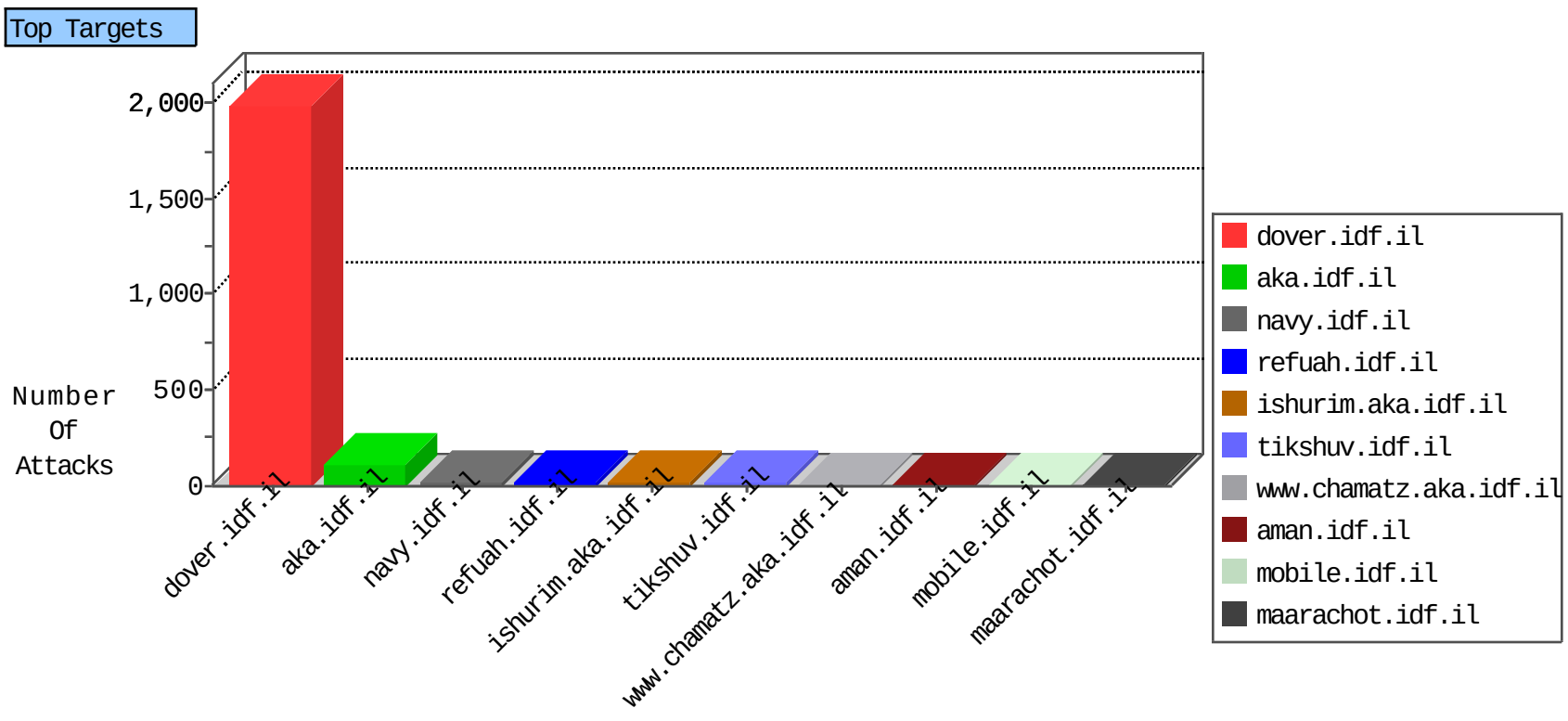
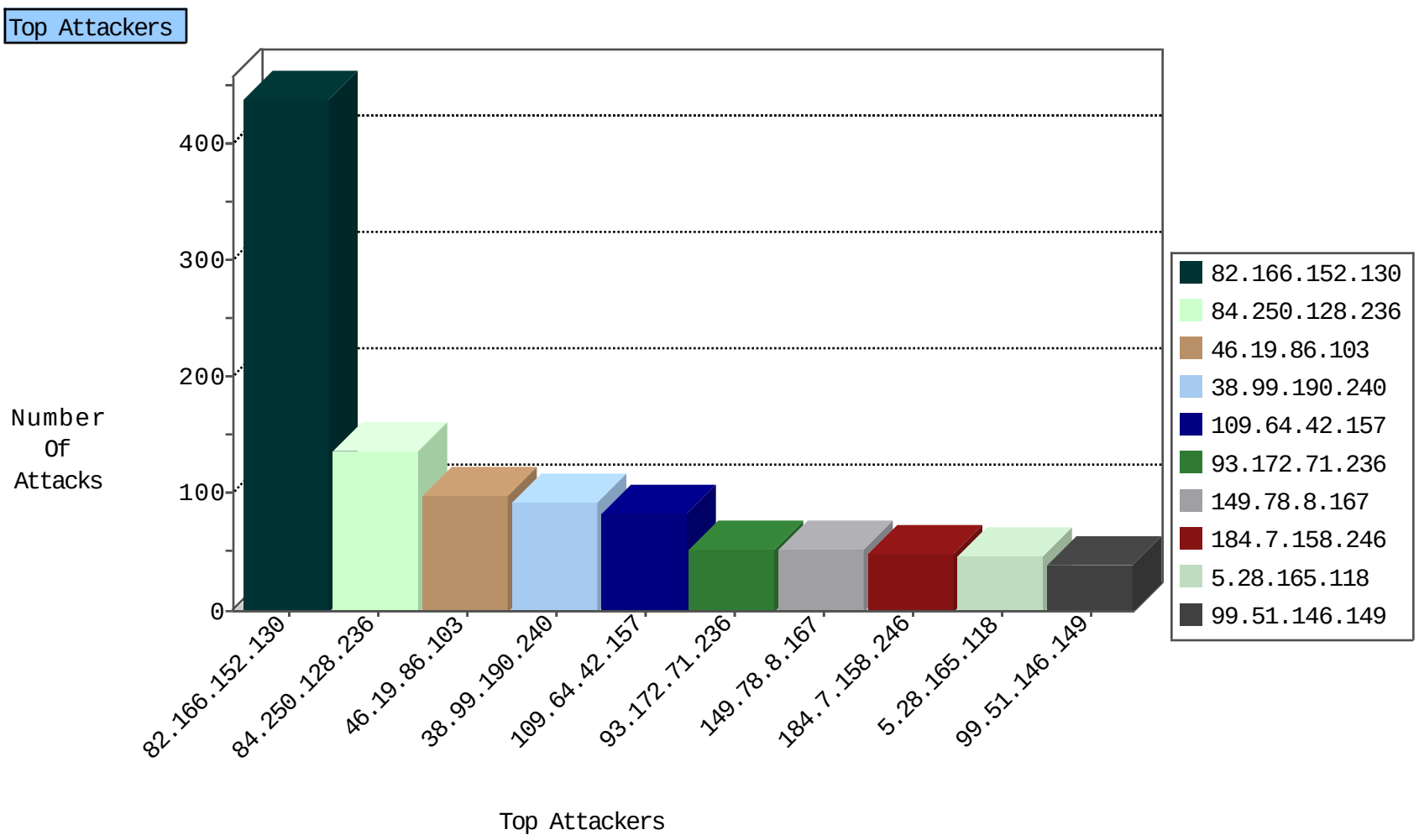
05-09-2015-20:03:02 to 05-09-2015-21:03:02

