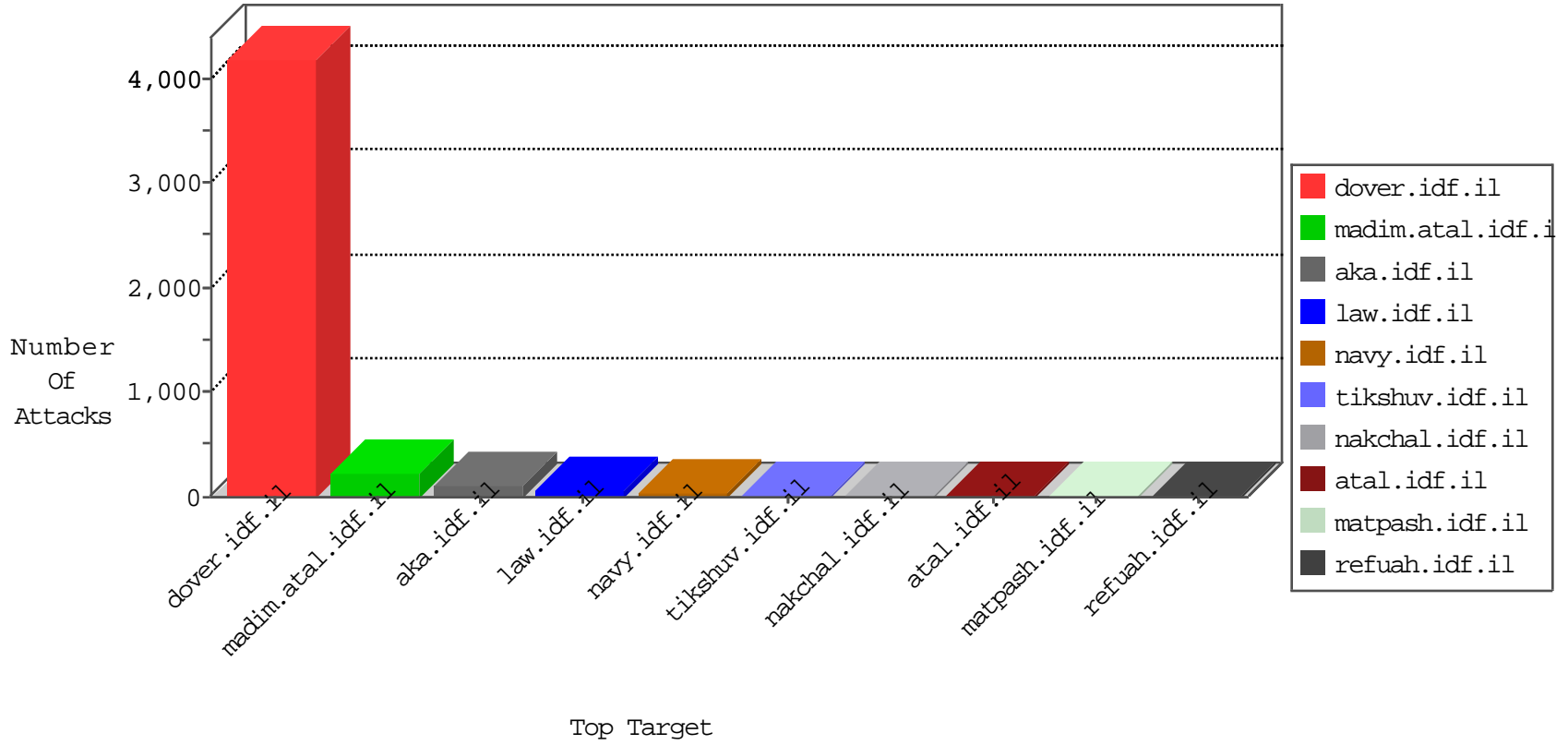


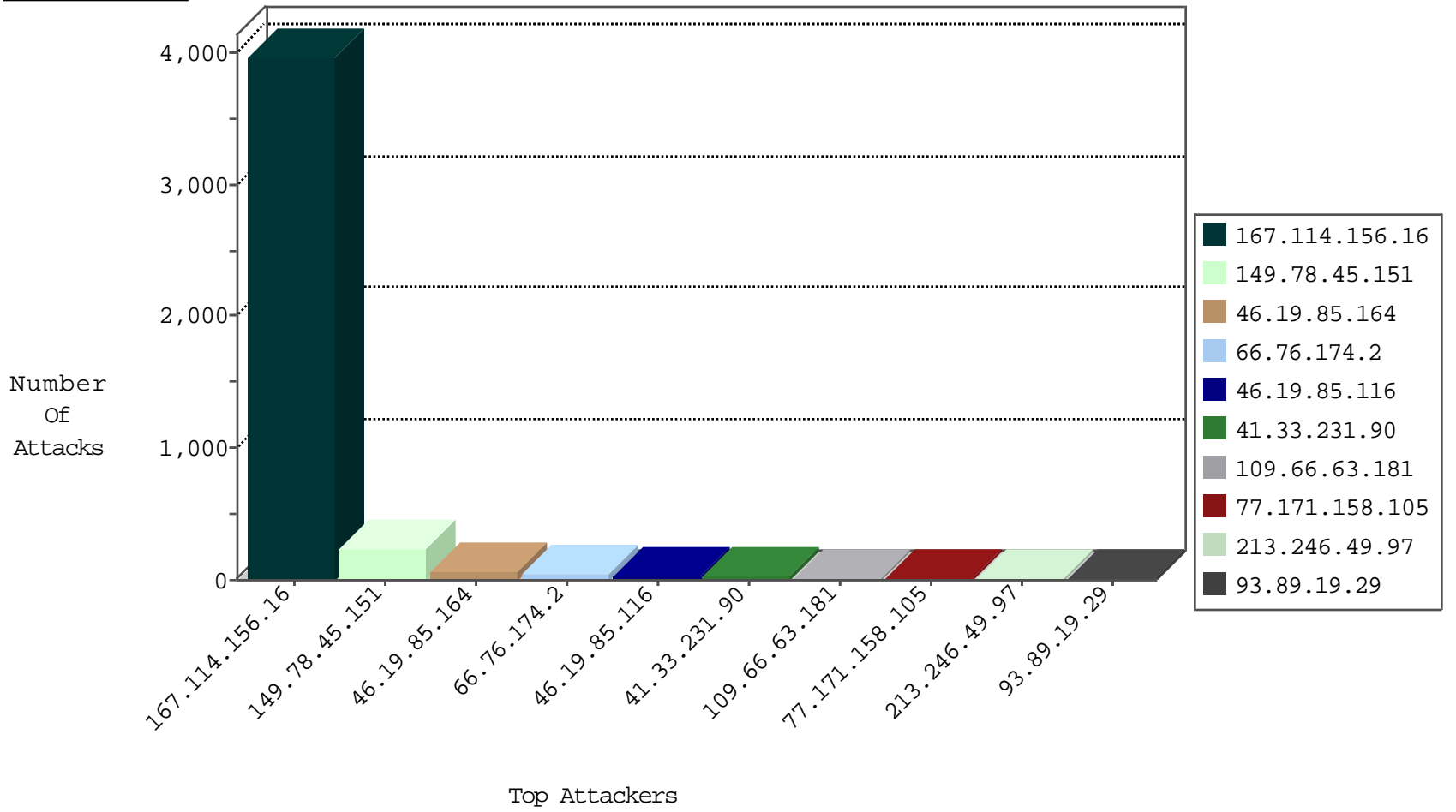
# IDF Under Attack Daily Report



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	3951
79.179.224.72	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	2
85.25.217.46	Germany	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
85.25.217.46	Germany	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
93.201.94.199	Germany	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
85.25.217.46	Germany	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
94.102.52.10	Netherlands	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
66.240.236.119	United States	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.161.33	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
66.76.174.2	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	5
66.76.174.2	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
93.89.19.29	Turkey	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
106.120.173.139	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
213.246.49.97	France	147.237.76.31	nakchal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
87.70.98.59	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
106.120.173.142	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	2
69.30.215.130	United States	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
185.106.92.47	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
185.106.92.47	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.187	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
188.214.249.152	Romania	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
106.38.241.106	China	147.237.76.42	refuah.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
62.98.38.146	Italy	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
163.47.12.170	India	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.85.164	147.237.77.216	Israel	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	36
66.76.174.2	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	31
213.246.49.97	147.237.76.31	France	nakchal.idf.il	SQL Injection - Select From	9
93.89.19.29	147.237.77.233	Turkey	atal.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
198.20.69.74	147.237.76.176	United States	test.ncore.idf.il	ET DROP Dshield Block Listed Source	1
185.106.92.47	147.237.77.226	Russian Federation	www.chamatz.aka.idf.il	ET WEB_SERVER Muieblackcat scanner	1
162.144.41.122	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
122.141.236.69	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
106.186.113.67	147.237.72.167	Japan	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
104.192.0.18	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
77.253.11.100	147.237.76.86	Poland	navy.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
198.20.69.74	147.237.76.42	United States	refuah.idf.il	ET DROP Dshield Block Listed Source	1
189.15.35.57	147.237.0.33	Brazil	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
179.43.141.214	147.237.8.27	Switzerland	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
122.141.236.69	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
108.67.169.124	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	1
106.186.113.67	147.237.72.166	Japan	aka.idf.il	ET SCAN NMAP -sS window 1024	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
109.66.63.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.85.164	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
