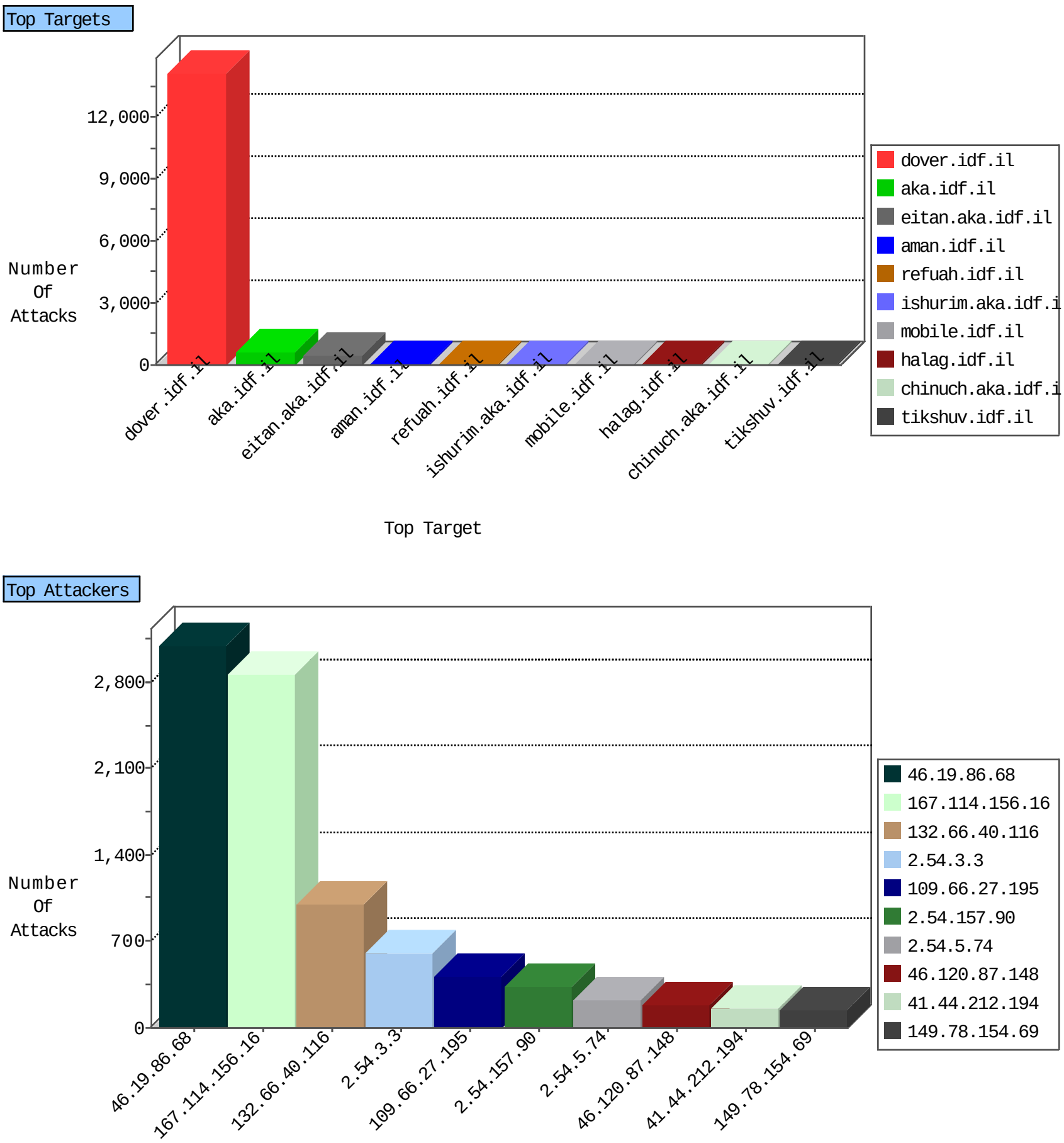
11-02-2015-19:04:02 to 11-02-2015-20:04:02

IDF Under Attack Daily Report



11-02-2015-19:04:02 to 11-02-2015-20:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3844
66.249.67.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	554
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	141
46.19.85.144	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	46
46.19.86.138	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	34
85.64.149.235	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
79.178.148.117	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	29
46.121.137.58	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	29
31.154.163.108	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
176.13.22.144	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	24
82.145.209.207	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	20
149.78.40.139	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	19
66.249.67.34	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	16
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	15
76.21.178.0	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	15
5.29.67.203	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	14
46.120.87.148	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
66.249.64.191	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	13
46.19.86.138	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
5.22.129.242	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
37.26.148.188	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
176.12.145.32	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
5.22.130.178	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
212.76.121.206	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
89.138.245.255	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
85.65.50.250	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
37.26.148.212	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
109.67.49.17	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.178.165.188	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.59.119.248	Russian Federation	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
5.28.129.119	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
85.250.145.44	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
192.117.129.216	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.85.28	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
79.182.193.40	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
176.59.119.248	Russian Federation	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
176.12.140.118	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
35.2.157.164	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
77.246.15.39	Italy	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.86.173	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
5.22.129.166	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
213.151.54.59	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
5.29.68.169	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
172.56.6.113	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
31.154.164.216	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.12.147.188	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
31.154.91.39	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
185.32.179.177	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
176.12.141.36	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2

