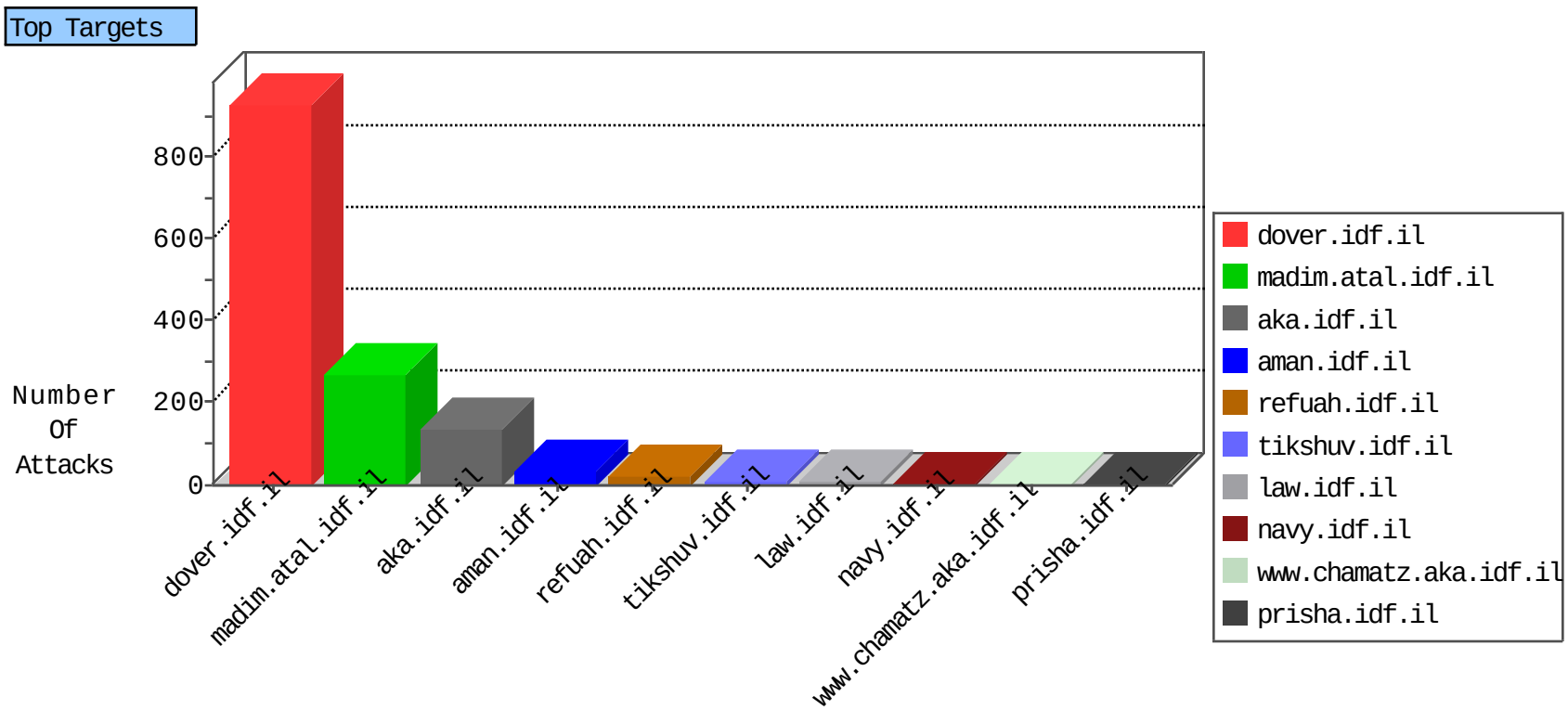
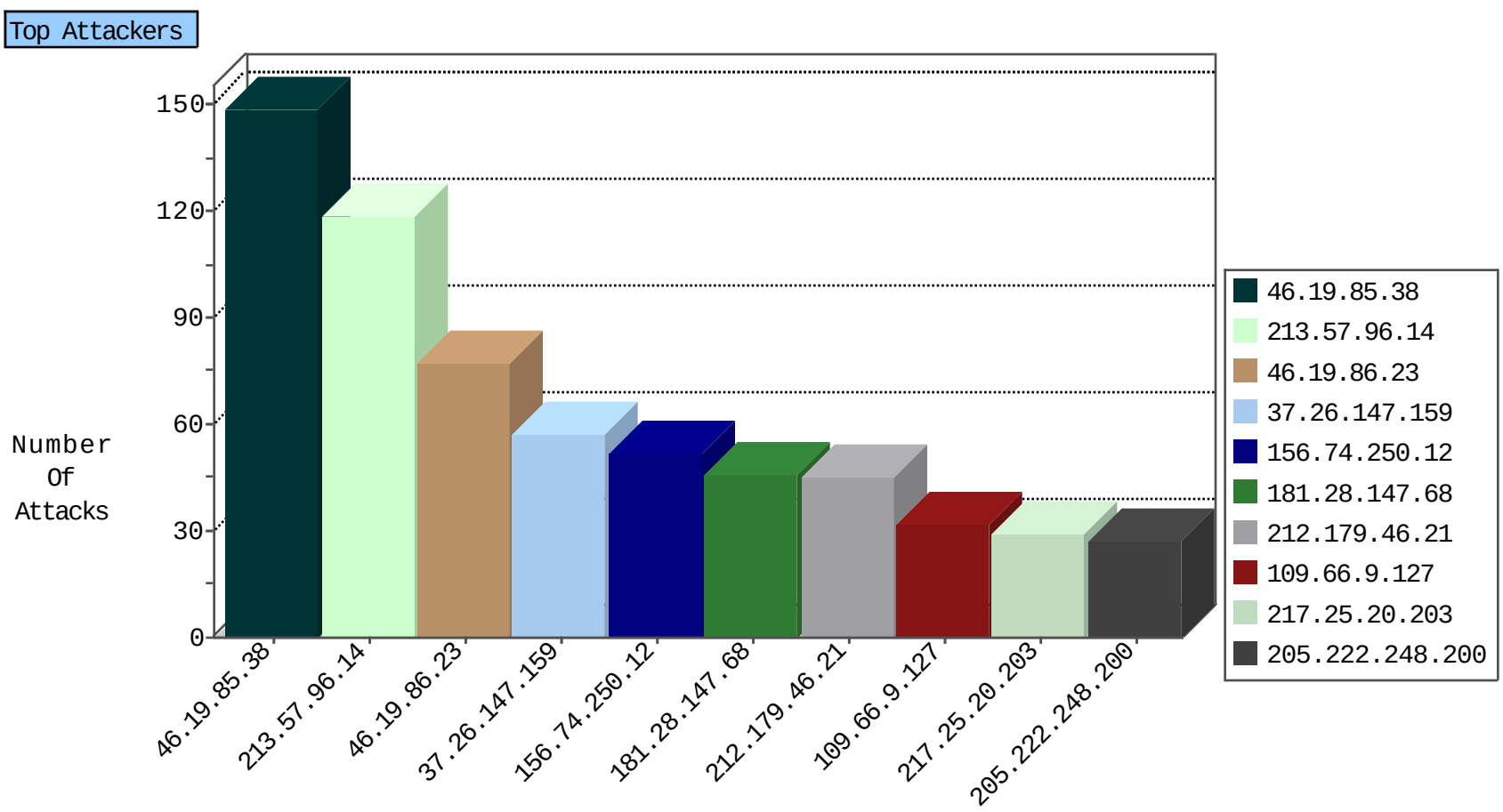
05-04-2015-20:03:09 to 05-04-2015-21:03:09

