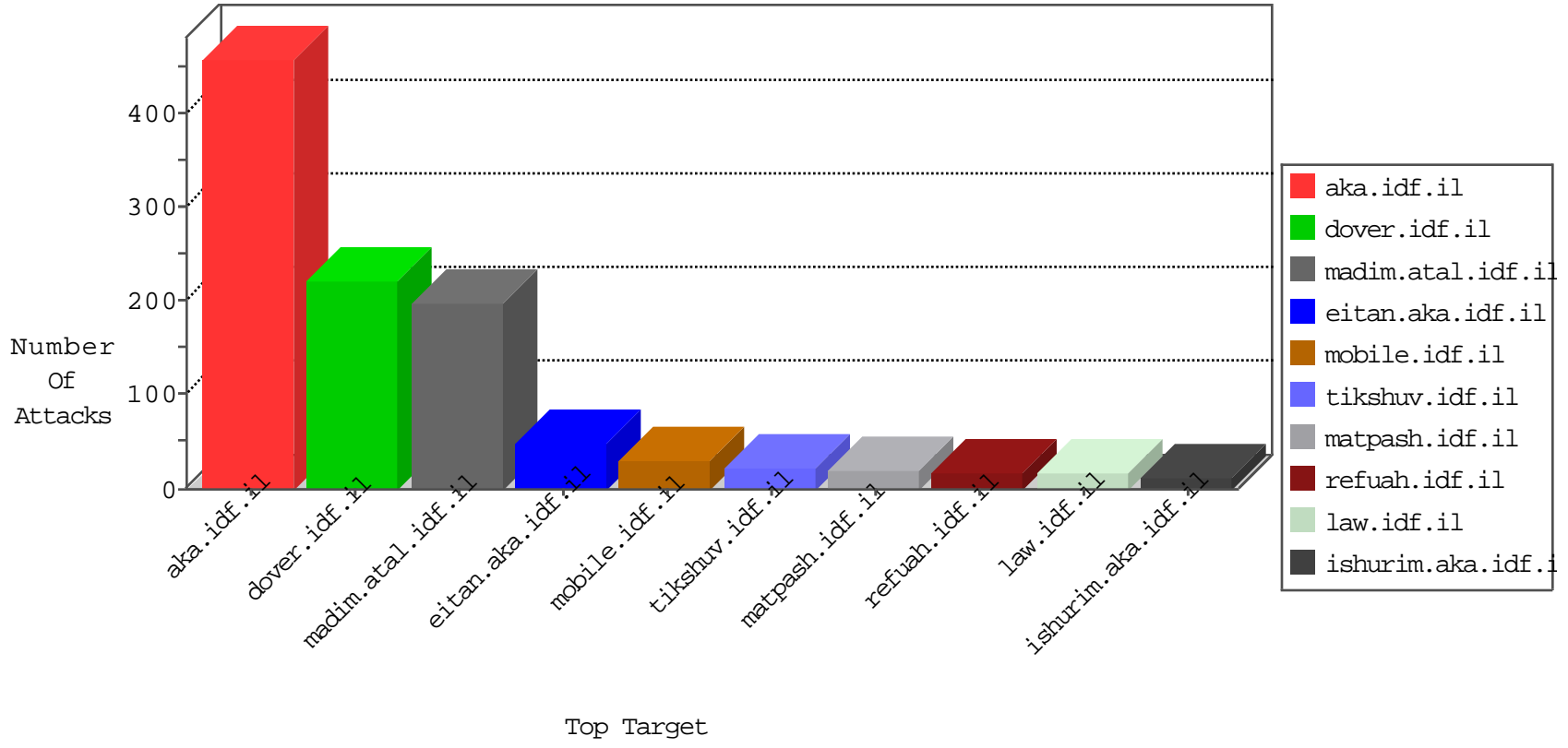


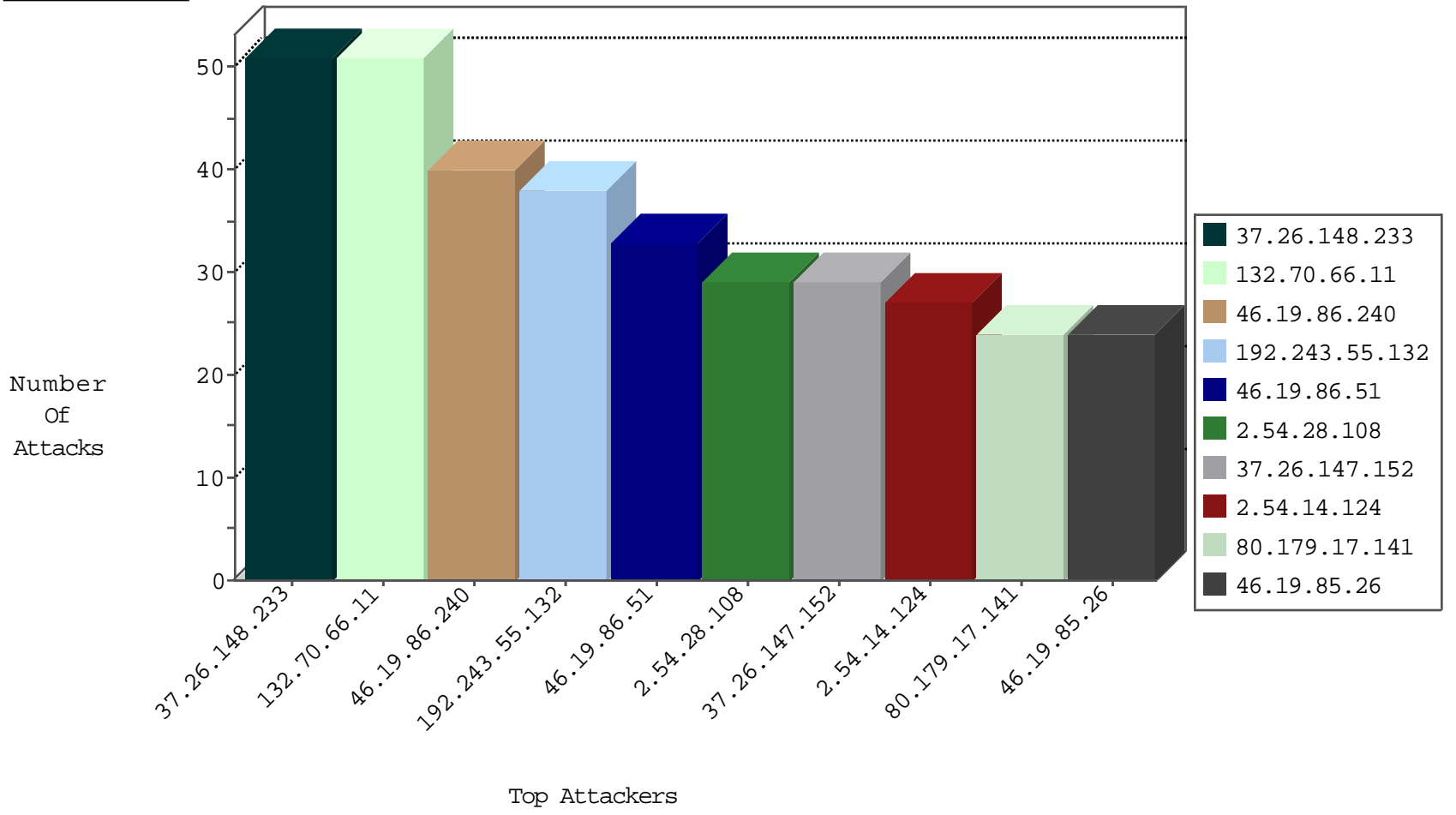
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
202.58.137.76	Australia	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
109.64.131.160	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
192.118.132.185	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
74.82.47.21	United States	147.237.77.234	halag.idf.il	Block_Udp_All_Nets	drop	1
184.105.247.211	United States	147.237.72.14	dover.idf.il(old)	Block_Udp_All_Nets	drop	1
10.0.0.166		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
202.58.137.96	Australia	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
184.105.247.247	United States	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	1
212.252.168.253	Turkey	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
164.132.54.194	Italy	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
62.117.59.30	Egypt	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
216.218.206.85	United States	147.237.77.243	mobile.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.101	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	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
37.142.161.146	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
158.69.214.11	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
2.54.181.172	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
86.34.138.111	Romania	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	2
91.121.211.59	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
149.202.49.56	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	2
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
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
98.119.105.221	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.120.178.168	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.240	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.102.252.110	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.132.54.176	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.25.106.78	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.147.193	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.2.49	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.0.67.133	147.237.8.24	Israel	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.106	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.121.105	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.151.57.195	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
109.65.238.211	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.148.233	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	46
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
2.54.14.124	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
80.179.17.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.85.26	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	24
31.154.27.186	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
2.52.46.208	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
