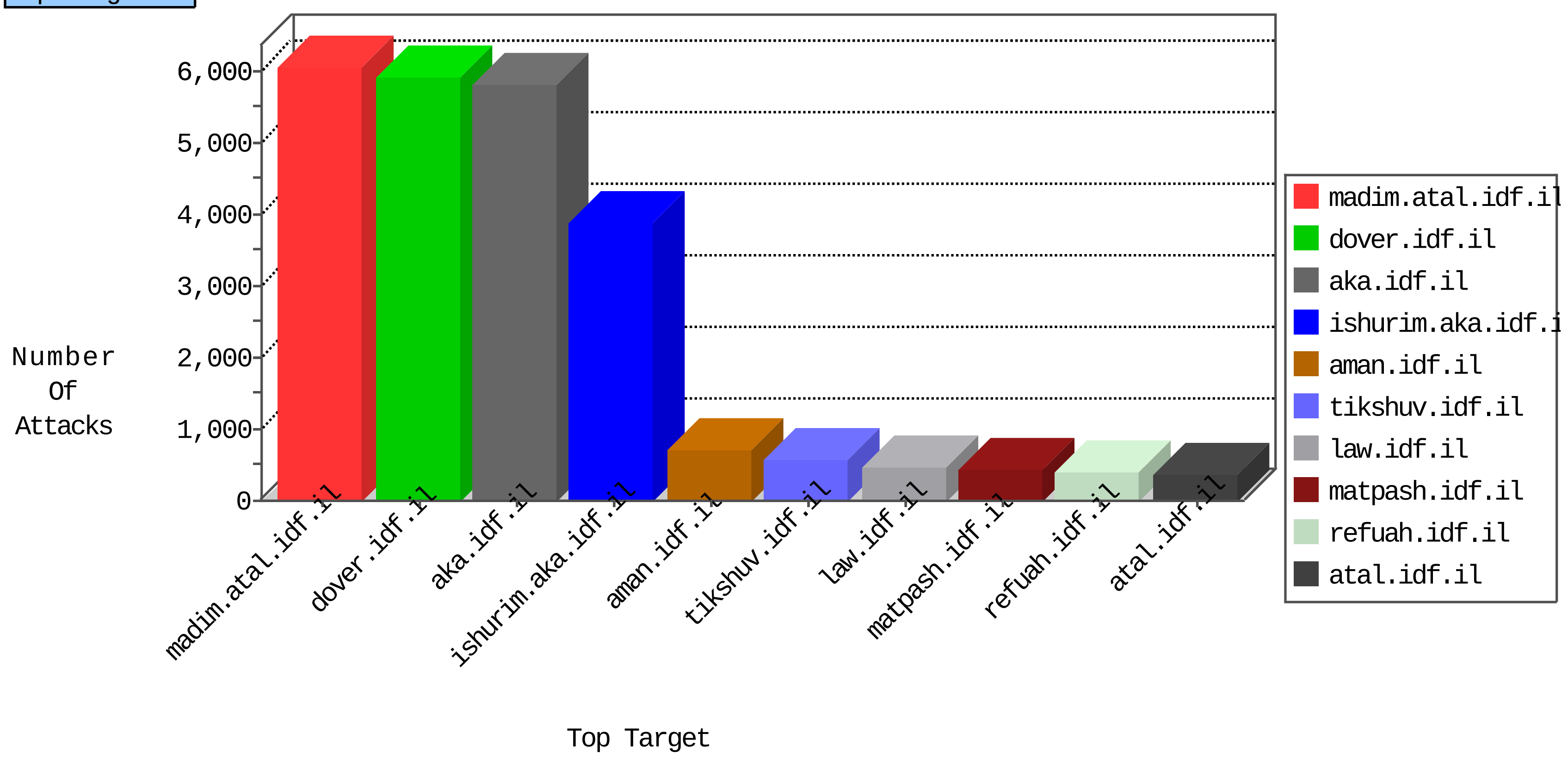
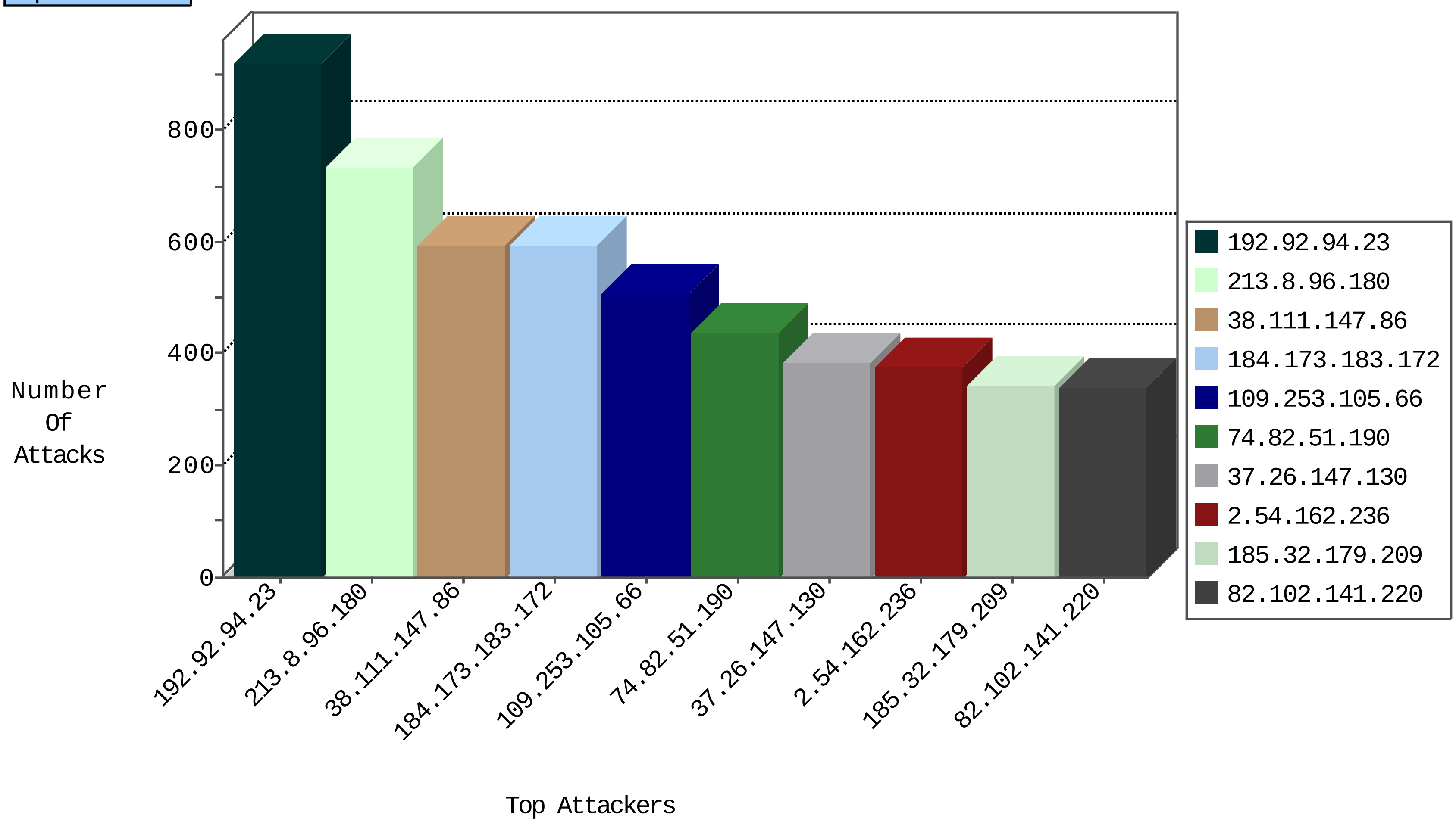
02-09-2015-00:00:05 to 02-10-2015-00:00:05

