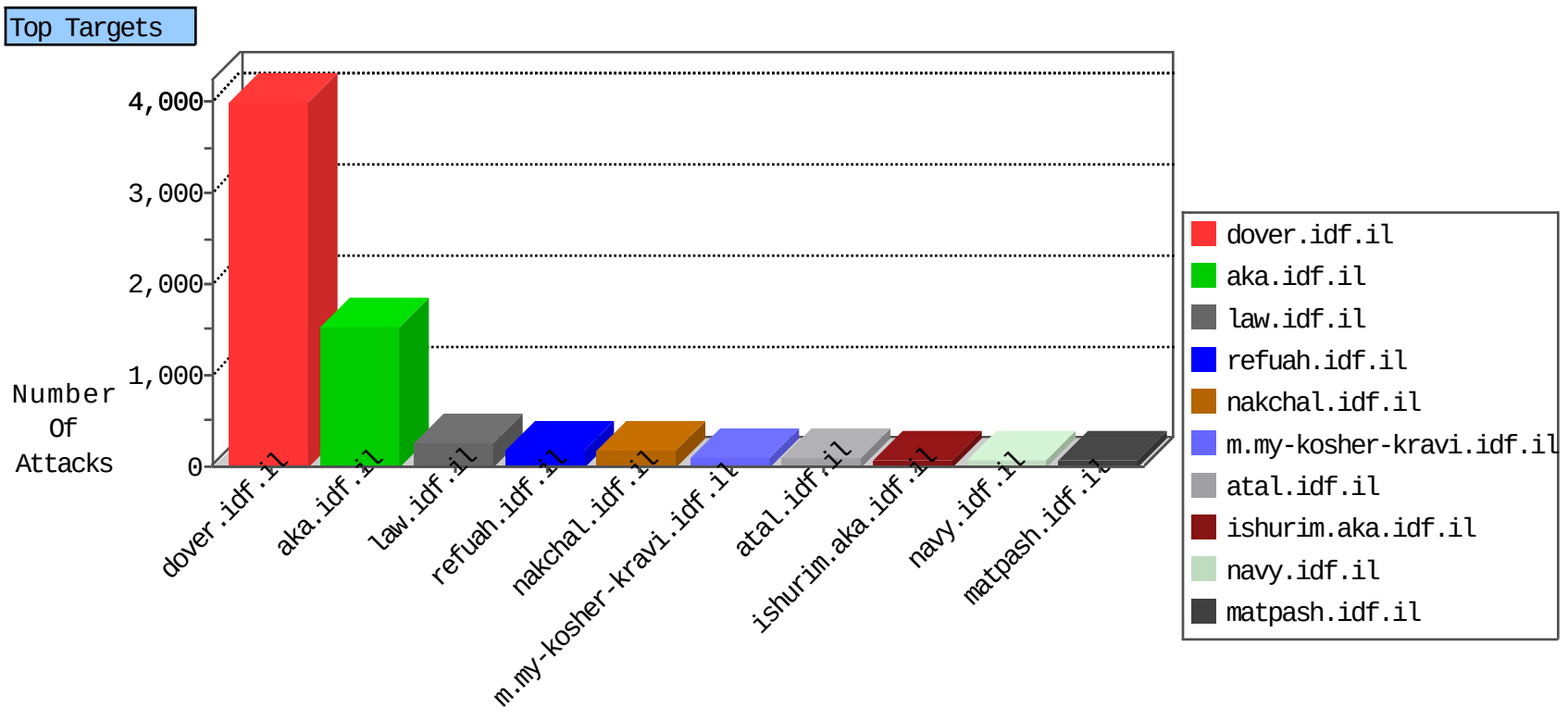
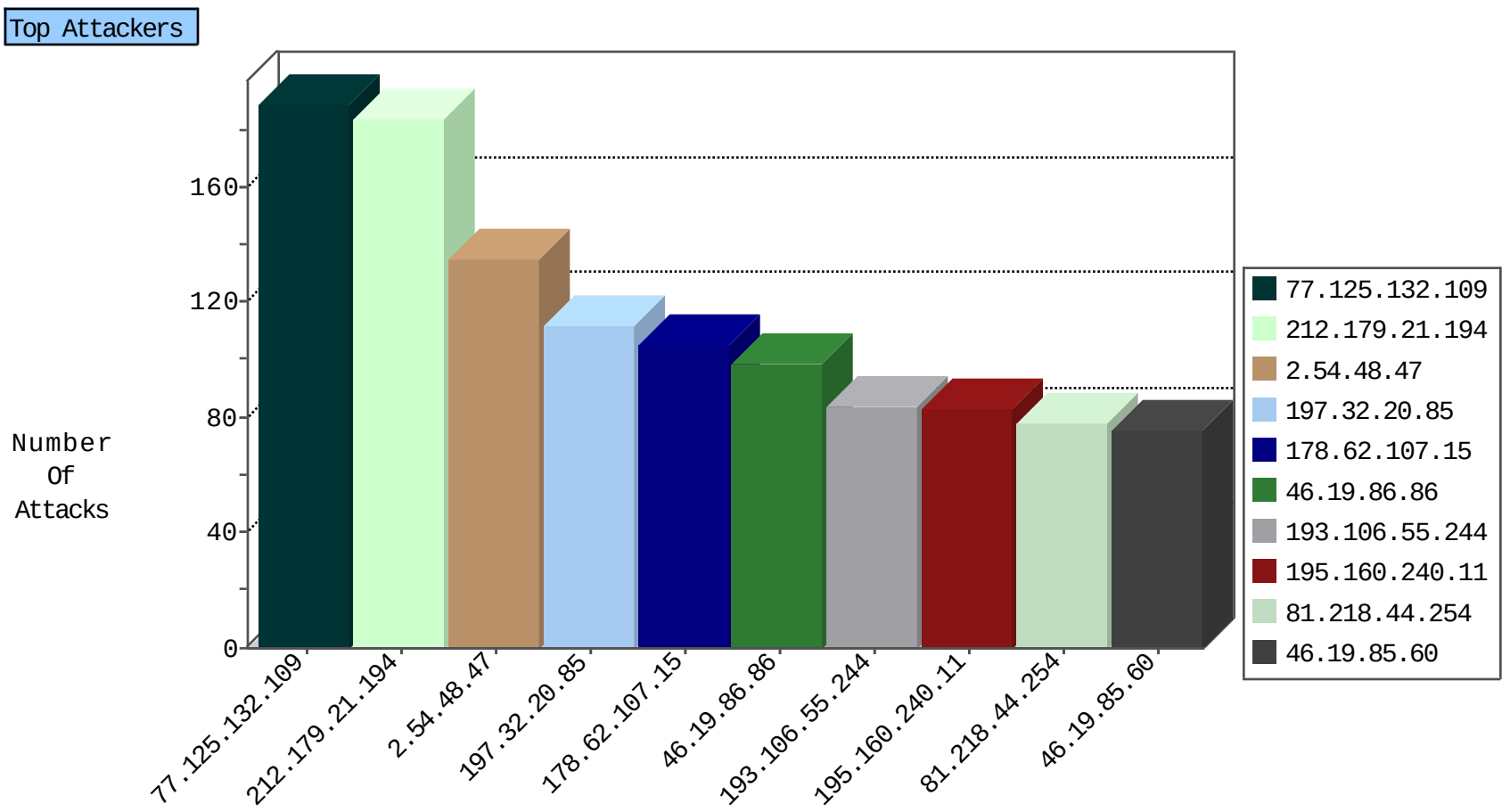
10-28-2015-15:04:02 to 10-28-2015-16:04:02