11-02-2015-19:04:02 to 11-02-2015-20:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.179.55.49	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
95.86.103.148	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
146.66.172.10	Russian Federation	147.237.77.216	dover.idf.il	15323: HTTP: User-Agent (MRSPUTNIK)	Block	1

11-02-2015-19:04:02 to 11-02-2015-20:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	3
66.249.64.186	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.208	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
2.54.3.3	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.12.202.110	147.237.8.45	Ukraine	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.98	147.237.72.14	United States	dover.idf.il(old)	ET DROP Dshield Block Listed Source	1
59.45.79.117	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
197.245.167.175	147.237.72.14	South Africa	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
173.1.121.85	147.237.76.86	United States	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
123.151.149.222	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
85.250.145.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.150.22	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.164.216	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.31.78	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
217.12.202.110	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
197.245.167.175	147.237.72.167	South Africa	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
96.225.47.128	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
85.108.130.21	147.237.0.34	Turkey	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
37.26.146.164	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.39.222.253	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1

11-02-2015-19:04:02 to 11-02-2015-20:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.68	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3105
132.66.40.116	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1000
2.54.3.3	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	605
2.54.157.90	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	340
109.66.27.195	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	312
2.54.5.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	228
46.120.87.148	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	162
41.44.212.194	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	153
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	149
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	124
80.179.9.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	110
82.102.169.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	101
80.179.9.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	93
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	92
213.57.138.34	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	89
46.19.85.144	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
85.65.74.148	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	80
212.68.153.97	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	74
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
46.19.86.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
109.64.161.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
2.52.26.143	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
176.13.22.144	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
82.166.22.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
173.255.225.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
185.120.126.40		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
86.85.187.97	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
197.134.80.204	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
154.5.208.43	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
66.249.78.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
46.19.85.24	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
38.112.184.50	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
217.103.108.229	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
85.250.145.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
151.80.31.112	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
109.64.121.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
84.110.35.29	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
66.249.78.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
66.249.84.165	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
100.100.58.161		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	25
176.59.119.248	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
173.220.141.227	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25

11-02-2015-19:04:02 to 11-02-2015-20:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.66.27.195	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	103
185.24.78.65	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	9
185.24.78.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	9
185.24.78.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	9
5.29.46.63	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	4
37.26.149.181	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
85.250.121.164	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	4
46.120.87.148	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtStreet in madim.atal.idf.il/1088-he/meretz.aspx	Block	4
5.29.46.63	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	4
5.29.46.63	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	4
176.13.1.252	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 176.13.1.252	Block	4
85.250.121.164	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	4
176.12.144.77	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
85.250.216.136	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	3
85.250.216.136	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	3
85.250.216.136	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
79.178.14.47	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
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	2
82.81.25.167	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
176.12.143.157	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
5.28.160.109	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
79.178.14.47	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
82.81.25.167	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
79.178.14.47	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	2
82.81.25.167	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	2
176.13.1.252	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	1
96.245.167.229	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.idf.il/1038-en/dover.aspx	Block	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/smalim/showbig.aspx	Block	1
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 106 cookies	Block	1
87.68.25.227	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/givyus/	Block	1
188.221.8.132	United Kingdom	147.237.76.42	refuah.idf.il	Abnormally Long Request method	Block	1
2.52.52.9	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.177.29.120	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 79.177.29.120	Block	1
93.172.159.41	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	1
188.221.8.132	United Kingdom	147.237.76.42	refuah.idf.il	Malformed URL t.â€¦â,ªÂ´Â¿Ö±Ë†nz3Ö±g×©×ƒ6Â°Ã¿â€š ×¡×¦Ö¶oÖµ×£fÂ?â„¢Â¨eÂ¡â,¬[[#26]]=×Ÿ×˜<Ö³[[#16]]×ž Â¶[[#25]]LÃŠ[[#17]]Â¸â,¬Ã¼	Block	1
5.29.108.171	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.106.227.11	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
79.183.225.100	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
77.126.10.88	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
109.64.60.233	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ...3&sideScroll in www.aka.idf.il/giyus/kadatz/	None	1
87.68.254.48	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	1
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
213.57.241.199	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
84.111.13.154	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
37.142.64.136	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1
188.221.8.132	United Kingdom	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Method Â¬[[#0]][[#0]][[#0]]BÂ¦ Â•Ã?Ã€bXdÃ¯MRÃ¬Ã¾nÂ?Ã?Â¬Â£[[#27]]Â?{tÃ‡ ^Ã?[[#5]]Â§*Ã³ÃµÂ¦pÂ±\Ã¯Ã€Âœ"Ã³[[#14]]Â¸Â¿Â–[[#22]]Â′ Ã´IÂ¹@RÂƒÃ±Ã„bEÃ–Â…Â¸Ã•	Block	1
79.177.29.120	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1

11-02-2015-19:04:02 to 11-02-2015-20:04:02