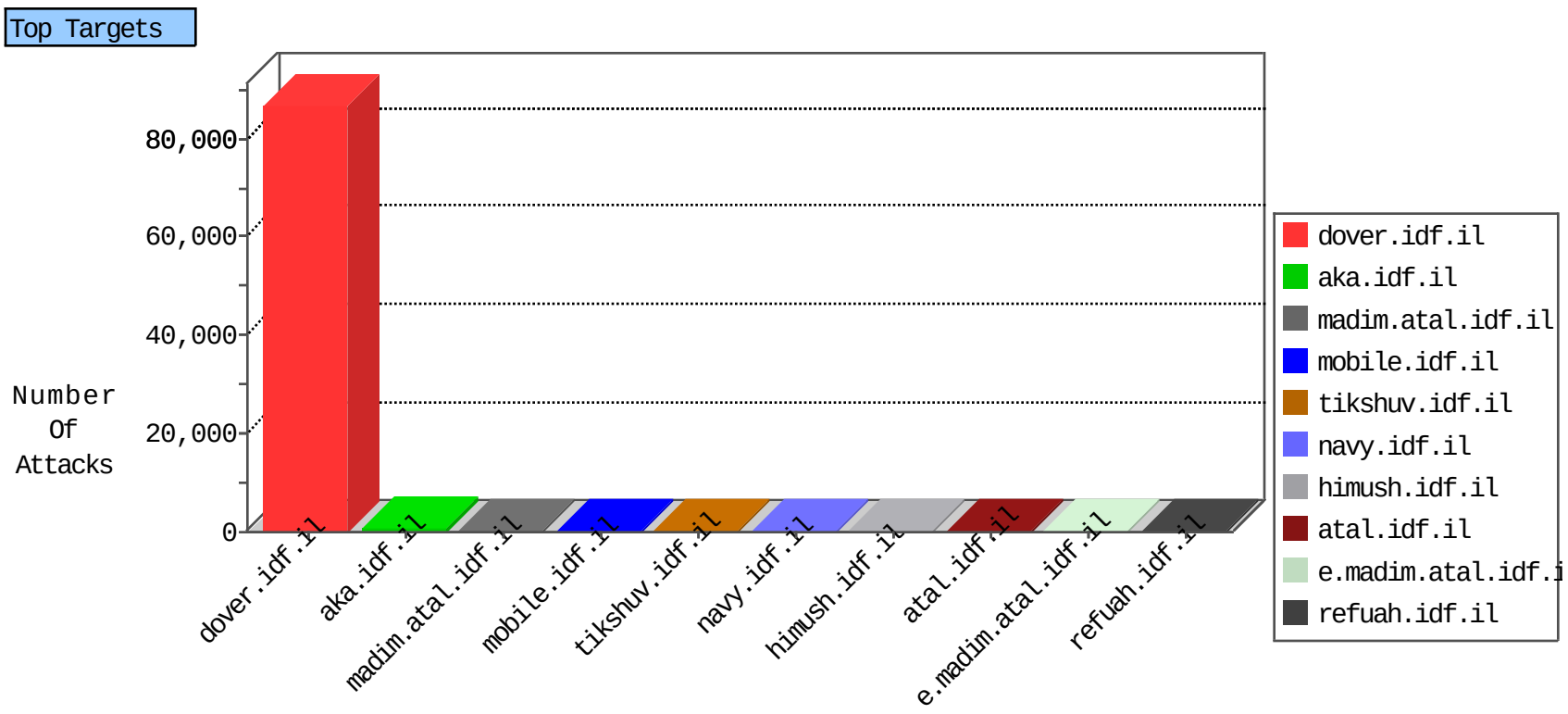
04-09-2016-18:04:04 to 04-09-2016-19:04:04

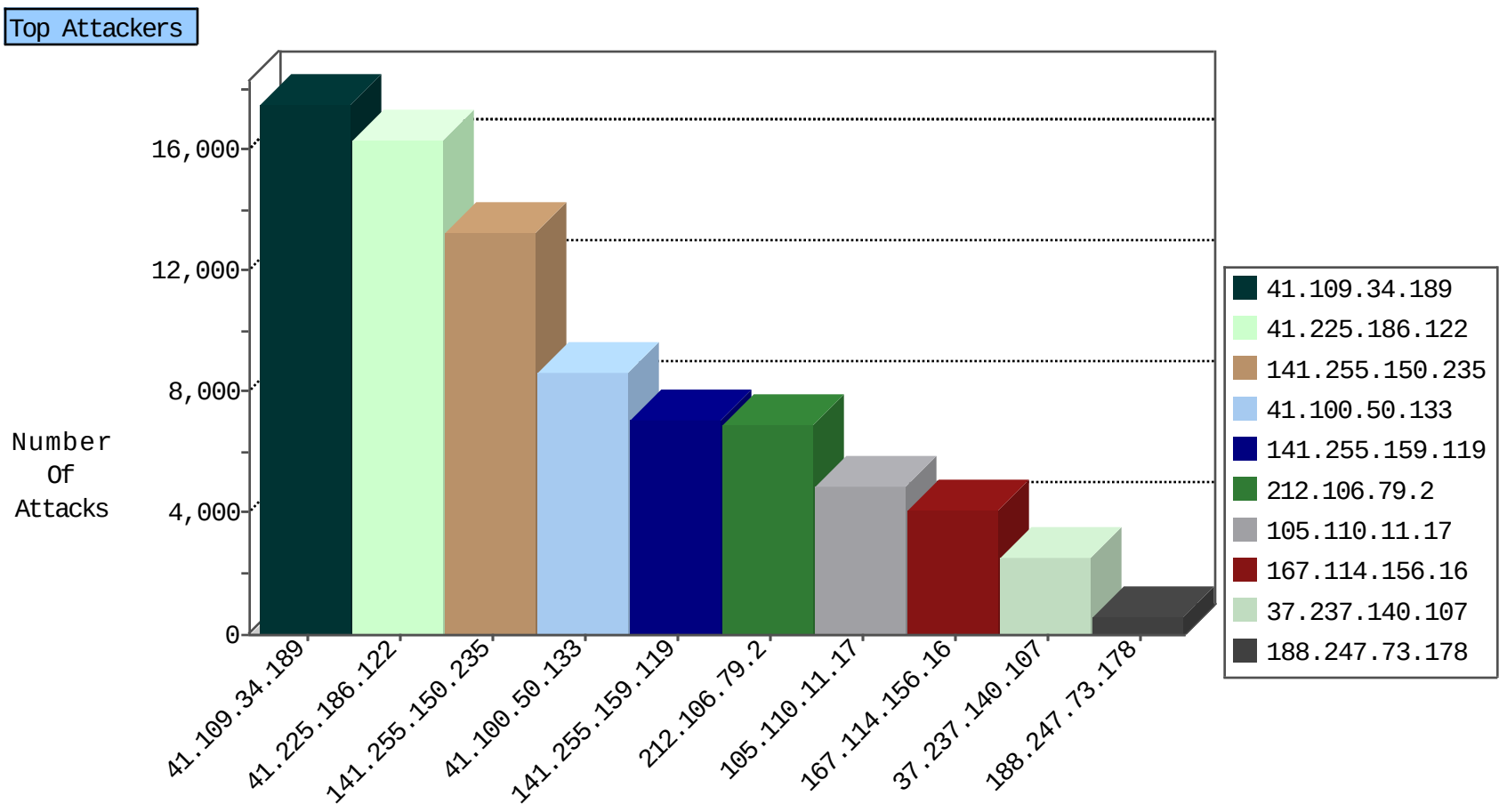
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

04-09-2016-18:04:04 to 04-09-2016-19:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
141.255.159.119	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	57054
41.109.34.189	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4601
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4064
105.110.11.17	Algeria	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	3963
80.255.4.76	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3295
37.106.143.122	Saudi Arabia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3217
197.0.79.194	Tunisia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1617
41.251.130.235	Morocco	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1453
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1387
178.39.218.11	Switzerland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1213
41.109.34.189	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1058
141.255.150.235	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	903
41.102.216.56	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	845
188.138.9.49	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	754
41.105.128.15	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	479
141.255.159.119	Netherlands	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	235
41.140.138.50	Morocco	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	225
157.55.39.65	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	197
212.106.79.2	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	93
105.110.11.17	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	93
188.247.73.178	Jordan	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	79
37.238.144.63	Iraq	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	30
37.237.140.107	Iraq	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	18
41.100.50.133	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	16
176.13.2.82	Israel	147.237.72.166	aka.idf.il	network flood IPv4 TCP-RST	drop	7
123.59.59.52	China	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	4
41.107.97.131	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
37.238.144.63	Iraq	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
37.237.140.16	Iraq	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
89.248.160.138	Netherlands	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1
37.238.144.63	Iraq	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	1
209.126.127.17	United States	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
123.151.42.61	China	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1
89.248.160.138	Netherlands	147.237.77.61	e.cogat.idf.il	Block_Ntp_All_Net	drop	1
188.247.72.73	Jordan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
156.203.4.82	Egypt	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	1
107.77.106.26	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
89.248.160.138	Netherlands	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
50.116.30.23	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
107.168.70.162	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-09-2016-18:04:04 to 04-09-2016-19:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	Block	20
79.180.7.56	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	13
80.255.4.76	Germany	147.237.77.216	dover.idf.il	C1000133: HTTP: Opisrael 2015 - key words and groups	Block	12
79.176.72.189	Israel	147.237.77.216	dover.idf.il	C1000133: HTTP: Opisrael 2015 - key words and groups	Block	12
