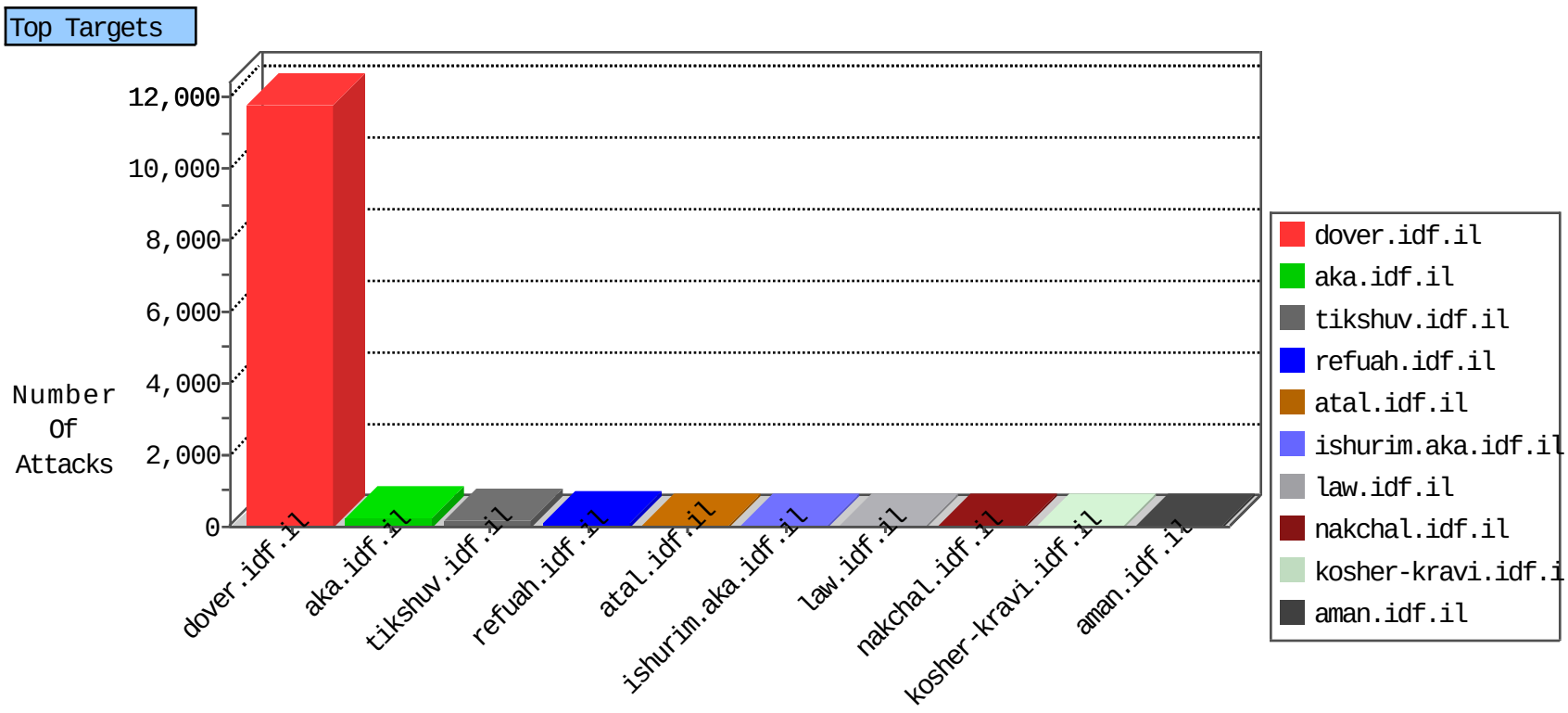
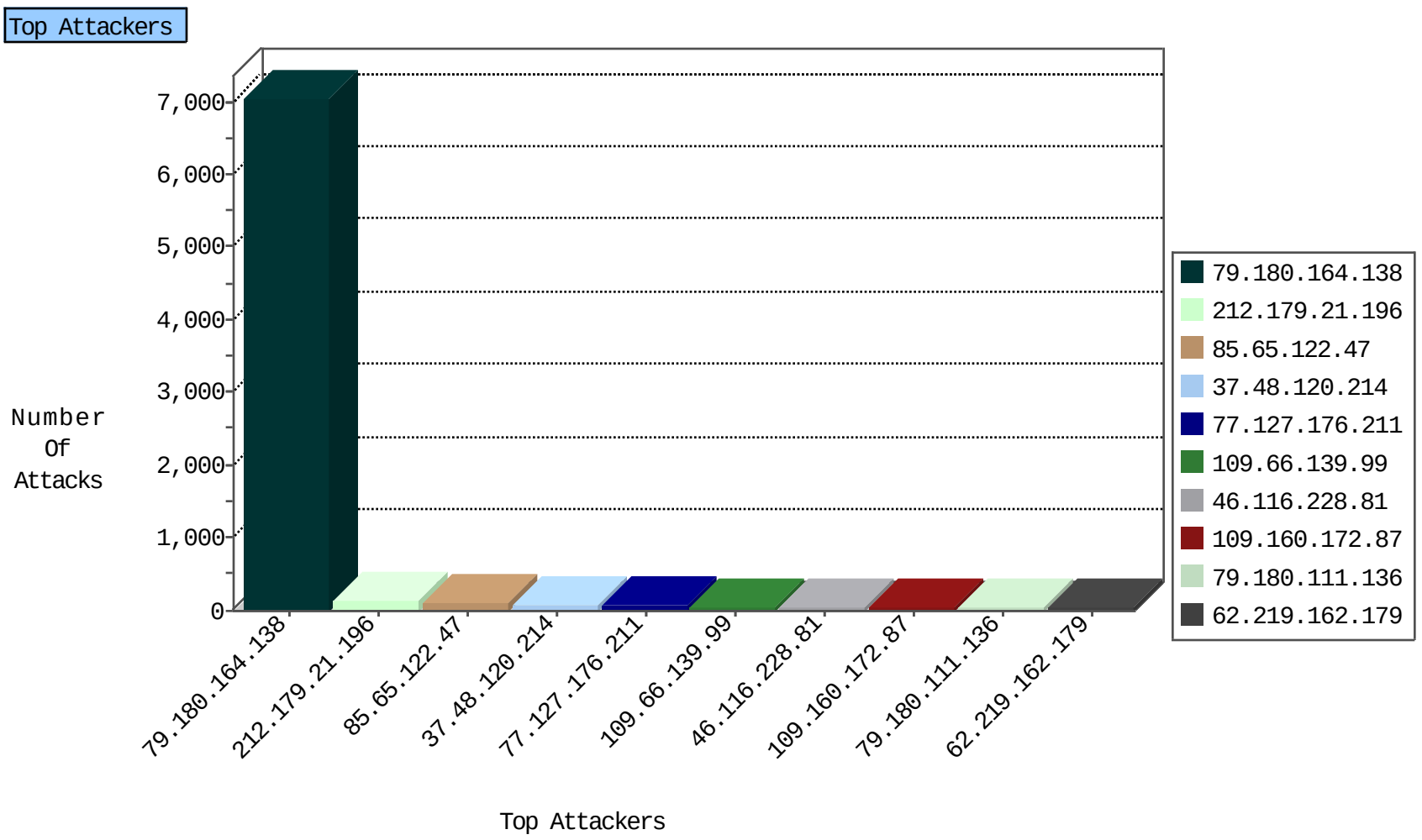
05-03-2015-16:03:02 to 05-03-2015-17:03:02

