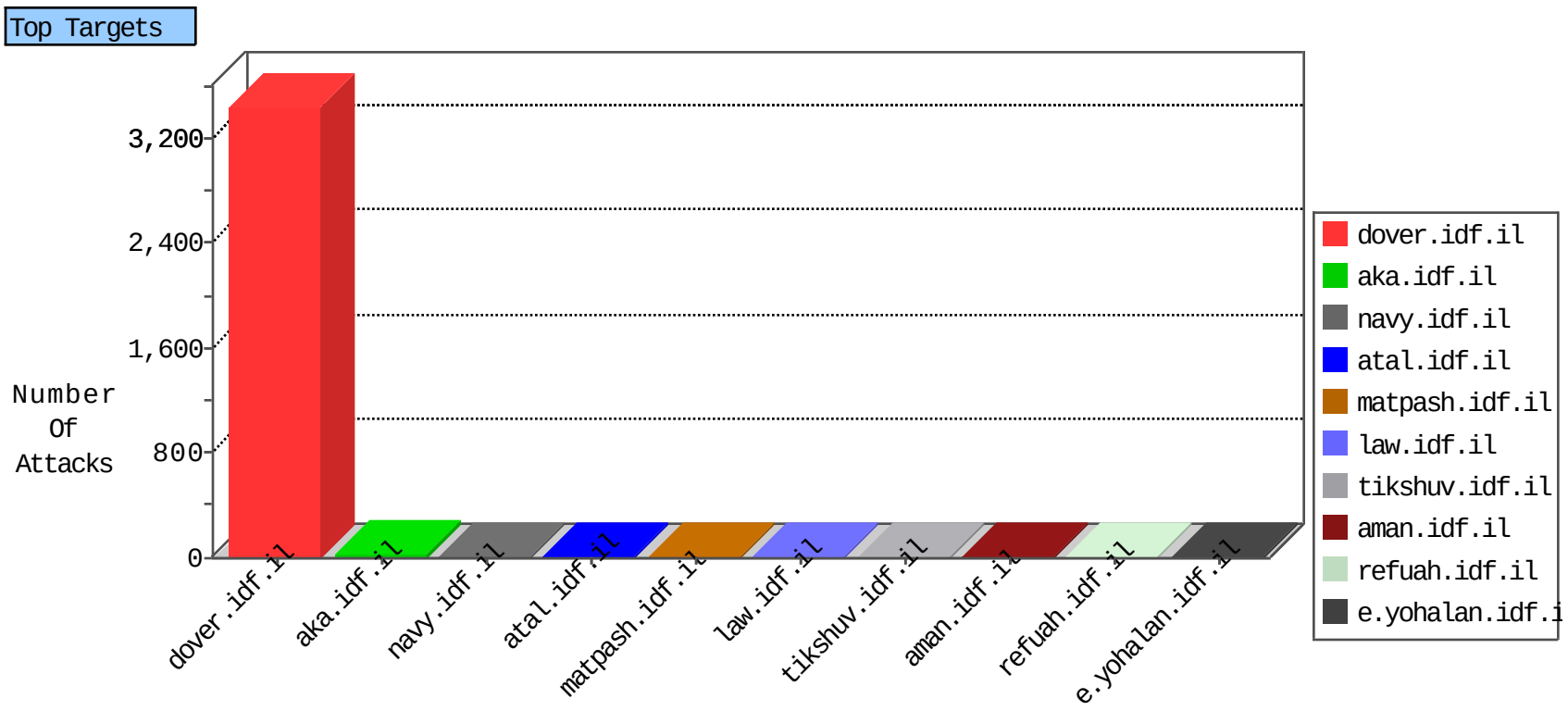
04-17-2015-06:03:09 to 04-17-2015-07:03:09

