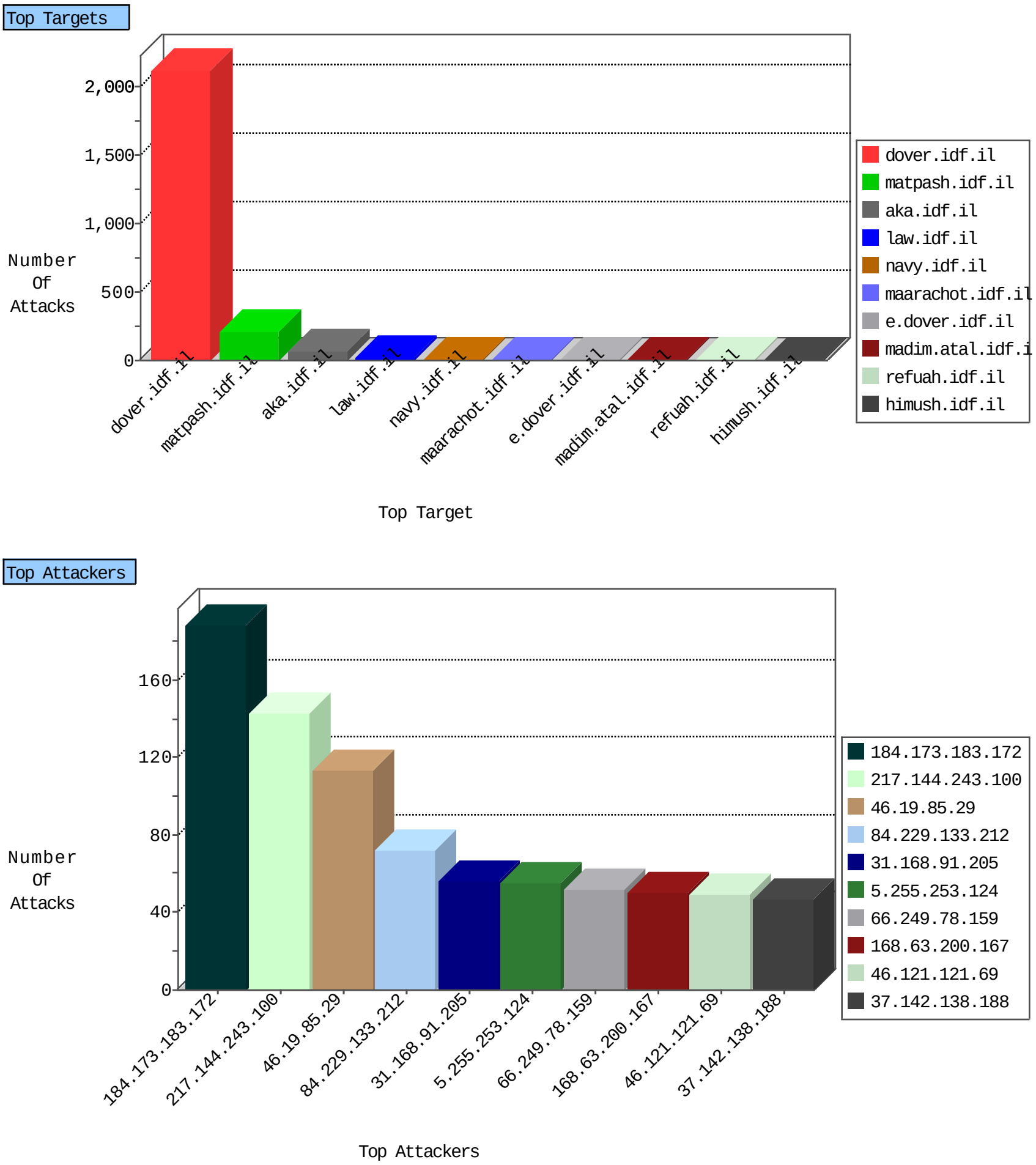
04-18-2015-10:03:03 to 04-18-2015-11:03:03

IDF Under Attack
04-18-2015-10:03:03



04-18-2015-10:03:03 to 04-18-2015-11:03:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.67.32	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	467
134.147.203.115	Germany	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	2
85.25.103.50	Germany	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
107.154.64.10	United States	147.237.76.42	refuah.idf.il	L4 Source or Dest Port Zero	drop	1
81.218.77.162	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	1

