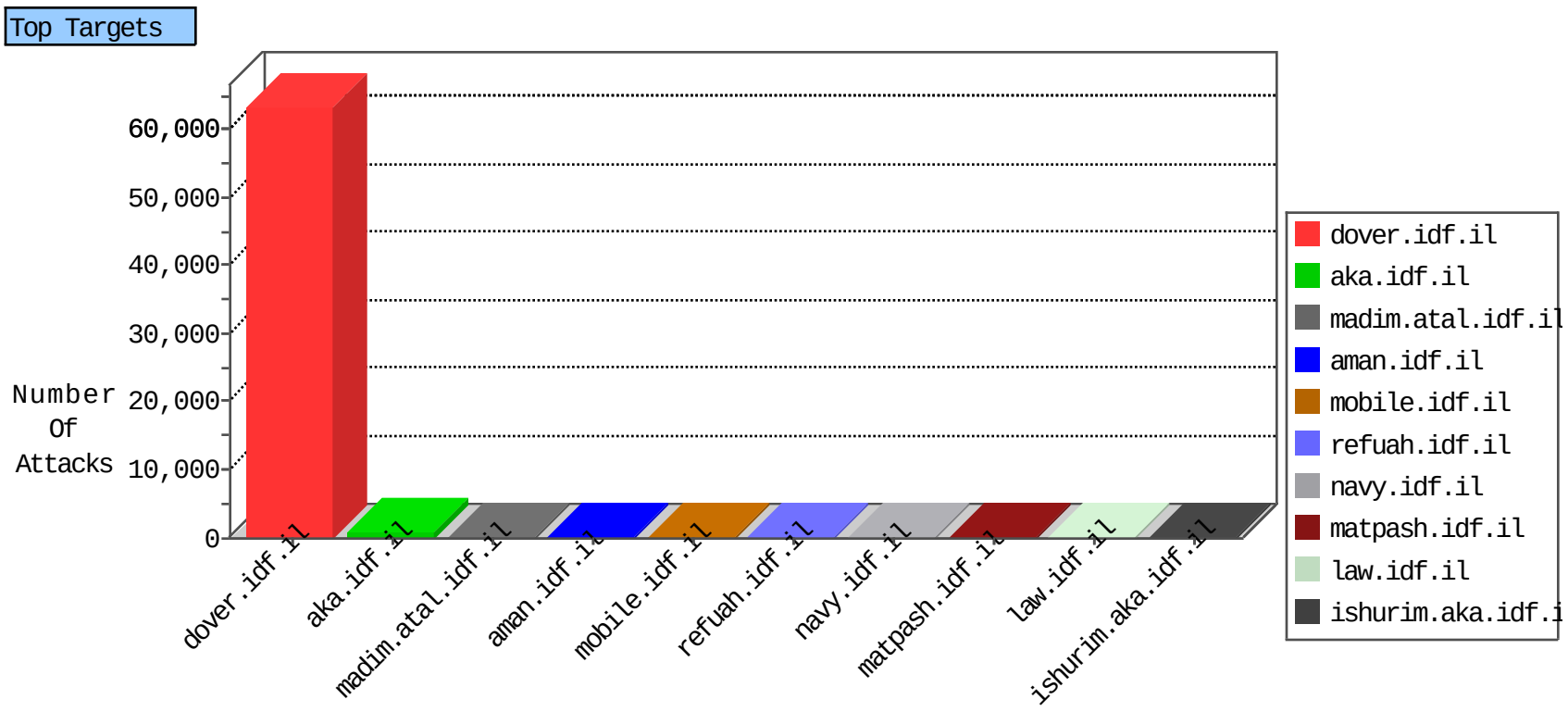
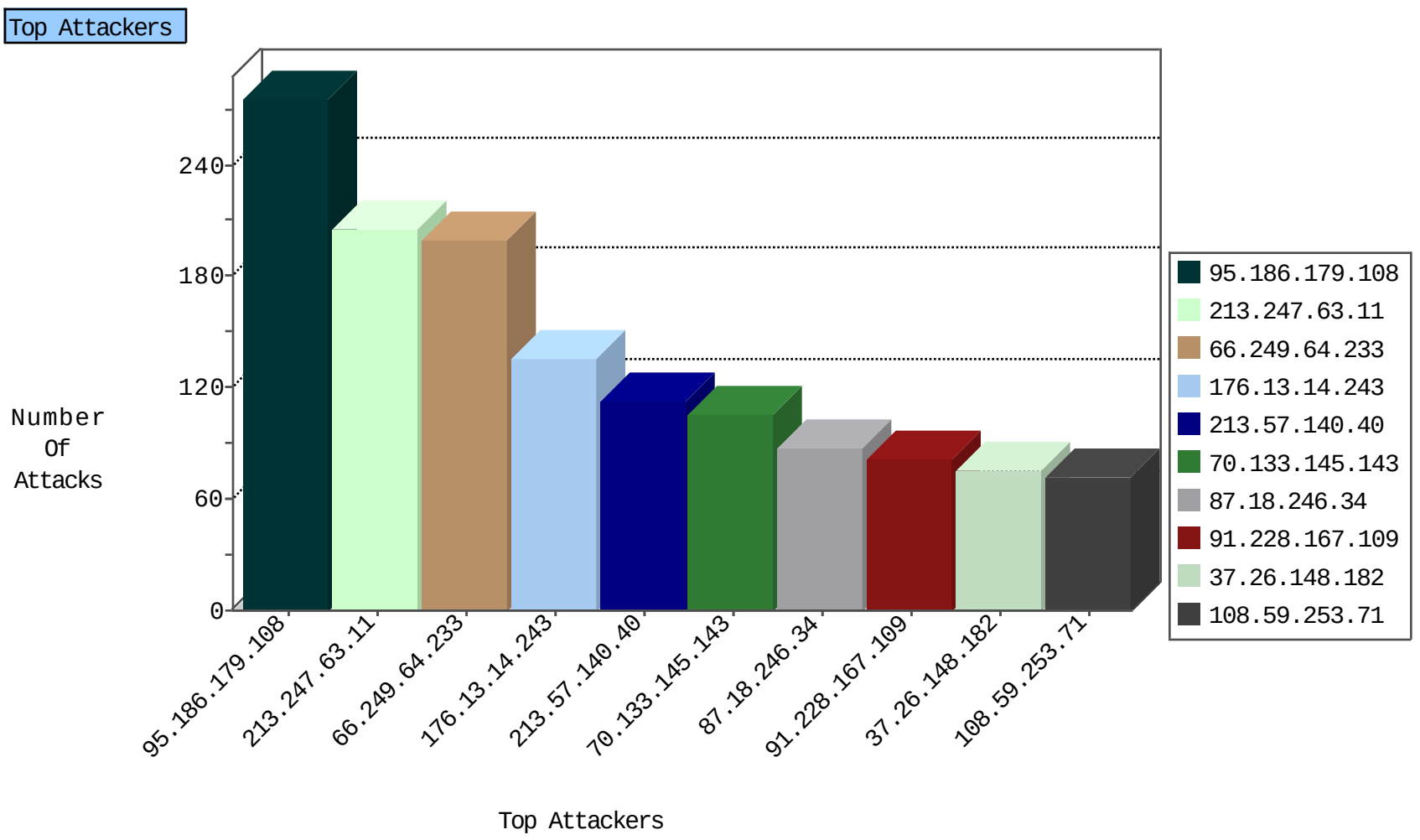
11-17-2015-18:04:00 to 11-17-2015-19:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-17-2015-18:04:00 to 11-17-2015-19:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
178.199.190.43	Switzerland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2991
95.186.179.108	Saudi Arabia	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	982
66.249.65.18	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	598
59.89.210.20	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	479
82.30.172.6	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	474
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	174
109.64.164.29	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
85.250.44.10	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
109.65.51.76	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
66.249.64.243	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
67.102.30.31	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
190.233.67.20	Peru	147.237.72.156	aman.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
5.29.147.28	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
68.66.19.52	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
135.23.218.3	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
24.105.202.2	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
88.30.140.127	Spain	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
2.54.177.216	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
83.233.8.124	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
219.97.185.90	Japan	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
64.18.229.57	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
110.92.16.113	New Zealand	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
80.99.23.17	Hungary	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
207.183.190.60	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
75.133.80.76	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
196.47.172.82	Cote D'Ivoire	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
37.131.141.5	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.135.196.124	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
24.226.81.9	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
89.233.213.13	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
71.85.24.22	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
172.91.213.0		147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
126.77.77.11	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
23.233.49.71	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
85.134.88.59	Finland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
213.226.252.30	Czech Republic	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
63.248.234.45	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
109.109.81.95	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
81.136.229.58	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
78.154.150.27	Latvia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
204.16.82.101	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
46.162.78.27	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
31.208.49.20	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
92.244.194.118	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
74.51.48.102	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
