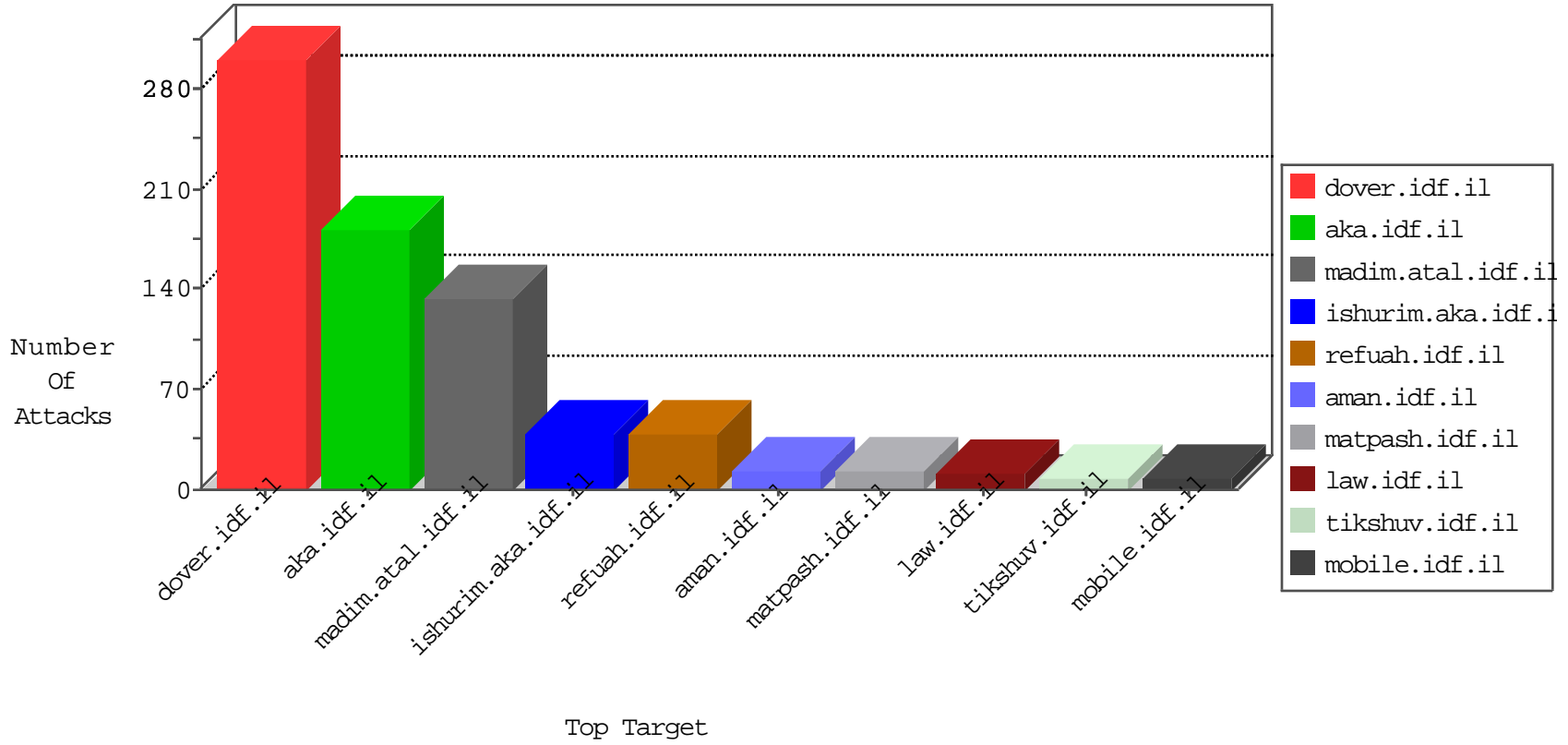
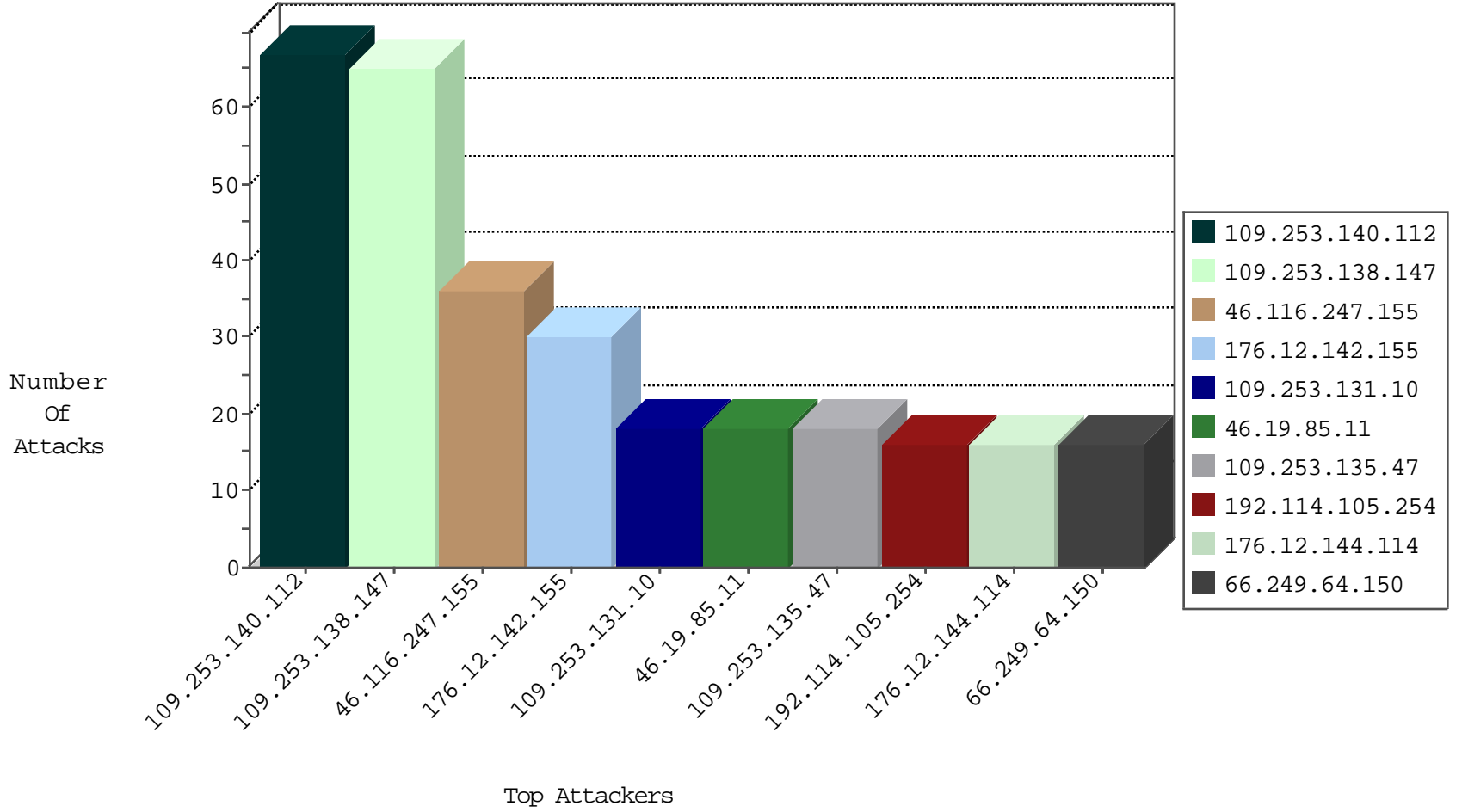


Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.197	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	474
46.116.247.155	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	353
114.79.52.217	Indonesia	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
79.177.20.53	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	2
71.6.216.41	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
71.6.216.50	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
121.115.68.176	Japan	147.237.76.148	ggcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
62.219.0.106	Israel	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
38.229.1.13	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
82.80.16.116	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
46.28.204.46	Switzerland	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
194.90.169.2	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
62.90.192.168	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
146.148.56.75		147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	4
46.19.85.119	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
149.88.86.111	United States	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
93.172.132.155	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
124.190.29.70	Australia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
84.95.215.111	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
85.64.69.215	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
84.110.48.68	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
180.149.246.30	India	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
85.25.43.94	Germany	147.237.77.212	e.dover.idf.il	7610: IP Reputation	Block	1
71.6.165.200	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
93.172.138.177	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.11	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
80.179.36.210	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
195.97.26.194	Greece	147.237.77.176	matpash.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
85.25.103.50	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.105	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
212.179.21.195	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

## Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
62.219.135.106	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
221.235.188.212	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
49.236.204.181	Malaysia	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
212.179.61.124	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
46.121.51.55	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
199.203.215.1	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.199.42	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
109.66.62.247	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.207	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
101.226.2.99	China	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -f -sS	1
2.54.152.238	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.106.109	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.22	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	1
61.240.144.67	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
49.236.204.181	Malaysia	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
212.235.22.200	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
49.236.204.181	Malaysia	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
212.116.173.226	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.112	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1
37.142.188.250	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