IDF Under Attack Daily Report





10-28-2015-15:04:02 to 10-28-2015-16:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.73	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6444
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4353
66.249.67.194	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3372
66.249.64.156	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	2355
145.83.2.6	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2180
68.180.230.240	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1845
66.249.64.161	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	1492
37.26.146.144	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1432
66.249.78.234	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1401
197.32.20.85	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1302
66.249.64.151	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	1266
50.201.138.211	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1101
66.249.78.173	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1101
66.249.67.210	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	969
66.249.67.216	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	838
157.55.39.41	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	578
66.249.67.79	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	540
66.249.67.224	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	450
68.180.228.112	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	321
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	310
108.162.13.146	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	293
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	279
178.62.107.15	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	276
37.26.148.166	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	221
66.102.8.173	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	123
66.249.67.202	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	82
82.80.41.234	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	73
66.249.78.159	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	52
194.90.89.245	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	35
46.19.86.67	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	32
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	29
134.191.232.71	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	27
46.121.202.44	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
2.54.52.223	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
109.65.51.172	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	24
176.12.137.226	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
31.154.18.65	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
77.125.132.109	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
176.13.12.99	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
46.19.86.67	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	14
46.19.85.44	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
2.52.23.141	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
192.115.83.5	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
2.52.57.196	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
79.180.152.204	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
82.80.219.164	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
195.160.240.11	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
2.52.148.235	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
93.173.245.197	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
82.166.22.82	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7

10-28-2015-15:04:02 to 10-28-2015-16:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
23.91.70.77	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	18
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
194.90.89.245	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

