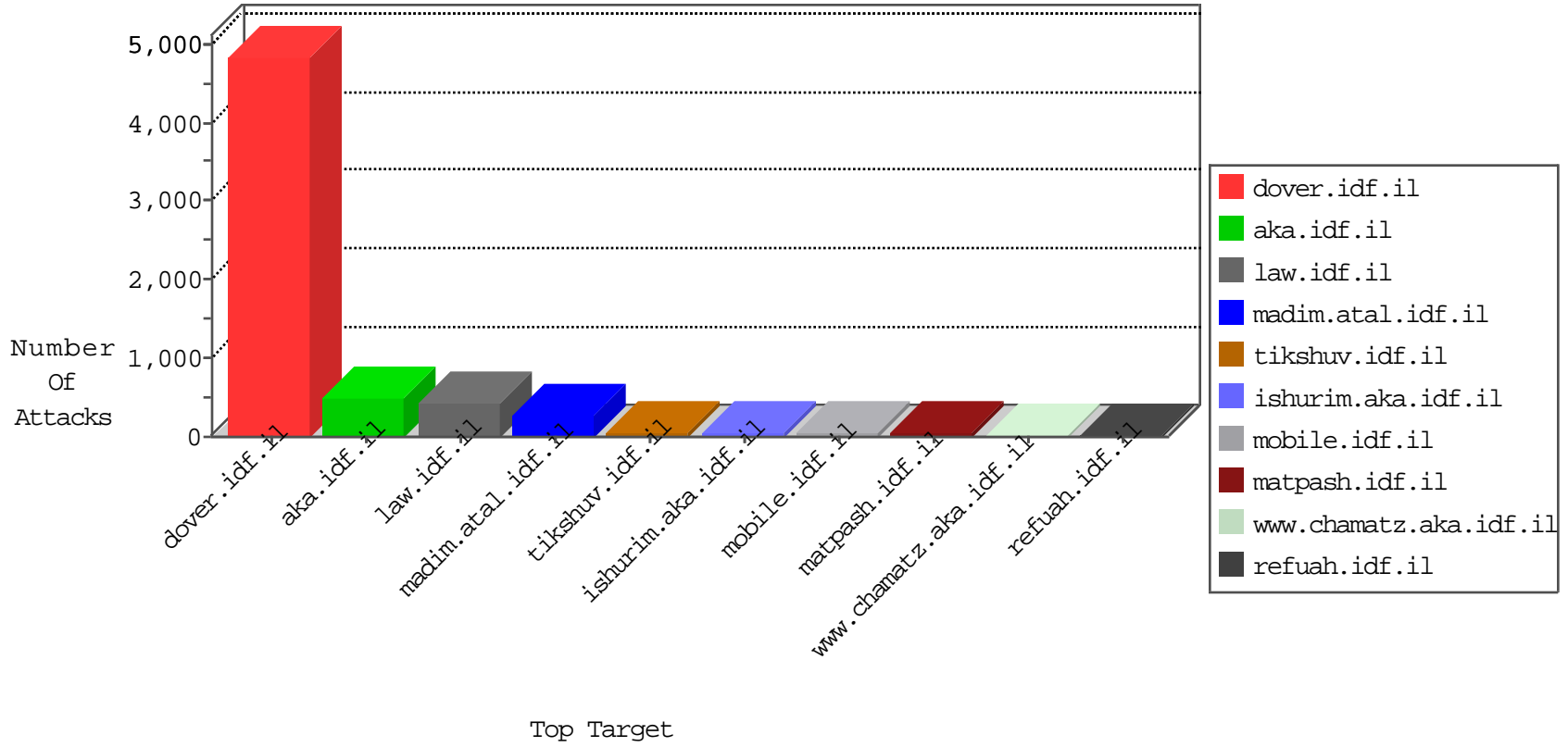


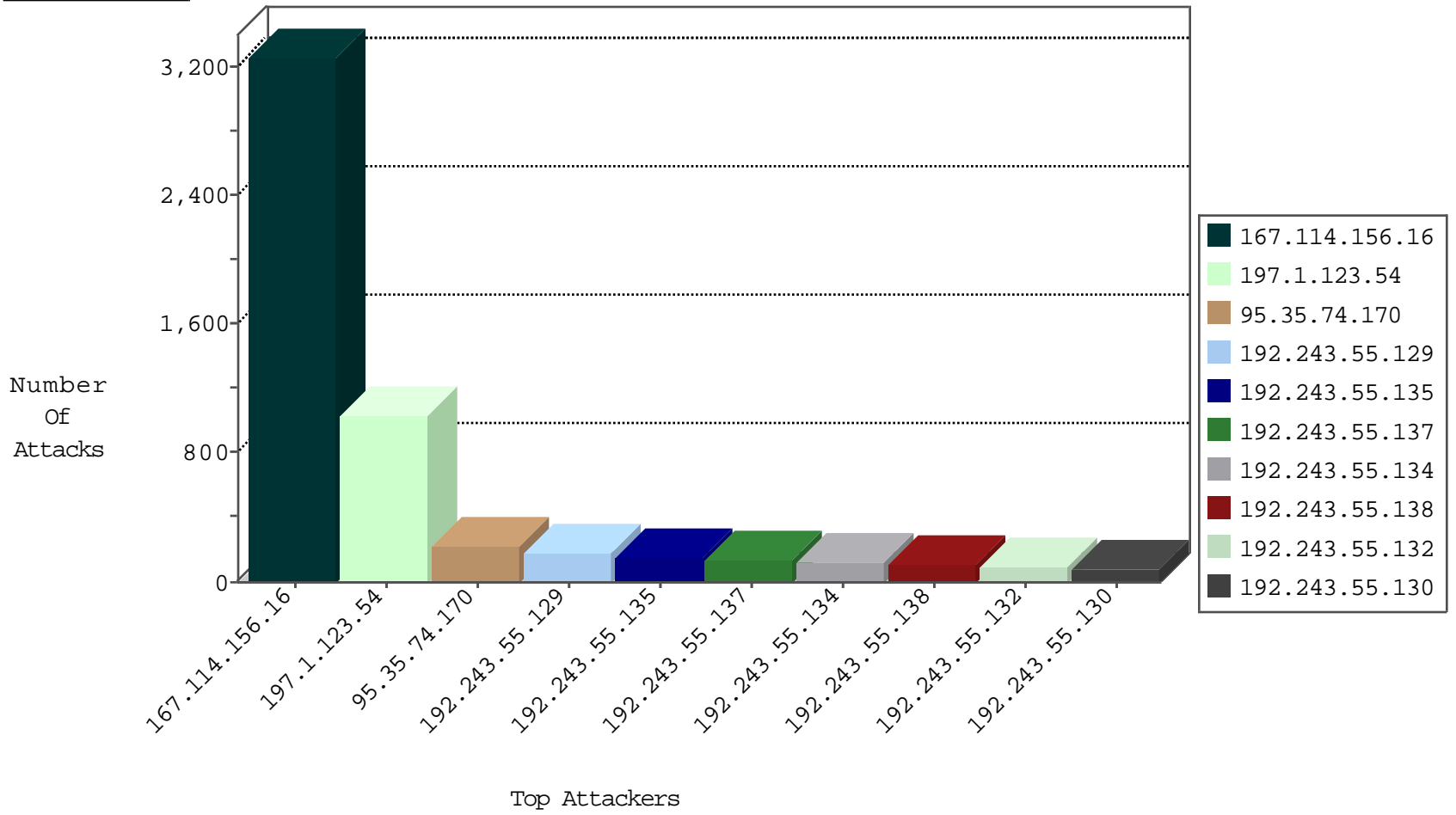
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	3253
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	55
79.180.111.215	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
82.145.217.106	Europe	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	3
213.151.55.232	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
82.145.209.62	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	2
185.35.62.141	Switzerland	147.237.76.176	test.ncore.idf.i	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
192.243.55.135	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
111.85.191.131	China	147.237.76.177	ncore.idf.il	JIM_Purple_Con_Limit_Http	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.108.93.19	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
80.246.130.105	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
89.139.61.114	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
213.8.204.2	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
61.135.189.99	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
106.120.173.85	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
123.126.113.161	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	3
162.210.196.97	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
162.210.196.98	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

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

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.1.123.54	Tunisia	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1030
192.116.159.251	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
41.226.78.171	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
192.243.55.135	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	22
192.243.55.129	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	20
141.0.15.163	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
64.233.172.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
192.243.55.129	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
192.243.55.129	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
192.243.55.137	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
109.253.209.130	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
2.54.176.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
192.243.55.134	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
192.243.55.132	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
192.243.55.137	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
192.243.55.134	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	12
192.243.55.135	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
192.243.55.129	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
192.243.55.130	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
192.243.55.131	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
192.243.55.135	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	12
64.233.172.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.134	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.135	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.134	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	10
192.243.55.137	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
192.243.55.129	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
192.243.55.137	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.130	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.131	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
192.243.55.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
192.243.55.132	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.243.55.136	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.137	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.243.55.135	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.137	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
