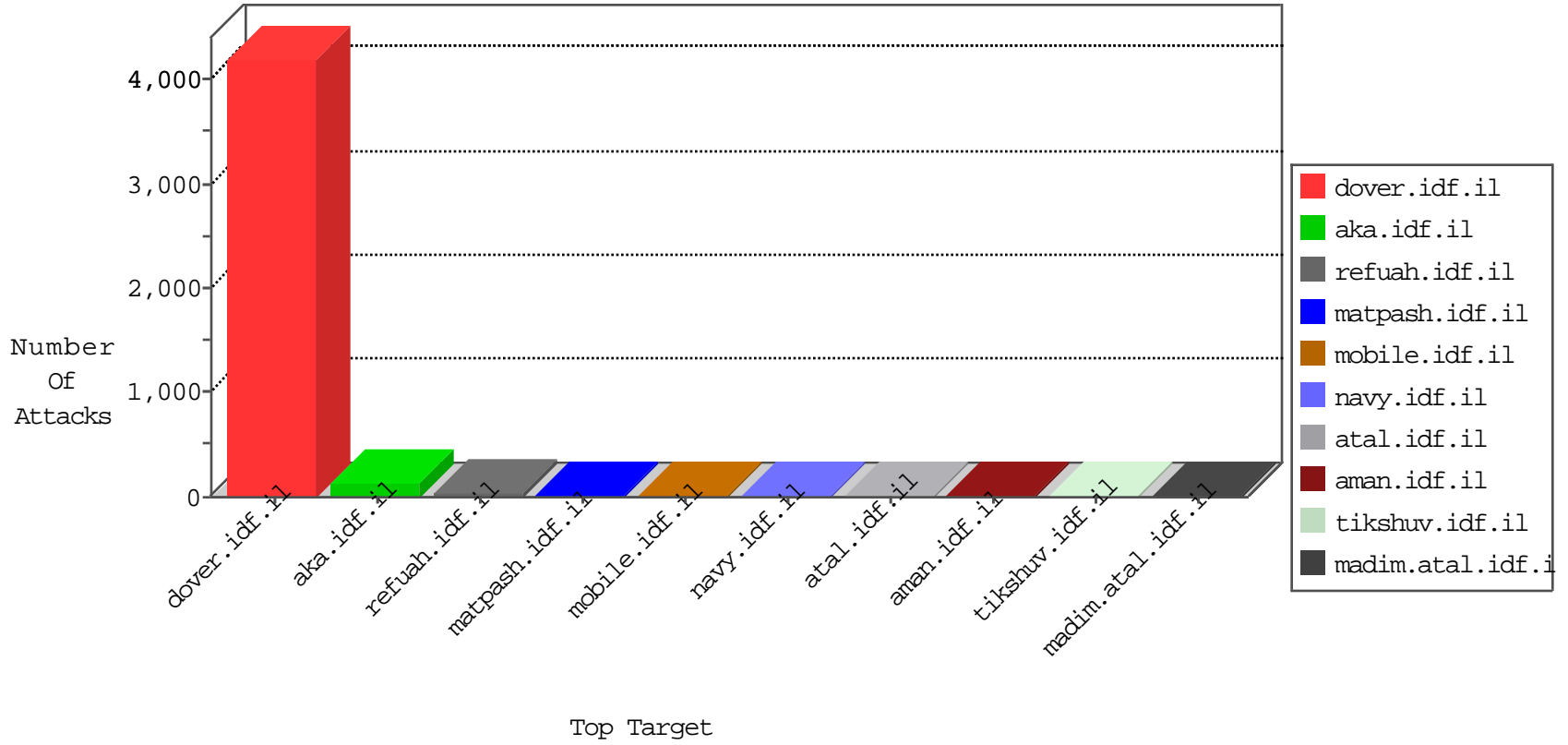




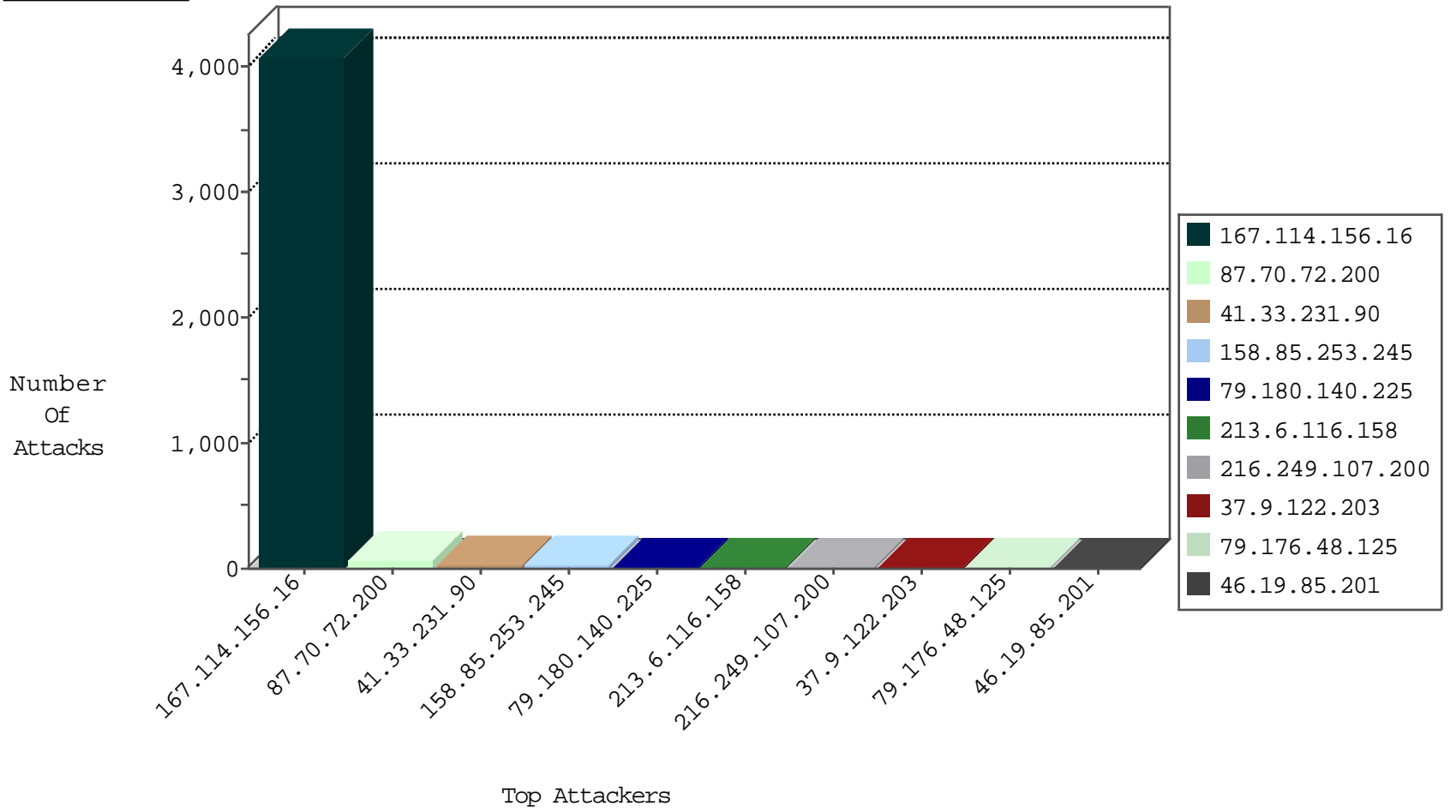
# IDF Under Attack Daily Report



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	4068
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
216.249.107.200	United States	147.237.72.166	aka.idf.il	Anomaly-TCP-shorthead	dest-reset	2
82.145.223.22	Europe	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	2
209.126.117.230	United States	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	1
77.41.88.44	Russian Federation	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	1
107.191.40.138	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
107.191.40.138	United States	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
45.32.95.13	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
45.32.95.13	Netherlands	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.116	Netherlands	147.237.8.46	e.chinuch.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
158.85.253.245	United States	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
106.38.241.144	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
216.249.107.200	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
185.106.92.47	Russian Federation	147.237.77.176	matpash.idf.il	20086: HTTP: Mueblackcat Security Scanner	Block	3
162.210.196.97	United States	147.237.77.216	dover.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
66.249.66.187	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	147.237.76.42	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
185.106.92.47	Russian Federation	147.237.77.176	matpash.idf.il	20085: HTTP: Mueblackcat Security Scanner Initial Request	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
158.85.253.245	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	13
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
216.249.107.200	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	4
66.249.93.18	147.237.76.42	Europe	refuah.idf.il	ET SCAN NMAP -sA (2)	2
216.227.58.7	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 3072	1
187.188.72.11	147.237.72.166	Mexico	aka.idf.il	ET SCAN NMAP -sS window 4096	1
185.106.92.47	147.237.77.176	Russian Federation	matpash.idf.il	ET WEB_SERVER Muieblackcat scanner	1
104.238.82.190	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential SSH Scan	1
42.159.237.58	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
216.227.58.7	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 4096	1
187.188.72.11	147.237.72.166	Mexico	aka.idf.il	ET SCAN NMAP -sS window 3072	1
162.144.41.122	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
106.186.113.67	147.237.76.177	Japan	noore.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
63.142.161.17	147.237.76.44	Canada	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
1.165.9.207	147.237.0.15	Taiwan	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	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	36
87.70.72.200	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32
87.70.72.200	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
79.180.140.225	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
