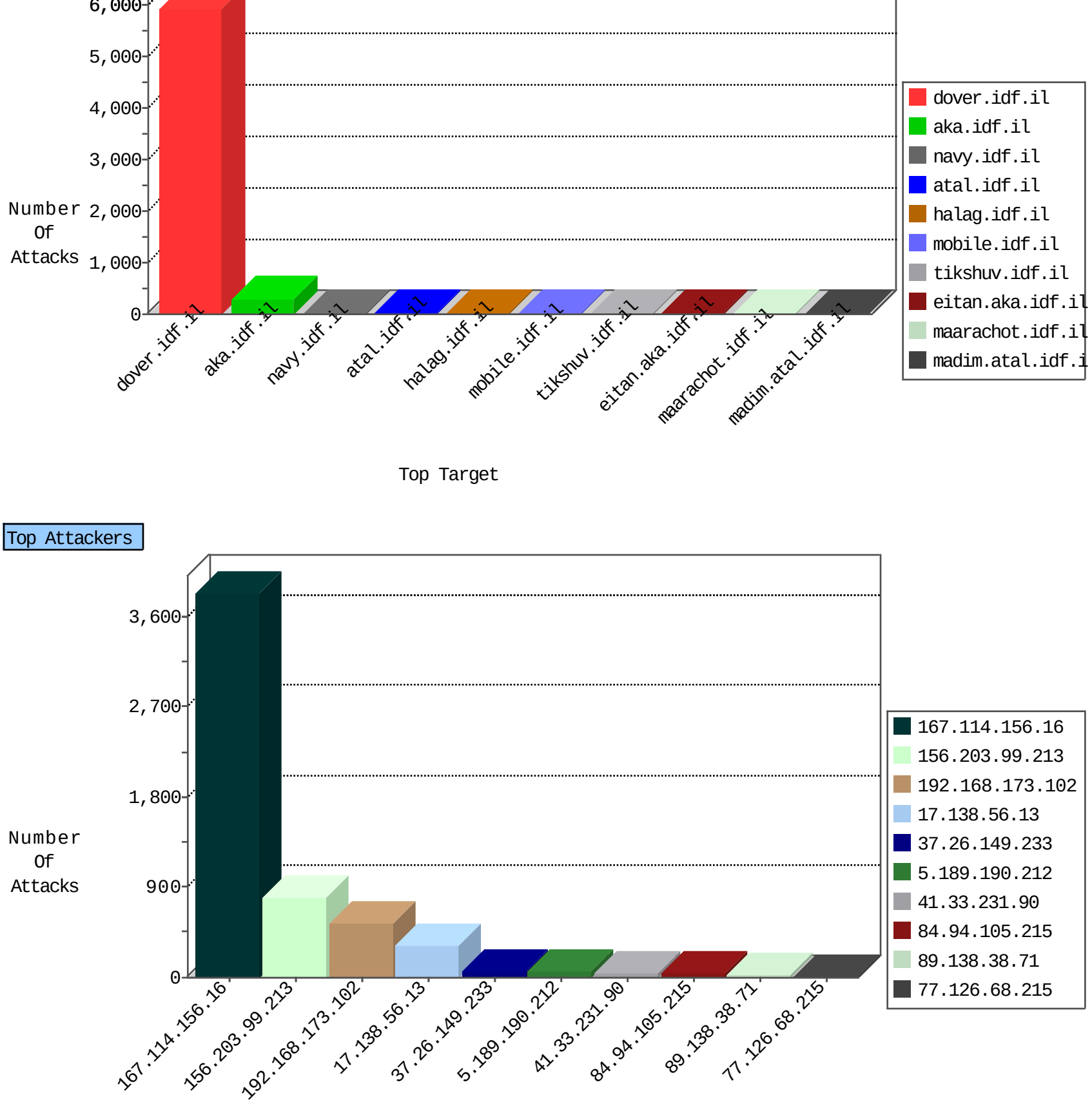
04-09-2016-11:04:09 to 04-09-2016-12:04:09

IDF Under Attack Daily Report



04-09-2016-11:04:09 to 04-09-2016-12:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	27152
156.203.99.213	Egypt	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	6112
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	3844
156.203.99.213	Egypt	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	196
156.203.99.213	Egypt	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	129
149.78.233.233	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	101
156.203.99.213	Egypt	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-lgn	dest-reset	29
156.203.99.213	Egypt	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	11
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	9
208.67.1.19	United States	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
208.67.1.19	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
185.70.184.164	Netherlands	147.237.77.61	e.cogat.idf.il	L4 Source or Dest Port Zero	drop	1
208.67.1.19	United States	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
208.67.1.19	United States	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.72.217	e.idf.il	Block_Udp_All_Nets	drop	1
208.67.1.19	United States	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
74.82.47.9	United States	147.237.8.27	e.madim.atal.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.77.205	prisha.idf.il	Block_Udp_All_Nets	drop	1
208.67.1.19	United States	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1

