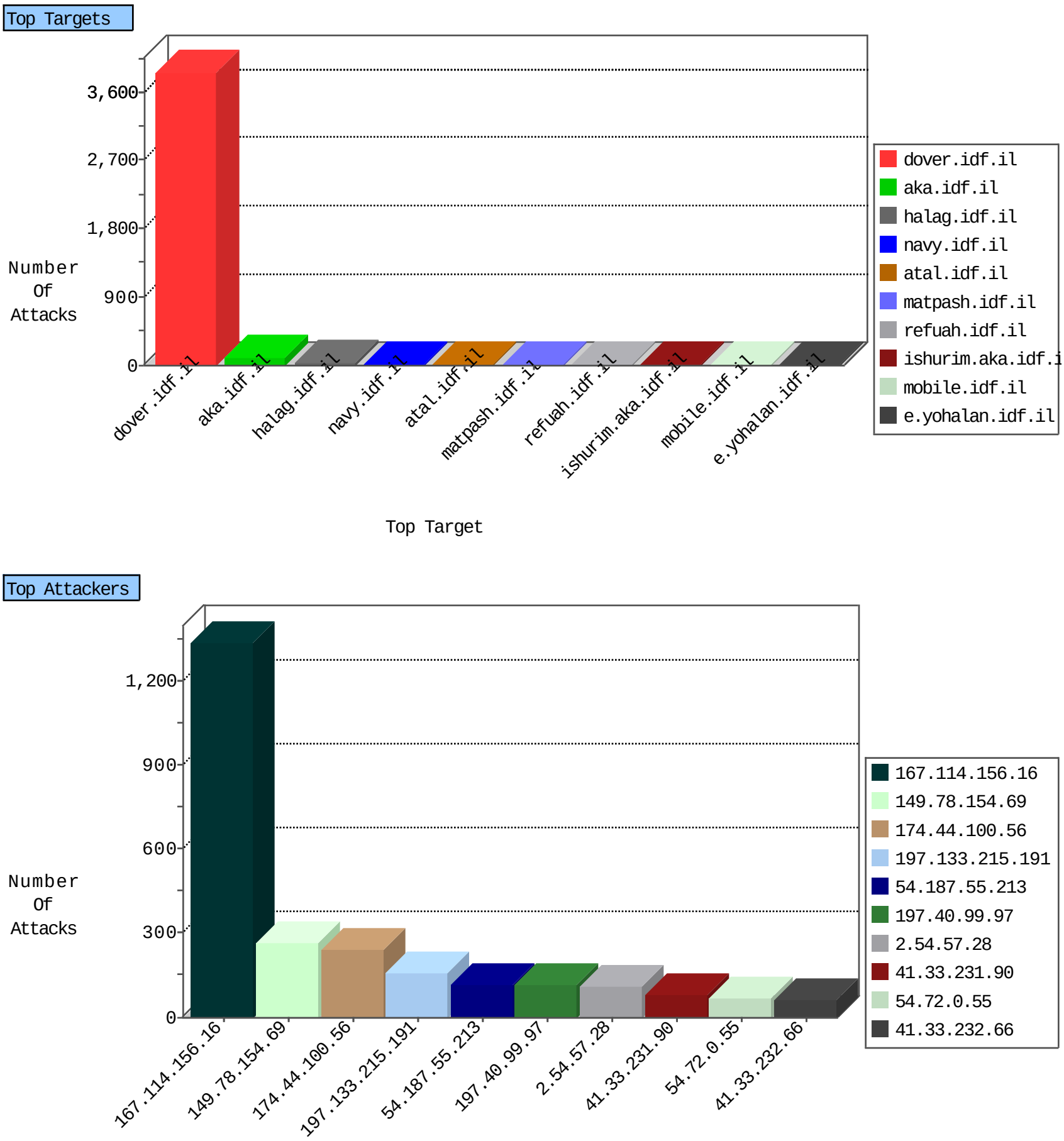
11-06-2015-05:04:08 to 11-06-2015-06:04:08

