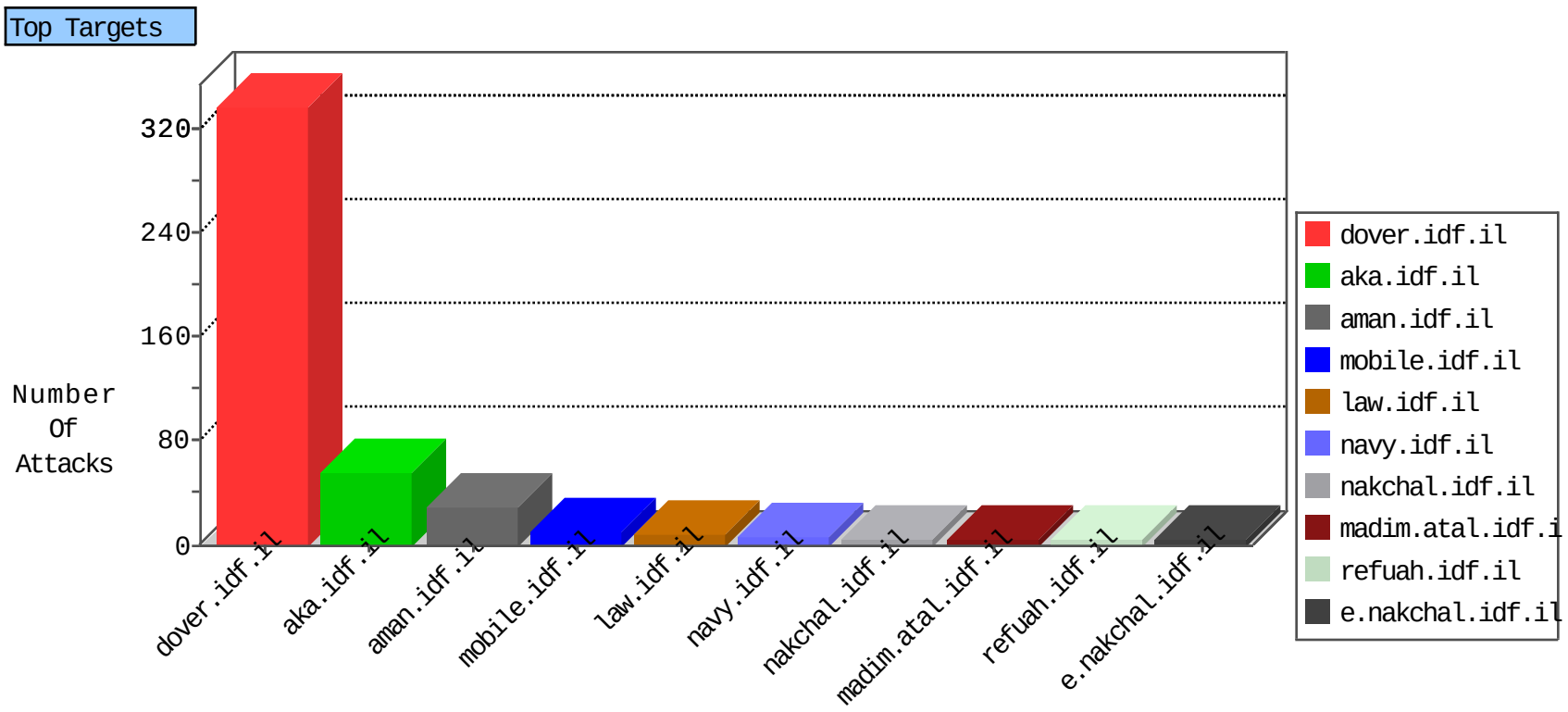
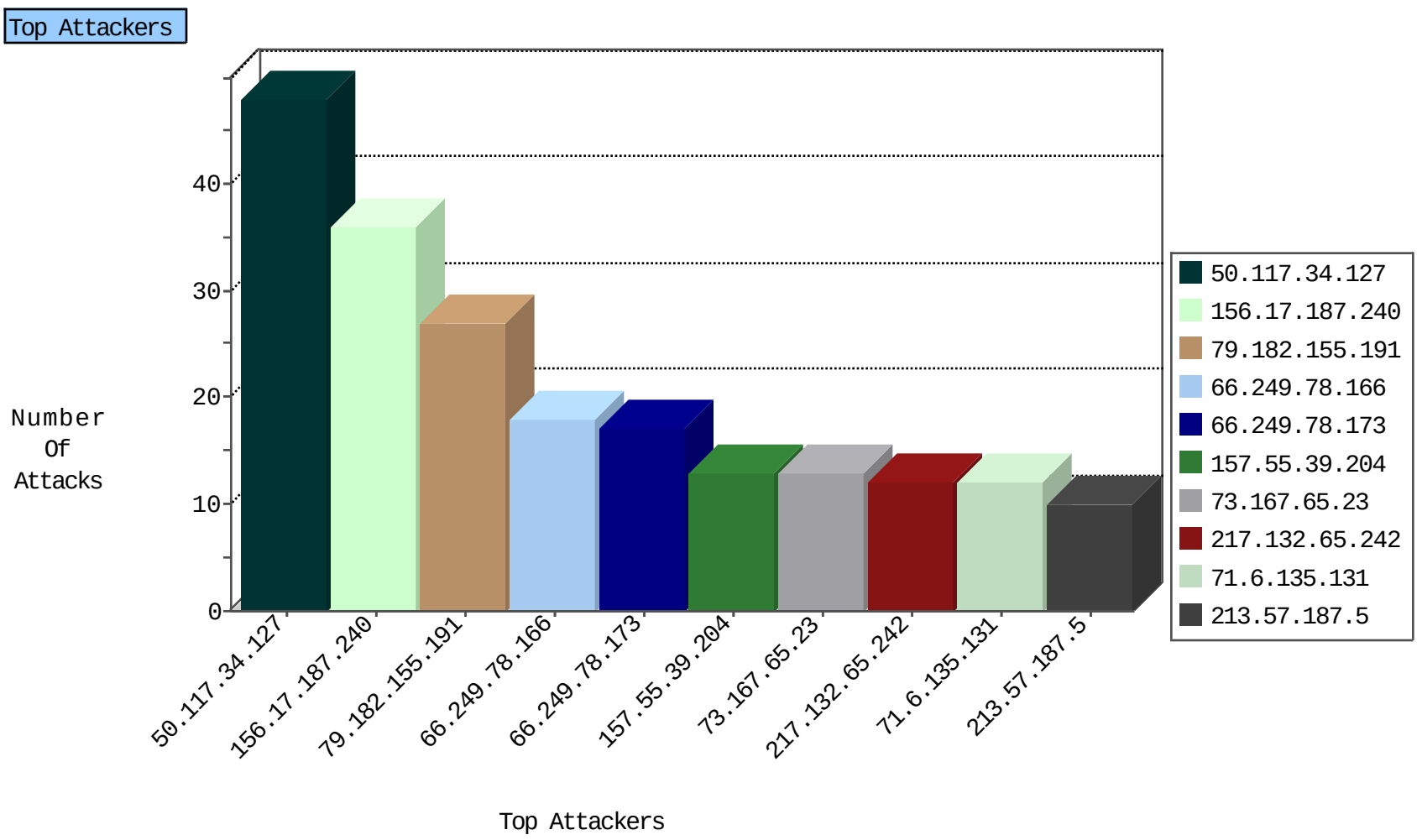
05-05-2015-01:03:01 to 05-05-2015-02:03:01

