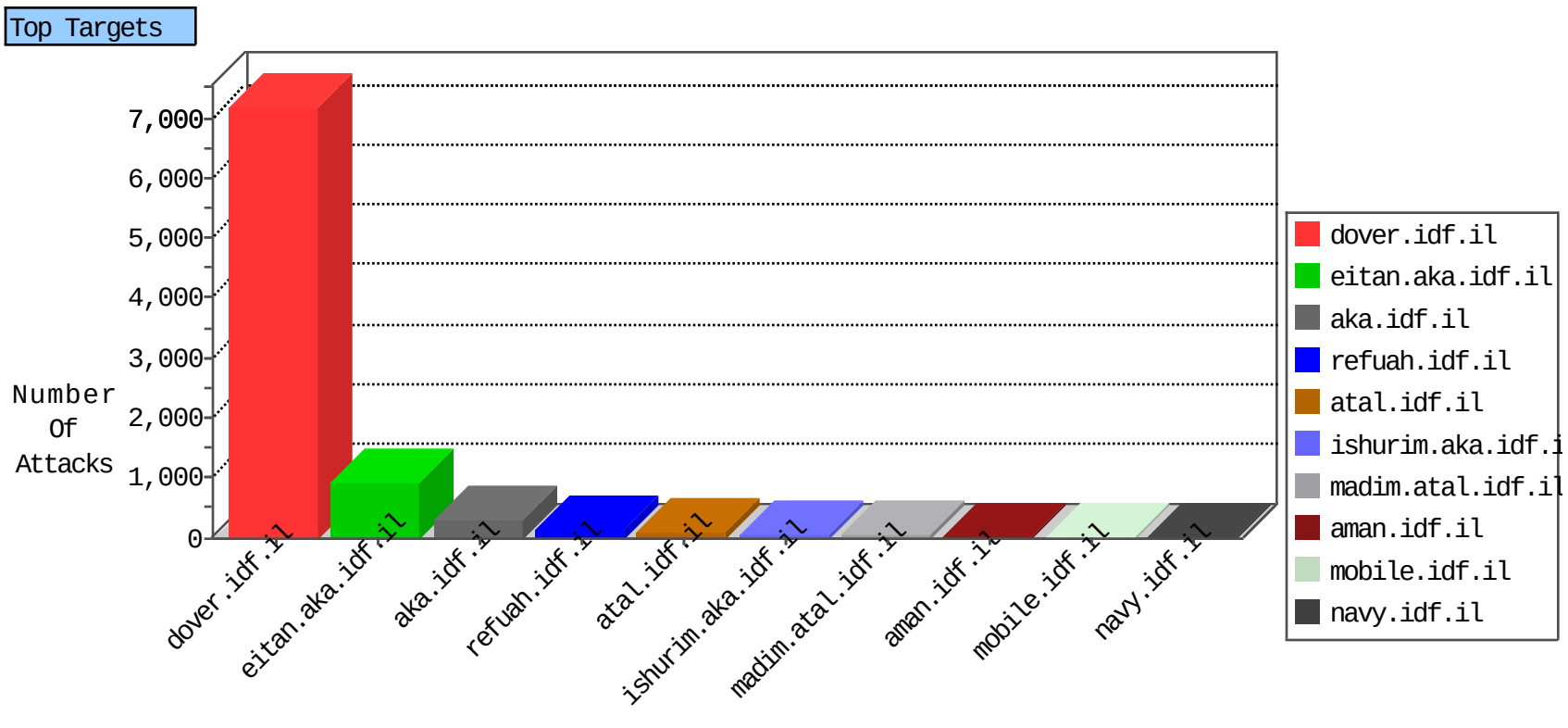
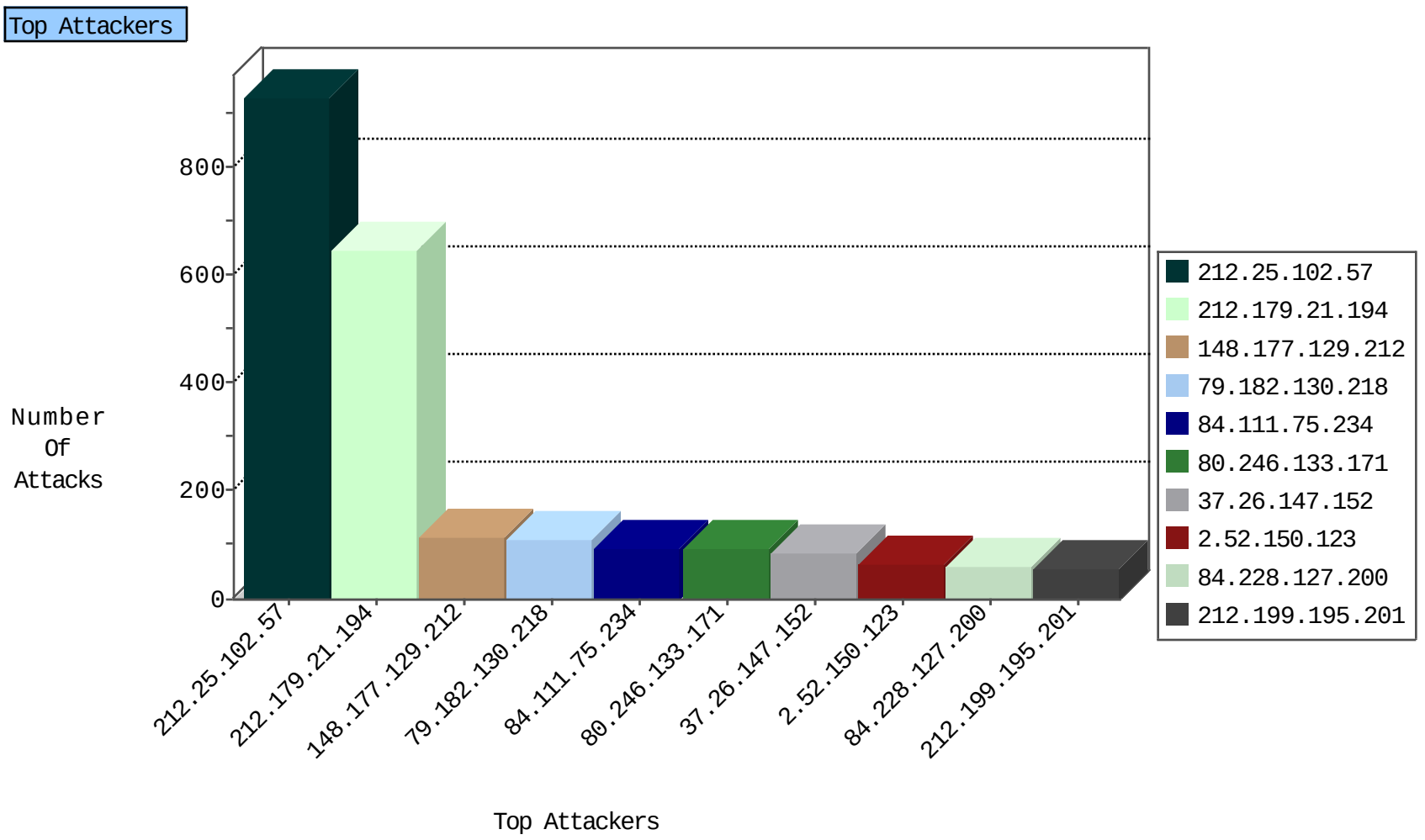
11-09-2015-10:04:06 to 11-09-2015-11:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-09-2015-10:04:06 to 11-09-2015-11:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.64.181	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3834
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	127
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	126
2.52.150.123	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	64
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	16
212.25.121.195	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	15
89.42.53.2	Romania	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	10
84.228.127.200	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
80.246.137.237	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
46.19.86.147	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
82.166.65.59	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
79.181.213.148	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	6
37.26.146.223	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
79.181.213.148	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	5
147.210.56.39	France	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	5
150.140.148.66	Greece	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
82.80.173.170	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
66.37.242.36	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
84.94.41.183	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
129.15.226.93	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
46.19.86.57	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
84.228.14.57	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
2.52.150.123	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
158.108.249.59	Thailand	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
95.35.151.233	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
77.235.133.191	Lebanon	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
200.201.25.11	Brazil	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
148.177.129.212	Europe	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Http	drop	3
147.210.58.39	France	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
152.66.204.26	Hungary	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3
62.219.162.242	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
37.26.149.197	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
89.203.133.7	Czech Republic	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
192.248.84.15	Sri Lanka	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
131.188.108.9	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
192.65.176.112	Puerto Rico	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
147.213.205.46	Slovakia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
37.26.149.199	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
200.162.143.45	Brazil	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
18.78.0.9	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
80.87.191.3	Czech Republic	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
220.73.173.103	Korea, Republic of	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
168.83.73.68	Argentina	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
140.117.75.30	Taiwan	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
163.1.158.29	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
212.43.65.92	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
211.115.217.124	Korea, Republic of	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2