189.2.255.40	Brazil	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
69.8.138.94	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
141.161.133.109	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

11-17-2015-18:04:00 to 11-17-2015-19:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.247.63.11	Netherlands	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	199
74.81.206.25	United States	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
213.247.63.11	Netherlands	147.237.77.216	dover.idf.il	12715: HTTP: Blind SQL Injection in URI	Block	7
188.165.15.208	France	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.230	France	147.237.76.86	navy.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-17-2015-18:04:00 to 11-17-2015-19:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	**Signature**	**Count**

11-17-2015-18:04:00 to 11-17-2015-19:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	192
70.133.145.143	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	105
87.18.246.34	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	87
91.228.167.109	Slovakia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	81
37.26.148.182	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	76
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
208.69.40.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
91.228.167.130	Slovakia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
213.57.140.40	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	59
213.57.140.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	54
72.211.107.62	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
37.201.168.1	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
81.109.230.219	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
69.171.231.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
85.250.205.194	Israel	147.237.77.243	mobile.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
194.135.152.184	Azerbaijan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
2.54.41.162	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
213.55.111.43	Ethiopia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
69.171.231.227	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
37.26.148.137	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
212.117.140.158	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
66.249.64.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
176.12.142.89	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
213.57.128.142	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
213.57.128.142	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
213.57.143.49	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
213.57.143.49	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
149.78.9.5	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
149.78.9.5	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
46.19.85.118	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
46.19.85.208	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
2.54.148.184	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
79.177.163.109	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.100.46.127		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
100.100.99.204		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
107.170.61.36	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