107.168.70.162	Japan	147.237.77.216	dover.idf.il	C1000133: HTTP: Opisrael 2015 - key words and groups	Block	4
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
2.54.149.61	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
87.69.225.219	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
188.138.9.49	Germany	147.237.77.216	dover.idf.il	10725: TCP: LOIC DDoS Tool	Block	2
141.255.159.119	Netherlands	147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-09-2016-18:04:04 to 04-09-2016-19:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
90.231.228.209	147.237.77.216	Sweden	dover.idf.il	ET WEB_SERVER LOIC Javascript DDoS Inbound	6
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
41.107.31.16	147.237.77.216	Algeria	dover.idf.il	SERVER-IIS multiple extension code execution attempt	2
41.107.31.16	147.237.77.216	Algeria	dover.idf.il	ET WEB_SERVER Possible Microsoft Internet Information Services (IIS) .asp Filename Extension Parsing File Upload Security Bypass Attempt (asp)	2
37.26.149.146	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
41.107.31.16	147.237.77.216	Algeria	dover.idf.il	SERVER-IIS Microsoft Windows IIS 6 multiple executable extension access attempt	2
174.37.194.144	147.237.8.27	United States	e.madim.atal.idf.i	ET SCAN NMAP -sA (2)	2
89.219.32.195	147.237.76.30	Kazakstan	himush.idf.il	ET WEB_SERVER Poison Null Byte	1
80.82.78.38	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
183.61.109.189	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -sS window 4096	1
183.61.109.189	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -f -sS	1
174.37.194.144	147.237.8.27	United States	e.madim.atal.idf.i	ET SCAN NMAP -sS window 3072	1
125.27.61.96	147.237.76.34	Thailand	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
114.199.230.194	147.237.77.235	Korea, Republic of	sviva.idf.il	ET SCAN NMAP -f -sS	1
80.82.78.38	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
218.108.132.58	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
41.251.130.235	147.237.77.216	Morocco	dover.idf.il	SERVER-WEBAPP adminlogin access	1
183.61.109.189	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -sS window 2048	1
174.37.194.144	147.237.8.27	United States	e.madim.atal.idf.i	ET SCAN NMAP -sS window 4096	1
114.199.230.194	147.237.77.235	Korea, Republic of	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
104.128.144.131	147.237.76.86	Canada	navy.idf.il	ET SCAN NMAP -sS window 4096	1

04-09-2016-18:04:04 to 04-09-2016-19:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
141.255.150.235	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13199
41.225.186.122	Tunisia	147.237.77.216	dover.idf.i	Bad TCP sequence		monitor	10555
41.109.34.189	Algeria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8402
41.100.50.133	Algeria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8039
212.106.79.2	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6642
141.255.159.119	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6618
105.110.11.17	Algeria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4438
41.109.34.189	Algeria	147.237.77.216	dover.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	2963
41.225.186.122	Tunisia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	2469
37.237.140.107	Iraq	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1816
41.225.186.122	Tunisia	147.237.77.216	dover.idf.i	drop		drop	1597
41.109.34.189	Algeria	147.237.77.216	dover.idf.i	drop		drop	1112
41.225.186.122	Tunisia	147.237.77.216	dover.idf.i	Bad TCP sequence	Invalid ACK number	alert	822
41.225.186.122	Tunisia	147.237.77.216	dover.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	683