46.19.85.116	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.85.116	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
141.0.14.90	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
37.46.39.217	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.26.149.214	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.180.170.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.188.75	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.116	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
89.108.144.116	Lebanon	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.116	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
77.171.158.105	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
74.89.106.151	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.1.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.134.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.32.179.73	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
84.110.33.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.16.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.32	United States	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.194.55	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.171.158.105	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.65.87.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.255.215.87	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.44	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
77.171.158.105	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
166.129.181.3	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.181.31.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.171.158.105	Netherlands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
166.129.181.3	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
87.70.20.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.142.68.52	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
84.95.208.20	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
79.177.127.85	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
46.19.85.164	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
84.111.10.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.59	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.22.135.188	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.177.127.85	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.19.85.164	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
79.177.127.85	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
66.249.66.191	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.164	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Urgent Data Enforcement	TCP segment with urgent pointer (no data). Urgent data indication was stripped. Please refer to sk36869.	drop	2
162.144.41.122	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
106.38.241.106	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.45.151	United States	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	226
54.227.3.234	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	8
54.145.224.236	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	7
54.196.88.2	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	4
23.20.38.178	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	4
46.19.85.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.119.127.129	Ukraine	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 46.119.127.129	Block	3
107.21.165.217	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	2
54.144.97.150	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	2
54.211.241.100	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	2
82.81.57.110	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	2
107.21.165.217	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	2
54.161.17.218	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	2
78.58.175.202	Lithuania	147.237.77.74	law.idf.il	Parameter Type Violation InfoCenterItem in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
178.154.189.201	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/592-6584-en/patzar.aspx,	Block	1
66.249.66.16	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/apple-app-site-association	Block	1
78.58.175.202	Lithuania	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1398-en/dover.aspx	Block	1
66.249.78.111	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
203.133.170.205	Korea, Republic of	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
141.212.122.209	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
93.61.127.89	Italy	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
78.58.175.202	Lithuania	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-en/cogat.aspx	Block	1
185.118.27.8	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/sidebar/sidebar.js	Block	1
123.59.59.52	China	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mafengwo.cn/14-he/patzar.aspx	Block	1
78.58.175.202	Lithuania	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/1398-en/dover.aspx	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
93.61.127.89	Italy	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/wp-login.php	Block	1
78.58.175.202	Lithuania	147.237.77.176	matpash.idf.il	Parameter Type Violation SortDir in www.cogat.idf.il/901-en/cogat.aspx	Block	1
185.118.27.13	Lebanon	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/scroller/jquery.jcarousel.js	Block	1
54.157.37.81	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
128.232.110.28	United Kingdom	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
79.181.31.62	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2113-he/cogat.aspx	Block	1
174.129.181.230	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
93.158.152.52	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1516-	Block	1
46.119.127.129	Ukraine	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
78.58.175.202	Lithuania	147.237.77.176	matpash.idf.il	Parameter Type Violation lang in www.cogat.idf.il/901-en/cogat.aspx	Block	1
186.89.157.173	Venezuela	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
66.249.66.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/ui/i18n/jquery-ui-i18n.js	Block	1
54.158.179.39	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
141.8.132.2	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/163-7183-	Block	1
5.255.253.10	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/320-en/patzar.aspx.	Block	1
78.58.175.202	Lithuania	147.237.77.74	law.idf.il	Parameter Type Violation FileName in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
176.9.58.227	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
46.119.127.129	Ukraine	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
78.58.175.202	Lithuania	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1398-en/dover.aspx	Block	1
186.89.157.173	Venezuela	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/wp-login.php	Block	1