101.226.2.99	China	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
37.26.147.144	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
77.125.223.39	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
176.12.142.155	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.131.10	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.253.135.47	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.144.114	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
192.114.105.254	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
66.249.64.142	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
109.253.131.6	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
176.12.149.202	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
207.241.229.96	United States	147.237.77.216	dover.idf.il	Web Servers Slow HTTP Denial of Service	Web Server Enforcement Violation	reject	10
66.249.64.146	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
46.19.85.11	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	8
46.19.86.26	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	8
192.187.126.162	United States	147.237.77.216	dover.idf.il	SAM rule	drop	drop	7
62.219.161.88	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	7
62.219.161.88	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	7
66.249.64.150	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
176.12.138.45	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
109.253.142.71	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
109.253.147.91	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
31.210.186.144	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
46.19.85.11	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	alert	5
46.19.86.75	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
46.19.85.119	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
93.172.132.155	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	5
80.246.140.13	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	4
46.19.85.37	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
149.88.91.88	United States	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
185.26.182.36	Europe	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	4
207.46.13.16	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
109.65.29.15	Israel	147.237.72.156	aman.idf.il	First packet isn't SYN	drop	drop	4
176.12.146.119	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
176.12.141.13	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
80.246.140.13	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
2.54.41.121	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
46.19.85.245	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
80.246.137.128	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	3
80.246.137.128	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
80.246.137.128	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	3
46.19.85.11	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
80.246.140.13	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	3
46.19.85.37	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
89.216.115.6		147.237.77.216	dover.idf.il	SAM rule	drop	drop	2
176.12.148.141	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
46.19.86.111	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
31.186.228.26	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
109.65.29.15	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
91.214.5.128	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	2
176.12.149.74	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
46.19.86.6	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
85.250.73.192	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	2