IDF Under Attack Daily Report



11-06-2015-05:04:08 to 11-06-2015-06:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.73	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4553
66.249.67.6	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3224
149.78.154.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3065
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2326
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
222.186.56.42	China	147.237.76.198	e.yohalan.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
180.97.106.36	China	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	drop	1
112.175.228.69	Korea, Republic of	147.237.77.234	halag.idf.il	Invalid TCP Flags	drop	1
180.97.106.162	China	147.237.76.86	navy.idf.il	block-sp-traf1	drop	1
183.60.48.25	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1

11-06-2015-05:04:08 to 11-06-2015-06:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.149.178.174	United Kingdom	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
198.20.69.74	United States	147.237.8.24	e.lifestyle.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

11-06-2015-05:04:08 to 11-06-2015-06:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	9
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
125.208.13.94	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
89.248.174.106	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
200.2.165.224	147.237.72.167	Suriname	ishurim.aka.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
193.107.16.206	147.237.0.34	Russian Federation	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
104.245.101.69	147.237.77.216		dover.idf.il	SERVER-WEBAPP admin.php access	1
46.151.52.8	147.237.76.42	Ukraine	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
40.115.58.160	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1

11-06-2015-05:04:08 to 11-06-2015-06:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	262
174.44.100.56	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	242
197.133.215.191	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	157
54.187.55.213	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	114
197.40.99.97	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	114
2.54.57.28	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	108
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	68
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	63
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	62
208.115.113.89	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	58
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	52
212.199.182.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
154.20.37.56	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	43
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
75.183.52.46	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	41
72.9.148.10	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	41
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
45.16.159.164		147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
165.225.72.54	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
66.249.81.218	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	31
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
157.55.2.139	United States	147.237.77.234	halag.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
66.249.81.212	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
82.80.25.221	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
66.249.69.42	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
79.176.150.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop		drop	24
66.249.69.34	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
157.55.39.208	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
131.118.85.100	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
110.174.76.65	Australia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
157.55.39.92	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
69.112.124.174	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
85.64.205.157	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
157.55.39.180	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
213.57.141.203	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
65.19.138.33	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
66.249.69.26	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.103.36	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
198.58.102.96	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
66.249.81.212	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
69.164.219.121	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
176.67.98.139	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
66.249.69.42	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
157.55.39.115	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
77.127.208.58	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
40.77.167.59	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
40.77.167.39	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.126.10	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.65.126.10	Block	7
187.149.197.237	Mexico	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 187.149.197.237	Block	6
104.236.201.44		147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 104.236.201.44	Block	3
109.65.126.10	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
162.243.215.132	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 162.243.215.132	Block	2
104.236.201.44		147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/sip_storage/	Block	2
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	1
62.210.88.201	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.google.pl/search	Block	1
182.118.60.35	China	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
109.65.126.10	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
66.249.78.4	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
207.46.13.60	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/	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
180.76.15.139	China	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
40.77.167.40	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/8/4538.pdf	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/see	Block	1
62.210.88.201	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.google.pl/search	Block	1
115.188.41.81	New Zealand	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	1
66.249.78.11	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
207.46.13.94	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/sip_storage/	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
182.118.45.212	China	147.237.76.30	himush.idf.il	Unauthorized URL Access to 147.237.76.30/	Block	1
40.77.167.90	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
104.236.201.44		147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
66.249.69.34	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.34	Block	1
66.249.65.83	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
187.149.197.237	Mexico	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/giyus/general/	Block	1
157.55.39.166	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.166	Block	1
66.249.79.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/1056-en/hamaz.aspx	Block	1
216.218.206.66	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.67.133	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
46.117.164.60	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
182.118.54.31	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
66.249.69.34	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	1
66.249.65.86	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
190.232.70.148	Peru	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
79.182.8.1	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
46.117.164.60	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 46.117.164.60	None	1
182.118.55.138	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.69.48	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
192.115.100.190	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/iturim/asp/wars.asp	Block	1
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
162.243.215.132	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	1
40.77.167.14	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/sip_storage/	Block	1