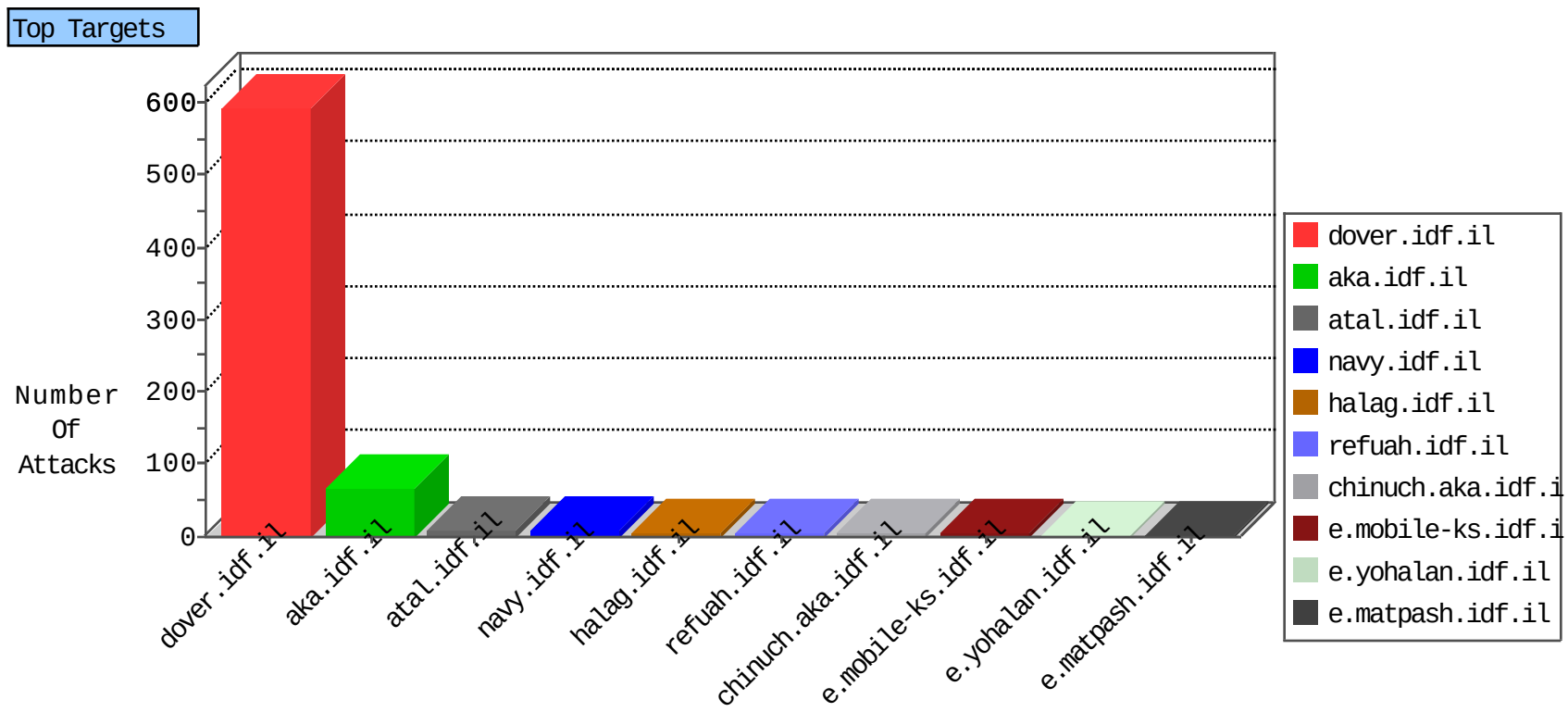
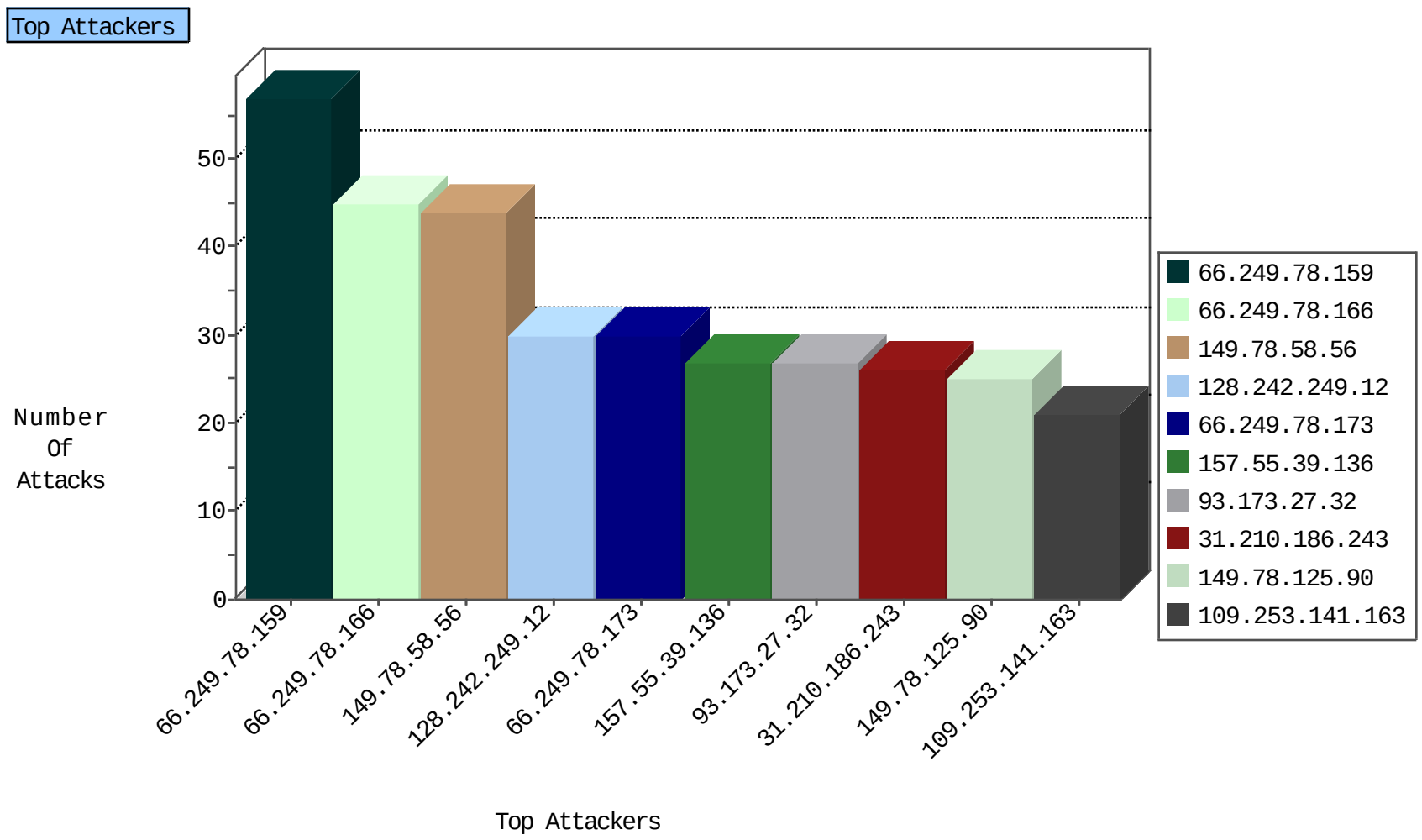
05-09-2015-11:03:04 to 05-09-2015-12:03:04