131.137.245.206	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.14.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	109
95.35.75.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
2.54.31.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
176.13.14.243	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.14.243	Block	27
185.32.179.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
46.19.86.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
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	9
208.115.113.88	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il/giyus/forum/asp/showforum.asp	Block	5
2.54.21.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.85.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.152	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
80.246.139.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
95.35.75.139	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
79.183.126.16	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	3
66.249.67.31	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	3
79.183.126.16	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/pages/fan_status.php	Block	3
84.108.116.223	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
77.125.77.105	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
5.144.55.11	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
176.12.140.184	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
84.108.116.223	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/ajax/pages/fan_status.php	Block	2
77.125.77.105	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/pages/fan_status.php	Block	2
85.64.16.140	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
5.144.55.11	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/pages/fan_status.php	Block	2
109.67.32.239	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	2
31.154.94.11	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.55.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
149.78.238.135	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.228.201.131	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
80.246.139.66	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 113 cookies	Block	1
5.45.254.226	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.66.105.117	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
79.177.163.109	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/9/2479.jpg	Block	1
2.52.167.192	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
93.173.128.210	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
85.65.14.195	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
46.19.86.74	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.12.139.188	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.110.175	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.67.194.35	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.148.135	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.64.42.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.183.201.7	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
188.161.153.68	Palestinian Territory, Occupied	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/590-en	Block	1
176.13.5.16	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.139.179.149	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
168.235.195.17	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 168.235.195.17	Block	1