IDF Under Attack
05-05-2015-01:03:01

Top Targets



Top Attackers



05-05-2015-01:03:01 to 05-05-2015-02:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2954
105.109.14.199	Algeria	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
78.192.108.247	France	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
105.109.14.199	Algeria	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
23.243.236.9	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2

05-05-2015-01:03:01 to 05-05-2015-02:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
71.6.135.131	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	2
66.240.192.138	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	2
66.240.236.119	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.19	madim.atal.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	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.148	gqcenter.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
71.6.135.131	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.212	e.dover.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
198.20.70.114	United States	147.237.76.201	e.atal.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
66.240.236.119	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.243	mobile.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
198.20.69.98	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
37.26.146.155	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.39	mobile.meitav.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
66.240.192.138	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1

05-05-2015-01:03:01 to 05-05-2015-02:03:01

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
156.17.187.240	Poland	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	35
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.78.22	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
104.155.211.71		147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
183.136.216.3	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
130.211.253.59		147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
130.211.253.59		147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 3072	1
130.211.253.59		147.237.72.166	aka.idf.il	ET SCAN NMAP -f -sS	1
119.90.139.72	China	147.237.77.74	law.idf.il	ET SCAN NMAP -f -sS	1
218.77.79.43	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
104.155.211.71		147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
218.77.79.43	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
183.136.216.3	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	1
156.17.187.240	Poland	147.237.77.216	dover.idf.il	SERVER-WEBAPP admin.php access	1
61.49.45.46	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
130.211.253.59		147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 4096	1
130.211.253.59		147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 2048	1
119.90.139.72	China	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 2048	1
106.39.95.194	China	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1

05-05-2015-01:03:01 to 05-05-2015-02:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
50.117.34.127	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
79.182.155.191	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	14
73.167.65.23	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
217.132.65.242	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
213.57.187.5	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
80.246.133.109	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
45.50.42.249		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
208.54.80.149	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
157.55.39.204	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
178.85.30.185	Netherlands	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.19.85.169	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
46.117.123.236	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
109.65.39.151	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
46.19.85.8	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
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
108.59.253.71	United States	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
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
85.65.231.70	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
209.73.137.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
50.117.34.160	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
65.55.210.25	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
79.182.185.145	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
66.249.64.76	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
23.27.44.3	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
162.243.210.161	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
108.46.109.74	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
79.181.107.86	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
65.19.138.34	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
23.243.236.9	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
176.12.144.27	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.151.212.26	Saudi Arabia	147.237.76.31	nakchal.idf.il	SAM rule	drop	drop	1
31.168.177.103	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
85.250.0.195	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
50.117.41.79	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
176.12.144.27	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	1
109.64.100.232	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
5.29.200.87	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
66.249.64.76	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
195.239.16.40	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.151.212.26	Saudi Arabia	147.237.76.38	e.e.meitav.idf.i	SAM rule	drop	drop	1
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1

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	16
209.36.43.66	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	10
79.182.155.191	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 79.182.155.191	Block	9
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	8
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	8
157.55.39.107	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
207.46.13.101	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
37.8.25.80	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.8.25.80	Block	4
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/print_text.asp	Block	4
84.109.126.235	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	3
46.19.85.29	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
157.55.39.204	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	2
157.55.39.137	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.137	Block	2
157.55.39.158	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/yohalan/main/main.asp	Block	2
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.74	Block	2
157.55.39.61	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.182.155.191	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/acunetix-wvs-test-for-some-inexistent-file	Block	2
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/print_text.asp	Block	2
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.65.119.221	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
50.117.41.17	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//	Block	1
37.8.25.80	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 37.8.25.80	Block	1
207.46.13.101	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giyus/qanda	Block	1
66.249.78.140	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/yohalan/forums/asp/showforum.asp	Block	1
157.55.39.158	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il//captcha.ashx	Block	1
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/print_text.asp	Block	1
66.249.64.177	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
50.117.41.97	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//	Block	1
122.57.22.83	New Zealand	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 122.57.22.83	Block	1
207.46.13.101	United States	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/shalishut/site/faq.aspx	None	1
79.182.155.191	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
157.55.39.107	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.107	Block	1
93.170.1.199	Ukraine	147.237.77.74	law.idf.il	Unknown HTTP Request Method COOK in URL www.law.idf.il/163-6958-en/patzar.aspx	Block	1
46.116.226.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/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
180.76.5.171	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/homefront/map.stm	Block	1
68.180.228.173	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Unknown Parameter 136cd360 in www.aka.idf.il/main/home/default.aspx	None	1
66.249.64.177	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/	Block	1
50.117.41.232	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//	Block	1
37.8.25.80	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/administr8	Block	1
157.55.39.192	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_text.asp	Block	1
157.55.39.107	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
107.170.106.208	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
50.117.34.80	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.99	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il//captcha.ashx	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Unknown Parameter siteid in www.aka.idf.il/sites/home/default.asp	None	1

05-05-2015-01:03:01 to 05-05-2015-02:03:01