IDF Under Attack
05-09-2015-11:03:04

Top Targets



Top Attackers



05-09-2015-11:03:04 to 05-09-2015-12:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.67.152	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1437
220.181.108.167	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	231
149.78.125.90	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	108
87.68.54.186	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	99
87.68.66.25	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
85.65.144.174	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
79.183.104.55	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
124.232.142.220	China	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
46.183.220.250	Latvia	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.132	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1

05-09-2015-11:03:04 to 05-09-2015-12:03:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	30
46.117.248.136	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
93.172.40.1	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
198.20.70.114	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
176.9.29.209	Germany	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
85.15.81.210	Russian Federation	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.177	ncore.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	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1

05-09-2015-11:03:04 to 05-09-2015-12:03:04

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	4
168.144.38.32	Canada	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 3072	1
221.235.189.244	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
142.54.181.100	United States	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 4096	1
218.89.137.3	China	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.189.244	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
112.84.178.36	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
218.89.137.3	China	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.189.244	China	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
91.238.134.92	Poland	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
212.18.232.63	United Kingdom	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 3072	1
85.112.5.190	Spain	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.189.244	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
203.194.234.109	Hong Kong	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.65	China	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.189.244	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	Cote D'Ivoire	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.64	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
221.235.189.244	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
221.235.189.244	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
168.144.38.32	Canada	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 4096	1
221.235.189.244	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
168.144.38.32	Canada	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.189.244	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
142.54.181.100	United States	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
218.89.137.3	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
221.235.189.244	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
91.238.134.92	Poland	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
212.18.232.63	United Kingdom	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 4096	1
85.112.5.190	Spain	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 2048	1
221.235.189.244	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
203.194.234.109	Hong Kong	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 3072	1
85.112.5.190	Spain	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -f -sS	1
221.235.189.244	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
203.194.234.109	Hong Kong	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.64	China	147.237.72.166	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
221.235.189.244	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	Cote D'Ivoire	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
221.235.189.244	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
168.144.38.32	Canada	147.237.76.86	navy.idf.il	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	1
221.235.189.244	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1

05-09-2015-11:03:04 to 05-09-2015-12:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
149.78.58.56	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	44
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
93.173.27.32	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
157.55.39.136	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
109.253.141.163	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
31.210.186.243	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	16
84.229.132.97	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
109.65.74.196	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
79.183.104.55	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
5.28.136.86	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
31.210.186.243	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
77.127.67.39	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
208.46.106.5	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
66.249.64.168	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
66.249.64.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
66.249.64.178	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
54.77.17.58	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
149.78.125.90	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	5
93.172.40.1	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
2.52.183.110	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
66.249.78.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
109.64.24.193	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
2.54.133.37	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
87.69.122.69	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
188.165.15.99	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
149.78.125.90	Israel	147.237.77.216	dover.idf.i		Bad TCP sequence	monitor	4
46.19.85.73	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
8.37.227.61	Anonymous Proxy	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
149.78.41.57	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
84.229.34.64	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
157.55.39.191	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
149.88.79.158	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
93.172.179.115	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
79.183.176.79	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
37.142.73.115	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
89.138.80.161	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
84.143.215.196	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
79.181.22.179	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
94.159.153.211	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
85.64.205.49	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
217.121.176.203	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
84.111.234.12	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	16
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	11
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	7
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	7
37.142.143.82	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
138.134.102.15	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	4
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.117.80.165	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
185.32.178.163	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	2
74.82.47.3	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
207.46.13.26	United States	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/shalishut/site/faq.aspx	None	1
66.249.67.206	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/klali.aspx	Block	1
46.19.85.73	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233//1134-he/atal.aspx	Block	1
188.165.15.230	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9014-he/refuah.aspx	Block	1
77.75.77.36	Czech Republic	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 77.75.77.36	Block	1
66.249.69.78	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//938-he/hamaz.aspx	Block	1
157.55.39.162	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.65.6.136	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
188.165.15.240	France	147.237.76.30	himush.idf.il	Unknown Parameter lang in www.chimush.atal.idf.il/994-he/himush.aspx	None	1
157.55.39.11	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/24112010yardeni.aspx	Block	1
77.75.77.36	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/feed/	Block	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/listpage/	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/entebbe1.stm<p rel=	Block	1
157.55.39.162	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.162	Block	1
109.67.161.189	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
198.20.69.74	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
46.121.108.84	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
79.177.108.109	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/kapatz/soldiercontact.aspx	None	1
66.249.78.111	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
31.13.112.118	Ireland	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/1132-8172-he	Block	1
168.144.38.32	Canada	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx	Block	1
46.121.108.84	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.181.22.15	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl63 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
142.54.161.131	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-16707-en/dover.aspx/trackback/	Block	1