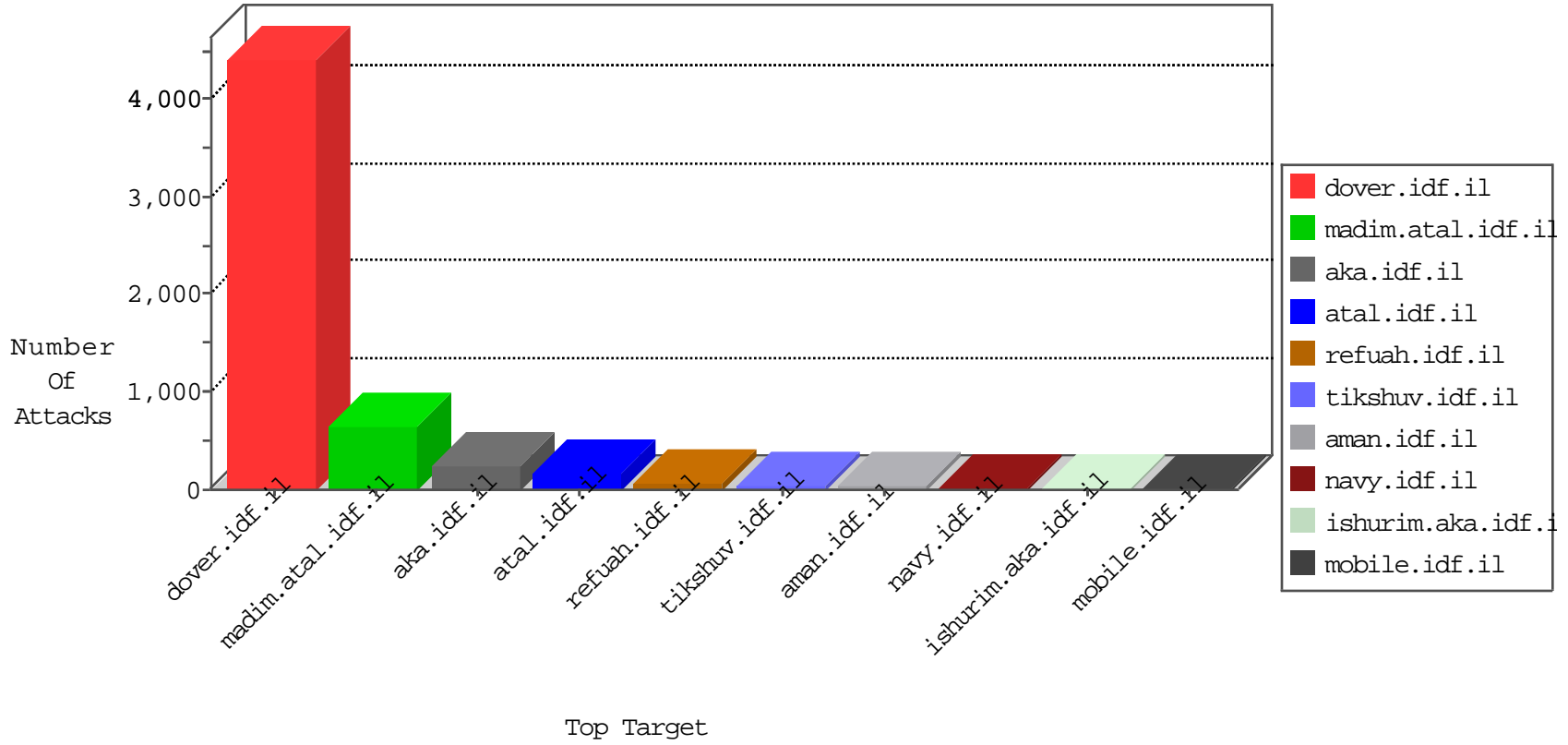


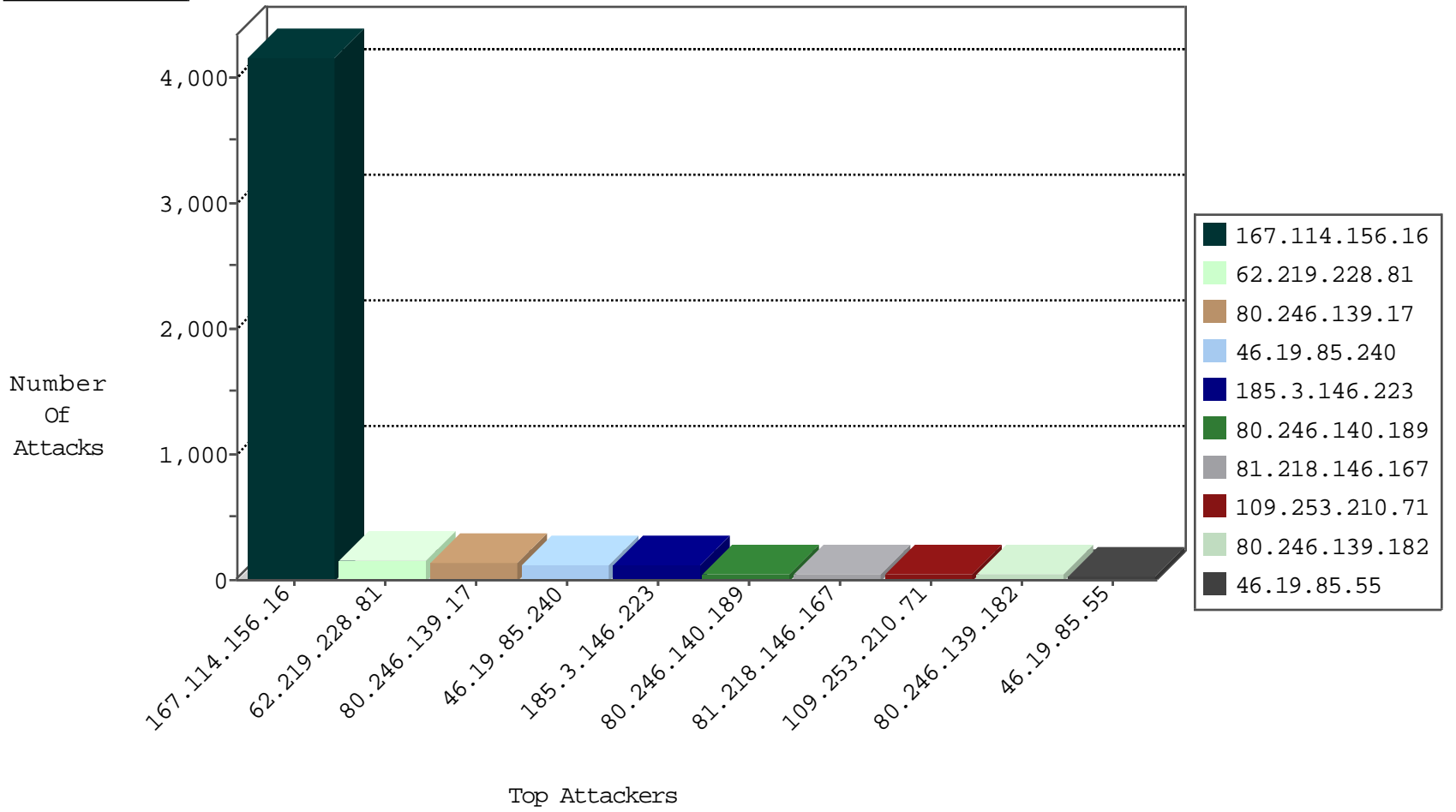
# IDF Under Attack Daily Report



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	4158
46.19.85.203	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	513
207.232.36.85	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	411
80.246.136.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	328
79.181.16.95	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	310
2.53.52.79	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	217
41.230.235.60	Tunisia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	111
41.209.115.123	Sudan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	37
213.8.100.81	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	19
185.3.147.171	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	11
109.67.219.190	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10
80.246.140.151	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
109.253.140.40	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
213.151.58.192	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
46.121.92.187	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
213.8.204.22	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
184.105.139.102	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
46.19.85.33	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
184.105.139.82	United States	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1
5.102.233.7	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
184.105.139.94	United States	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.70	United States	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1
216.72.40.186	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
80.179.223.150	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
212.143.110.33	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
184.105.139.106	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
46.19.85.80	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
184.105.139.86	United States	147.237.72.166	aka.idf.il	Block_Ntp_All_Net	drop	1
179.43.144.50	Switzerland	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
84.94.32.197	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.32.176.6	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
72.37.140.37	Italy	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
184.105.139.94	United States	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.78	United States	147.237.8.46	e.chinuch.idf.il	Block_Ntp_All_Net	drop	1
216.218.206.109	United States	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.106	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1
2.185.161.155	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
184.105.139.86	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	1
179.43.144.50	Switzerland	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	1
213.151.35.213	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
91.195.162.2	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
199.203.131.177	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
74.82.47.29	United States	147.237.8.14	e.orchot.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.102	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.82	United States	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
156.207.7.229	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
212.179.54.237	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.94.180.40	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	15
79.178.26.28	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
82.102.168.106	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