2.54.170.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.85.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
87.68.78.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
188.120.154.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
37.26.146.148	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
188.120.154.94	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.117.167.66	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
185.120.125.38		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.200.163	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.60	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.15.185	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.173.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.22.131.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.179.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
2.52.46.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.125	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.138.127	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
80.178.97.80	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
81.218.170.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.15.240	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
109.67.3.210	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.125	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
37.26.146.202	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.148.233	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
199.203.8.2	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.13.133	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	4
212.179.210.200	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.106	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
66.249.66.133	United States	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.179.210.200	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.54.34.97	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.52.13.133	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
199.203.8.2	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.118.64.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.174	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.35.142	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
132.70.66.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
46.19.86.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
46.19.86.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
37.26.147.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
2.54.28.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
176.13.0.16	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
37.26.146.218	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
176.13.10.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.214.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
131.253.25.187	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.253.147.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.15.185	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.179.202.129	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
178.214.86.39	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/894-ar	Block	2
46.43.72.69	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Distributed Parameter Type Violation on www.cogat.idf.il/938-en/cogat.aspx parameter SearchText	Block	2
46.19.85.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.130.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ishur	Block	2
41.242.140.15	South Africa	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
37.26.146.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.253.130.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.148.208	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.8.55.152	Palestinian Territory, Occupied	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1135-he/atal.aspx	Block	1
203.127.96.200	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	1
66.220.145.245	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/favicon.ico	Block	1
185.32.179.77	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.12	Israel	147.237.77.176	matpash.idf.il	Unknown HTTP Request Method v45 in URL	Block	1
173.208.136.114	United States	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
37.26.146.250	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.151.46.40	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/112265.pdf&sa=u&ved=0ahukewiuvdm7oa tlahxciiwkhtboakiqfggkmae&usg=afqjcnhge7qfxmephuxly6mtbgoryf-75a	Block	1
2.52.142.114	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
193.41.209.2	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catI in www.aka.idf.il/main/giyus/general.aspx	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/toolfs.asp	Block	1
37.187.56.66	France	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 37.187.56.66	Block	1
37.26.146.141	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
203.127.96.253	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
85.158.139.228	United Kingdom	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.66.176	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
185.32.179.136	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
173.208.136.114	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
109.253.193.9	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/login parameter Password	Block	1
213.151.57.195	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.151.57.195	Block	1
2.54.25.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
193.41.209.2	Israel	147.237.72.166	aka.idf.il	Unknown Parameter d in www.aka.idf.il/main/giyus/general.aspx	None	1
37.187.56.66	France	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1
132.70.66.11	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ct100\$ContentPlaceholder1\$txtCaptcha in madim.atal.idf.il/mobile/login.aspx	Block	1
105.112.23.241	Nigeria	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
37.26.146.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1