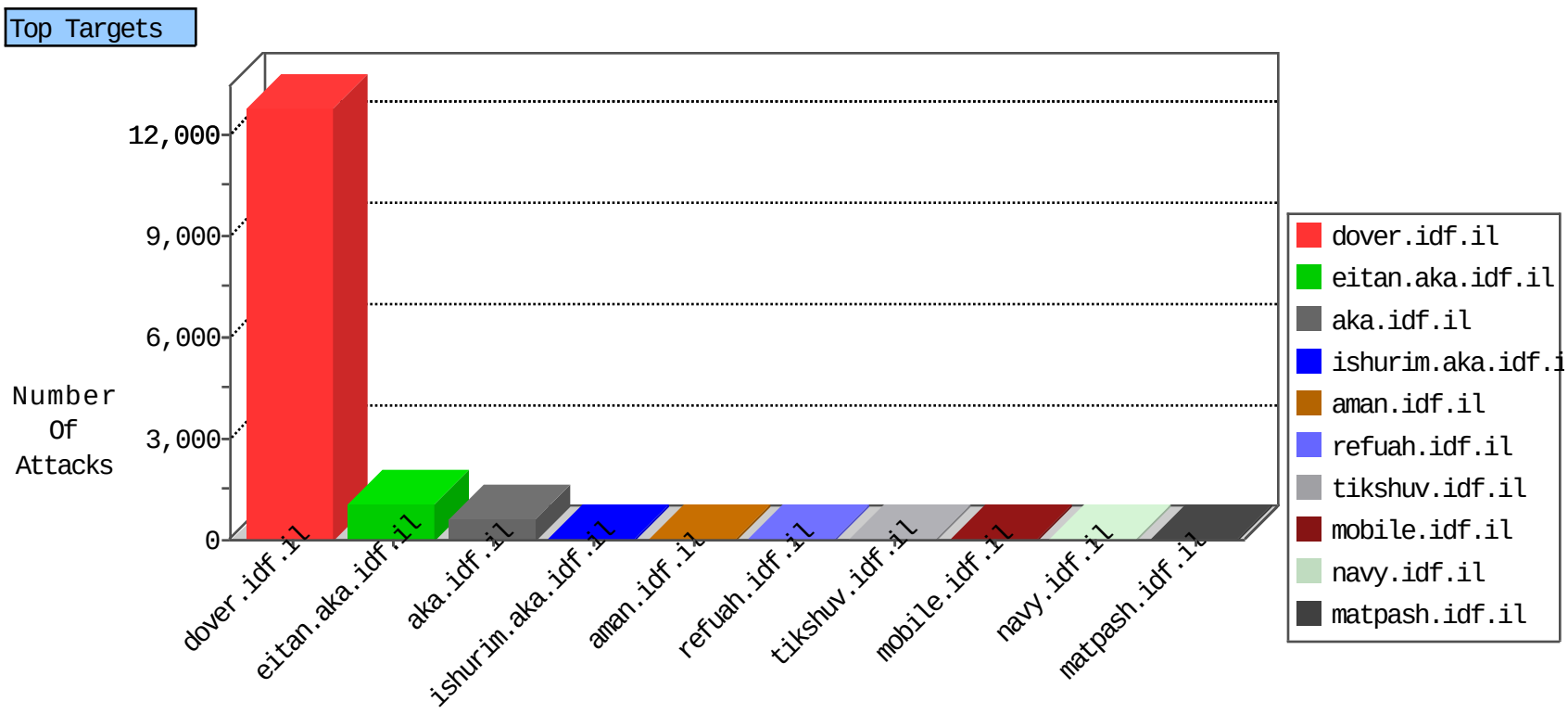
11-02-2015-15:04:03 to 11-02-2015-16:04:03

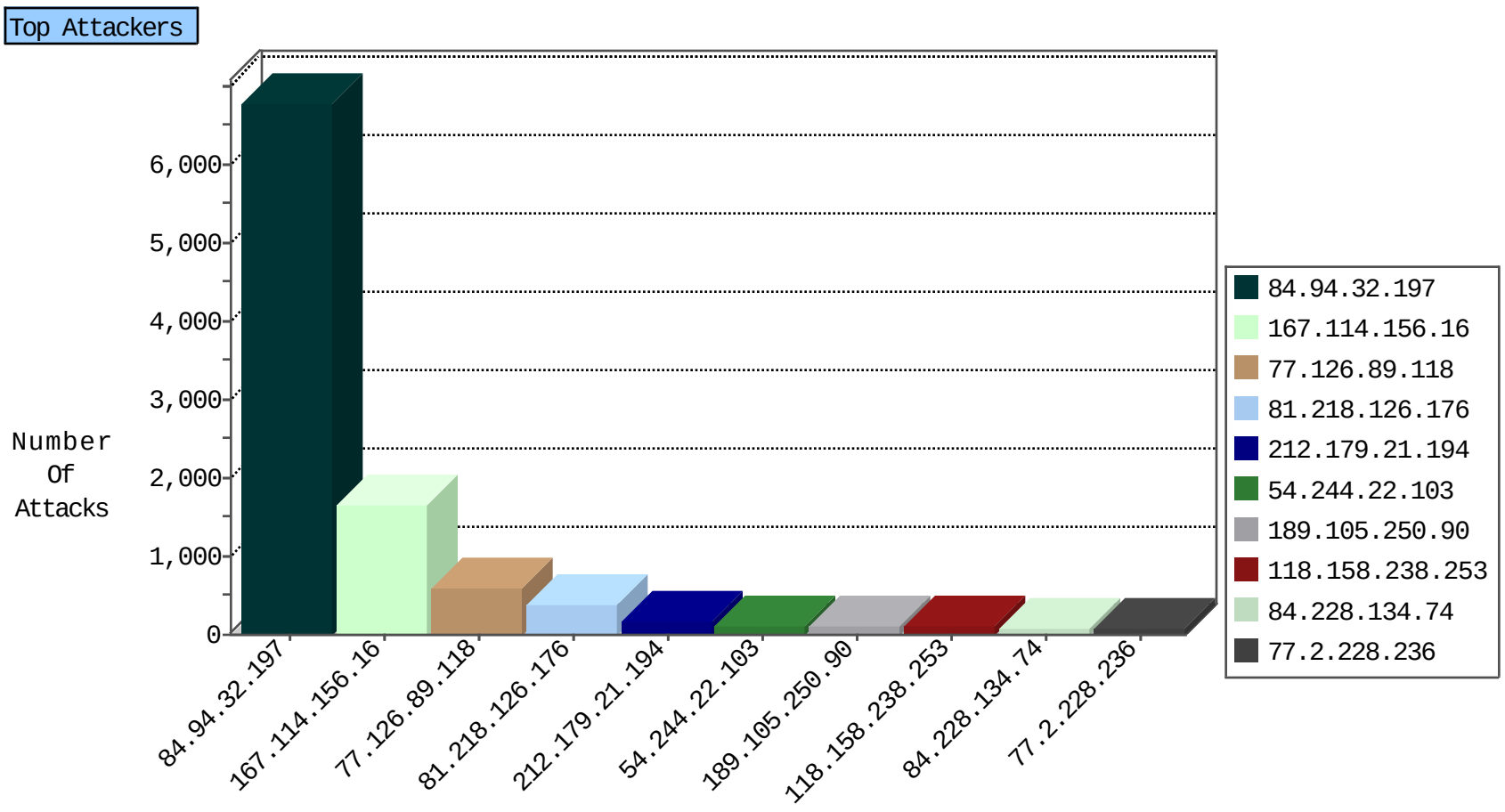
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-02-2015-15:04:03 to 11-02-2015-16:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2841
46.19.86.4	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	166
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	130
31.154.6.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	80
46.19.85.236	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	36
109.160.233.49	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	33
62.219.92.239	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
31.168.97.114	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
2.54.34.240	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	24
37.142.64.9	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	24
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
46.19.85.236	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
213.57.134.190	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	16
193.43.244.102	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
162.192.193.185	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
79.179.180.5	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
176.13.5.209	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
213.151.53.59	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
79.177.171.210	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
79.176.198.119	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
122.0.25.138	Malaysia	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
176.58.67.58	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
81.218.235.10	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.86.138	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
87.59.230.158	Denmark	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.2.75	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
79.178.63.111	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
79.178.103.162	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.19.86.11	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
46.116.99.71	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
213.57.167.5	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
152.26.30.243	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.19.86.68	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.19.85.91	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
185.32.179.48	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
82.80.219.164	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
77.125.108.204	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
46.121.59.197	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
176.13.10.218	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
122.0.25.138	Malaysia	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.13.19.169	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
77.125.108.204	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	2
212.29.214.138	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.19.86.226	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
46.19.86.68	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.19.85.179	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.54.2.75	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

11-02-2015-15:04:03 to 11-02-2015-16:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.60.30	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	11
91.228.248.251	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
152.62.109.210	Europe	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

11-02-2015-15:04:03 to 11-02-2015-16:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
64.233.172.155	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
213.151.53.59	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.125	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
