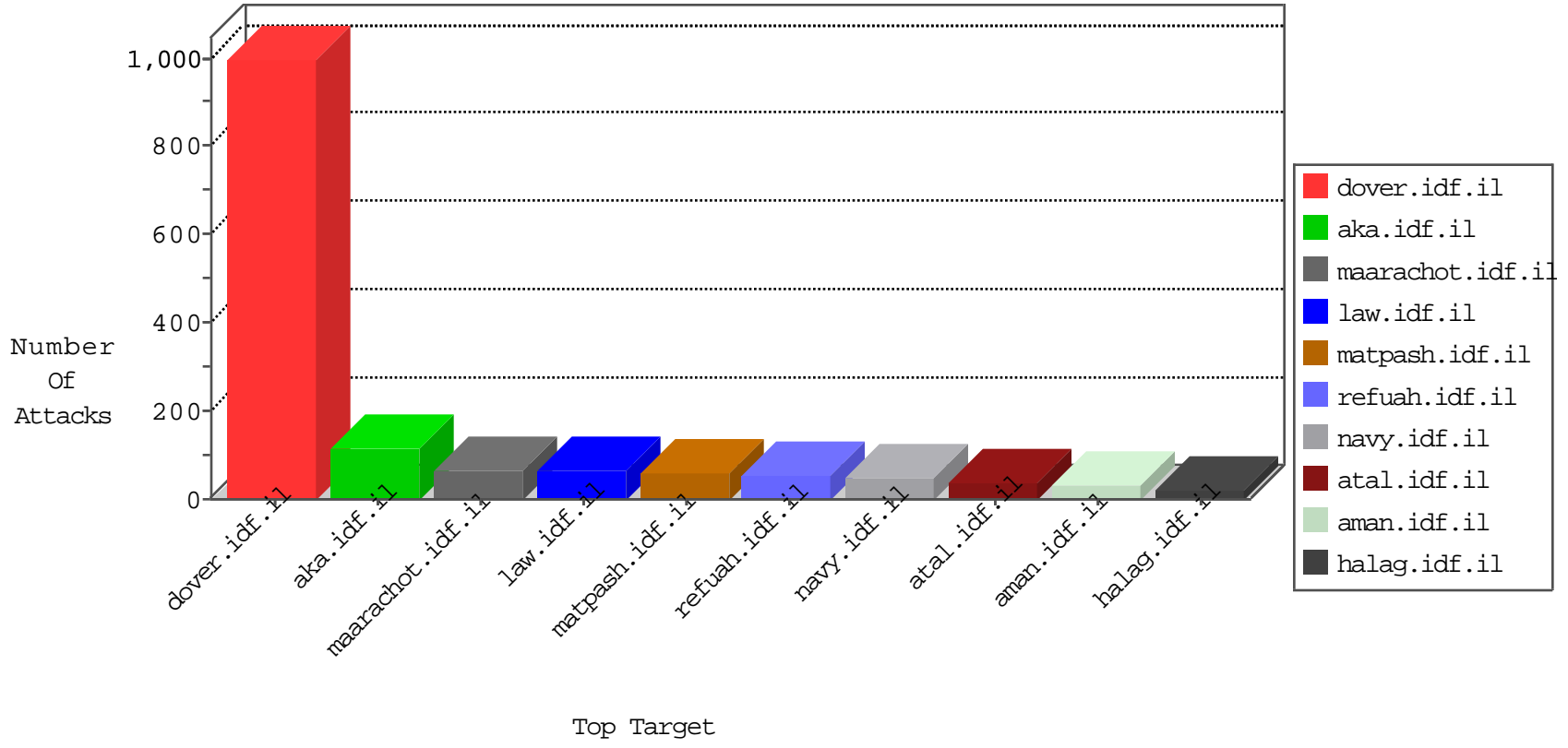
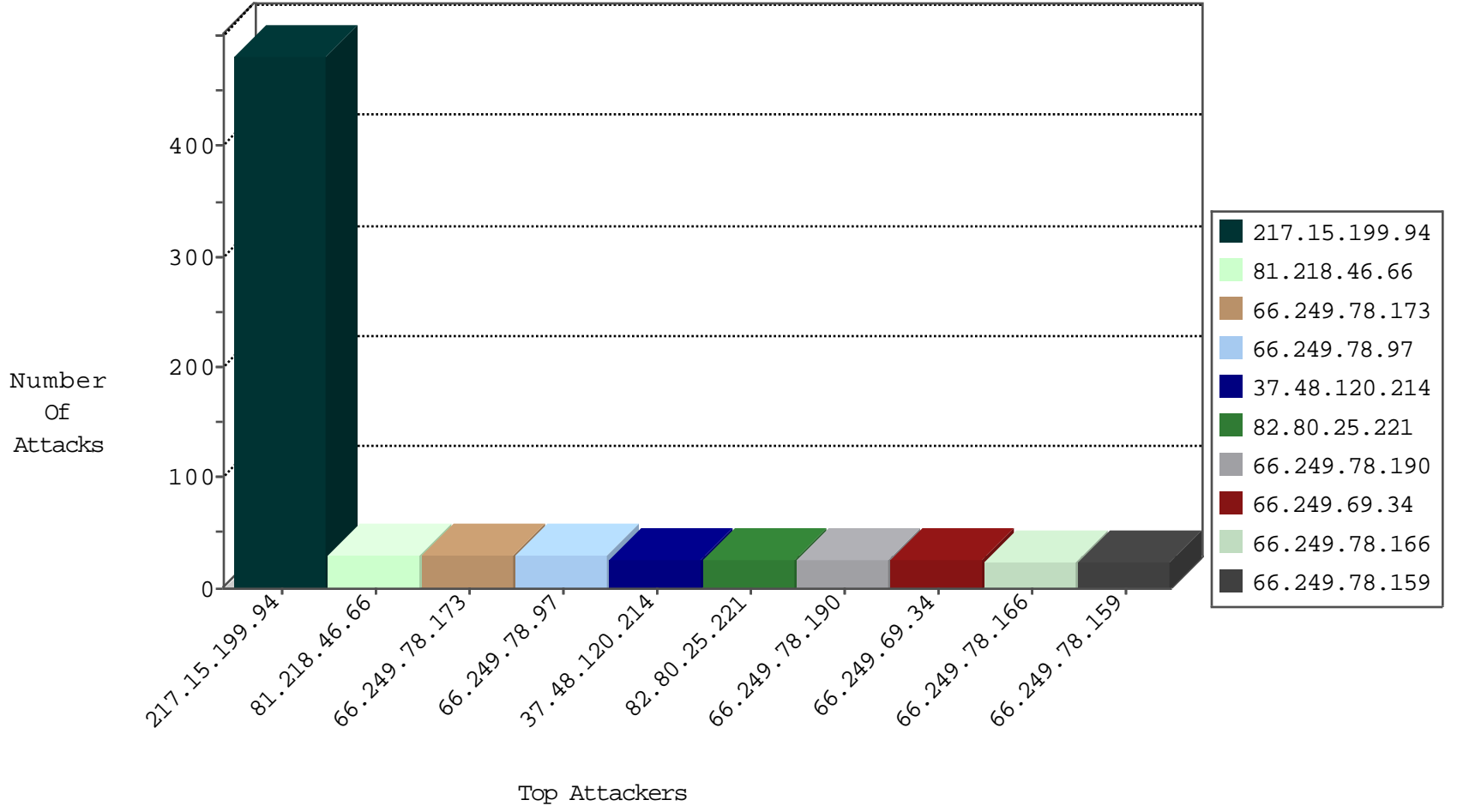




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.101	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	396
84.109.113.197	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	175
85.250.109.70	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	31
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	30
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	26
66.249.69.34	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	25
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	24
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	24
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	22
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	21
66.249.78.96	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	19
66.249.69.93	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	18
66.249.69.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	16
66.249.80.67	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	16
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	16
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	14
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	13
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	13
66.249.78.89	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	13
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	12
66.249.65.196	United States	147.237.0.19	madim.atal.idf.il	Block_Ip_Web_In	drop	12
66.249.69.128	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	11
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	11
66.249.69.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	9
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	9
66.249.78.22	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	9
66.249.78.15	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	9
66.249.69.101	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	9
66.249.78.82	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	7
66.249.78.93	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	6
66.249.80.75	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6
66.249.64.151	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	6
66.249.69.16	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	6
66.249.69.109	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.78.167	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	6
66.249.67.147	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	6
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	6
66.249.78.79	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	6
66.249.78.60	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	5
66.249.64.196	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	5
66.249.78.86	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	5
66.249.64.147	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	5
66.249.78.74	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	5
66.249.78.25	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	5
66.249.93.239	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	5
66.249.78.38	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	5
66.249.69.61	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	4
66.249.69.105	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ip_Web_In	drop	4
66.249.64.59	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	4