IDF Under Attack
05-04-2015-20:03:09

Top Targets



Top Attackers



05-04-2015-20:03:09 to 05-04-2015-21:03:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
79.178.8.124	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	91
89.138.215.229	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85
220.181.108.92	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	61
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
84.108.97.5	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
172.245.109.82	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
71.6.216.54	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
212.179.46.21	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
80.82.78.186	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
124.232.142.220	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
10.0.0.21		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

05-04-2015-20:03:09 to 05-04-2015-21:03:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	16
93.173.27.205	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
86.134.190.155	United Kingdom	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
66.240.192.138	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
84.108.47.185	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
31.7.57.198	Switzerland	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
31.7.57.198	Switzerland	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
31.7.57.198	Switzerland	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
109.67.190.217	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.236.119	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
84.109.178.247	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
31.7.57.198	Switzerland	147.237.77.205	prisha.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
188.138.9.50	Germany	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
46.19.86.108	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.26.232.147	Russian Federation	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
31.7.57.198	Switzerland	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
132.66.235.47	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.236.119	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
31.7.57.198	Switzerland	147.237.77.216	dover.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
66.240.236.119	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.227	e.hamaz.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
79.177.171.180	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
31.7.57.198	Switzerland	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
132.66.235.47	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.236.119	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
31.7.57.198	Switzerland	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	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	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
46.120.79.200	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	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
79.181.33.149	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

