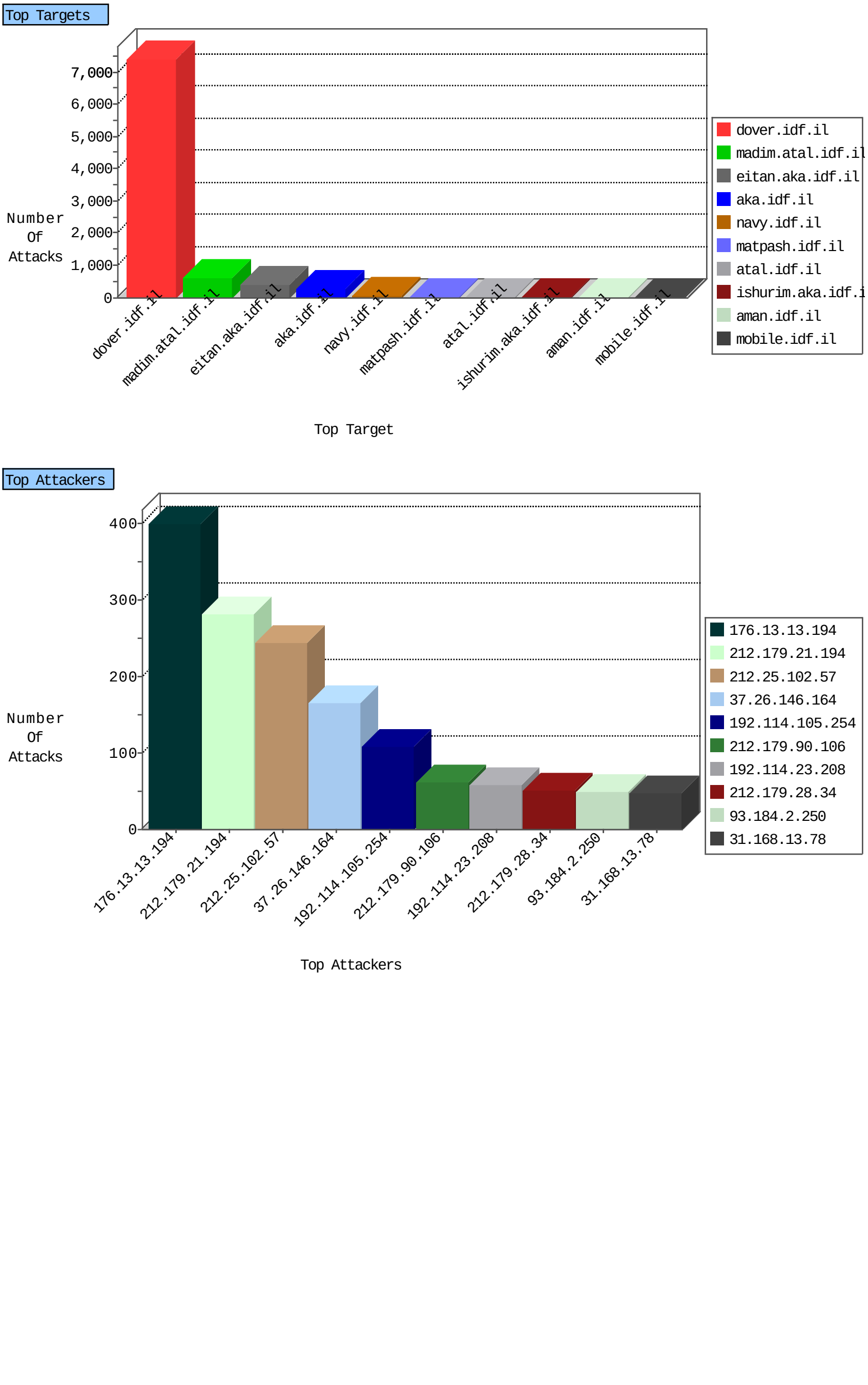
11-09-2015-09:04:09 to 11-09-2015-10:04:09