87.70.72.200	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
89.139.228.62	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
79.180.140.225	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.201	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.46.13.144	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.9.122.203	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
79.176.48.125	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
79.176.48.125	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
66.102.9.117	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	5
5.28.190.211	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.121.204.110	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
216.249.107.200	United States	147.237.72.166	aka.idf.il	IP Fragments	Failed to generate IP packet from fragments	drop	4
212.179.243.32	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.9.122.203	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.86.37	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.46.41.54	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.178.129.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.57.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
182.239.70.35	Hong Kong	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.178.153.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.147.242	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.132.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.154.189.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.154.162.14	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.46.13.132	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.228.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.189.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.235	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.102.242.66	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
185.135.69.50	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
182.239.70.35	Hong Kong	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.19.86.31	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
37.9.122.203	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack		reject	2
78.34.56.6	Germany	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.86.37	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
37.26.149.192	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
185.3.144.33	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
162.144.41.122	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.19	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.201	United States	147.237.0.35	akaws.idf.il	drop		drop	1
216.243.31.2	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
64.125.239.184	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
94.230.86.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.32.179.46	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.6.116.158	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 213.6.116.158	Block	13
79.179.97.72	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.179.97.72	Block	4
109.64.17.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.147.242	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	2
79.180.170.53	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct109 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/3394.jpg	Block	1
213.8.204.8	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/news/mobile	Block	1
180.76.15.10	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
37.59.109.136	France	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/old/wp-admin/	Block	1
93.172.150.196	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
203.127.96.221	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
149.78.159.120	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/894-he/miluum.aspx	Block	1
87.70.72.200	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.66.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1644-he/refuah.aspx	Block	1
213.8.204.46	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/gyius	Block	1
184.105.247.194	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
46.19.85.42	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1
79.179.97.72	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/gyius/	Block	1
207.46.13.37	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
46.19.85.201	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.157	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/sip_storage/files/8/69778.xls/	Block	1
87.70.72.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/gyius/general.aspx	Block	1
220.255.146.134	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
184.168.193.33	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/blog/wp-admin/	Block	1
46.19.85.42	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version __atuvs=57120c405a8a31a3000; _pk_id.20.8afc=65b3405e92c4003b.1460800588.1.1460800588.; _pk_ses.20.8afc=*	Block	1
79.179.182.1	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 79.179.182.1	Block	1
66.249.64.229	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
157.55.39.200	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/901-8504/tikshuv.aspx	Block	1
87.70.72.200	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/gyius/forum/asp/showforum.asp	Block	1
220.255.148.148	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
185.3.144.33	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 185.3.144.33	Block	1
46.19.85.42	Israel	147.237.77.216	dover.idf.il	Malformed URL __atuvc=1	Block	1
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
79.179.182.1	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/templates/homepage/mobile	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/2254.jpg	Block	1
213.6.116.158	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/general/mobile	Block	1
157.55.39.236	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluum	Block	1
89.138.204.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
74.208.152.22	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/wp/wp-admin/	Block	1
203.127.96.216	Singapore	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
46.19.85.42	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method 5duexlwzaj24kjdy4; in URL __atuvc=1	Block	1
141.212.122.209	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1