05-04-2015-20:03:09 to 05-04-2015-21:03:09

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
37.142.124.230	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.22	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
109.65.106.26	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.67	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
183.136.216.3	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
132.66.235.47	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
31.7.57.198	Switzerland	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
104.155.229.233		147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
104.155.229.165		147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
94.102.60.140	Netherlands	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243		147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
216.227.215.152	United States	147.237.0.33	idf.il	GPL SCAN superscan echo	1
61.240.144.65	China	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
183.136.216.3	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
182.72.109.162	India	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
104.155.229.233		147.237.77.205	prisha.idf.il	ET SCAN NMAP -f -sS	1
95.173.184.12	Turkey	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
84.110.74.115	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.127	United States	147.237.0.34	tikshuv.idf.il	SERVER-IIS asp-dot attempt	1

05-04-2015-20:03:09 to 05-04-2015-21:03:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
46.19.86.23	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	77
37.26.147.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	56
156.74.250.12	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	52
181.28.147.68	Argentina	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	46
109.66.9.127	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
217.25.20.203	Azerbaijan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
205.222.248.200	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
104.183.182.15		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
37.26.147.164	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
66.87.116.44	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
2.54.1.83	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
66.249.81.212	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
79.181.162.19	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
190.74.114.7	Venezuela	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
46.19.85.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
66.249.81.215	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
37.26.146.227	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
109.253.144.244	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
66.249.81.218	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
78.108.169.33	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
86.134.190.155	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
81.218.157.237	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
79.180.140.104	Israel	147.237.76.42	refuah.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	7
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
212.179.46.21	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
24.90.111.185	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
79.180.140.104	Israel	147.237.76.42	refuah.idf.i	SYN retransmit with different window scale	Bad TCP sequence	alert	5
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
132.70.66.9	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
204.45.15.186	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
46.120.75.145	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
5.29.251.17	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
77.127.13.142	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
83.130.108.105	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
105.102.238.166	Algeria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
79.180.134.34	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
2.52.55.206	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.19.85.239	Israel	147.237.76.42	refuah.idf.i	Invalid ACK number	Bad TCP sequence	monitor	3
80.246.139.122	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	3
37.26.147.156	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
212.76.107.227	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
2.52.172.226	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
46.19.85.148	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
66.249.64.76	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
212.199.205.69	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.85.38	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.38	Block	148
213.57.96.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	119
213.151.59.163	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	11
157.55.39.107	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
79.180.120.227	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.180.120.227	Block	7
157.55.39.61	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
87.69.241.92	Israel	147.237.72.156	aman.idf.il	PHP Attempt	Block	4
46.19.85.173	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
5.144.57.220	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
84.109.115.200	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
31.44.131.233	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	4
79.177.161.88	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
157.55.39.191	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.191	Block	3
79.180.120.227	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	3
80.246.130.93	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	2
198.20.69.74	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	2
213.57.188.177	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	2
207.46.13.101	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.67.52.67	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
93.172.213.39	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	2
2.54.12.17	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
79.180.140.104	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	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
185.35.62.11	Switzerland	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
76.14.88.105	United States	147.237.76.42	refuah.idf.il	Abnormally Long Request method	Block	1
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.64.104.232	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.78.125	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/templates/getfile/getfile.aspx	Block	1
85.64.23.12	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.77	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//mobile/	Block	1
157.55.39.191	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_text.asp	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
2.54.140.30	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
149.88.24.109	United States	147.237.0.16	my-kosher-kravi.idf.il	Multiple MSSQL Data Retrieval with Implicit Conversion Errors(+) from 149.88.24.109	None	1
66.249.67.62	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/164-4013-he/patzar.aspx	Block	1
94.159.152.130	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	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
76.14.88.105	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Method	Block	1
37.26.146.226	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/home.asp/	Block	1
109.65.26.175	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.78.127	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/site/general.asp...669&docid=72592	Block	1
66.249.64.177	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/	Block	1
79.179.131.118	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.102.124.70	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
149.88.70.207	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
66.249.75.49	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/938-he/atal.aspx	Block	1