10-28-2015-15:04:02 to 10-28-2015-16:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
23.91.70.77	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	27
176.106.227.174	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.213	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
125.65.165.215	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
125.65.165.215	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
87.69.41.177	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.161.82	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.64.149.201	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.60.241	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.108.25.49	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.60.30	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.178.137.3	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
194.90.34.226	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
78.175.203.42	147.237.72.14	Turkey	dover.idf.il(old	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
190.59.13.241	147.237.0.19	Trinidad and Tobago	madim.atal.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.120.104.233	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.8.91	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.61	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
125.65.165.215	147.237.76.38	China	e.e.meitav.idf.i	ET SCAN Potential SSH Scan	1
37.26.148.238	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.122.169	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.174.189	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.50.2	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.132.248	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.228.11.98	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.89.137.3	147.237.76.34	China	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
2.52.143.205	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.201.224	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
79.177.43.33	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
190.128.136.222	147.237.77.170	Paraguay	maarachot.idf.il	ET SCAN Potential SSH Scan	1
46.121.115.27	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

10-28-2015-15:04:02 to 10-28-2015-16:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.125.132.109	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	180
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	140
197.32.20.85	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	107
46.19.86.86	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	95
178.62.107.15	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	95
193.106.55.244	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	75
46.19.86.15	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	74
37.26.146.144	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
195.160.240.11	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
46.19.85.60	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
80.179.20.132	Israel	147.237.76.42	refuah.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	57
79.177.187.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
176.13.2.136	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
195.226.71.212	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
37.142.123.143	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	35
109.29.249.20	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
62.219.234.175	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
2.54.48.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
37.142.113.193	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	27
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
85.250.241.206	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
2.54.43.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
100.100.44.62		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	26
79.178.179.239	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
64.233.172.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
66.249.78.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
66.249.78.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
46.19.86.212	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
213.57.126.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
79.182.101.50	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
176.13.12.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
100.100.33.111		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
134.191.232.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
2.54.137.36	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
37.142.230.166	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
37.75.211.208	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
37.142.121.242	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
5.28.175.214	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
149.88.237.134	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
2.54.52.223	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12

10-28-2015-15:04:02 to 10-28-2015-16:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.48.47	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	105
81.218.44.254	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	75
80.246.130.183	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	73
157.55.39.208	United States	147.237.77.74	law.idf.il	Distributed Suspicious Response Code	Block	60
192.118.64.29	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	60
74.66.134.223	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	45
176.13.4.7	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Double URL Encoding from 176.13.4.7	Block	45
194.90.89.245	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 194.90.89.245	Block	30
37.75.211.208	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	30
194.90.89.245	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	30
37.26.146.188	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	30
80.246.139.54	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	30
79.179.97.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	30
147.236.38.29	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	30
188.120.152.210	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	30
77.125.87.117	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	30
37.26.148.166	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	30
82.80.219.164	Israel	147.237.76.31	nakchal.idf.il	Distributed Suspicious Response Code	Block	30
2.52.181.58	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	30
46.19.86.213	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eof	Block	30
80.246.133.4	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	30
79.177.187.71	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	30
66.249.67.216	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	15
31.184.238.103	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/894-he/chinuch.aspx	Block	15
79.180.199.70	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	15
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	15
2.54.29.146	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	15
77.237.138.202	Czech Republic	147.237.77.176	matpash.idf.il	Unauthorized URL Access to /	Block	15
66.249.78.81	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/style/shared/layoutdev.css	Block	15
46.117.70.225	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	15
89.139.12.229	Israel	147.237.0.15	kosher-kravi.idf.il	Distributed Suspicious Response Code	Block	15
80.246.137.179	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
66.249.69.47	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/shared/usercontrols/headerupper/	Block	15
207.46.13.137	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	15
5.29.248.12	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$txtPassword in www.aka.idf.il/main/giyus/faq.aspx	None	15
79.178.186.245	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	15
66.249.67.192	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il/sip_storage/files/6/×©×§×•×¤×™×ª 10	Block	15
184.105.139.68	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	15
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.6	Block	15
142.54.187.44	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.cloud.ph/	Block	15
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	15
46.19.85.216	Israel	147.237.76.31	nakchal.idf.il	Distributed Illegal HTTP Version	Block	15
82.166.228.10	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	15
66.249.75.110	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/watercrafts.aspx	Block	15
66.249.67.224	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/www.navy.idf.il	Block	15
79.182.112.166	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	15
66.249.67.79	Israel	147.237.77.74	law.idf.il	Distributed Suspicious Response Code	Block	15
2.54.43.239	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 2.54.43.239 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	15
77.237.138.202	Czech Republic	147.237.77.233	atal.idf.il	Unauthorized URL Access to /	Block	15
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/april/1.	Block	15

10-28-2015-15:04:02 to 10-28-2015-16:04:02