11-09-2015-10:04:06 to 11-09-2015-11:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-09-2015-10:04:06 to 11-09-2015-11:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
132.73.204.49	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.61	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.32.197	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.13.78	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.194.193.5	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.166.199.89	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
202.3.255.12	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	1
80.246.137.141	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
79.183.198.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
167.97.194.113	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
79.181.135.144	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
148.105.142.40	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
66.249.81.212	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
140.170.37.94	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
46.19.86.232	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
134.209.107.125	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
46.19.86.6	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
95.217.172.75	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
37.26.149.180	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.22.127.25	147.237.77.216	Netherlands	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
2.54.168.213	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
205.145.193.5	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.137.184	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.151.86.41	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
80.246.130.247	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
194.50.175.83	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.113.58	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
159.223.136.101	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
79.177.5.141	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
147.50.15.102	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
66.249.67.224	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
138.43.221.59	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
46.19.86.67	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

11-09-2015-10:04:06 to 11-09-2015-11:04:06

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	590
79.182.130.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	109
148.177.129.212	Europe	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	108
84.111.75.234	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	95
80.246.133.171	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	94
37.26.147.152	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
193.34.56.101	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
62.219.162.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
2.52.150.123	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
213.204.127.27	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
84.228.127.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
212.199.195.201	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	47
46.19.86.6	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
212.25.102.57	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
77.235.133.191	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
46.19.85.38	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	35
95.86.85.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
84.94.41.183	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
176.13.17.136	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
209.88.198.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
80.246.133.92	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
46.19.86.57	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
84.94.230.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
94.159.156.104	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
209.132.186.36	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
79.180.217.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
31.154.19.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
132.64.240.126	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
217.132.221.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
192.114.105.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
77.126.88.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
79.183.198.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
212.199.146.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
31.168.96.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
2.54.43.87	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
212.143.3.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
176.12.147.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.19.86.84	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.19.86.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
59.23.214.63	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
192.117.150.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
37.26.147.251	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
199.203.215.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
2.54.54.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
84.95.198.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13

11-09-2015-10:04:06 to 11-09-2015-11:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.25.102.57	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	851
212.25.102.57	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.25.102.57	Block	35
37.26.148.231	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	22
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	18
46.19.86.12	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
31.184.197.106	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 31.184.197.106	Block	6
5.9.73.211	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 5.9.73.211	Block	6
31.184.197.106	Russian Federation	147.237.72.166	aka.idf.il	PHP Attempt	Block	5
46.19.86.79	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
81.218.251.252	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
2.54.182.129	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
194.90.88.105	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized HTTP Method	Block	4
176.12.151.67	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
194.90.88.105	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 194.90.88.105	Block	3
37.26.148.244	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
31.184.197.106	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/forums/forums.asp	Block	2
80.74.107.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/0/2320.	Block	2
176.13.8.144	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.45	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
84.94.176.7	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.138	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.26.149.148	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.85.15	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.17.136	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1135-he/atal.aspx	Block	1
79.180.214.16	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
213.149.223.82	Italy	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
142.54.174.69	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.cloud.ph/	Block	1
46.117.215.113	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	1
2.54.8.192	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
109.64.181.183	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1
185.32.179.154	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
37.26.149.178	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.133.29.134	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.186.10.67	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
62.219.161.81	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.179.162.137	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1250-he/atal.aspx	Block	1
46.19.86.86	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.52.59.199	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.64.155.24	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
46.19.85.38	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.20.1	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
213.151.35.218	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.146.138	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
149.78.237.68	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
52.23.156.32	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
212.25.122.125	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/	Block	1
2.54.43.214	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1

11-09-2015-10:04:06 to 11-09-2015-11:04:06