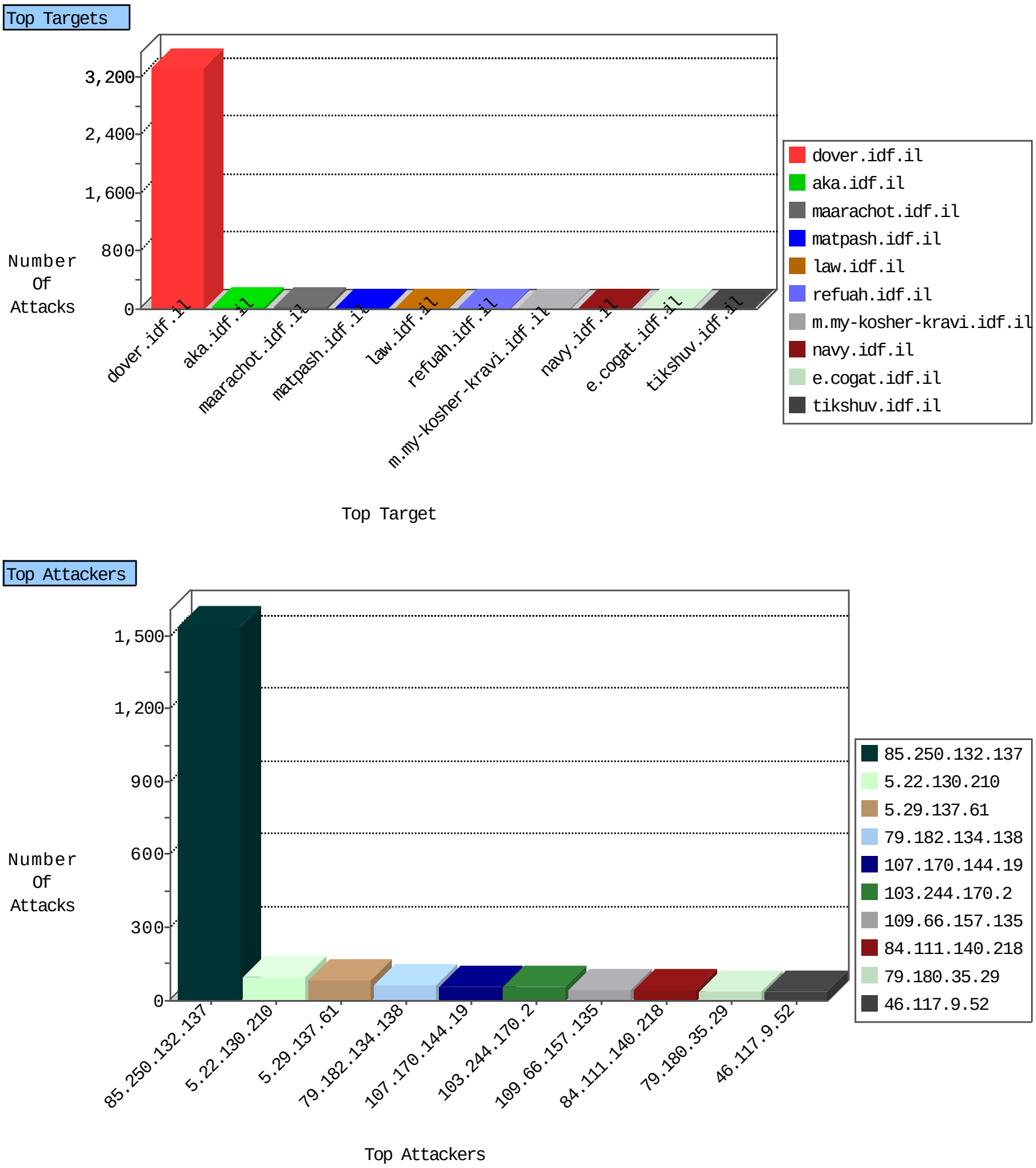
04-18-2015-09:03:02 to 04-18-2015-10:03:02

IDF Under Attack
04-18-2015-09:03:02



04-18-2015-09:03:02 to 04-18-2015-10:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.101	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	3032
192.3.194.138	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
204.42.253.132	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
209.88.157.240	Israel	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1