IDF Under Attack
Daily Report



11-09-2015-09:04:09 to 11-09-2015-10:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.25.121.195	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	33
89.42.53.2	Romania	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	6
91.90.121.11	Romania	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	6
140.113.226.125	Taiwan	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	5
150.140.151.2	Greece	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	5
46.19.85.188	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
91.103.80.2	Russian Federation	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
2.52.23.113	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
193.226.37.96	Romania	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
133.6.88.11	Japan	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
168.122.46.11	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
79.177.196.77	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
142.151.128.8	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
150.140.151.98	Greece	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
160.216.161.7	Czech Republic	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
132.248.18.105	Mexico	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
207.4.226.63	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
160.124.112.4	South Africa	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
147.162.62.74	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
80.246.136.5	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
147.46.30.5	Korea, Republic of	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
222.122.49.3	Korea, Republic of	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
118.129.171.62	Korea, Republic of	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
190.36.60.15	Venezuela	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
185.32.179.35	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
208.7.233.7	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
18.78.0.12	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
131.188.9.67	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
80.246.139.15	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
140.113.20.65	Taiwan	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
147.83.138.61	Spain	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
195.160.240.11	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
194.29.174.25	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
150.140.136.68	Greece	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
89.33.88.126	Romania	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
165.246.149.2	Korea, Republic of	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
5.154.249.27	Romania	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
160.80.13.103	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
188.240.45.13	Romania	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
37.26.149.135	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
132.160.30.21	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
66.102.59.24	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
157.159.225.10	France	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
209.175.60.2	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
130.228.234.7	Denmark	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
118.98.72.66	Indonesia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
150.140.148.66	Greece	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
201.22.148.42	Brazil	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2

11-09-2015-09:04:09 to 11-09-2015-10:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
132.74.56.238	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
212.235.37.65	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2

11-09-2015-09:04:09 to 11-09-2015-10:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.250.91.230	147.237.76.86	Germany	navy.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	19
77.127.197.79	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
37.26.146.152	147.237.77.233	Israel	atal.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	3
80.246.133.154	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
2.54.24.8	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.114.105.246	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
118.241.234.224	147.237.77.216	Japan	dover.idf.il	portscan: TCP Distributed Portscan	1
66.102.8.238	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
41.218.183.38	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.61.134	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.118.11.120	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.100.84.253	147.237.8.45		e.eitan.idf.	ET SCAN NMAP -sS window 1024	1
82.80.17.247	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.93.196	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.213.223	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.249.12	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
14.215.176.149	147.237.77.234	China	halag.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
212.179.90.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

11-09-2015-09:04:09 to 11-09-2015-10:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	122
192.114.105.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	109
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	102
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
192.114.23.208	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
212.179.28.34	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
31.168.13.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
212.143.110.33	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
193.188.136.30	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
79.181.166.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
66.249.93.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
81.218.251.252	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
2.52.150.123	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
213.8.241.234	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
185.120.126.59		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
46.19.85.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
147.236.34.110	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
212.199.101.60	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
46.19.86.160	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
93.184.2.250	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
193.138.227.76	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
46.19.86.146	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
66.249.93.196	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
192.114.23.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
79.181.165.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
46.19.86.120	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
212.179.91.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
212.143.3.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
192.115.29.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
46.19.85.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
79.177.115.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
79.182.62.125	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
212.179.185.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
77.42.129.119	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
192.114.91.229	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
37.26.148.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
46.19.86.82	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
46.19.85.167	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
93.184.2.250	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	20
66.249.93.192	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
46.19.85.252	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
46.19.86.201	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
2.52.60.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
62.219.99.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
195.160.240.11	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
79.181.170.248	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18

11-09-2015-09:04:09 to 11-09-2015-10:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.13.194	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.13.194	Block	238
212.25.102.57	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	219
176.13.13.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	112
37.26.146.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	83
37.26.146.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	81
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 212.179.21.194	Block	51
176.13.13.194	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 176.13.13.194	Block	50
46.19.86.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
31.168.103.115	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 31.168.103.115	Block	15
46.19.86.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
212.25.102.57	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.25.102.57	Block	7
208.115.111.72	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.111.72	Block	7
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/shared/ajax/lightboxmediagallery.aspx	Block	6
37.26.146.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.217	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.217	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CaptchaText in mobile.idf.il/authentication/login	Block	3
46.19.86.237	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
14.215.176.21	China	147.237.77.234	halag.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
176.13.15.121	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
14.215.176.148	China	147.237.77.234	halag.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
217.132.67.246	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
212.235.37.65	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	2
14.215.176.149	China	147.237.77.234	halag.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
208.115.111.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	2
37.26.149.140	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
195.95.183.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
2.52.174.220	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.137.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2113-he/cogat.aspx	Block	1
37.26.146.160	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.32.179.112	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
151.80.31.136	Italy	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8804-he/refuah.aspx	Block	1
213.8.129.139	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
31.168.103.115	Israel	147.237.72.166	aka.idf.il	Unknown Parameter wb48617274 in www.aka.idf.il/main/home/resources/images/bar/gimlaim.gif	None	1
2.54.128.64	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
81.218.206.192	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.49	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.114.23.209	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.52.23.113	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.180.107.91	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.168.103.115	Israel	147.237.72.166	aka.idf.il	Unknown Parameter wb48617274 in www.aka.idf.il/main/home/resources/images/bulleticon.gif	None	1
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.69.213.24	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
80.246.138.142	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.149.141	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.68	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/templates/shared/usercontrols/navmenu/mazi.idf.il	Block	1
2.52.175.58	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1

11-09-2015-09:04:09 to 11-09-2015-10:04:09