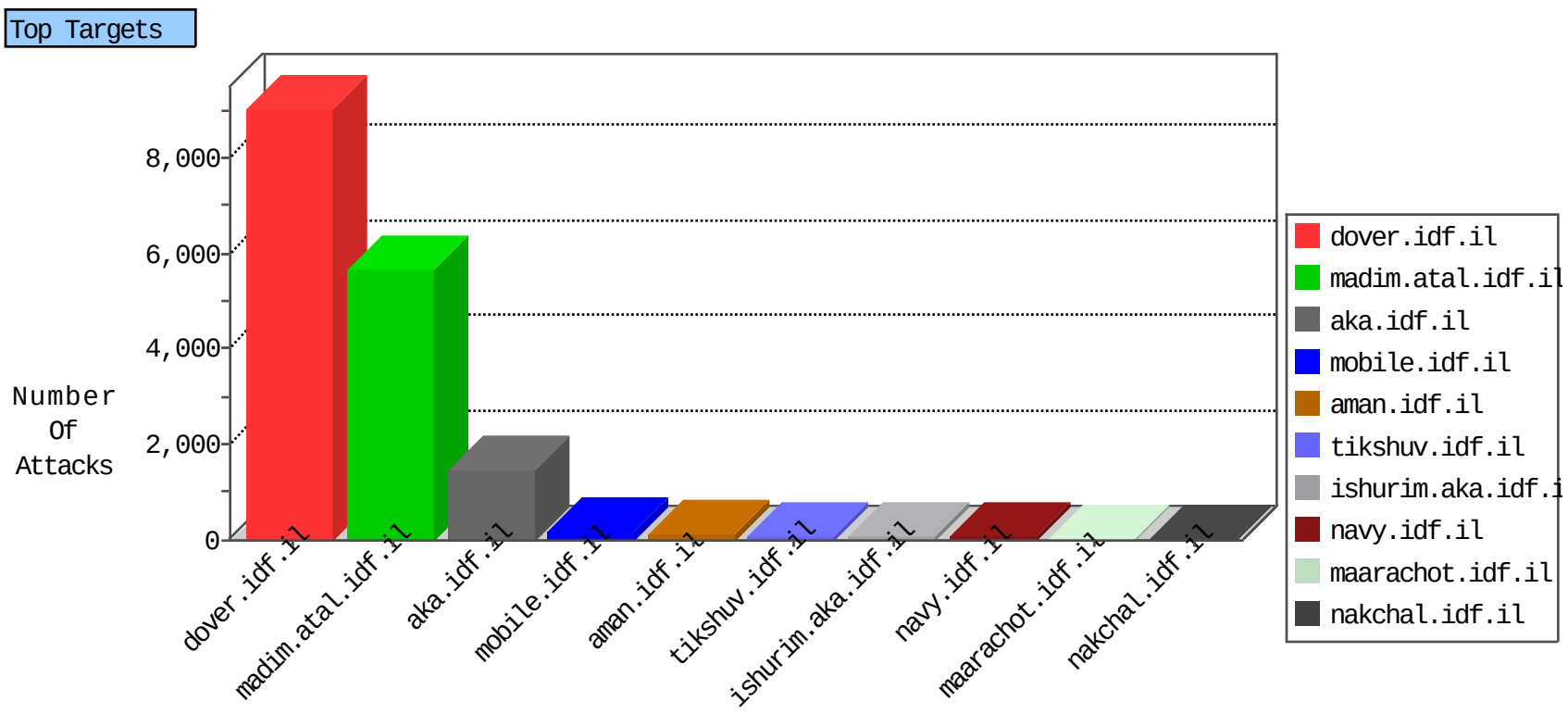
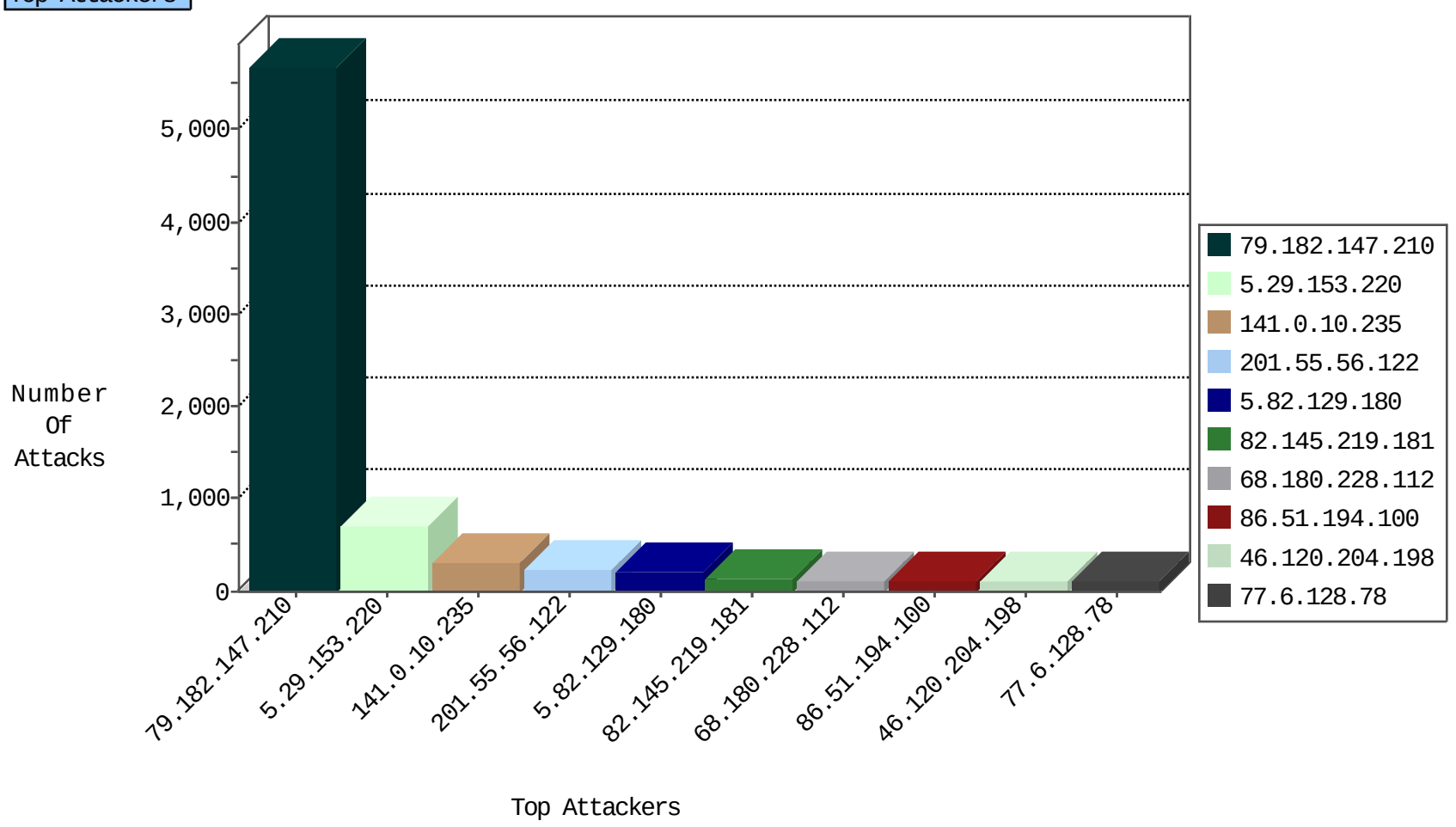
10-26-2015-19:04:06 to 10-26-2015-20:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-26-2015-19:04:06 to 10-26-2015-20:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.153.220	Israel	147.237.72.166	aka.idf.il	TCP Scan (vertical)	drop	3572
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	700
93.173.235.112	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	55
94.159.176.127	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	34
31.183.48.94	Poland	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
185.120.126.14		147.237.77.216	dover.idf.il	SYN Flood full table	drop	28
173.11.20.29	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	27
185.32.179.161	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
67.164.68.166	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
37.26.147.158	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	16
100.100.71.196		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15
89.138.84.183	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	13
37.26.149.148	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
109.67.178.71	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
109.65.57.41	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
176.13.8.171	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
87.68.153.105	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
109.65.33.176	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
2.52.1.152	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
2.54.20.145	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
165.255.87.224		147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
85.250.211.151	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
213.151.35.218	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
79.181.163.112	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
84.226.110.21	Switzerland	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
77.127.158.49	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
81.218.154.224	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
84.110.209.148	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
79.182.224.239	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
80.246.137.58	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
84.108.214.39	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
62.90.235.170	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
84.110.209.121	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
176.12.139.42	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
176.13.16.30	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
87.69.109.221	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
85.65.73.156	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
109.186.173.85	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.13.16.171	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
93.173.12.57	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.52.62.104	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
93.173.12.57	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
46.117.181.92	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
185.32.179.216	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
31.154.91.179	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
149.78.97.146	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.177.9.97	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.12.147.17	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
149.78.196.165	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
5.102.254.64	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4

