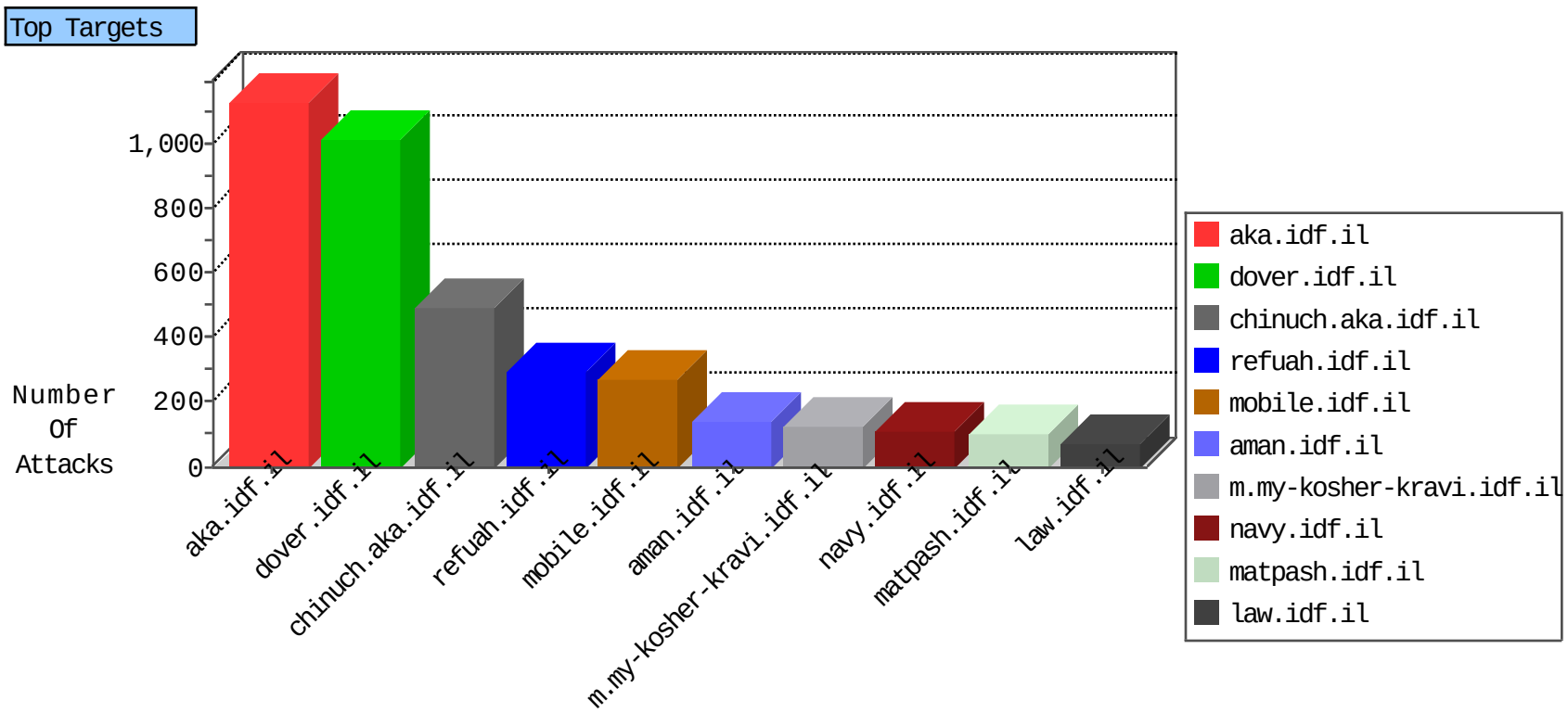
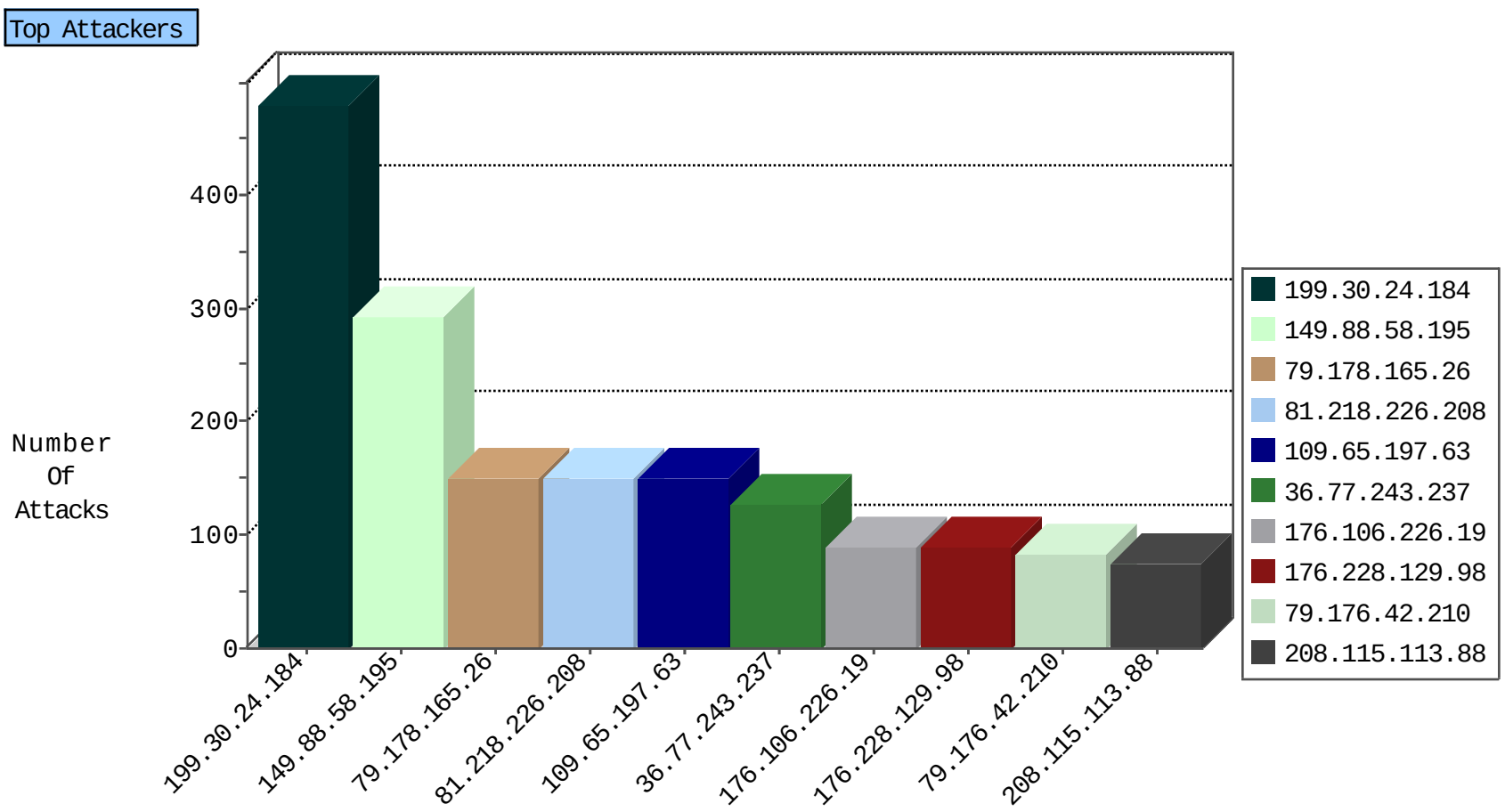
10-30-2015-08:04:09 to 10-30-2015-09:04:09

