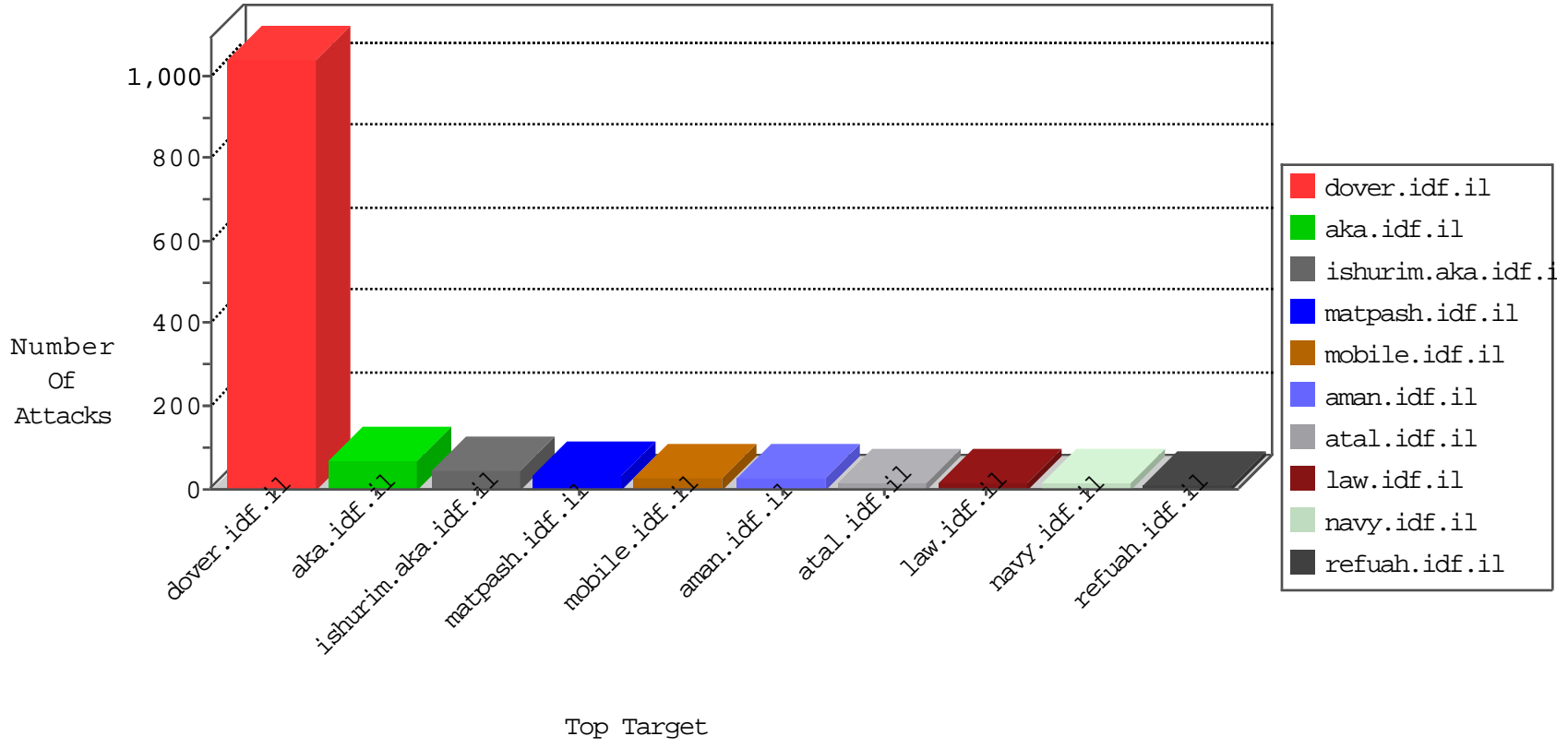
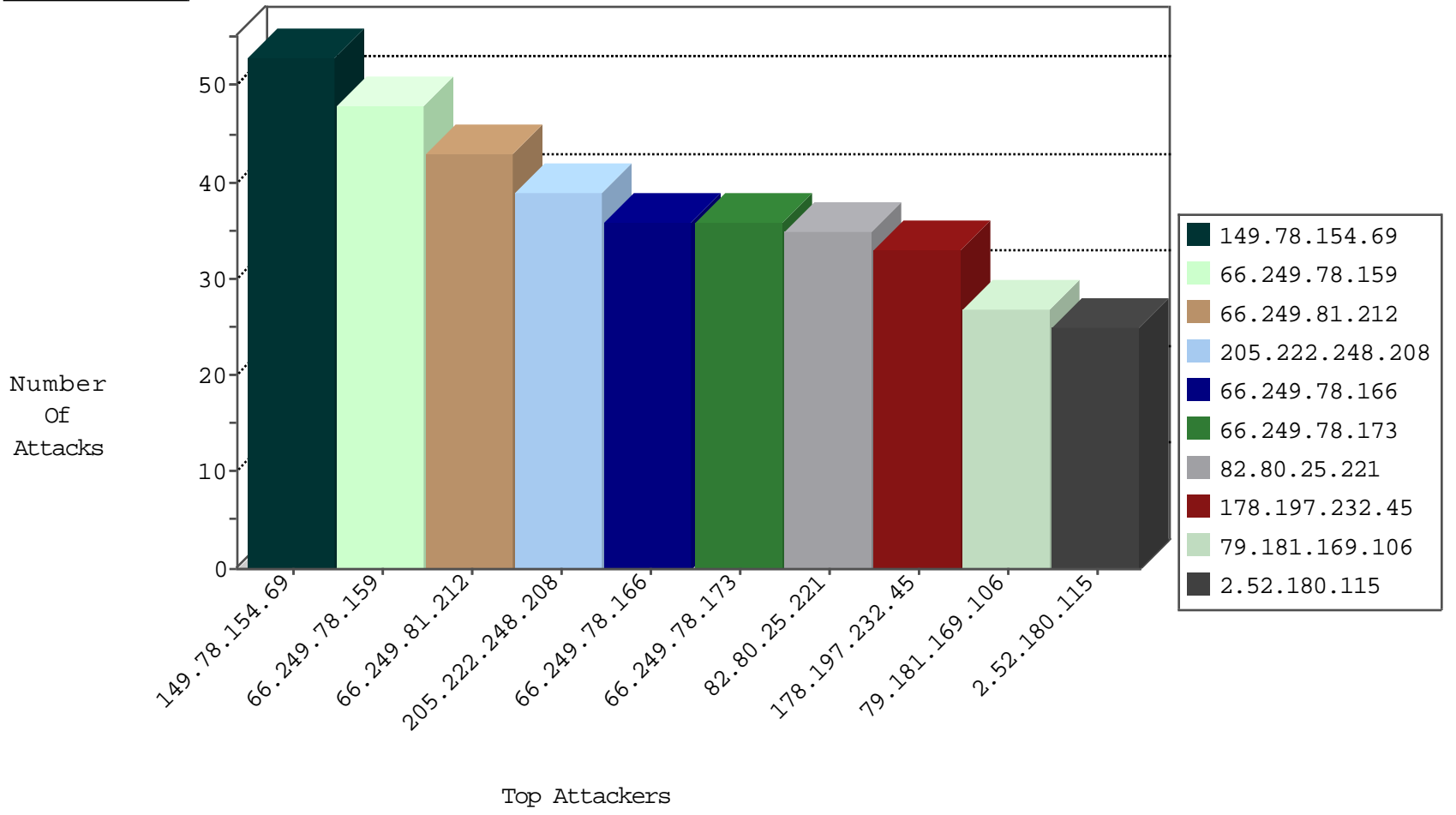


Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.67.126	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3197
84.109.39.30	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	176
46.120.5.188	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	163
178.197.232.45	Switzerland	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	forward	142
95.86.83.21	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	100
85.250.155.159	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76
94.159.230.158	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69
95.86.83.21	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	forward	61
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
111.203.147.72	China	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
80.178.136.2	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
5.102.192.107	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
5.102.192.107	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
198.20.70.114	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	2
71.6.167.142	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
95.86.96.79	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
84.228.130.106	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
71.6.165.200	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.148	ggcenter.aka.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
71.6.165.200	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
46.116.210.130	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.138.9.50	Germany	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
198.100.144.83	Canada	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
71.6.165.200	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
94.159.143.65	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
212.235.60.161	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	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1

## Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.78.89	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.190	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
87.68.77.142	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.29	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
46.116.174.45	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
113.176.14.89	Vietnam	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 3072	1
203.194.234.109	Hong Kong	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -f -sS	1
59.41.39.125	China	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 3072	1
203.113.9.143	Thailand	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
59.41.39.125	China	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -f -sS	1
188.138.9.51	Germany	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
149.78.227.153	United States	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
139.194.166.217	Indonesia	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
113.176.14.89	Vietnam	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 4096	1
203.194.234.109	Hong Kong	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.66	China	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
203.113.9.143	Thailand	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
59.41.39.125	China	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 2048	1
178.19.107.114	Poland	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