04-09-2016-11:04:09 to 04-09-2016-12:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.71.37.41	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
106.38.241.149	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
199.30.25.177	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
156.203.99.213	Egypt	147.237.77.216	dover.idf.il	10725: TCP: LOIC DDoS Tool	Block	1

04-09-2016-11:04:09 to 04-09-2016-12:04:09

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	3
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
156.203.99.213	147.237.77.216	Egypt	dover.idf.il	ET CURRENT_EVENTS Inbound Low Orbit Ion Cannon LOIC DDOS Tool desu string	2
141.101.178.137	147.237.76.176	Russian Federation	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
106.184.2.29	147.237.77.216	Japan	dover.idf.il	ET SCAN Potential SSH Scan	1
84.200.15.174	147.237.0.17	Germany	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
208.100.26.228	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
178.162.199.206	147.237.77.216	Germany	dover.idf.il	SERVER-IIS trace.axd access	1
145.132.1.222	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
145.132.1.222	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -f -sS	1
141.101.178.137	147.237.76.177	Russian Federation	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
121.40.195.144	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
84.200.15.174	147.237.0.17	Germany	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
84.200.15.174	147.237.0.17	Germany	m.my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
208.100.26.228	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
145.132.1.222	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
141.101.178.137	147.237.76.199	Russian Federation	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1

04-09-2016-11:04:09 to 04-09-2016-12:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	375
17.138.56.13	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	261
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	173
156.203.99.213	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	127
17.138.56.13	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	49
5.189.190.212	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
156.203.99.213	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	26
37.26.149.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
89.138.38.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
37.26.149.233	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	22
84.94.105.215	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
77.126.68.215	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
84.94.105.215	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.19.85.254	Israel	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
5.189.190.212	Germany	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	10
37.26.149.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.27	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.186.49.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.226.26.144	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
207.46.13.67	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
79.179.61.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.54.164.112	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.116.209.191	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.109.152.101	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.10.227.2	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.178.24.19	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
156.203.99.213	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	6
85.64.112.228	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.65	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.67.210.152	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.211.228.121	Qatar	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.116.113.49	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
85.64.136.134	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
84.94.105.215	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
207.46.13.107	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.182.194.241	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
188.247.76.108	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.120.126.111	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
87.70.34.85	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

04-09-2016-11:04:09 to 04-09-2016-12:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
156.203.99.213	Egypt	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 156.203.99.213	Block	28
156.203.99.213	Egypt	147.237.77.216	dover.idf.il	Multiple Malformed URL from 156.203.99.213	Block	25
109.64.88.236	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.64.88.236	Block	8
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	6
219.155.147.158	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	5
219.155.147.158	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 219.155.147.158	Block	4
156.203.99.213	Egypt	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 156.203.99.213	Block	2
84.111.1.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.32.179.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
197.231.70.20	Gabon	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 197.231.70.20	Block	2
185.120.125.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.27.106.60	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 185.27.106.60	Block	2
84.94.114.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.126.68.215	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20315-he/dover.aspx	Block	1
197.231.70.20	Gabon	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
178.162.199.206	Germany	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
217.132.146.134	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.79.120	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
46.43.126.57	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/admin	Block	1
79.177.196.12	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/5/size100x0/3045.jpg	Block	1
178.162.199.206	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/trace.axd	Block	1
5.10.229.226	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
85.250.185.104	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
66.249.79.124	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/webresource.axd	Block	1
46.120.150.5	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
80.246.136.201	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.66.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
207.46.13.120	United States	147.237.72.166	aka.idf.il	Unknown Parameter 4f9c0c80 in www.aka.idf.il/main/home/default.aspx	None	1
185.10.3.15	Russian Federation	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1294-en/dover.aspx parameter id	Block	1
37.187.114.171	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to /irj/portal	Block	1
71.227.55.147	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
54.153.33.152	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
196.128.108.41	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
169.229.3.90	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/ts.php	Block	1
84.94.105.215	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
207.46.13.174	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
40.77.167.54	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/captcha.ashx	Block	1
151.249.196.141	Belarus	147.237.77.216	dover.idf.il	Parameter Type Violation id in www.idf.il/1294-en/dover.aspx	Block	1
219.155.147.158	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/plus/mytag_js.php	Block	1
71.227.55.147	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
54.153.33.152	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
196.128.108.41	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
178.162.199.206	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.162.199.206	Block	1
66.249.69.93	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.69.93	Block	1
185.27.106.60	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
46.43.126.57	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Admin Blocking	Block	1

04-09-2016-11:04:09 to 04-09-2016-12:04:09