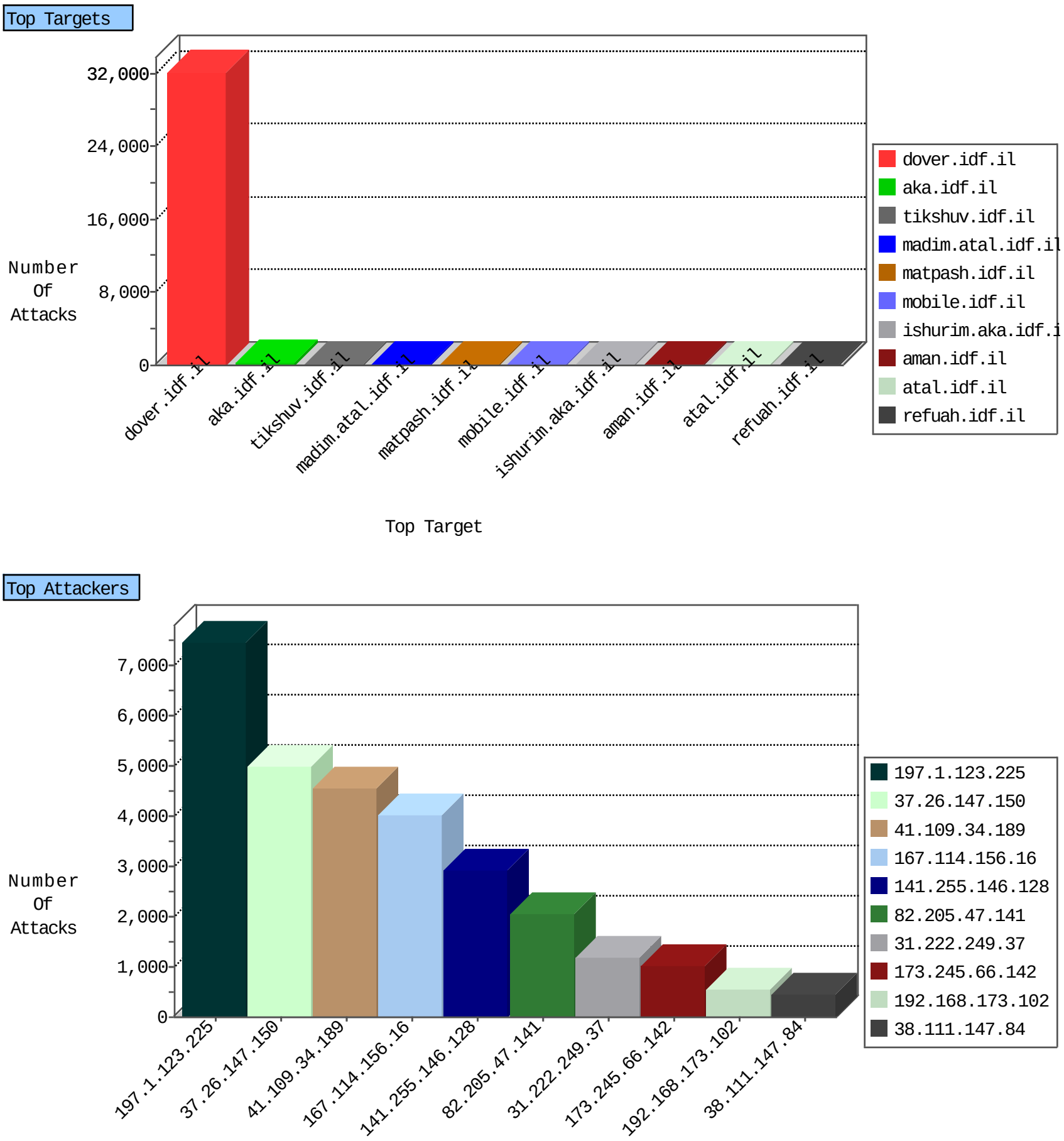
04-09-2016-20:04:02 to 04-09-2016-21:04:02

IDF Under Attack Daily Report



04-09-2016-20:04:02 to 04-09-2016-21:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.109.34.189	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4543
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4030
197.1.123.225	Tunisia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1472
105.197.139.98	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	862
141.255.146.128	Netherlands	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	821
213.57.49.148	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	623
154.107.55.52	Tunisia	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	154
191.101.67.220	Belarus	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	146
65.55.212.77	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	108
141.255.146.128	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	79
105.101.24.152	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	78
79.176.72.189	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	57
105.101.228.125	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	43
105.101.17.163	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	31
46.117.177.70	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	23
77.125.108.163	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
46.116.122.230	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
149.200.221.33	Jordan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
79.177.191.184	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
79.177.111.182	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
149.78.154.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
62.219.212.131	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
79.177.191.184	Israel	147.237.0.19	madim.atal.idf.il	Block_Udp_All_Nets	drop	6
149.50.98.113	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
188.225.183.149	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
168.235.197.54	United States	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
84.108.25.233	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
79.183.154.152	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
69.30.198.148	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	2
105.108.19.193	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
109.186.49.99	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
188.225.183.149	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
168.235.197.54	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
74.91.23.106	United States	147.237.77.74	law.idf.il	block-sp-traf1	forward	2
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
197.132.183.22	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
178.152.216.67	Qatar	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
162.243.99.146	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
41.251.123.169	Morocco	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
173.208.197.251	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	2
107.150.32.60	United States	147.237.0.15	kosher-kravi.idf.i	block-sp-traf1	forward	2
105.101.6.173	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
5.102.242.206	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	2
185.120.125.23	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
68.180.231.43	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
173.208.197.254	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2

