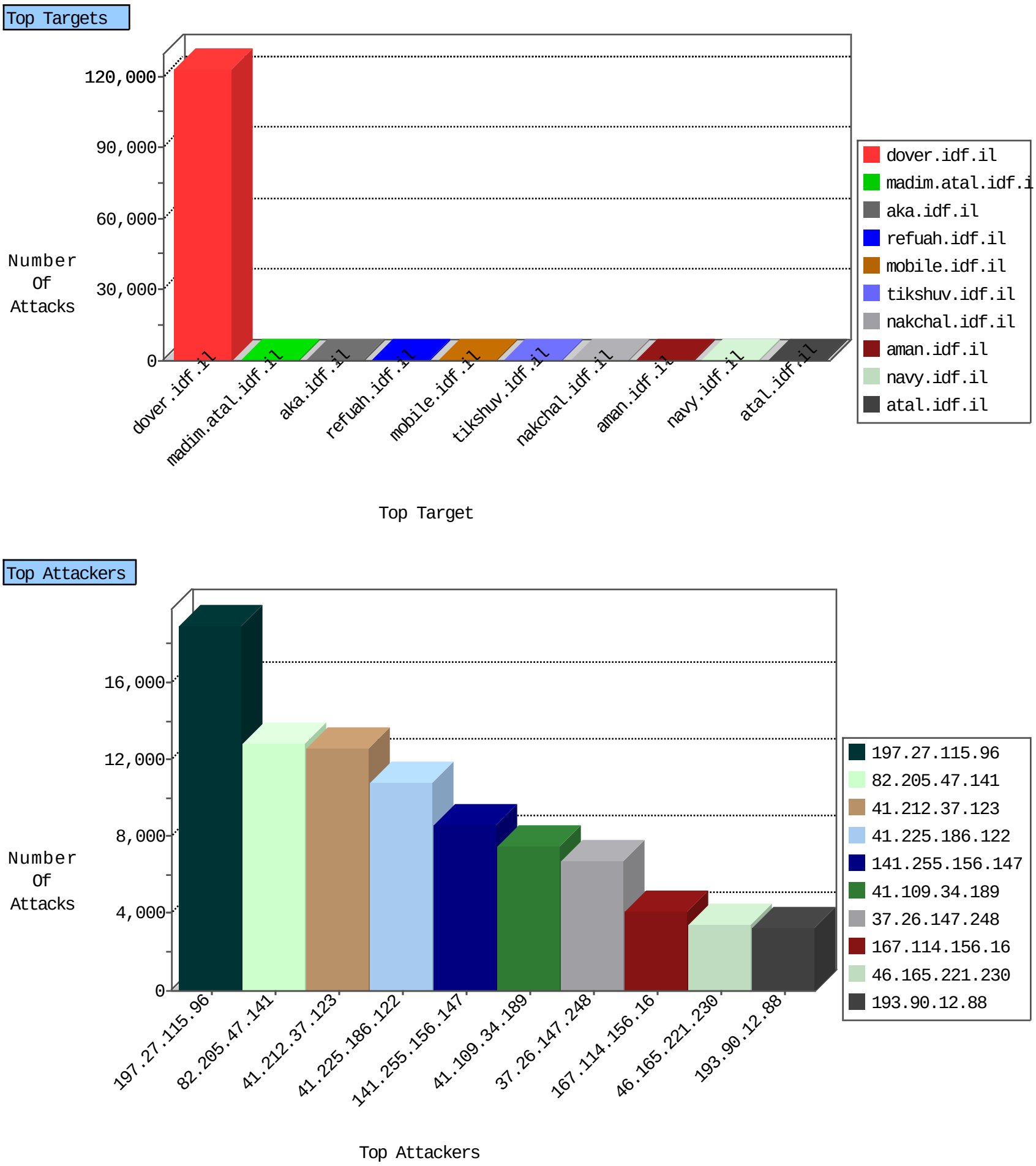
04-09-2016-19:04:01 to 04-09-2016-20:04:01

IDF Under Attack Daily Report



04-09-2016-19:04:01 to 04-09-2016-20:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
194.150.168.79	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8441
90.231.228.209	Sweden	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7889
41.109.34.189	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4966
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4128
65.19.167.131	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3841
46.19.85.79	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3782
176.10.104.243	Switzerland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3653
93.115.95.205	Anonymous Proxy	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3539
216.17.101.79	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3488
197.16.135.221	Tunisia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2941
105.157.81.32	Morocco	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2633
117.220.123.207	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2608
197.7.198.64	Tunisia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2036
197.27.115.96	Tunisia	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	1730
197.27.115.96	Tunisia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	842
41.140.138.50	Morocco	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	810
193.95.29.11	Tunisia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	756
176.10.99.201	Switzerland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	745
41.225.186.122	Tunisia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	738
141.255.156.147	Netherlands	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	472
37.236.190.8	Iraq	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	440
156.210.211.117	Egypt	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	233
41.232.63.102	Egypt	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	199
41.232.44.177	Egypt	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	198
41.212.37.123	Kenya	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	186
197.29.7.216	Tunisia	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	171
197.27.115.96	Tunisia	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	163
197.7.198.64	Tunisia	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	149
80.255.4.76	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	119
171.25.193.77	Sweden	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-dun	dest-reset	89
64.62.219.55	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	83
46.32.123.181	Jordan	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	66
46.165.221.230	Germany	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	58
193.90.12.88	Norway	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-dun	dest-reset	51
37.26.147.248	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	43
141.255.150.235	Netherlands	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	36
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	34
193.171.202.150	Austria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	26
46.121.108.159	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	25
84.108.190.72	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	14
149.78.154.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	14
197.29.7.216	Tunisia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	13
185.120.125.23	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	12
212.199.182.150	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
37.238.144.63	Iraq	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
149.78.65.41	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
5.102.253.6	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
213.57.197.181	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
84.111.6.199	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
46.19.86.136	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6

