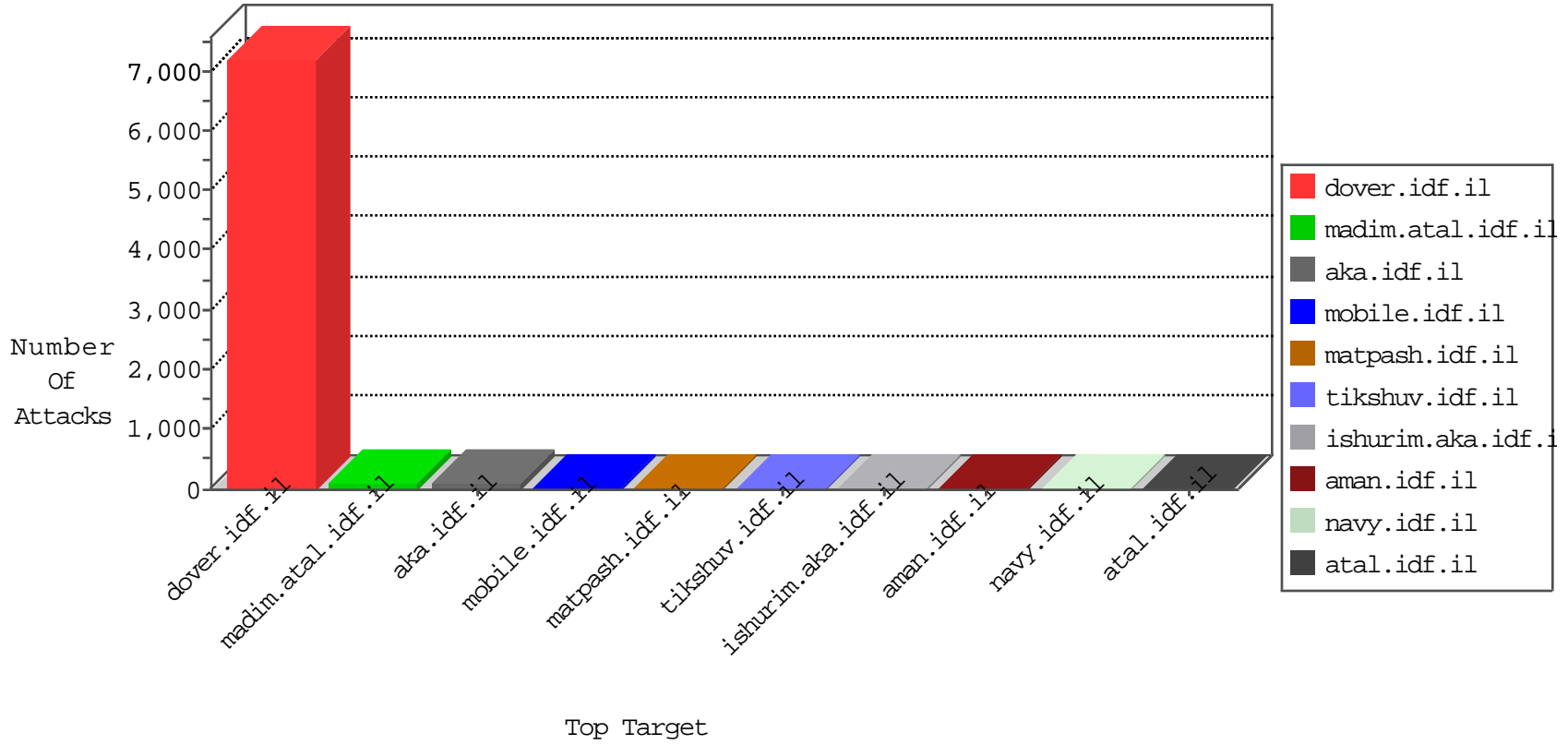




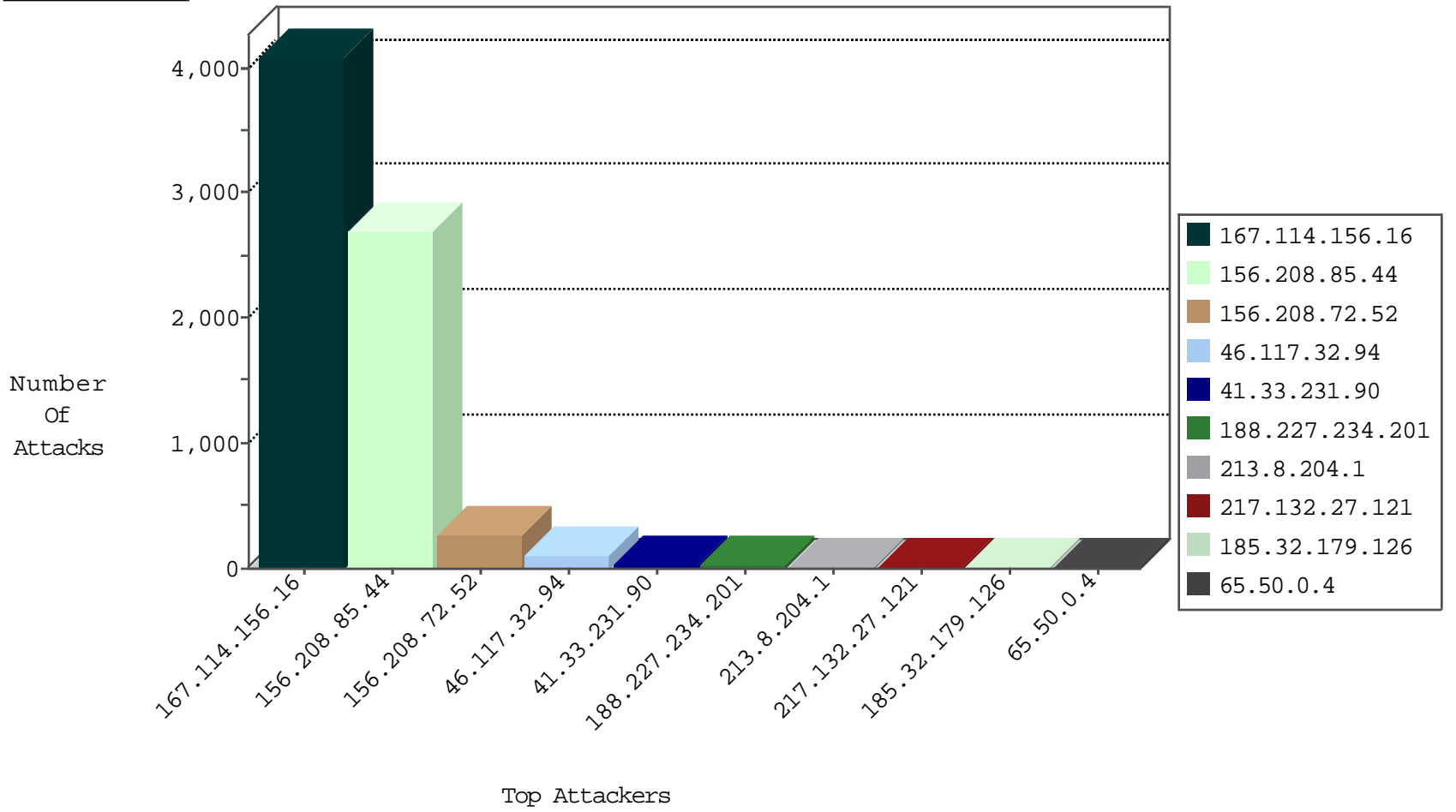
# IDF Under Attack Daily Report



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	4077
156.208.85.44	Egypt	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2650
156.208.72.52	Egypt	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	220
120.132.50.135	China	147.237.77.233	atal.idf.il	block-sp-trafl	forward	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
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	forward	2
94.102.49.116	Netherlands	147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	1
45.32.95.13	Netherlands	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
185.70.184.164	Netherlands	147.237.72.14	dover.idf.il(old)	JLM_Under_Attack_Con_Https	drop	1
45.32.95.13	Netherlands	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.180.139.202	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
109.64.153.33	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
178.151.143.163	Ukraine	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	3
109.253.197.52	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
144.76.8.132	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
5.28.160.203	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
144.76.93.46	Germany	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
151.80.31.168	France	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	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
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
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
85.173.82.207	147.237.76.200	Russian Federation	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
220.231.195.122	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -sS window 3072	1
85.173.82.207	147.237.76.176	Russian Federation	test.noore.idf.il	ET SCAN Potential SSH Scan	1
216.227.58.7	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 3072	1
85.173.82.207	147.237.76.30	Russian Federation	himush.idf.il	ET SCAN Potential SSH Scan	1
187.161.180.183	147.237.72.14	Mexico	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.227.67.163	147.237.0.16	Sweden	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
156.208.72.52	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
106.186.113.67	147.237.77.212	Japan	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
104.238.82.190	147.237.76.30	United States	himush.idf.il	ET SCAN Potential SSH Scan	1
85.173.82.207	147.237.77.212	Russian Federation	e.dover.idf.il	ET SCAN Potential SSH Scan	1
85.173.82.207	147.237.77.121	Russian Federation	e.navy.idf.il	ET SCAN Potential SSH Scan	1
85.173.82.207	147.237.76.198	Russian Federation	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
220.231.195.122	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
85.173.82.207	147.237.76.148	Russian Federation	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
65.181.123.161	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
156.208.85.44	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