IDF Under Attack
05-03-2015-16:03:02

Top Targets



Top Attackers



05-03-2015-16:03:02 to 05-03-2015-17:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
87.68.76.153	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	325
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	196
10.0.0.8		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
2.54.140.119	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	9
82.102.169.113	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
109.64.112.198	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
89.138.225.231	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
83.114.109.196	France	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
84.228.22.248	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
192.114.105.254	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
192.117.136.82	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
81.218.32.172	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
176.12.139.207	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
54.72.73.168	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
195.37.190.86	Germany	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
176.12.148.209	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
64.246.161.30	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	drop	1
203.176.181.57	Indonesia	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
109.64.150.54	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
80.230.89.44	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
124.232.142.220	China	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

05-03-2015-16:03:02 to 05-03-2015-17:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
85.250.126.107	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
109.66.139.99	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
62.219.121.213	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
194.114.146.227	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
66.240.192.138	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.212	e.dover.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
198.20.70.114	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
37.142.86.121	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	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.85	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1

05-03-2015-16:03:02 to 05-03-2015-17:03:02

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.78.89	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.96	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.67	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.67	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
212.143.169.105	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.65	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
207.232.27.5	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.64	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
194.90.88.105	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
46.121.70.8	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.127.79	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.104	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
84.94.60.40	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
37.26.147.181	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
77.125.32.212	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
5.29.183.68	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.67	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.67	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
212.106.94.176	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.64	China	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	1
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1
50.87.144.145	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
176.12.147.200	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
46.116.167.57	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
84.109.49.95	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
46.19.85.15	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
80.246.133.162	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
5.135.199.12	France	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1

05-03-2015-16:03:02 to 05-03-2015-17:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
79.180.164.138	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7056
212.179.21.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	125
85.65.122.47	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	118
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	76
77.127.176.211	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	74
46.116.228.81	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	55
109.160.172.87	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	51
79.180.111.136	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	51
62.219.162.179	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
213.8.90.192	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
212.143.186.38	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
212.199.218.50	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
109.253.159.7	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	44
109.66.139.99	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	43
109.186.34.130	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
31.154.7.4	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
207.232.27.5	Israel	147.237.76.42	refuah.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	38
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
37.26.148.229	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
109.67.193.248	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
85.250.24.64	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
212.179.46.19	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
62.0.34.177	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
62.219.121.213	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
176.12.139.1	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
5.102.254.240	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
85.250.126.107	Israel	147.237.76.42	refuah.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	29
157.55.39.191	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
46.19.85.202	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
52.16.5.197	United States	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	25
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
93.173.148.187	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
62.219.99.130	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
121.72.232.102	New Zealand	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
192.114.105.254	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
109.64.121.71	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
203.176.181.57	Indonesia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
94.159.207.165	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
80.246.133.242	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
70.208.75.96	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
77.127.189.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
46.19.85.91	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.183.138.35	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	14
213.151.63.193	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	14
79.177.148.25	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
157.55.39.61	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
84.108.10.12	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	5
84.111.107.114	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	5
2.54.169.64	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	4
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	4
176.12.151.201	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	4
5.29.137.226	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
85.65.79.78	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
212.179.5.3	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/	Block	3
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	3
31.168.204.167	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
95.86.97.60	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/rabanut/webresource.axd	Block	3
157.55.39.61	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.61	Block	3
5.28.146.251	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
89.138.84.9	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
79.177.109.250	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
89.138.84.9	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
79.177.109.250	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
98.124.175.24	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
46.229.164.102	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	3
93.172.5.181	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.229.164.113	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.229.164.113	Block	2
79.182.183.134	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/×œ×›×ª×‘×™ ×″×žכ×? ×″	Block	2
109.253.159.193	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	2
79.178.152.143	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
109.67.182.113	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
81.218.48.37	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
212.76.100.16	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
89.138.84.9	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/scripts/css3pie.htc	Block	2
207.46.13.101	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
212.179.5.3	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.179.5.3	Block	2
2.54.138.45	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.37	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 66.249.78.37	Block	1
188.138.17.205	France	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/	Block	1
79.180.122.151	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.66	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/rights/asp/info.asp	Block	1
157.55.39.66	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
46.116.167.57	Israel	147.237.77.216	dover.idf.il	Distributed NULL Character in Method	Block	1
109.253.159.193	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
77.127.253.78	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.232.27.5	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	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
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training/	Block	1
66.249.64.197	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/×‘×žש×″×″	Block	1
157.55.39.191	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/info04.stm	Block	1

05-03-2015-16:03:02 to 05-03-2015-17:03:02