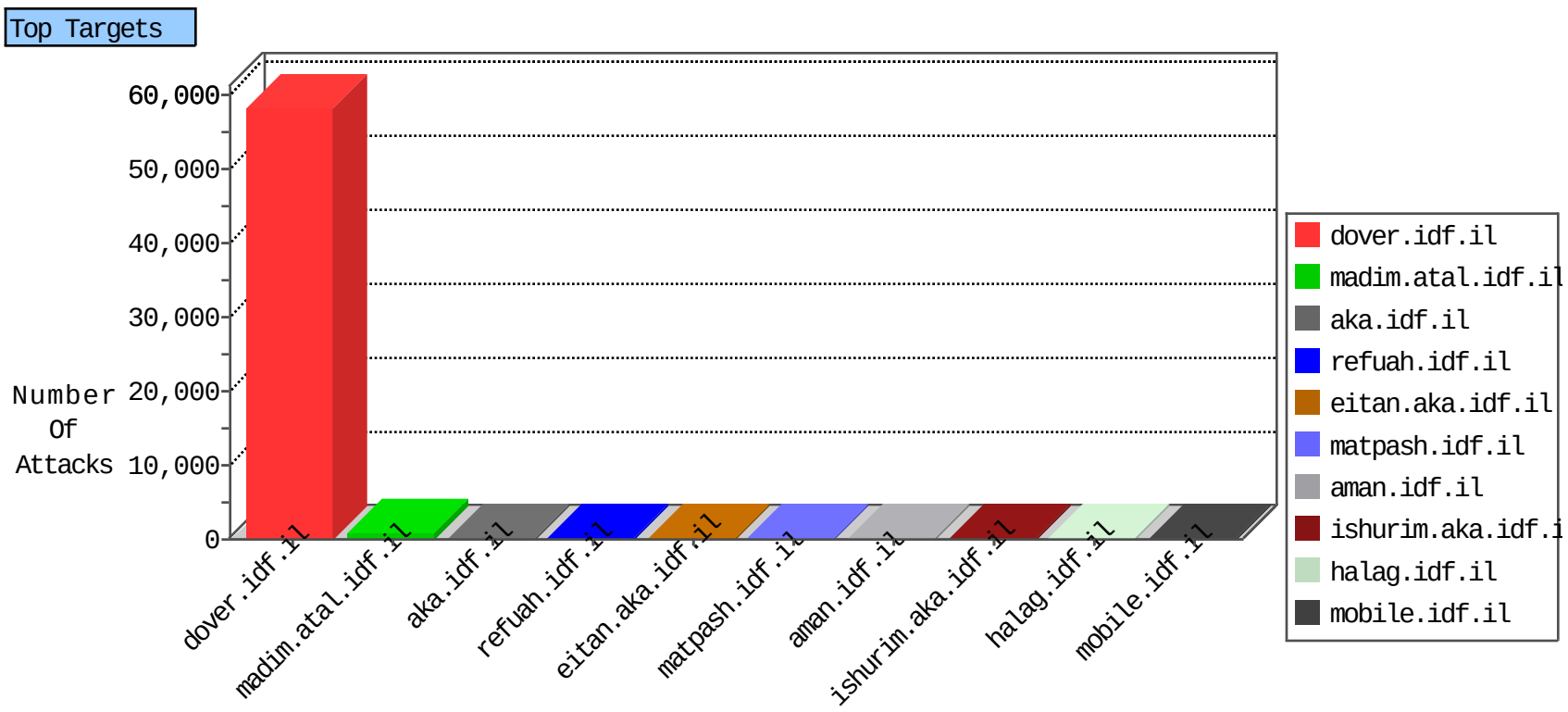
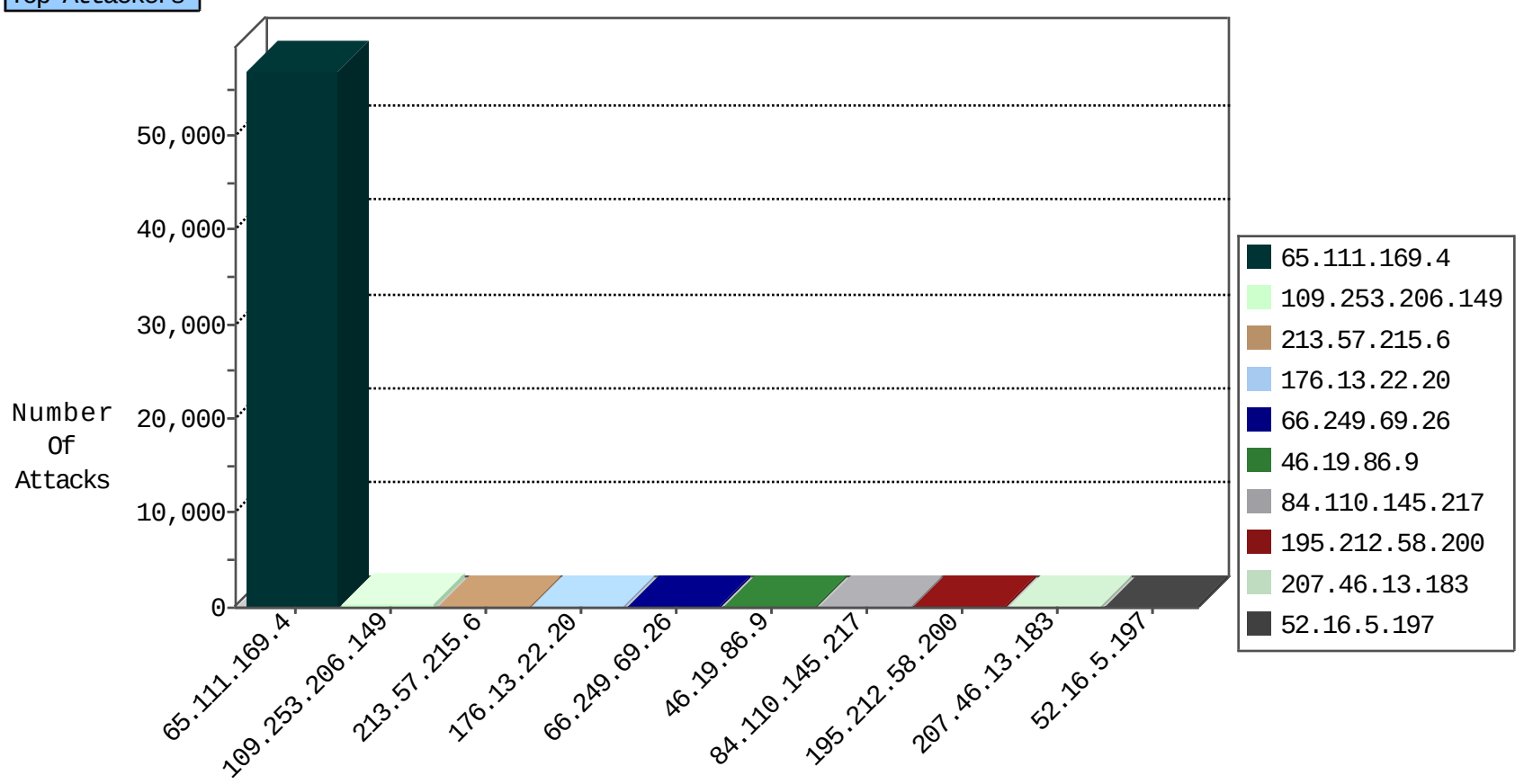
02-17-2016-11:04:04 to 02-17-2016-12:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-17-2016-11:04:04 to 02-17-2016-12:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
65.111.169.4	United States	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	32279
65.111.169.4	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	225
65.111.169.4	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	101
66.249.69.26	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	75
80.179.127.145	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	63
195.212.58.200	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	32
46.32.127.176	Jordan	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	26
50.87.144.145	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	25
66.249.91.14	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
109.152.40.83	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
185.57.80.147	Romania	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	17
66.249.69.42	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	17
73.54.32.24	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	17
195.212.58.200	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
37.26.146.151	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	15
176.205.22.43	United Arab Emirates	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	14
66.249.93.103	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	13
207.46.13.183	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	13
46.16.142.100	Cyprus	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	13
199.59.148.209	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
83.150.7.4	Switzerland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
155.69.16.255	Singapore	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
37.26.148.209	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
66.249.91.22	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
66.249.69.34	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
46.16.142.100	Cyprus	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
66.249.69.34	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
46.16.142.100	Cyprus	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
82.205.57.7	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
37.201.170.241	Germany	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
37.26.148.237	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
37.26.146.151	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
157.55.39.94	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
207.46.13.183	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
82.213.48.38	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
198.1.101.123	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
37.26.148.248	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
157.55.39.94	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	7
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
185.46.214.59	Switzerland	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
213.6.119.154	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
85.75.30.225	Greece	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
208.109.97.62	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
195.212.58.200	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	6
178.214.91.155	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
192.118.27.253	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
107.170.142.158	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
178.214.91.155	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	5
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
107.170.78.137	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5