04-10-2015-07:03:04 to 04-10-2015-08:03:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
208.90.177.48	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
114.79.61.38	Indonesia	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
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	24
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
113.28.150.74	Hong Kong	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
113.28.150.74	Hong Kong	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
113.28.150.74	Hong Kong	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.168	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
60.18.162.244	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 2048	1
27.50.132.60	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.168	Japan	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
193.107.16.206	Russian Federation	147.237.76.34	yohalan.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
43.255.191.168	Japan	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
113.28.150.74	Hong Kong	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
113.28.150.74	Hong Kong	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
60.18.162.244	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
27.50.132.60	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 2048	1
60.18.162.244	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -f -sS	1
27.50.132.60	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.168	Japan	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
213.136.84.245	Germany	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.168	Japan	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
193.107.16.206	Russian Federation	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.168	Japan	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
217.15.199.94	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	481
81.218.46.66	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
176.12.136.107	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
84.108.226.224	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
70.197.231.220	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
176.12.149.214	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
121.54.70.12	Philippines	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
89.139.185.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
173.33.112.226	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
54.72.73.168	United States	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
178.8.72.116	Germany	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
178.8.72.116	Germany	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	6
157.55.39.42	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
178.8.72.116	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
178.8.72.116	Germany	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	6
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
46.19.86.131	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
37.247.36.80	Netherlands	147.237.8.14	e.orchot.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	5
67.84.47.213	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
73.136.138.5	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
207.46.13.82	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