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.253.140.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	67
109.253.138.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	65
46.19.85.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	13
2.52.130.155	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
212.235.23.193	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
149.88.91.88	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1302	Block	2
66.249.93.245	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	2
109.253.132.225	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
201.147.155.194	Mexico	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	2
212.179.61.124	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	2
207.10.200.26	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
2.52.163.121	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	2
207.10.200.26	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/hebrew/insignia/insignia.stm	Block	2
66.249.64.142	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/may/information3.stm	Block	1
213.57.222.55	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.67.174.104	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/payslips.aspx	None	1
84.108.204.96	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/authentication.service.aspx/getuserdetails	Block	1
37.59.29.19	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
192.187.108.59	United States	147.237.77.216	dover.idf.il	E-mail collector robots l4	Block	1
176.12.143.83	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.177.39.242	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/kapatz/relativecontact.aspx	None	1
109.253.137.64	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.236	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/webresource.axd	Block	1
46.19.86.146	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
212.117.140.170	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/smalim/scriptresource.axd	None	1
87.68.228.165	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/5/	Block	1
5.29.76.104	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/payslips.aspx	None	1
180.149.246.30	India	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
80.246.140.133	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.128.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.150	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.150	Block	1
85.65.16.200	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/authentication.service.aspx/getuserdetails	Block	1
37.142.77.94	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
192.187.108.59	United States	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
176.12.148.141	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
79.183.21.29	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.120.83.232	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/sachar/faq.aspx	None	1
212.117.140.170	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/smalim/webresource.axd	None	1
87.69.47.83	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00\$ctl00\$cphMain\$cphSachar\$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	1
184.105.247.195	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
80.246.141.232	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.125.242.224	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
157.55.39.55	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
66.249.64.150	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/hebrew/ie-welcome.stm	Block	1
85.65.177.49	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
46.19.85.11	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
176.12.149.74	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1