IDF Under Attack
Daily Report

Top Targets



Top Attackers



10-30-2015-08:04:09 to 10-30-2015-09:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.34	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3413
66.249.69.76	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3200
66.249.69.84	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1194
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	106
212.76.100.144	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
185.32.179.129	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	24
84.111.155.155	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	23
213.57.118.66	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
46.117.241.133	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
46.19.86.175	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
82.205.0.136	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
79.181.27.142	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
84.108.126.86	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
213.57.118.66	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
185.32.179.129	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
79.176.42.210	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.86.175	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
5.22.129.235	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
46.117.241.133	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
80.246.136.199	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.13.22.127	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
5.22.129.215	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
79.177.190.37	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
78.137.4.31	Ukraine	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
37.26.147.138	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
61.147.103.92	China	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
176.13.9.143	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
213.57.214.9	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
80.246.136.199	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
85.12.238.254	Russian Federation	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	2
64.233.172.178	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
183.61.253.215	China	147.237.76.177	ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
46.101.3.227	Russian Federation	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
176.13.6.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
2.54.184.181	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
78.137.4.31	Ukraine	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.101.3.227	Russian Federation	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
5.22.130.103	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
46.174.52.15	Russian Federation	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
2.54.184.181	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
64.233.172.170	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
10.0.0.5		147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
46.117.241.133	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
10.0.0.5		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

10-30-2015-08:04:09 to 10-30-2015-09:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.29.74.207	Russian Federation	147.237.77.74	law.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1
162.210.196.97	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1

10-30-2015-08:04:09 to 10-30-2015-09:04:09

Top Attackers In IDS

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

10-30-2015-08:04:09 to 10-30-2015-09:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.88.58.195	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	266
36.77.243.237	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	127
80.246.130.241	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
162.243.32.128	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	50
37.26.148.177	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
100.100.29.200		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	22
66.249.93.196	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.249.93.192	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
77.158.88.42	France	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
100.100.43.54		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
46.19.86.143	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	14
79.181.189.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
66.249.64.133	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
46.19.85.173	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	13
79.176.42.210	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.103.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.93.200	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.23.4		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
85.250.95.141	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
157.55.39.8	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
202.79.209.95	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
168.187.227.162	Kuwait	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.237	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.180.62.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
77.126.229.180	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	9
151.80.31.112	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
220.255.98.6	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.93.196	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
79.181.27.142	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.213	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.102.7.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
80.246.136.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.117.241.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
79.181.108.212	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.117	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
118.37.223.172	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
73.151.195.68	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
84.111.155.155	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.246.136.144	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.157.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

10-30-2015-08:04:09 to 10-30-2015-09:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.30.24.184	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	480
81.218.226.208	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	105
79.178.165.26	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.178.165.26	Block	75
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	75
109.65.197.63	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	75
109.65.197.63	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	75
79.178.165.26	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	75
79.176.42.210	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	60
176.106.226.19	Israel	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	45
84.228.49.104	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	45
176.106.226.19	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/ajax/updatestatus.php	Block	45
176.228.129.98	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	45
176.228.129.98	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	45
81.218.226.208	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	45
5.29.46.33	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	30
46.19.85.86	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	30
77.126.229.180	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	30
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	30
176.13.0.246	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	30
72.9.148.10	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	30
5.29.46.33	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	30
74.82.47.3	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on 147.237.0.17/	Block	15
66.249.75.91	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/894-he	Block	15
157.55.39.55	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-14816-he/dov	Block	15
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	15
94.153.51.81	Ukraine	147.237.77.74	law.idf.il	Distributed Unknown HTTP Request Method	Block	15
176.13.0.246	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.13.0.246	None	15
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.204	Block	15
141.212.121.192	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	15
66.249.67.235	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/13102010masaiyot.aspx	Block	15
31.131.103.105	Ukraine	147.237.77.74	law.idf.il	Parameter Type Violation pos in www.mag.idf.il/261-2107-en/patzar.aspx	Block	15
213.87.127.178	Russian Federation	147.237.77.74	law.idf.il	Distributed Unknown HTTP Request Method	Block	15
77.126.28.224	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	15
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
176.12.140.230	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
95.86.112.51	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mai/n/giyus	Block	15
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	15
79.179.108.23	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	15
5.29.215.250	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
176.13.4.29	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	15
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/13022011yezu.aspx	Block	15
141.212.121.192	United States	147.237.77.235	sviva.idf.il	Unauthorized URL Access to 147.237.77.235/	Block	15
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
213.151.32.163	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
85.65.192.207	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	15
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/coordinationgaza/news_gaza/pages/130trucks.aspx	Block	15
176.12.150.73	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
80.246.136.243	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	15
5.29.246.89	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	15

10-30-2015-08:04:09 to 10-30-2015-09:04:09