188.247.73.178	Jordan	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	495
41.100.50.133	Algeria	147.237.77.216	dover.idf.i	drop		drop	479
17.138.56.13	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	445
37.237.140.107	Iraq	147.237.77.216	dover.idf.i	drop		drop	414
192.168.173.102		147.237.77.216	dover.idf.i	Geo-location enforcement	Geo-location inbound enforcement	monitor	348
41.251.130.235	Morocco	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	329
79.181.11.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	189
212.106.79.2	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	drop		drop	150
41.109.34.189	Algeria	147.237.77.216	dover.idf.i	Bad TCP sequence	Invalid ACK number	monitor	139
41.109.34.189	Algeria	147.237.77.216	dover.idf.i	Bad TCP sequence		monitor	124
188.138.9.49	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	118
41.100.50.133	Algeria	147.237.77.216	dover.idf.i	Bad TCP sequence	Invalid ACK number	monitor	103
24.205.57.72	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	102
41.109.34.189	Algeria	147.237.77.216	dover.idf.i	Bad TCP sequence	Invalid ACK number	alert	97
37.237.140.107	Iraq	147.237.77.216	dover.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	97
37.237.140.107	Iraq	147.237.77.216	dover.idf.i	Bad TCP sequence	SYN retransmit with different window scale	alert	95
156.210.37.235	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	89
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	69
5.29.86.96	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	66
185.54.167.23	Iraq	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	65
109.67.228.35	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	60
107.77.106.26	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	57
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	56
220.181.132.194	China	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	53
45.35.64.142	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	46
79.181.214.137	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
212.199.182.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
84.94.191.141	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	41
101.199.108.50	China	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
41.109.43.180	Algeria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
37.237.140.107	Iraq	147.237.77.216	dover.idf.i	Bad TCP sequence	Invalid ACK number	alert	39
109.186.48.148	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	35
105.104.122.112	Algeria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	35
78.151.146.147	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
85.255.232.47	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34

04-09-2016-18:04:04 to 04-09-2016-19:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.27.105.99	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	332
37.26.149.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	110
37.26.148.202	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1129-he/dover.aspx	Block	24
46.19.85.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
41.251.130.235	Morocco	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.251.130.235	Block	12
41.107.31.16	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.107.31.16	Block	7
141.255.150.235	Netherlands	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 141.255.150.235	Block	6
41.251.130.235	Morocco	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 41.251.130.235	Block	5
37.26.146.148	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.52.155.59	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	3
