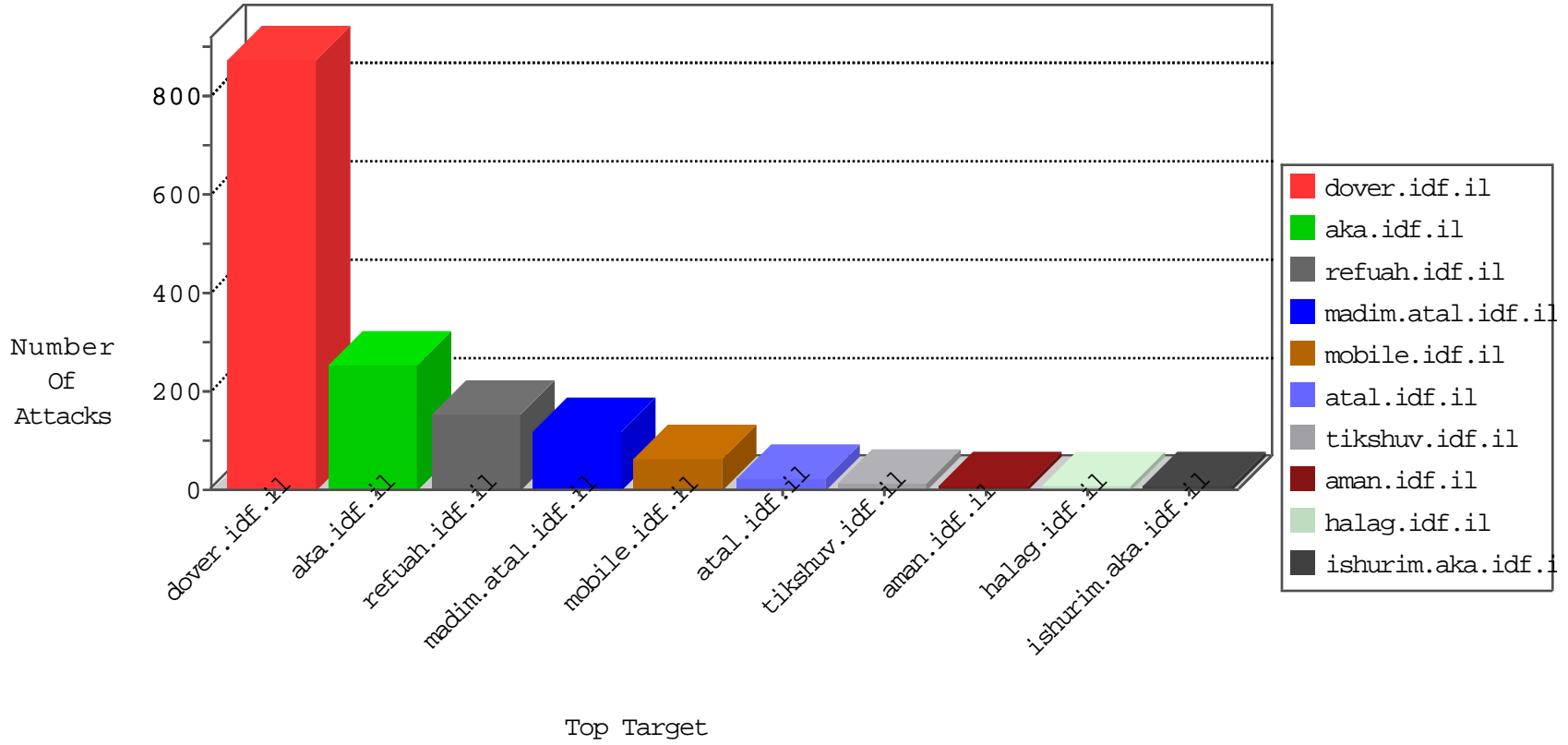


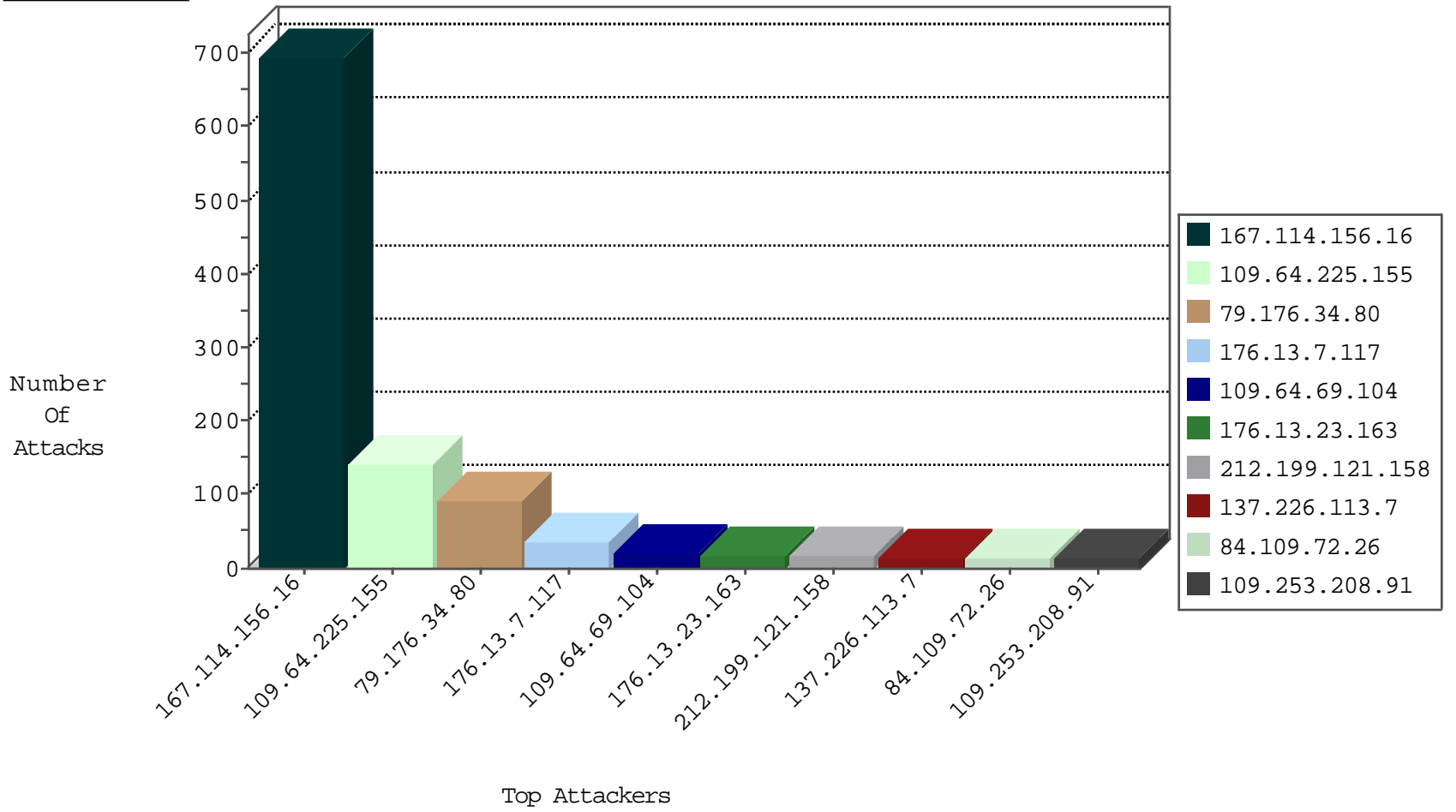
# IDF Under Attack Daily Report



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	DOS-Tool-SwitchbladG	dest-reset	4000
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
190.151.180.28	El Salvador	147.237.76.148	ggcenter.aka.idf.il	L4 Source or Dest Port Zero	drop	3
185.56.28.67	Netherlands	147.237.77.235	sviva.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.207	Netherlands	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
199.26.90.15	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
185.56.28.67	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.154	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
37.142.203.55	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.165.197.142	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
176.13.12.107	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.79.241	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
212.235.40.29	Israel	147.237.72.166	aka.idf.il	C1000008: HTTP: Xenu UserAgent	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	4
66.249.93.128	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sA (2)	2
199.101.186.238	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 3072	1
85.105.74.172	147.237.72.167	Turkey	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
199.101.186.238	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -f -sS	1
71.6.158.166	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
180.97.106.162	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
58.253.96.122	147.237.76.200	China	eitan.aka.idf.il	ET SCAN NMAP -sS window 4096	1
180.97.106.36	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
162.213.36.63	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 3072	1
162.213.36.63	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -f -sS	1
109.253.141.39	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
95.173.184.12	147.237.0.200	Turkey	m4u.idf.il	ET SCAN Potential SSH Scan	1
199.101.186.238	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 2048	1
79.177.24.84	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.98	147.237.76.31	United States	nakchal.idf.il	ET DROP Dshield Block Listed Source	1
71.6.158.166	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -f -sS	1
190.196.178.78	147.237.0.16	Chile	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
66.195.91.180	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
180.97.106.36	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
41.59.21.59	147.237.0.34	Tanzania, United Republic of	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
177.238.43.226	147.237.77.179	Mexico	e.mazi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
162.213.36.63	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 2048	1
159.122.220.109	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.77.121	Canada	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.176.34.80	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	91
