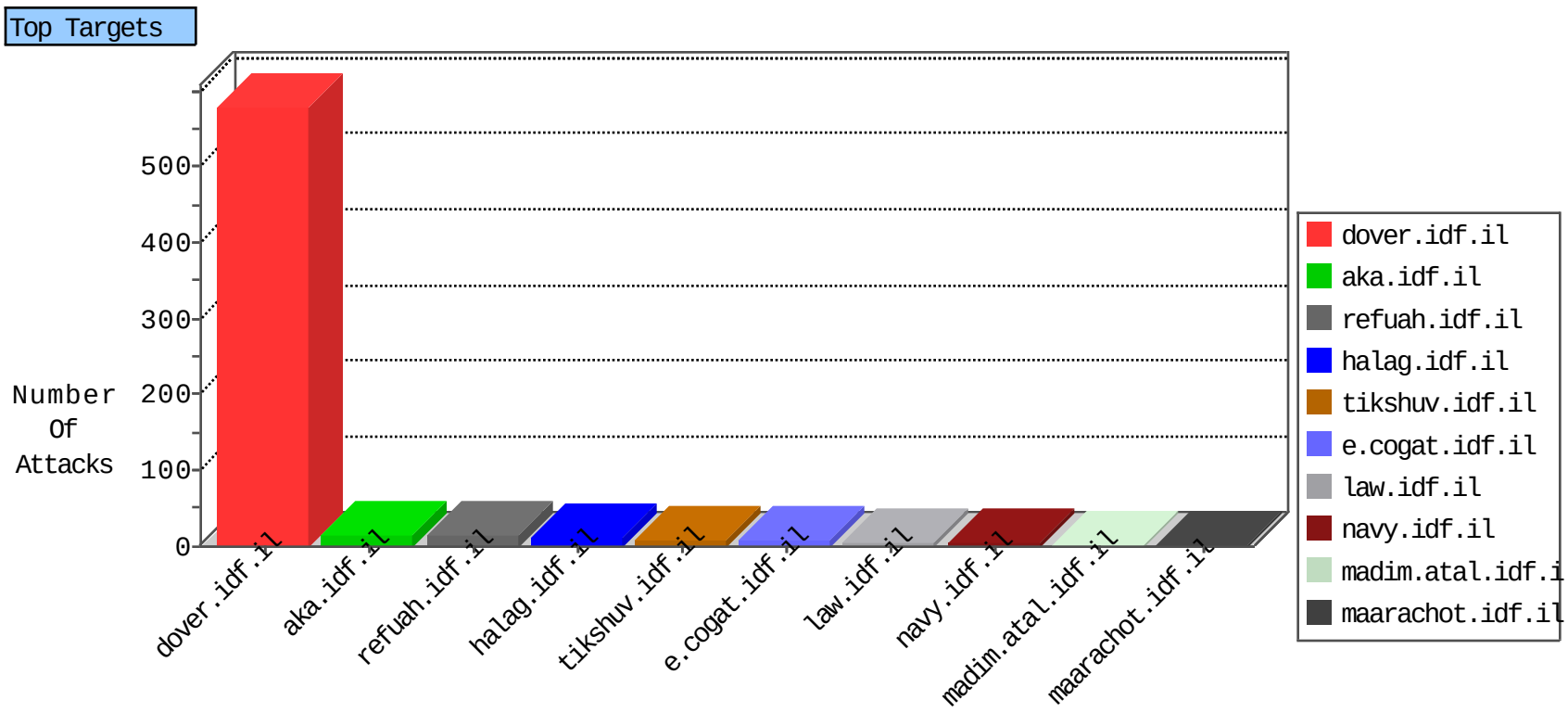
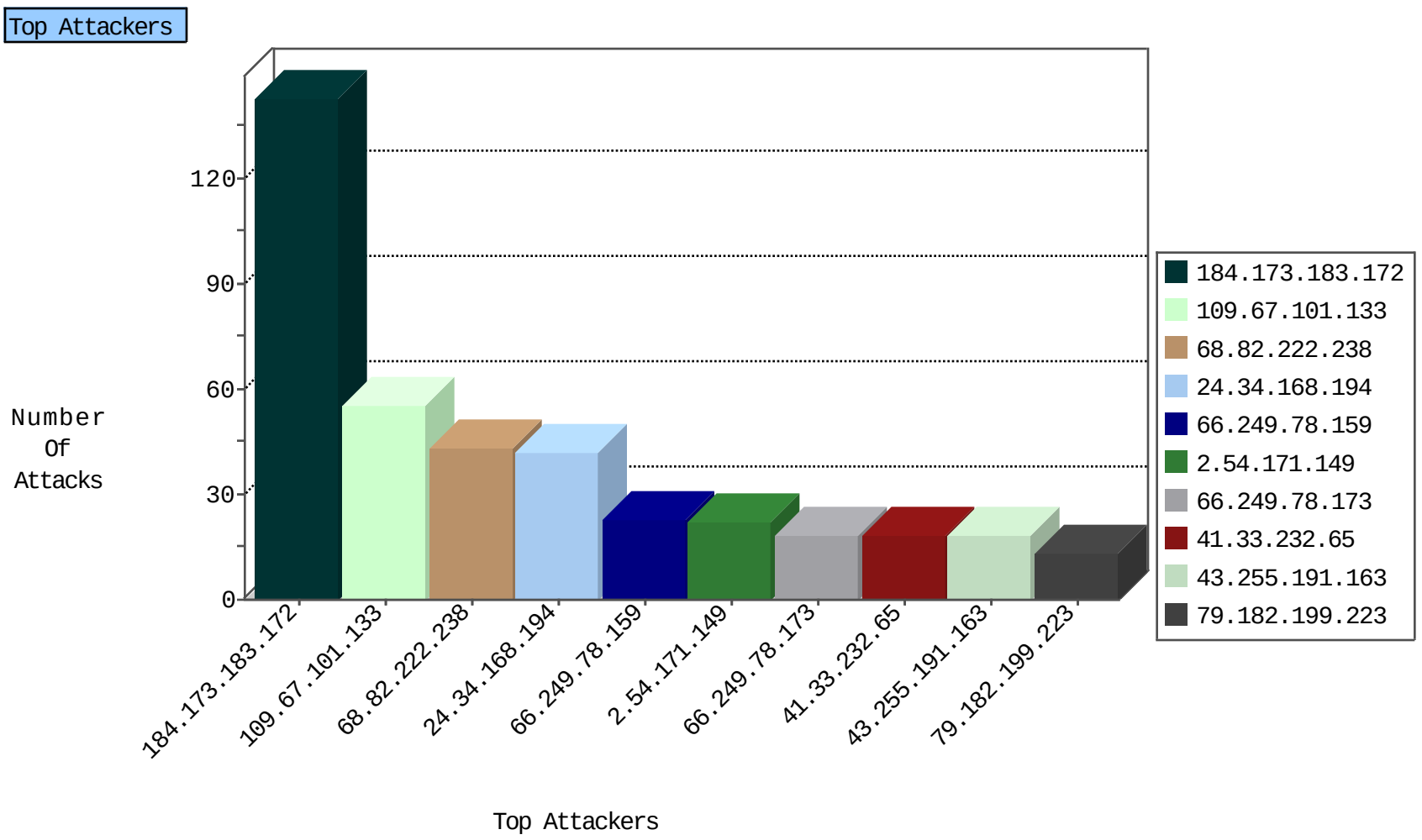
04-29-2015-02:03:09 to 04-29-2015-03:03:09