42.159.237.58	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
106.186.113.67	147.237.77.233	Japan	atal.idf.il	ET SCAN NMAP -sS window 1024	1
106.186.113.67	147.237.77.176	Japan	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.95.87	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
85.173.82.207	147.237.77.176	Russian Federation	matpash.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
156.208.72.52	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	46
156.208.85.44	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	41
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
188.227.234.201	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	28
217.132.27.121	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
213.8.204.1	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
176.13.11.229	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
65.50.0.4	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
2.55.2.200	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
37.26.147.167	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
2.53.152.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
132.66.222.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.120.125.38	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.31	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.102.8.238	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.22.130.88	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
201.175.108.99	Mexico	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
84.108.109.23	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.154.169.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.32.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.86.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.169.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.130.100	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.253.157.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.195.210	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.180.121.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.129.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.95.86.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.123.12	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.253.215.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.139.202	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
5.102.195.210	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.64.190.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.108.109.23	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.176.123.12	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
185.27.105.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.15.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.129.97	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.66.28.154	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.29.114.5	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.178.117.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.142.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.117.113.185	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
157.55.39.32	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2

04-16-2016-16:04:01 to 04-16-2016-17:04:01

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
156.208.72.52	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
185.3.147.148	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
207.46.13.136	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.117.32.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	92
185.32.179.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
185.3.147.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
2.53.8.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
213.8.204.1	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
65.50.0.4	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.186.180.184	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ct100\$ContentPlaceholder1\$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
37.142.228.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/164-3447-he/	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
157.55.39.163	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/general.aspx	Block	1
84.228.251.242	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/article/mobile	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
201.175.108.99	Mexico	147.237.77.74	law.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
40.77.167.18	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
156.208.72.52	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
81.111.195.163	United Kingdom	147.237.77.74	law.idf.il	PHP Attempt	Block	1
184.105.247.196	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
89.138.167.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/resource/userfollowresource/create/	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/4/60984.pdf	Block	1
207.46.13.147	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
46.19.85.16	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/news/mobile	Block	1
156.208.85.44	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
81.111.195.163	United Kingdom	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/wp-login.php	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
46.19.86.106	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.19.86.106	Block	1
157.55.39.32	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/miktzoa/	Block	1
81.111.195.163	United Kingdom	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	1
66.249.66.50	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
120.132.50.135	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.qyer.com/894-he/atal.aspx	Block	1
66.249.79.119	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
46.19.86.106	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	1
157.55.39.37	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluim/templates/www.behazdaa.org	Block	1
81.111.195.163	United Kingdom	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/3491.jpg	Block	1
201.175.108.99	Mexico	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1