61.135.189.122	China	147.237.76.31	nakchal.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
176.233.237.19	Turkey	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
95.235.11.21	147.237.77.216	Italy	dover.idf.il	GPL SCAN nmap TCP	2
31.168.103.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.10.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.54.237	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.203.109.83	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.41.80	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.248.172.140	147.237.76.148	Netherlands	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.57	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.35.100	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
216.72.40.185	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
208.100.26.228	147.237.77.226	United States	www.chamatz.aka.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
82.80.198.164	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.117.13.146	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.3.146.223	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	90
81.218.146.167	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	51
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
185.3.146.223	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
107.167.106.191	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
46.19.85.55	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
45.59.183.9	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.140	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	9
2.53.11.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.55	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
46.19.85.55	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
80.178.212.183	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.55	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.203	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.179.196.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.203	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.80	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.181.16.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.203	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
93.172.244.14	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.80	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.13.144	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.203	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.13.203	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.55.29.11	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.80	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.160.154	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
87.70.91.176	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.121.137.23	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.80	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
37.26.149.136	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
80.246.133.179	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
85.214.28.229	Germany	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
37.26.149.136	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
185.3.146.223	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
2.54.160.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.240	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.67.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.14.249	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.128.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.117.225.224	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
94.230.86.136	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.95.252.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.49.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.126.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.17.11	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
62.219.228.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	148
80.246.139.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	129
46.19.85.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	115
80.246.140.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
109.253.210.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
80.246.139.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
109.253.134.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
37.26.148.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
185.32.179.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
80.246.139.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
185.120.125.40	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	5
2.53.39.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.18.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.139.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.167.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.120.125.40	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 185.120.125.40	Block	3
80.246.130.81	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
80.246.139.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.130.242	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
149.88.22.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	2
109.253.193.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.179.117.49	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	2
80.246.139.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.7.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.12.219	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/movies/20_10_03_strike_eng.asf	Block	1
111.119.221.218	India	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
5.102.195.83	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct117 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
199.203.131.177	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
87.69.109.24	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ https://twitter.com/	Block	1
185.3.147.147	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct183 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Illegal Byte Code Character in Method %E'03`0	Block	1
46.116.67.234	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	1
2.52.168.179	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
176.13.13.203	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.4	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1234-he/atal.aspx	Block	1
212.143.212.222	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/0/	Block	1
87.69.190.81	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
185.32.176.6	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Illegal Byte Code Character in URL	Block	1
79.179.117.49	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.179.117.49	Block	1
46.116.67.234	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/4/	Block	1
185.120.125.40	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/3/	Block	1
80.246.140.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
80.246.133.179	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1440-he/atal.aspx	Block	1
66.249.78.11	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1233-he/atal.aspx	Block	1
149.88.110.150	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1