IDF Under Attack
05-09-2015-20:03:02





05-09-2015-20:03:02 to 05-09-2015-21:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.160	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	825
79.180.175.184	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	162
109.64.163.66	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
5.55.99.149	Greece	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
220.181.108.111	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	5
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
109.66.121.31	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
93.174.93.218	Netherlands	147.237.72.156	aman.idf.il	block-sp-traf1	drop	2
37.26.148.164	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
89.139.15.223	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.121.64.46	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
149.78.10.198	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
108.84.124.223	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
5.102.254.17	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
190.245.24.46	Argentina	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

05-09-2015-20:03:02 to 05-09-2015-21:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
85.250.79.201	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
79.182.33.60	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.167.142	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
5.29.194.154	Israel	147.237.77.226	www.chamatz.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.72.217	e.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
198.20.69.98	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
46.117.82.156	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
182.178.128.97	Pakistan	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
85.25.103.50	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.234	halag.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	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1

05-09-2015-20:03:02 to 05-09-2015-21:03:02

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
81.218.126.164	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.65.67	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.126	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.67	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
149.78.238.42	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.67.182.113	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.158	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
218.89.137.3	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.66	China	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
212.18.232.63	United Kingdom	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.65	China	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
144.0.0.60	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
125.39.116.219	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.130		147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
78.187.76.94	Turkey	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
212.18.232.63	United Kingdom	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.65	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
212.18.232.63	United Kingdom	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.64	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
125.39.116.219	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 4096	1

05-09-2015-20:03:02 to 05-09-2015-21:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
82.166.152.130	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	439
84.250.128.236	Finland	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	138
46.19.86.103	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	98
38.99.190.240	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	92
109.64.42.157	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	83
149.78.8.167	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	52
93.172.71.236	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	52
184.7.158.246	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	48
5.28.165.118	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
99.51.146.149	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
46.19.86.177	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
149.88.53.247	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
149.78.194.200	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
46.19.85.69	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
109.160.236.82	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	22
80.229.244.2	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
149.88.104.174	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
109.66.147.175	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
157.55.39.204	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
46.116.205.37	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
89.139.180.244	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
109.160.236.82	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	alert	12
93.173.12.120	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
149.78.238.42	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
77.71.56.103	Bulgaria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
37.140.141.37	Russian Federation	147.237.76.86	navy.idf.il	SAM rule	drop	drop	10
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
157.55.39.136	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
87.69.232.100	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
89.138.39.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
37.26.148.164	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
77.127.101.167	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
79.176.15.25	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
66.249.73.185	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
157.55.39.66	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
37.26.147.231	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
84.228.234.234	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
109.186.39.89	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
2.54.134.244	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
192.249.64.249	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
5.22.135.105	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
67.194.229.137	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
37.26.147.156	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
109.66.171.224	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
85.250.152.218	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
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	4
66.249.73.193	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.193	Block	3
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.201	Block	3
46.121.213.16	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.66.144.150	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
93.173.9.241	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.86.158	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
98.213.218.12	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.stm	Block	2
87.69.193.65	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/0/113110.pdf<hr><div	Block	2
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.185	Block	1
149.78.34.253	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/shurim/main	Block	1
93.174.93.218	Netherlands	147.237.72.156	aman.idf.il	NULL Character in Method	Block	1
84.228.83.175	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
203.133.170.144	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1208-2.stm	Block	1
66.249.78.199	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.214	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
37.26.147.193	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.177.190.203	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18774-en/dover.aspxfor	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
94.230.86.183	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giys	Block	1
52.1.167.198	United States	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on 147.237.77.176//	Block	1
85.250.79.201	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1730-he/refuah.aspx	Block	1
66.249.64.219	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
109.160.236.82	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il./	Block	1
93.174.93.218	Netherlands	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Method	Block	1
79.180.149.169	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.117	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
52.5.111.243	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on 147.237.0.34//	Block	1
66.249.79.87	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.249.67.79	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/templates/getfile/getfile.aspx	Block	1
109.253.149.30	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
46.116.205.37	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233//1134-he/atal.aspx	Block	1
93.174.93.218	Netherlands	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Method from 93.174.93.218	Block	1
79.181.173.5	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
180.76.4.154	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	1
109.64.100.232	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/fatah/hebrew/main_index.stm	Block	1
52.6.169.50	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/hebrew/ns-welcome.stm	Block	1
93.172.6.228	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.92	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/261-6366-he/patzar.aspx	Block	1
109.253.149.30	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 109.253.149.30	None	1
93.174.93.218	Netherlands	147.237.72.156	aman.idf.il	Multiple NULL Character in Method from 93.174.93.218	Block	1
46.117.180.83	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
79.182.105.139	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
188.165.15.99	France	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
66.249.78.158	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
109.65.107.69	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	1
52.7.97.214	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1

05-09-2015-20:03:02 to 05-09-2015-21:03:02