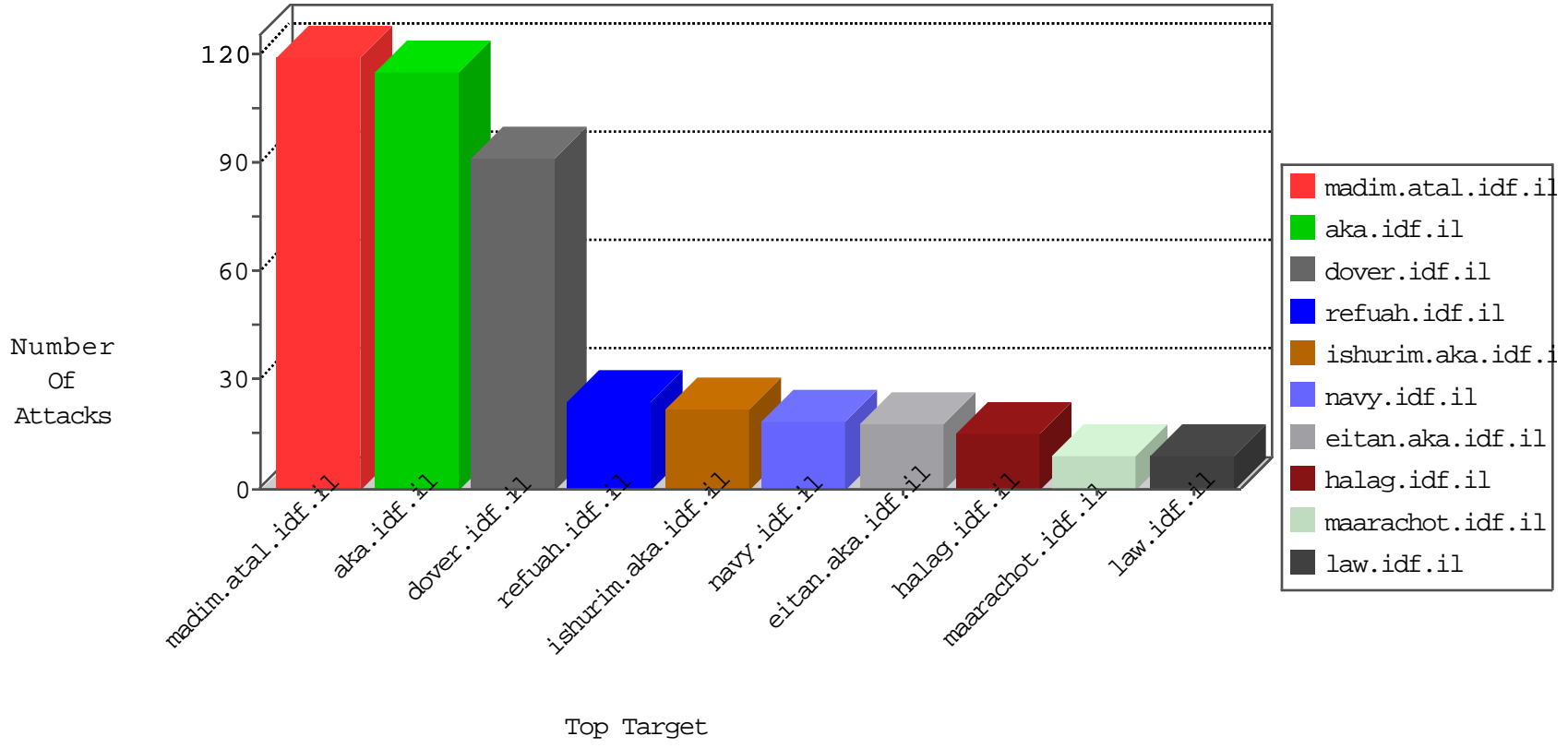


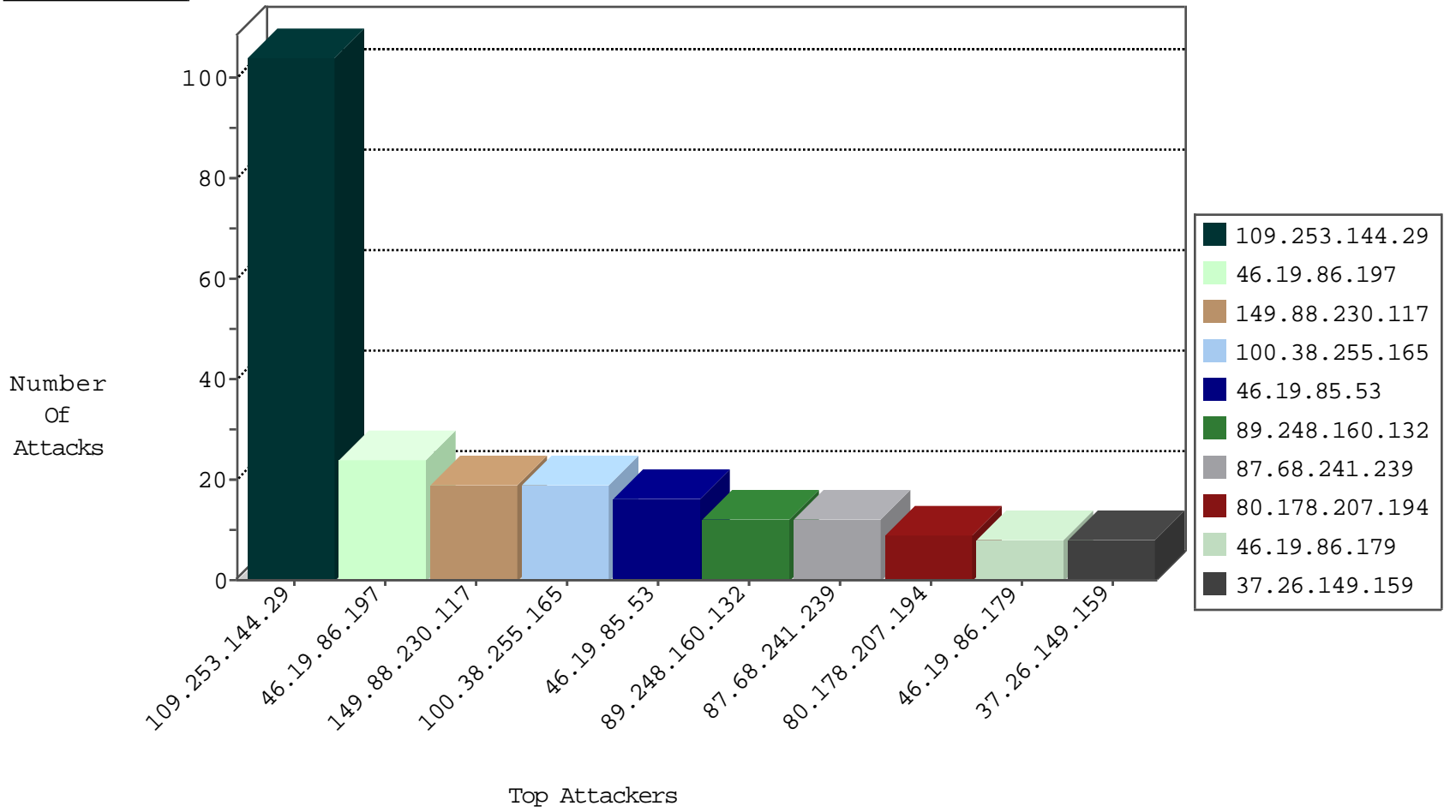
# IDF Under Attack Daily Report



## Top Targets



## Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
89.248.160.132	Netherlands	147.237.77.235	sviva.idf.il	block-sp-trafl	forward	2
89.248.160.132	Netherlands	147.237.72.167	ishurim.aka.idf.il	block-sp-trafl	forward	2
89.248.160.132	Netherlands	147.237.77.19	law-forum.idf.il	block-sp-trafl	forward	2
121.169.15.88	Korea, Republic of	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	2
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
89.248.160.132	Netherlands	147.237.77.205	prisha.idf.il	block-sp-trafl	forward	2
216.218.206.79	United States	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	1
121.169.15.88	Korea, Republic of	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.96	United States	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
216.218.206.83	United States	147.237.77.19	law-forum.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.67	United States	147.237.8.14	e.orchot.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
89.248.172.207	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
50.207.53.162	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
216.218.206.99	United States	147.237.8.45	e.eitan.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.67	United States	147.237.8.46	e.chinuch.idf.il	Block_Udp_All_Nets	drop	1
216.218.206.67	United States	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
216.218.206.111	United States	147.237.0.200	m4u.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.72	United States	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.58.86.211	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4
108.59.8.70	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
92.241.37.112	Jordan	147.237.77.216	dover.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	2
151.80.31.151	Italy	147.237.76.86	navy.idf.il	C1000146: HTTP: AhrefBot crawler	Block	2
51.254.143.24	United Kingdom	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	2
51.254.143.24	United Kingdom	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
151.80.31.154	Italy	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	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
151.80.31.151	Italy	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
85.250.81.245	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.130.215	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
37.139.27.231	147.237.77.234	Netherlands	halag.idf.il	ET SCAN NMAP -sS window 1024	1
13.68.31.54	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 3072	1
216.55.143.94	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER PHP Crawler	1
185.93.185.246	147.237.8.24		e.lifestyle.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.219.238.10	147.237.72.166		aka.idf.il	ET SCAN NMAP -sS window 1024	1
84.109.125.71	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
13.68.31.54	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 4096	1
218.246.0.97	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
178.62.94.12	147.237.0.200	United States	m4u.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
46.19.86.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
149.88.230.117	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