04-09-2016-20:04:02 to 04-09-2016-21:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.108.68.54	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	14
109.65.215.249	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	4
46.19.86.81	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	3
141.255.146.128	Netherlands	147.237.77.216	dover.idf.il	12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	3
65.55.210.105	United States	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	2
2.52.140.0	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	2
2.53.59.232	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	2
61.135.189.122	China	147.237.76.31	nakchal.idf.i	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
157.55.39.201	United States	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	1
191.101.67.220	Belarus	147.237.77.216	dover.idf.il	C1000133: HTTP: Opisrael 2015 - key words and groups	Block	1

04-09-2016-20:04:02 to 04-09-2016-21:04:02

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	25
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	4
178.62.96.169	147.237.77.216	United Kingdom	dover.idf.il	ET WEB_SERVER LOIC Javascript DDoS Inbound	3
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.102.9.115	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sA (2)	2
46.151.52.139	147.237.76.176	Ukraine	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
40.84.149.32	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 2048	1
208.100.26.228	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.149.138	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.154.54.169	147.237.0.17	France	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
162.248.100.195	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
40.84.149.32	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 4096	1
40.84.149.32	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -f -sS	1
198.20.69.98	147.237.77.233	United States	atal.idf.il	ET DROP Dshield Block Listed Source	1
162.248.100.195	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
141.101.178.137	147.237.72.166	Russian Federation	aka.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

04-09-2016-20:04:02 to 04-09-2016-21:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.1.123.225	Tunisia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7459
141.255.146.128	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	2101
82.205.47.141	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1377
37.26.147.150	Israel	147.237.77.216	dover.idf.i	drop	SAM rule	drop	1154
173.245.66.142	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1035
38.111.147.84	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	437
82.205.47.141	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	drop	SAM rule	drop	391
31.222.249.37	Jordan	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	378
192.168.173.102		147.237.77.216	dover.idf.i	Geo-location enforcement	Geo-location inbound enforcement	monitor	359
31.222.249.37	Jordan	147.237.77.216	dover.idf.i	Bad TCP sequence		monitor	307
82.205.47.141	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	drop		drop	260
31.222.249.37	Jordan	147.237.77.216	dover.idf.i	Bad TCP sequence		alert	257
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	197
205.203.135.1	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	102
37.26.147.248	Israel	147.237.77.216	dover.idf.i	drop	SAM rule	drop	99
5.102.242.206	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	82
212.156.70.118	Turkey	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	82
31.222.249.37	Jordan	147.237.77.216	dover.idf.i	drop	Unexpected post SYN packet - RST or SYN expected	drop	70
105.197.139.98	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	69
149.200.221.33	Jordan	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	68
31.222.249.37	Jordan	147.237.77.216	dover.idf.i	drop		drop	62
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	60
139.162.216.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	48
37.26.147.150	Israel	147.237.77.216	dover.idf.i	drop		drop	46
86.169.22.42	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	45
31.222.249.37	Jordan	147.237.77.216	dover.idf.i	Bad TCP sequence	SYN retransmit with different window scale	alert	44
198.251.61.125	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
109.253.221.155	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
109.67.228.35	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
168.235.197.54	United States	147.237.77.216	dover.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	36
31.222.249.37	Jordan	147.237.77.216	dover.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	35
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	35
160.157.184.75	Tunisia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
24.16.23.37	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
95.86.111.226	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	32
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	31
45.79.193.204	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	29
173.234.159.250	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
94.96.144.103	Saudi Arabia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
154.107.55.52	Tunisia	147.237.77.216	dover.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
197.7.210.86	Tunisia	147.237.77.216	dover.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
197.45.132.217	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
52.29.253.128	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
37.26.148.240	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
2.54.188.177	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
46.117.177.70	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
136.243.5.203	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
109.67.33.170	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18

04-09-2016-20:04:02 to 04-09-2016-21:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.147.150	Israel	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	1252
37.26.147.150	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1252
37.26.147.150	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1252
2.53.22.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
17.142.156.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	4
46.19.86.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.201.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.10.71	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	2
157.55.39.65	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
2.54.176.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.10.71	Israel	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	2
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/2271.jpg	Block	1
197.7.207.224	Tunisia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
154.107.55.52	Tunisia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
79.182.128.75	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
213.8.204.24	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
66.249.65.12	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
37.187.114.171	France	147.237.77.235	sviva.idf.il	Unauthorized URL Access to /irj/portal	Block	1
5.29.244.85	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mivtza	Block	1
105.102.84.32	Algeria	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
66.249.66.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/3467.jpg	Block	1
197.7.210.86	Tunisia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
154.121.251.131	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
82.166.235.55	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
2.52.157.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.57.38.217	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.65.217	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
176.228.18.185	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
37.237.186.71	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
105.102.186.47	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/'	Block	1
69.30.198.148	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.tt985.com/	Block	1
46.116.63.149	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl25 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
206.190.136.245	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 206.190.136.245	Block	1
84.111.81.189	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
213.151.35.213	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/undefined	Block	1
66.249.65.224	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/8/66098.pdf	Block	1
185.22.32.16	Lebanon	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/clientscripts/jquery/	Block	1
41.101.86.139	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
31.222.249.37	Jordan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
107.150.32.60	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.tt782.com/	Block	1
74.91.23.106	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.tt985.com/	Block	1
46.117.62.227	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
206.190.136.245	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/7/size220x0/	Block	1
157.55.39.205	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1
37.26.149.249	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
88.252.234.29	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/a	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/2359.jpg	Block	1
188.225.183.149	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1

04-09-2016-20:04:02 to 04-09-2016-21:04:02