176.13.7.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
109.64.225.155	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
109.64.69.104	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
176.13.23.163	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
84.109.72.26	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
212.29.224.93	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
81.4.163.106	Cyprus	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.208.91	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
85.65.12.215	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	6
109.253.196.157	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.65.12.215	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
2.54.97.241	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.199.121.158	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
82.80.164.59	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.143.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.78.31.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.75	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
95.86.97.46	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.22.129.102	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.75	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
5.102.196.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.140	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.102.196.122	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
176.13.8.193	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
109.65.81.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.199.121.158	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.179.179.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.214.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
137.226.113.7	Germany	147.237.76.30	himush.idf.il	drop	SAM rule	drop	3
66.249.93.191	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.143.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
188.120.148.242	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.65.242.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.199.121.158	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.180.66.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.226.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.116	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
137.226.113.7	Germany	147.237.76.34	yohalan.idf.il	drop	SAM rule	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
188.120.154.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.52.153.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.64.225.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	112
109.64.225.155	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
109.253.208.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
94.230.93.95	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
77.125.114.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	2
79.179.27.232	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.179.27.232	Block	2
85.65.12.215	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1815-he/dover.aspx	Block	1
40.77.167.21	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	1
94.230.93.69	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.29.54.102	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
79.179.27.232	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
62.90.49.247	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
37.26.146.201	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.65.100.239	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/templates/sendtofriend/sendtofriend.aspx	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1
46.19.86.69	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/text.css	Block	1
176.13.8.193	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
5.29.57.35	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 5.29.57.35 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
80.255.192.237	United Kingdom	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.64.37	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
37.46.38.189	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.64.244.192	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
46.214.165.206	Romania	147.237.77.74	law.idf.il	PHP Attempt	Block	1
176.13.23.163	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
94.230.93.111	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.29.57.35	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
80.255.192.237	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-content/themes/antioch/lib/scripts/download.php	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
37.142.64.121	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
109.65.11.224	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	1
94.230.93.15	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.176.34.80	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
207.46.13.165	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/templates/shared/usercontrols/navmenu/	Block	1
46.214.165.206	Romania	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
109.64.69.104	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
8.37.232.218	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
82.80.164.59	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
38.81.65.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
109.253.196.157	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
94.230.93.66	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
5.22.135.116	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
212.29.249.176	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
62.0.110.85	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.146.197	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1