139.194.166.217	Indonesia	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
139.194.166.217	Indonesia	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	53
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	46
66.249.81.212	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
205.222.248.208	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
82.80.25.221	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
79.181.169.106	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
2.52.180.115	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
178.254.80.239	Luxembourg	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	22
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
2.52.0.85	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
89.139.171.189	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
66.249.81.218	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
178.197.232.45	Switzerland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
46.19.86.225	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
46.19.85.189	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
66.249.81.215	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
84.109.113.3	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
95.86.96.79	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
5.29.59.129	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
95.86.70.139	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
46.19.85.187	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
5.102.196.12	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	10
212.235.8.225	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
66.249.69.38	United States	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
109.65.138.246	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
182.118.20.148	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
31.168.146.182	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
46.116.174.45	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
31.210.186.181	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
144.160.226.91	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	8
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
109.65.126.234	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
172.56.11.210	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
182.250.246.200	Japan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
46.120.130.94	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
109.65.139.226	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
66.249.64.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
149.88.76.244	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
109.253.55.229	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
66.249.81.215	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.19.86.245	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
109.66.21.207	Israel	147.237.76.30	himush.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	6
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
66.249.64.178	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
31.210.186.181	Israel	147.237.77.176	matpash.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
2.89.123.182	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
73.149.108.198	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.180.127.108	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.180.127.108	Block	5
213.151.32.163	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	5