100.38.255.165	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
46.19.85.53	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
80.178.207.194	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.253.200.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.234	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.20.73	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.254.0	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.179.9.7	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
37.26.149.159	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
46.19.86.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
193.104.77.4	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.183.93	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.179	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.65.131.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
169.54.244.84	Netherlands	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
79.182.111.123	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.141.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.168.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.16.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
147.236.38.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.53	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
87.68.241.239	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.161.249	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.178.207.194	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	3
109.253.192.123	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
46.19.86.179	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
185.3.147.226	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
37.26.149.159	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
37.26.149.159	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
82.102.169.113	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
212.47.246.187	France	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.103	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
8.37.227.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
169.54.244.84	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
213.57.228.40	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.229.29.167	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
77.42.197.164	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.105.139.83	United States	147.237.76.148	ggcenter.aka.idf.il	drop		drop	1
46.19.85.103	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
212.47.246.187	France	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.119.167.19		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
62.0.211.129	Israel	147.237.76.147	chinuch.aka.idf.il	drop	First packet isn't SYN	drop	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.144.29	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
104.12.80.51	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 104.12.80.51	Block	6
94.187.125.217	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
87.68.241.239	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 87.68.241.239	Block	4
77.42.197.164	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
87.68.241.239	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.14.57	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
178.135.80.183	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
109.253.206.52	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.210.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
199.30.25.110	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.24.17	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.2.168	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.24.23	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.12.65	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
87.68.241.239	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	2
37.26.148.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
199.30.25.81	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
65.55.210.61	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
169.54.244.84	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
66.249.66.45	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size338x0/sip_storage	Block	1
37.237.200.146	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
104.12.80.51	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar	Block	1
89.248.160.132	Netherlands	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to www.safeskyhacks.com/forums/forum.php	Block	1
185.106.92.65		147.237.77.170	maarachot.idf.il	Unauthorized Request Content Type text/html	Block	1
149.88.230.117	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/print.css	Block	1
66.90.183.203	United States	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
100.38.255.165	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/1105-en/contactus.aspx	Block	1
66.249.69.33	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
46.28.105.11	Czech Republic	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp/wp-admin/	Block	1
89.248.160.132	Netherlands	147.237.77.235	sviva.idf.il	Unauthorized URL Access to www.safeskyhacks.com/forums/forum.php	Block	1
199.30.25.143	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.125.106.57	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
185.106.92.65		147.237.77.216	dover.idf.il	Unauthorized Request Content Type from 185.106.92.65	Block	1
66.90.183.203	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
100.38.255.165	United States	147.237.76.200	eitan.aka.idf.il	Unknown Parameter r in www.eitan.aka.idf.il/templates/opcontactus/govcaptchaimage.axd	None	1
37.26.146.159	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.69.41	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/5/111025.pdf	Block	1
46.117.120.170	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
91.135.102.167	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	1
217.160.63.130	Germany	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/old/wp-admin/	Block	1
79.177.39.150	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
188.43.123.70	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation FileName in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
37.26.148.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
100.38.255.165	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
199.30.25.43	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1927-he/cogat.aspx	Block	1
180.76.15.30	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery.plugins/jquery.charts.js	Block	1
46.117.120.170	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 46.117.120.170	Block	1