95.35.74.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	219
93.172.178.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
5.22.129.96	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	15
64.79.85.205	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 64.79.85.205	Block	14
31.168.164.118	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 31.168.164.118	Block	14
199.30.25.84	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
185.120.126.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
46.117.251.167	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.117.251.167	Block	5
197.15.95.245	Tunisia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/0000000000000000	Block	4
65.55.210.205	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
199.30.24.129	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
199.30.24.202	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
79.176.62.8	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.176.62.8	Block	3
65.55.210.201	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
109.253.207.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.250.106.225	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	3
46.117.251.167	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	3
109.253.209.130	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
94.159.166.52	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mivtza	Block	2
46.19.85.103	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
90.228.175.90	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	2
176.13.10.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.129.175	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
80.178.9.153	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 80.178.9.153	Block	1
192.243.55.129	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
31.168.164.118	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/1125-he/idfg.asp	Block	1
85.250.168.199	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	1
68.180.229.226	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/540-he/patzar.aspx	Block	1
50.118.145.105	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
185.99.46.109	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
93.173.76.103	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.178.9.153	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files	Block	1
65.55.210.215	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.243.55.131	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/movies/strike_heb2.asf	Block	1
154.16.138.15	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
40.77.167.37	United States	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31/	Block	1
87.69.160.252	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.22.129.98	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
80.246.133.3	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
192.243.55.133	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	1
66.249.78.22	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/320/patzar.aspx	Block	1
157.55.39.120	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/milum/templates/www.behazdaa.org.il	Block	1
89.139.228.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
64.79.85.205	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/shared/usercontrols/headerupper/	Block	1
192.243.55.129	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/maslulimlist.aspx	Block	1
5.29.106.84	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
85.250.106.225	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.250.106.225	Block	1
192.243.55.135	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gallery.aspx	Block	1
66.249.78.82	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1