02-17-2016-11:04:04 to 02-17-2016-12:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-17-2016-11:04:04 to 02-17-2016-12:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
2.52.135.233	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
194.114.146.227	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
180.76.15.157	147.237.72.166	China	aka.idf.il	portscan: TCP Distributed Portscan	1
79.181.217.210	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.156	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.74.92	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.235	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.171.128	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
58.253.96.122	147.237.77.205	China	prisha.idf.il	ET SCAN NMAP -sS window 3072	1
46.19.85.237	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-17-2016-11:04:04 to 02-17-2016-12:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
65.111.169.4	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55532
46.19.86.9	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
185.57.80.147	Romania	147.237.77.216	dover.idf.il	drop	SAM rule	drop	26
46.117.67.23	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	26
207.46.13.183	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
109.64.9.29	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
2.52.137.174	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	23
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	22
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	22
66.249.69.26	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	21
66.249.69.26	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	20
79.180.198.234	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
157.55.39.94	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
81.218.251.251	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
37.26.148.209	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
80.179.5.176	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
132.72.8.167	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
52.16.5.197	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
212.143.220.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.163	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	10
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
37.201.170.241	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
37.26.146.130	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
213.6.119.154	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
176.13.12.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
93.184.3.246	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.16.142.100	Cyprus	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.79.6	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
93.184.3.246	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
46.16.142.100	Cyprus	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
207.46.13.183	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
40.77.167.38	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
207.46.13.181	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
109.0.199.190	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.10	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
40.77.167.38	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
208.115.113.92	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.10	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.102.222.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.94	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
194.90.151.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

02-17-2016-11:04:04 to 02-17-2016-12:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.206.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	212
109.253.206.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	205