IDF Under Attack
Daily Report

Top Targets



Top Attackers



02-09-2015-00:00:05 to 02-10-2015-00:00:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.67.12	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	8116
94.230.86.46	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	1483
79.182.54.63	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1341
79.183.151.247	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	772
31.168.103.115	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	751
66.249.67.156	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	651
5.102.247.218	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	625
149.78.230.95	United States	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	459
5.102.253.46	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	455
79.183.142.78	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	252
109.186.145.183	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	232
85.64.3.180	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	223
79.176.126.5	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	180
5.28.140.2	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	178
149.88.124.148	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	172
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	172
79.180.105.56	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	168
149.78.244.24	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	167
77.127.10.169	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	166
2.54.36.119	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	161
79.176.126.5	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	160
85.65.32.11	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	143
85.64.3.180	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	133
77.125.74.38	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	133
37.142.214.112	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	123
79.180.2.233	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	122
109.64.58.240	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	121
84.108.237.48	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	113
84.108.93.76	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	111
77.126.187.46	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	110
2.54.146.52	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	106
37.142.191.46	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	102
46.19.86.167	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	100
194.90.186.193	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	96
46.120.31.40	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	91
46.117.88.251	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	88
84.108.38.114	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	86
79.180.2.233	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	80
37.142.227.19	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	79
66.249.78.51	United States	147.237.77.234	halag.idf.il	TCP handshake violation, first packet not syn	drop	79
91.135.102.170	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	77
132.72.81.160	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	75
37.142.118.186	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	75
37.46.46.10	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
109.64.176.168	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69
93.173.5.120	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69
87.69.48.241	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69
149.78.253.218	United States	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	67
212.179.215.239	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	65
79.176.121.207	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	64