04-18-2015-10:03:03 to 04-18-2015-11:03:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	189
217.253.92.21	Germany	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
85.25.103.50	Germany	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
46.116.235.127	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.176	test.ncore.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
66.240.192.138	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.201	e.atal.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
198.20.69.98	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1

04-18-2015-10:03:03 to 04-18-2015-11:03:03

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	6
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	6
66.249.78.197	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	4
66.249.78.204	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.190	United States	147.237.77.176	matpash.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
81.218.77.162	Israel	147.237.77.176	matpash.idf.il	GPL SCAN nmap TCP	2
66.249.73.203	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
176.97.40.227	Russian Federation	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
176.97.40.227	Russian Federation	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
176.97.40.227	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	1
104.167.96.44		147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.65	China	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
82.214.114.5	Macedonia, the Former Yugoslav Republic of	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 3072	1
82.214.114.5	Macedonia, the Former Yugoslav Republic of	147.237.0.200	m4u.idf.il	ET SCAN NMAP -f -sS	1
81.200.91.2	Russian Federation	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
176.97.40.227	Russian Federation	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
176.97.40.227	Russian Federation	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
104.167.96.44		147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.65	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
94.77.237.230	Saudi Arabia	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
82.214.114.5	Macedonia, the Former Yugoslav Republic of	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 2048	1
81.200.91.2	Russian Federation	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 3072	1

04-18-2015-10:03:03 to 04-18-2015-11:03:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
217.144.243.100	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	143
46.19.85.29	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	114
84.229.133.212	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	72
31.168.91.205	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	56
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	53
46.121.121.69	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	49
37.142.138.188	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
84.211.16.251	Norway	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	44
85.65.36.232	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
168.63.200.167	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
80.246.141.53	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
84.109.31.191	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
2.52.12.210	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
176.12.148.4	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
89.138.244.85	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
46.120.232.147	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
109.253.143.56	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
85.64.146.246	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
108.59.253.71	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
85.64.119.198	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
109.253.130.183	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
46.19.86.106	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
109.253.134.234	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
46.121.64.181	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
188.120.136.56	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
176.12.151.43	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
2.54.37.70	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
109.253.141.62	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
136.243.36.88	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
5.22.130.146	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
109.253.131.172	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
46.116.235.127	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
46.117.215.214	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
84.109.85.198	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
149.88.103.158	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
66.249.78.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
168.63.200.167	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
176.12.137.156	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
37.8.55.216	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
66.249.64.72	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
94.77.237.230	Saudi Arabia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
66.249.78.159	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
109.66.179.134	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	8
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	7
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	5
178.60.205.53	Spain	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
80.246.141.53	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
198.1.96.30	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	2
37.187.50.84	France	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
66.249.64.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
80.246.130.215	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1110-8.stm	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
195.154.56.130	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/rk=0/rs=x2jlhjdlx2rzpg0dwhxkqu0n_fm-	Block	1
66.249.64.69	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1235-he/atal.aspx	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
62.141.38.154	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
69.171.112.117	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
66.249.78.87	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
217.253.92.21	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.59	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/edim/yoman/enlarge.asp	Block	1
180.76.4.22	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
37.26.147.150	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/hebrew/ie-welcome.stm	Block	1
198.1.96.30	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	1
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.20	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/x©x§x•x¤x™xª 10	Block	1
157.55.39.178	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
2.54.20.33	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/templates/sendtofriend/sendtofriend.aspx	Block	1
66.249.64.61	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/brothers/news/	Block	1
184.105.247.196	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
85.114.96.61	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
37.26.147.162	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/kapatz/citizencontact.aspx	None	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.67.120	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
66.249.64.28	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/scriptresource.axd	Block	1
176.12.148.138	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
5.22.129.157	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
77.125.110.150	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/l	Block	1
188.143.232.62	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.64.63	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sachar/forms/downloadform.asp	Block	1
95.173.171.236	Turkey	147.237.76.30	himush.idf.il	Illegal HTTP Version	Block	1
37.187.50.84	France	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
207.46.13.104	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.73.203	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
66.249.64.59	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
178.60.205.53	Spain	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
79.183.8.69	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	1
192.99.39.235	Canada	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1