IDF Under Attack
04-29-2015-02:03:09

Top Targets



Top Attackers



04-29-2015-02:03:09 to 04-29-2015-03:03:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.104	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	3879
220.181.108.156	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	103
82.145.218.1	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	5
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
124.232.142.220	China	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
76.102.248.174	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

04-29-2015-02:03:09 to 04-29-2015-03:03:09

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	143
50.57.157.221	United States	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	3
198.20.69.98	United States	147.237.76.147	chinuch.aka.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
66.240.192.138	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
109.201.152.239	Netherlands	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.205	prisha.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
71.6.165.200	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.31	nakchal.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
71.6.167.142	United States	147.237.77.74	law.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
85.25.103.50	Germany	147.237.77.170	maarachot.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

04-29-2015-02:03:09 to 04-29-2015-03:03:09

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	6
46.116.184.0	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
2.54.54.119	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.163	Japan	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
217.91.181.112	Germany	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.65	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
208.39.68.33	United States	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 3072	1
43.255.191.163	Japan	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
199.101.186.200	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.163	Japan	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
199.30.25.34	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.163	Japan	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
114.112.96.133	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
217.91.181.112	Germany	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
61.183.128.6	China	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
199.101.186.200	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 3072	1
43.255.191.163	Japan	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
199.101.186.200	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 3072	1
43.255.191.163	Japan	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
199.101.186.200	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.163	Japan	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	United States	147.237.76.38	e.e.meitav.idf.il	ET DROP Dshield Block Listed Source	1
43.255.191.163	Japan	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
178.19.107.114	Poland	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

04-29-2015-02:03:09 to 04-29-2015-03:03:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
109.67.101.133	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	55
24.34.168.194	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
68.82.222.238	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
2.54.171.149	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
79.182.199.223	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
80.246.133.190	Israel	147.237.77.234	halag.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	9
99.178.126.147	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	7
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
90.31.95.82	Martinique	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
66.249.64.72	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
109.64.132.52	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
68.82.222.238	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
68.82.222.238	United States	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	5
62.24.252.133	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
212.76.127.111	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
157.55.39.176	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
37.247.36.97	Netherlands	147.237.77.61	e.cogat.idf.i	Geo-location inbound enforcement	Geo-location enforcement	drop	4
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	4
212.76.127.212	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
8.37.227.69	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	4
59.19.204.220	Korea, Republic of	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
24.22.22.231	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
212.76.127.44	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unexpected post SYN packet - RST or SYN expected	drop	drop	3
66.249.78.102	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
50.17.35.129	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
2.98.249.17	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
99.178.126.147	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
85.65.231.213	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
2.54.7.212	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
207.46.13.95	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unexpected post SYN packet - RST or SYN expected	drop	drop	2
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
50.97.52.131	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
24.34.168.194	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
85.72.40.4	Greece	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.54.54.119	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2

04-29-2015-02:03:09 to 04-29-2015-03:03:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.180.2.144	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 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
46.19.85.230	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	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
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-8509-he/dover.aspx	Block	1
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/resources/content	Block	1
180.210.204.141	Singapore	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1283-he/refuah.aspx	Block	1
66.249.75.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
61.135.190.201	China	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to 147.237.0.19/	Block	1
80.246.133.190	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.109	Block	1
66.249.67.54	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/templates/getfile/getfile.aspx	Block	1
183.12.169.234	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/0119-3.stm	Block	1
66.249.75.117	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.24	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-9987-he/dover.aspx	Block	1
109.203.99.4	United Kingdom	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
66.249.67.70	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/421-he/patzar.aspx	Block	1
46.19.123.125	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
207.46.13.41	United States	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.mag.idf.il//993/patzar.aspx	Block	1
72.29.127.17	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
66.249.78.21	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/mobile/	Block	1
66.249.64.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
157.55.39.176	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal/address.stm	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	1
66.249.67.108	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/993/patzar.aspx	Block	1
46.120.157.94	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
217.17.85.40	Lithuania	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
72.46.135.146	United States	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18241-he/dover.aspx	Block	1
66.249.64.44	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1153-he/dover.aspx	Block	1
157.55.39.182	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/320/patzar.aspx	Block	1
66.249.67.120	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9755-he/refuah.aspx	Block	1
54.186.248.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
220.181.108.113	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/merkava3-p	Block	1

04-29-2015-02:03:09 to 04-29-2015-03:03:09