10-26-2015-19:04:06 to 10-26-2015-20:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-26-2015-19:04:06 to 10-26-2015-20:04:06

Top Attackers In IDS

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

10-26-2015-19:04:06 to 10-26-2015-20:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.0.10.235	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	315
201.55.56.122	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	228
5.82.129.180	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	211
82.145.219.181	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	126
86.51.194.100	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	115
77.6.128.78	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	108
2.54.37.88	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	101
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	99
24.190.175.146	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	90
37.26.149.184	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	88
79.180.2.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	73
207.141.39.157	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
46.19.85.189	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
87.68.29.215	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
84.108.40.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
37.26.146.145	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
31.205.105.179	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
109.65.59.208	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
46.19.85.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
93.173.158.73	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
197.133.127.69	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
98.210.37.154	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
89.139.0.202	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
2.54.20.145	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
77.125.146.16	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
80.246.130.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
62.219.167.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
79.177.9.97	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
37.142.180.169	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	44
50.84.173.174	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
64.233.172.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
37.142.233.109	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	37
93.173.233.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
79.182.224.239	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
79.179.154.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
2.54.47.34	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
82.145.211.217	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
212.179.42.242	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
176.13.0.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
165.255.87.224		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
109.186.173.85	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
216.255.123.98	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
37.26.146.188	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
90.3.210.138	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
109.67.178.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29

10-26-2015-19:04:06 to 10-26-2015-20:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.182.147.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	5680
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	56
80.246.130.186	Israel	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1065-he/dover.aspx parameter SearchText	Block	42
77.125.146.16	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	42
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	42
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
46.120.204.198	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/ajax/updatestatus.php	Block	28
46.120.204.198	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	28
79.180.4.124	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	28
46.120.204.198	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	28
109.160.171.146	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	28
176.13.16.171	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	28
2.54.20.145	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	28
109.160.171.146	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	28
46.120.204.198	Israel	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	28
176.13.22.165	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	14
66.249.64.243	Israel	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	14
109.66.1.52	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	14
2.54.22.254	Israel	147.237.0.19	madim.atal.idf.il	Cookie Tampering on cookie Login: Expected ********** ********** ********** **********, Observed ********** ********** ********** ****	None	14
87.68.84.175	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
79.176.148.165	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	14
212.34.11.82	Jordan	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	14
112.119.194.188	Hong Kong	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	14
95.86.85.26	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	14
79.182.195.205	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
178.62.209.185	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/general.aspx?docid=70956	Block	14
77.125.146.16	Israel	147.237.72.166	aka.idf.il	Double URL Encoding - parameter: search in www.aka.idf.il/main/giyus/pniothandler1.asmx/search	Block	14
66.249.67.129	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	14
109.67.18.219	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 109.67.18.219 (Open Mode)	None	14
5.22.131.251	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
87.69.92.192	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	14
79.176.158.200	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	14
212.34.11.82	Jordan	147.237.77.216	dover.idf.il	Illegal HTTP Version Safari/537.36	Block	14
176.12.137.189	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	14
95.86.94.92	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
178.62.209.185	United Kingdom	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/getfile/getfile.aspx?filename=xhbyb3nly3v0aw9ulwrvy3ncyxzpcm90x3nhbwltxgktmtu4ltaylnbkzg==&infocenteritem=true	Block	14
66.249.69.51	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
109.67.18.219	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	14
87.69.162.250	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pniasubmittedsuccessfully.aspx	None	14
37.142.68.53	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	14
212.34.11.82	Jordan	147.237.77.216	dover.idf.il	Multiple Malformed URL from 212.34.11.82	Block	14
176.13.6.8	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
109.64.103.241	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1135-he/atal.aspx	Block	14
2.52.62.104	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
87.68.17.48	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	14
77.237.138.202	Czech Republic	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /	Block	14
188.143.232.11	Russian Federation	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 188.143.232.11	Block	14
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	14
87.69.162.250	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	14

10-26-2015-19:04:06 to 10-26-2015-20:04:06