02-09-2015-00:00:05 to 02-10-2015-00:00:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
192.92.94.23	Europe	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	922
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	435
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	288
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	131
192.118.64.29	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	53
109.186.228.104	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	44
138.134.102.15	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	38
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	30
212.25.82.123	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	24
212.179.132.203	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
207.232.36.85	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	10
91.238.161.4	United Kingdom	147.237.77.216	dover.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	7
212.34.12.161	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
84.95.1.230	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
84.94.103.185	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
212.34.12.122	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
81.218.97.114	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
86.24.46.13	United Kingdom	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
5.22.135.254	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
82.211.223.3	Denmark	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	6
89.139.173.72	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
176.126.252.12	Romania	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	5
79.177.181.232	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
84.111.110.243	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
182.50.130.87	Singapore	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
46.19.85.239	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
72.167.232.62	United States	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
80.246.141.29	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
2.54.4.152	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
63.143.34.40	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
109.65.50.195	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
62.90.131.34	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
80.246.141.249	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
184.168.193.35	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
46.19.85.1	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
212.150.189.2	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
198.20.70.114	United States	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	3
85.25.103.50	Germany	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	3
89.216.115.8		147.237.77.216	dover.idf.il	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	3
85.25.103.50	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	3
198.20.70.114	United States	147.237.77.121	e.navy.idf.il	DVRep_P-N_40-59	Permit	3
5.196.198.224	Germany	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.122	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
198.20.70.114	United States	147.237.76.30	himush.idf.il	DVRep_P-N_40-59	Permit	3
109.186.148.115	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
198.20.70.114	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	3
198.20.70.114	United States	147.237.76.202	e.halag.idf.il	DVRep_P-N_40-59	Permit	3
85.25.103.50	Germany	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	3
188.138.9.50	Germany	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	3
212.179.46.22	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3

02-09-2015-00:00:05 to 02-10-2015-00:00:05

Top Attackers In ID

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	119
72.167.232.62	United States	147.237.72.166	aka.idf.il	SQL Injection - Select From	78
182.50.130.87	Singapore	147.237.72.166	aka.idf.il	SQL Injection - Select From	61
66.249.67.12	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	57
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	52
212.117.143.250	Israel	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	50
74.82.51.190	United States	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	47
61.160.224.128	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	42
184.168.193.35	United States	147.237.77.74	law.idf.il	SQL Injection - Select From	38
182.50.130.87	Singapore	147.237.77.74	law.idf.il	SQL Injection - Select From	35
89.248.162.228	Netherlands	147.237.77.170	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	34
63.143.34.40	United States	147.237.77.74	law.idf.il	SQL Injection - Select From	33
74.82.51.190	United States	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	32
94.230.86.46	Israel	147.237.72.167	ishurim.aka.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	28
74.82.51.190	United States	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	28
74.82.51.190	United States	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	24
74.82.51.190	United States	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	23
141.212.122.58	United States	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	22
74.82.51.190	United States	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	20
74.82.51.190	United States	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	20
61.160.224.128	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	19
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	19
208.91.199.41	Virgin Islands, British	147.237.72.166	aka.idf.il	SQL Injection - Select From	18
74.82.51.190	United States	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	17
181.48.219.134	Colombia	147.237.77.19	law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	16
89.248.162.228	Netherlands	147.237.8.14	e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	15
91.149.157.169	Belarus	147.237.72.166	aka.idf.il	SQL Injection - Select From	15
122.228.207.190	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	14
122.228.207.190	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	14
61.160.224.128	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	13
74.82.51.190	United States	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	13
122.228.207.190	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	13
122.228.207.190	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	12
88.208.200.53	United Kingdom	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	12
74.82.51.190	United States	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	12
74.82.51.190	United States	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	12
89.248.162.228	Netherlands	147.237.76.44	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	12
74.82.51.190	United States	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	12
89.248.162.228	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	12
122.228.207.190	China	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	12
89.248.162.228	Netherlands	147.237.76.202	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	11
74.82.51.190	United States	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	11
122.228.207.190	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	11
89.248.162.228	Netherlands	147.237.0.19	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	10
74.82.51.190	United States	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	10
74.82.51.190	United States	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	10
141.212.122.59	United States	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	10
185.32.178.227	Israel	147.237.72.167	ishurim.aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	10
89.248.162.228	Netherlands	147.237.77.178	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	9
74.82.51.190	United States	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	9