37.26.148.182	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
180.210.201.106	147.237.76.31	Singapore	nakchal.idf.il	ET SCAN Potential SSH Scan	1
2.54.42.14	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.228.179.86	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
128.199.41.247	147.237.72.166	Singapore	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
87.69.206.57	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.250.21.155	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.109.88.153	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.161	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.199.57.207	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.251	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
180.210.201.106	147.237.76.34	Singapore	yohalan.idf.il	ET SCAN Potential SSH Scan	1
5.8.66.101	147.237.76.86	Russian Federation	navy.idf.il	ET SCAN Potential SSH Scan	1
180.210.201.106	147.237.0.17	Singapore	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
176.13.5.227	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.66.166.128	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.69.32.52	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.64.108.78	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

11-02-2015-15:04:03 to 11-02-2015-16:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
84.94.32.197	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6796
77.126.89.118	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	552
81.218.126.176	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	369
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	140
118.158.238.253	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	104
189.105.250.90	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	103
84.228.134.74	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
77.2.228.236	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	82
37.26.148.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	74
197.144.46.1	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
193.104.77.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
216.185.58.119	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
149.78.51.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
109.64.53.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
149.78.31.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
46.19.85.80	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
207.232.28.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
79.178.112.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
213.55.104.253	Ethiopia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
194.90.83.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
54.72.0.55	Ireland	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	38
54.244.22.103	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	38
134.196.163.223	Thailand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
2.54.133.111	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	33
176.228.38.123	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
31.154.6.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
100.100.121.69		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	31
41.194.80.2	Satellite Provide	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
152.62.109.210	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
192.114.91.232	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
91.143.226.143	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
109.67.179.90	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
62.219.196.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
207.46.13.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
213.57.167.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
64.233.172.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