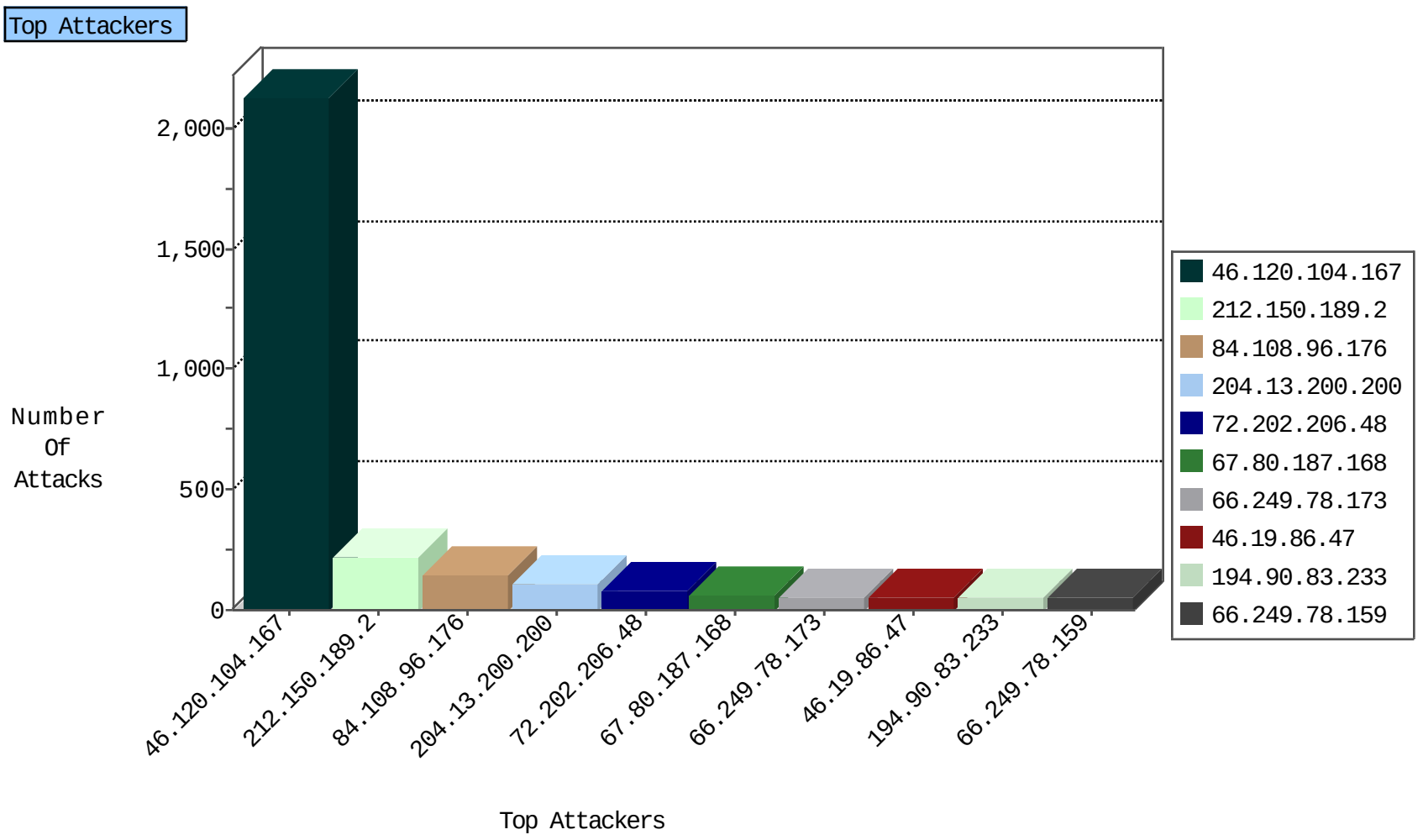
IDF Under Attack
04-17-2015-06:03:09

Top Targets



Top Target

Top Attackers



Top Attackers

04-17-2015-06:03:09 to 04-17-2015-07:03:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
204.13.200.200	United States	147.237.77.216	dover.idf.il	Frk_Purple_Con_Limit_Http	drop	3
204.13.200.200	United States	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	2
108.27.115.55	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
80.82.70.198	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
85.25.103.50	Germany	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
219.78.5.195	Hong Kong	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

04-17-2015-06:03:09 to 04-17-2015-07:03:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.240.236.119	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	2
78.108.161.226	Lebanon	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.176.73.208	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.50	e.tikshuv.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	147.237.77.19	law-forum.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
66.240.192.138	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.200	eitan.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
71.6.135.131	United States	147.237.8.50	e.tikshuv.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
85.25.103.50	Germany	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.19	madim.atal.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