04-09-2016-19:04:01 to 04-09-2016-20:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.134.114.87	Spain	147.237.77.216	dover.idf.il	C1000133: HTTP: Opisrael 2015 - key words and groups	Block	12
109.67.62.225	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
197.7.198.64	Tunisia	147.237.77.216	dover.idf.il	C1000133: HTTP: Opisrael 2015 - key words and groups	Block	6
46.19.86.194	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	3
66.249.78.120	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
5.39.107.135	France	147.237.77.216	dover.idf.il	C1000133: HTTP: Opisrael 2015 - key words and groups	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
157.55.39.201	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
197.6.14.44	Tunisia	147.237.77.216	dover.idf.il	10725: TCP: LOIC DDoS Tool	Block	1

04-09-2016-19:04:01 to 04-09-2016-20:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
82.205.47.141	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	ET WEB_SERVER LOIC Javascript DDoS Inbound	40
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	9
90.231.228.209	147.237.77.216	Sweden	dover.idf.il	ET WEB_SERVER LOIC Javascript DDoS Inbound	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
82.205.47.141	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
106.246.247.117	147.237.0.34	Korea, Republic of	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
106.246.247.117	147.237.0.15	Korea, Republic of	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
45.32.233.114	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
24.37.53.226	147.237.8.28	Canada	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
13.92.187.228	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
180.76.170.207	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
119.93.69.131	147.237.76.30	Philippines	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
106.246.247.117	147.237.0.16	Korea, Republic of	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
13.92.187.228	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
13.92.187.228	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1
174.37.194.144	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 4096	1

04-09-2016-19:04:01 to 04-09-2016-20:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.212.37.123	Kenya	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12552
82.205.47.141	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12054
197.27.115.96	Tunisia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11936
41.225.186.122	Tunisia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10752
141.255.156.147	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8170
197.27.115.96	Tunisia	147.237.77.216	dover.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	6329
46.165.221.230	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	3372
193.90.12.88	Norway	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	3234
185.129.62.63	Denmark	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	3051
88.200.73.100	Slovenia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	2785
94.249.51.221	Jordan	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	2522
41.109.34.189	Algeria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	2499
65.19.167.130	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1539
46.185.244.209	Jordan	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1528
216.17.101.79	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1495
178.175.128.50	Moldova, Republic of	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1334
18.248.1.85	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1119
93.115.95.216	Anonymous Proxy	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1110
195.154.56.44	France	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1093
146.185.177.103	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	993
37.238.144.63	Iraq	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	948
192.42.116.16	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	814
194.150.168.79	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	787
85.93.218.204	Luxembourg	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	715
79.172.193.32	Hungary	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	710
62.210.37.82	France	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	704
82.205.47.141	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	652
185.38.14.215	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	602
88.252.234.29	Turkey	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	456
197.29.7.216	Tunisia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	413
192.168.173.102		147.237.77.216	dover.idf.i	Geo-location enforcement	Geo-location inbound enforcement	monitor	356
85.159.214.74	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	327
46.120.44.158	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	239
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	194
84.108.118.186	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	160
79.180.129.34	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	156
205.203.135.1	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	153
64.233.172.155	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	149
156.210.211.117	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	139
41.232.44.177	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	137
197.27.115.96	Tunisia	147.237.77.216	dover.idf.i	drop		drop	137
41.232.63.102	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	135
94.228.34.203	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	132
37.220.35.202	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	125
64.233.172.163	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	118
109.67.228.35	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	114
79.181.129.226	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	110
71.119.103.238	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	98
212.199.182.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	94
197.16.135.221	Tunisia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	83

04-09-2016-19:04:01 to 04-09-2016-20:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.147.248	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	2151
37.26.147.248	Israel	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 37.26.147.248	Block	2150
37.26.147.248	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 37.26.147.248	Block	2150
46.19.86.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	186
109.253.202.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	108
2.53.60.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
82.205.47.141	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Automated Vulnerability Scanning V1	Block	50
185.120.125.3	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	8
46.19.85.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
79.178.151.100	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.178.151.100	Block	5
185.120.125.3	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/	Block	4
46.19.86.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.210	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.19.86.210	Block	3
109.253.217.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	3
46.19.86.70	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.120.125.3	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 185.120.125.3	Block	2
109.253.193.122	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9043-he/refuah.aspx	Block	1
197.27.115.96	Tunisia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
46.116.138.217	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
157.55.39.17	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
105.106.31.23	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
41.225.186.122	Tunisia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
213.57.218.132	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.180.53.230	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
66.249.65.224	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/authenticationservice.asmx/getauthuser	Block	1
41.107.17.12	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
85.97.100.81	Turkey	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
77.237.138.202	Czech Republic	147.237.77.176	matpash.idf.il	Unauthorized URL Access to /	Block	1
2.54.179.238	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
197.113.186.225	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
62.201.226.115	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
157.55.39.194	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/hinuch	Block	1
105.108.6.55	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/favicon.ico	Block	1
41.232.63.102	Egypt	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
79.181.49.168	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1086-12925-en/dover.aspx&amp	Block	1
46.19.86.210	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	1
41.140.138.50	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he/dover.aspx'	Block	1
93.173.13.97	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.177.32.152	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 106 cookies	Block	1
5.29.168.35	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
197.189.214.18	South Africa	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
162.210.197.53	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/favicon.ico	Block	1
66.249.65.16	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
109.65.194.107	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
79.182.185.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
197.1.123.225	Tunisia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/favicon.ico	Block	1

04-09-2016-19:04:01 to 04-09-2016-20:04:01