173.220.141.227	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
185.26.182.35	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
37.26.146.239	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.126.89.118	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	47
37.142.227.53	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 37.142.227.53	Block	13
212.179.21.194	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 212.179.21.194	Block	7
132.70.66.11	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 132.70.66.11	Block	6
5.29.46.63	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	6
84.229.27.138	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
62.219.134.230	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	6
5.29.46.63	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	6
81.218.126.176	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 81.218.126.176	Block	6
84.229.27.138	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	6
84.229.27.138	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	6
5.29.46.63	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
77.126.41.129	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	4
77.126.41.129	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	4
212.179.21.194	Israel	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	4
77.126.41.129	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	4
91.228.248.251	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on www.logistics.atal.idf.il/sip_storage/files/7/size338x0/1877.jpg	Block	3
176.12.140.205	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Double URL Encoding from 176.12.140.205	Block	3
87.68.62.43	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
176.13.10.123	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
37.142.68.123	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	2
185.32.179.177	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
87.69.29.67	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
212.179.60.30	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	2
91.228.248.251	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/4/2094.jpg	Block	2
87.69.29.67	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	2
87.69.29.67	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
85.64.108.78	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
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
149.78.83.17	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
212.179.21.194	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/ajax/updatestatus.php	Block	1
89.138.77.41	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
84.109.114.72	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.29.103.111	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	1
185.24.78.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	1
176.12.140.205	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Double URL Encoding - parameter: ReturnUrl in m.my-kosher-kravi.idf.il/templates/login.aspx	Block	1
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
212.25.102.57	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/l	Block	1
81.218.126.176	Israel	147.237.76.200	eitan.aka.idf.il	Too Many 404: Response Code per Session	Block	1
149.210.158.71	Netherlands	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 149.210.158.71	Block	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
212.179.60.30	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 212.179.60.30	Block	1
79.176.147.204	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	1
2.54.3.154	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
132.70.66.11	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar	Block	1
66.249.75.62	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/1094-he/patzar.aspx	Block	1
212.29.214.138	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/7/size338x0/1877.jpg	Block	1