79.180.127.108	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	4
167.115.115.2	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
82.166.20.17	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
85.64.97.217	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.81.212	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/home.aspx	Block	1
66.249.64.130	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/gyus/forum/asp/showforum.asp	Block	1
109.66.21.207	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.himush.atal.idf.il/	Block	1
82.15.215.141	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.stm	Block	1
207.46.13.26	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/brothers/klali	Block	1
66.249.78.11	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/modules/forums/forum.aspx	Block	1
31.168.188.26	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/chinuch	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/eitan/listpage/default.asp	None	1
94.159.236.22	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.93.249	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
173.236.170.209	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
66.249.67.126	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
111.1.36.166	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/newsite/english/documents.asp	Block	1
82.102.141.254	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	1
207.46.13.99	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.78.153	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	1
37.142.106.112	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.139	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/ima.stm	Block	1
95.86.86.254	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
176.221.15.122	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/0916-4b.stm	Block	1
66.249.67.206	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
111.1.36.166	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/documents.asp	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/newsite/english/main.stm	Block	1
46.19.85.111	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.162	United States	147.237.72.166	aka.idf.il	Unknown Parameter 03ebfc30 in aka.idf.il/iturim/asp/results.asp	None	1
95.86.92.51	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https://www.aka.idf.il/	Block	1
183.89.136.119	Thailand	147.237.77.74	law.idf.il	Distributed Unknown HTTP Request Method	Block	1
66.249.69.82	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
116.102.134.52	Vietnam	147.237.77.74	law.idf.il	Unknown HTTP Request Method COOK in URL www.law.idf.il/14-en/patzar.aspx	Block	1
84.228.1.22	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	1
217.132.84.113	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
46.118.119.63	Ukraine	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	1
157.55.39.162	United States	147.237.72.166	aka.idf.il	Unknown Parameter sorderby in aka.idf.il/iturim/asp/results.asp	None	1
104.128.138.216		147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
80.246.138.4	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
66.249.75.117	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.157.51.62	Sweden	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/newsite/english/documents.asp	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/edim/fund/ÃfE'Ãçâ, -âe?ÃfÃçÃçæš Ã-Ã<Ã*ÃfE'Ãçâ, -âe?ÃfÃçÃçæšÃ-Ã, Ã?ÃfE'Ãçâ, -âe?ÃfæšÃ, ÃšÃfE'Ãçâ, -âe?Ãfæ Ã, Ã%ÃfE'Ãçâ, -âe?ÃfÃçÃçæšÃ-Ã, Ã?	Block	1