2.53.60.250	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.142.72.86	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
213.57.226.144	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
141.0.14.147	Europe	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/english/php	Block	2
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx	Block	2
41.107.31.16	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/php	Block	2
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	2
2.52.155.59	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.52.155.59	Block	2
89.219.32.195	Kazakstan	147.237.76.30	himush.idf.il	Illegal Byte Code Character in Header Name [[#0]œ[[#0]]•[[#0]]/[[#0]]5À[[#18]][[#0]]	Block	1
66.249.65.217	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/scriptresource.axd	Block	1
31.13.113.65	Ireland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/php	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1153-12355-he/mmmmmmm=d50782ffmmmmmmm_d50782ff	Block	1
89.219.32.195	Kazakstan	147.237.76.30	himush.idf.il	Malformed URL ¸[[#20]]¸	Block	1
40.77.167.1	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/links.aspx	Block	1
197.116.103.181	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-ar	Block	1
149.78.23.55	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 149.78.23.55	Block	1
46.116.217.9	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
99.237.143.157	Canada	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/bamachane/	Block	1
89.219.32.195	Kazakstan	147.237.76.30	himush.idf.il	Illegal Byte Code Character in Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]]^^_i[[#22]]5fâÜþwxÓþv+bCJÈ2µ•[[#17]]Ò©‰¥K•š&[[#0]][[#0]][[#28]]À/À+À0À,À[[#19]]À	Block	1
37.236.190.8	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
217.78.57.193	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
31.13.113.80	Ireland	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
141.255.150.79	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
89.219.32.195	Kazakstan	147.237.76.30	himush.idf.il	NULL Character in Header Name at [[#0]œ[[#0]]•[[#0]]/[[#0]]5À[[#18]][[#0]]	Block	1
41.100.50.133	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
37.26.148.202	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.26.148.202	Block	1
207.46.13.41	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list7.htm	Block	1
87.69.205.224	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation searchText in www.atal.idf.il/994-he/atal.aspx	Block	1
66.220.145.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
157.55.39.108	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/misrot.aspx	Block	1
41.109.34.189	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
105.110.62.13	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
89.219.32.195	Kazakstan	147.237.76.30	himush.idf.il	Illegal Byte Code Character in URL ¸[[#20]]¸	Block	1
37.238.144.63	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
66.249.78.96	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
31.13.113.80	Ireland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	1
188.72.126.26	Germany	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	Block	1
41.251.130.235	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/admin/	Block	1
89.219.32.195	Kazakstan	147.237.76.30	himush.idf.il	NULL Character in Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]]^^_i[[#22]]5fâÜþwxÓþv+bCJÈ2µ•[[#17]]Ò©‰¥K•š&[[#0]][[#0]][[#28]]À/À+À0À,À[[#19]]À	Block	1
41.107.31.16	Algeria	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1

04-09-2016-18:04:04 to 04-09-2016-19:04:04