04-18-2015-09:03:02 to 04-18-2015-10:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
71.6.167.142	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	2
188.138.9.50	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	2
87.69.225.116	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
71.6.165.200	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
5.28.157.246	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1

04-18-2015-09:03:02 to 04-18-2015-10:03:02

Top Attackers In IDS

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	26
66.249.67.40	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	14
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
66.249.78.197	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.30	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.81.201	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.81	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.32	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
2.52.45.239	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
221.235.188.212	China	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
115.238.246.186	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
202.71.25.29	India	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
173.208.188.250	United States	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
37.220.34.55	Netherlands	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
115.238.246.186	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
109.253.128.66	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
221.235.188.212	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
202.71.25.29	India	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
58.20.54.249	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
202.71.25.29	India	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -f -sS	1
58.20.54.249	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
173.208.188.250	United States	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
58.20.54.249	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
173.208.188.250	United States	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1

04-18-2015-09:03:02 to 04-18-2015-10:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
85.250.132.137	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1541
5.22.130.210	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	97
5.29.137.61	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	84
79.182.134.138	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	63
107.170.144.19	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	55
103.244.170.2	India	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50
109.66.157.135	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	46
84.111.140.218	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	43
79.180.35.29	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
46.117.9.52	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
84.229.174.125	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
79.178.111.175	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
93.173.230.47	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
151.236.176.75	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
80.110.120.121	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
37.26.147.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
109.160.237.200	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
109.253.141.176	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
31.25.77.53	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
46.19.85.110	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
31.25.77.53	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
79.178.118.145	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
149.78.232.51	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
46.19.85.110	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
79.182.163.20	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
119.73.253.5	Singapore	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
46.19.86.16	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
2.54.31.85	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
2.54.63.48	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
82.205.13.71	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
220.255.1.92	Singapore	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
204.237.22.235	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
66.249.64.74	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
185.6.57.75	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
136.243.36.88	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
172.11.130.137	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
192.114.91.230	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
46.244.95.228	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
46.116.172.158	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
77.127.246.113	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
220.255.1.29	Singapore	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
185.6.57.75	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
220.255.1.66	Singapore	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	3
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	3
41.79.76.33	South Africa	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
198.46.82.210	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	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
212.113.132.65	United Kingdom	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
41.79.76.33	South Africa	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	2
37.187.131.50	France	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
198.46.149.165	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
66.249.73.203	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	2
198.46.82.210	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
50.87.119.130	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
162.253.145.121	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
66.249.73.211	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	2
198.46.82.210	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
69.12.89.164	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
212.113.132.65	United Kingdom	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
66.249.64.59	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.22.130.173	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	1
180.76.4.144	China	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on 147.237.77.176//	Block	1
125.65.81.124	China	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/feburary/23.stm	Block	1
41.79.76.33	South Africa	147.237.77.170	maarachot.idf.il	Distributed Admin Blocking	Block	1
157.55.39.130	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
37.187.131.50	France	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
180.252.62.126	Indonesia	147.237.77.74	law.idf.il	Unknown HTTP Request Method COOK in URL www.law.idf.il/14-en/patzar.aspx	Block	1
136.243.36.88	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 136.243.36.88	Block	1
198.46.149.165	United States	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/chinuch	Block	1
78.111.186.212	Ukraine	147.237.77.74	law.idf.il	Distributed Unknown HTTP Request Method	Block	1
66.249.67.49	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
198.46.82.210	United States	147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	1
155.94.254.143		147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
50.87.119.130	United States	147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	1
162.253.145.121	United States	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
81.218.2.118	Israel	147.237.72.166	aka.idf.il	Unknown Parameter isTaz in www.aka.idf.il/main/sachar/	None	1
41.79.76.33	South Africa	147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	1
157.55.39.5	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/toolfs.asp	Block	1
203.133.168.157	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0115-1.stm	Block	1
109.253.156.140	Israel	147.237.72.166	aka.idf.il	Unknown Parameter isTaz in aka.idf.il/main/sachar/	None	1