02-09-2015-00:00:05 to 02-10-2015-00:00:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
213.8.96.180	Israel	147.237.72.167	ishurim.aka.idf.i	First packet isn't SYN	drop	drop	363
38.111.147.86	United States	147.237.72.166	aka.idf.il		drop	drop	307
213.8.96.180	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	214
78.108.161.226	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	191
38.111.147.86	United States	147.237.0.34	tikshuv.idf.il		drop	drop	159
213.8.96.180	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	155
38.111.147.86	United States	147.237.76.86	navy.idf.il		drop	drop	114
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	94
137.95.1.11	United States	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	93
188.244.33.125	Russian Federation	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	83
78.108.161.226	Lebanon	147.237.0.34	tikshuv.idf.il	First packet isn't SYN	drop	drop	78
66.249.93.152	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	78
66.249.93.158	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	78
5.22.135.254	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	71
37.26.147.244	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	63
185.6.58.49	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	60
66.249.78.44	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	46
192.116.81.173	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	45
109.253.134.16	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
41.254.6.106	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
176.12.146.78	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	40
87.69.92.239	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	39
89.204.154.145	Germany	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	38
66.249.93.155	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
176.12.142.83	Israel	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
46.19.86.79	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	37
109.253.128.43	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
46.19.86.231	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
77.126.89.218	Israel	147.237.72.167	ishurim.aka.idf.i	First packet isn't SYN	drop	drop	34
176.12.147.43	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
80.246.133.120	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	33
87.68.167.96	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
79.181.143.217	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	31
212.143.186.38	Israel	147.237.72.166	aka.idf.il	'Proxy-Authorization' header length exceeded maximum allowed length	HTTP Format Sizes	monitor	31
77.126.200.171	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	31
109.253.142.198	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
79.179.131.186	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.144.143	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.128.113	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
94.230.86.46	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid ACK number	Bad TCP sequence	monitor	29
84.95.226.177	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	29
94.200.150.221	United Arab Emirates	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	28
109.253.128.215	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
132.76.50.6	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
109.253.136.190	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
176.12.137.218	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
176.12.144.253	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
66.249.78.37	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
46.19.85.79	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	25

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.253.105.66	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.105.66	Block	508
37.26.147.130	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 37.26.147.130	Block	376
2.54.162.236	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	375
185.32.179.209	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	342
2.54.34.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	339
82.102.141.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	325
185.32.178.250	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	273
46.19.85.187	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	270
46.19.86.33	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	269
37.26.147.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	263
109.67.140.87	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	252
185.32.179.227	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	245
62.90.174.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	243
2.54.34.177	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	224
91.242.33.8	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 91.242.33.8	Block	199
80.246.139.154	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	194
109.253.156.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	168
109.253.137.72	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	152
46.121.103.245	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	149
130.226.228.12	Denmark	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 130.226.228.12	Block	141
176.12.138.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	109
46.19.85.88	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	105
46.19.85.136	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.136	Block	104
109.253.143.174	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	78
37.26.148.157	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	69
46.121.103.245	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	58
109.253.136.100	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	55
109.253.156.6	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	54
94.230.89.123	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 94.230.89.123	Block	52
2.54.6.215	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	51
109.253.147.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	43
109.253.140.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	41
46.19.85.121	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	35
109.253.159.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	34
184.74.50.54	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 184.74.50.54	Block	32
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	32
46.19.86.190	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	31
207.46.13.124	United States	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 207.46.13.124	Block	30
109.253.134.135	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	29
95.86.115.58	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	29
46.19.85.142	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	29
46.19.86.28	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	27
109.253.142.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	26
213.57.63.183	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.57.63.183	Block	23
31.168.197.238	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	21
66.249.78.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	20
80.246.130.143	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	19
2.54.48.62	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	18
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	17
79.183.51.95	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.183.51.95	Block	17