213.57.215.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	109
213.57.215.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	102
176.13.22.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	87
84.110.145.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	78
176.13.22.20	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.22.20	Block	52
109.253.206.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	9
79.176.35.237	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 79.176.35.237	Block	8
209.88.157.156	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 209.88.157.156	Block	8
79.178.116.68	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.178.116.68	Block	7
2.54.38.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.253.204.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
209.88.157.156	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	5
46.19.85.15	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	4
79.178.116.68	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	4
213.151.49.171	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	4
176.13.1.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.4.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.246	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
46.19.85.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
149.78.57.44	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$96 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	2
2.54.169.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
74.82.47.3	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
212.76.112.169	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/67778.pdf&sa=u&ved=0ahukewiglo-uuf7kahuevxokhd81dqiqfggcmag&usg=afqjcneyouaucishaxeci3pvrjlz8csweg	Block	1
62.210.162.209	France	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
105.102.134.175	Algeria	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
40.77.167.58	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/default.aspx	Block	1
169.229.3.91	United States	147.237.77.19	law-forum.idf.il	Illegal Byte Code Character in Method	Block	1
81.218.251.251	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 81.218.251.251	Block	1
79.178.116.68	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	1
213.57.177.102	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	1
2.54.38.227	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1381	Block	1
146.185.234.48	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/tags/tags.aspx	Block	1
109.66.41.206	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$85 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
66.249.64.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/2391.jpg	Block	1
207.46.13.183	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
89.139.232.217	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/ajax/updatestatus.php	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Illegal Byte Code Character in Method	Block	1
2.54.187.221	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/login.aspx	None	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Header Name	Block	1
80.246.130.132	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in www.atal.idf.il/1440-he/atal.aspx	Block	1
2.52.156.208	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1133-he/atal.aspx	Block	1
109.253.210.147	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
79.176.35.237	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
212.179.129.6	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
62.210.162.209	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
184.105.139.68	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
105.102.134.175	Algeria	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Abnormally Long Request method	Block	1

02-17-2016-11:04:04 to 02-17-2016-12:04:04