04-17-2015-06:03:09 to 04-17-2015-07:03:09

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	31
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
52.4.243.253	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	4
52.6.13.145	United States	147.237.77.216	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	4
66.249.78.204	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.137	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.30	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
221.235.188.212	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
193.107.17.72	Russian Federation	147.237.77.233	atal.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
221.235.188.212	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
98.143.148.107	United States	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
203.172.184.212	Thailand	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
203.172.184.212	Thailand	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
66.249.67.90	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
203.172.184.212	Thailand	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
203.172.184.212	Thailand	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
203.172.184.212	Thailand	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
193.107.17.72	Russian Federation	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
178.135.50.34	Lebanon	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
221.235.188.212	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
91.238.134.92	Poland	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 1024	1
203.172.184.212	Thailand	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
80.55.55.59	Poland	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 3072	1
203.172.184.212	Thailand	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
203.172.184.212	Thailand	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
203.172.184.212	Thailand	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
203.172.184.212	Thailand	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1

04-17-2015-06:03:09 to 04-17-2015-07:03:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
46.120.104.167	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2130
84.108.96.176	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	141
204.13.200.200	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	100
212.150.189.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	96
72.202.206.48	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	76
67.80.187.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	65
46.19.86.47	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	49
194.90.83.233	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	49
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	46
79.177.16.30	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
213.204.127.33	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
109.253.145.11	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
99.237.251.182	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
189.217.82.27	Mexico	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
120.18.234.87	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
207.46.13.77	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
157.55.39.33	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
207.46.13.1	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
207.46.13.31	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
79.178.161.179	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
67.61.96.121	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
66.249.64.76	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
95.151.181.91	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
81.183.127.0	Hungary	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
90.83.198.171	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
209.6.133.65	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
173.35.224.172	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
74.89.29.153	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
37.142.93.224	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
187.217.195.35	Mexico	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
84.108.212.84	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
95.86.114.195	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
213.57.201.189	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.19.86.237	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
66.249.78.102	United States	147.237.77.216	dover.idf.il		drop	drop	3
186.158.141.52	Argentina	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
78.108.161.226	Lebanon	147.237.0.34	tikshuv.idf.i	First packet isn't SYN	drop	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	6
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	4
188.165.15.78	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.78	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
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
66.249.78.20	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/templates/sendtofriend/sendtofriend.aspx	Block	1
207.46.13.104	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.20	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
52.4.243.253	United States	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 52.4.243.253 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
66.249.67.157	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 54.245.64.111	Block	1
66.249.79.71	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//m/	Block	1
66.249.78.67	Israel	147.237.76.30	himush.idf.il	Unknown Parameter SortDir in chimush.atal.idf.il/1324-he/himush.aspx	None	1
207.46.13.104	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/tizmoret/klali/default.asp	None	1
66.249.67.28	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/giyus/general.aspx	Block	1
74.82.47.2	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
52.4.243.253	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.73.203	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	1
188.165.15.78	France	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
66.249.79.127	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
66.249.78.81	Israel	147.237.76.30	himush.idf.il	Unknown Parameter SortDir in chimush.atal.idf.il/1324-he/himush.aspx	None	1
207.46.13.133	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.133	Block	1
66.249.67.36	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/giyus/general.aspx	Block	1
52.5.183.76	United States	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on 147.237.77.176//	Block	1
74.82.47.2	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
66.249.73.219	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2003/november/27a.stm	Block	1
199.30.24.157	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/info.stm	Block	1
46.117.9.52	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/templates/sendtofriend/sendtofriend.aspx	Block	1
222.210.213.49	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.249.67.82	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
52.6.13.145	United States	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 52.6.13.145 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.55	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//m/	Block	1
66.249.73.229	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
207.46.13.31	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.31	Block	1
66.249.67.5	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.5	Block	1
69.30.240.46	United States	147.237.77.170	maarachot.idf.il	Illegal HTTP Version	Block	1
49.248.118.246	India	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general	Block	1
66.249.78.133	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/templates/oprolescategory/oprolescategory.in.aspx	Block	1
66.249.67.90	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
52.6.13.145	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
180.76.4.185	China	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31//	Block	1
66.249.79.55	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/m/	Block	1

04-17-2015-06:03:09 to 04-17-2015-07:03:09