157.55.39.114	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
208.90.177.48	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
173.24.90.220	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
109.66.60.83	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
31.168.244.111	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
69.196.253.30	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
128.242.249.14	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
12.197.154.136	United States	147.237.76.199	e.nakchal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	3
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
85.250.109.70	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
79.179.6.13	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
176.12.146.154	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
209.89.210.192	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
188.165.15.241	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
198.58.103.114	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
85.250.200.20	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
184.173.183.174	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.54.50.7	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
79.180.119.125	Israel	147.237.77.216	dover.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
84.228.23.230	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash	Block	3
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
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	2
190.107.176.148	Chile	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
85.250.125.62	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/payslips.aspx	None	1
217.12.204.117	Ukraine	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/shared/usercontrols/headerupper/	Block	1
157.55.39.171	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluum.	Block	1
37.8.17.108	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en	Block	1
207.46.13.79	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
149.78.175.12	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
217.12.204.117	Ukraine	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/shared/usercontrols/headerupper/	Block	1
157.55.39.172	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/miluum.	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	1
207.46.13.82	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-16786-he	Block	1
149.78.175.12	United States	147.237.72.166	aka.idf.il	Unknown Parameter q in www.aka.idf.il/main/giyus/login.aspx	None	1
217.12.204.117	Ukraine	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 217.12.204.117	Block	1
188.40.28.160	Germany	147.237.77.216	dover.idf.il	Extremely Long HTTP Request	Block	1
209.126.230.74	United States	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 209.126.230.74 (Protocol violation (SSL_CONN_SERVER_HELLO))	None	1
157.55.39.6	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/	Block	1
217.12.204.117	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
188.40.28.160	Germany	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method	Block	1
209.126.230.74	United States	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_SERVER_HELLO)	None	1
5.29.109.163	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
217.15.199.94	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1