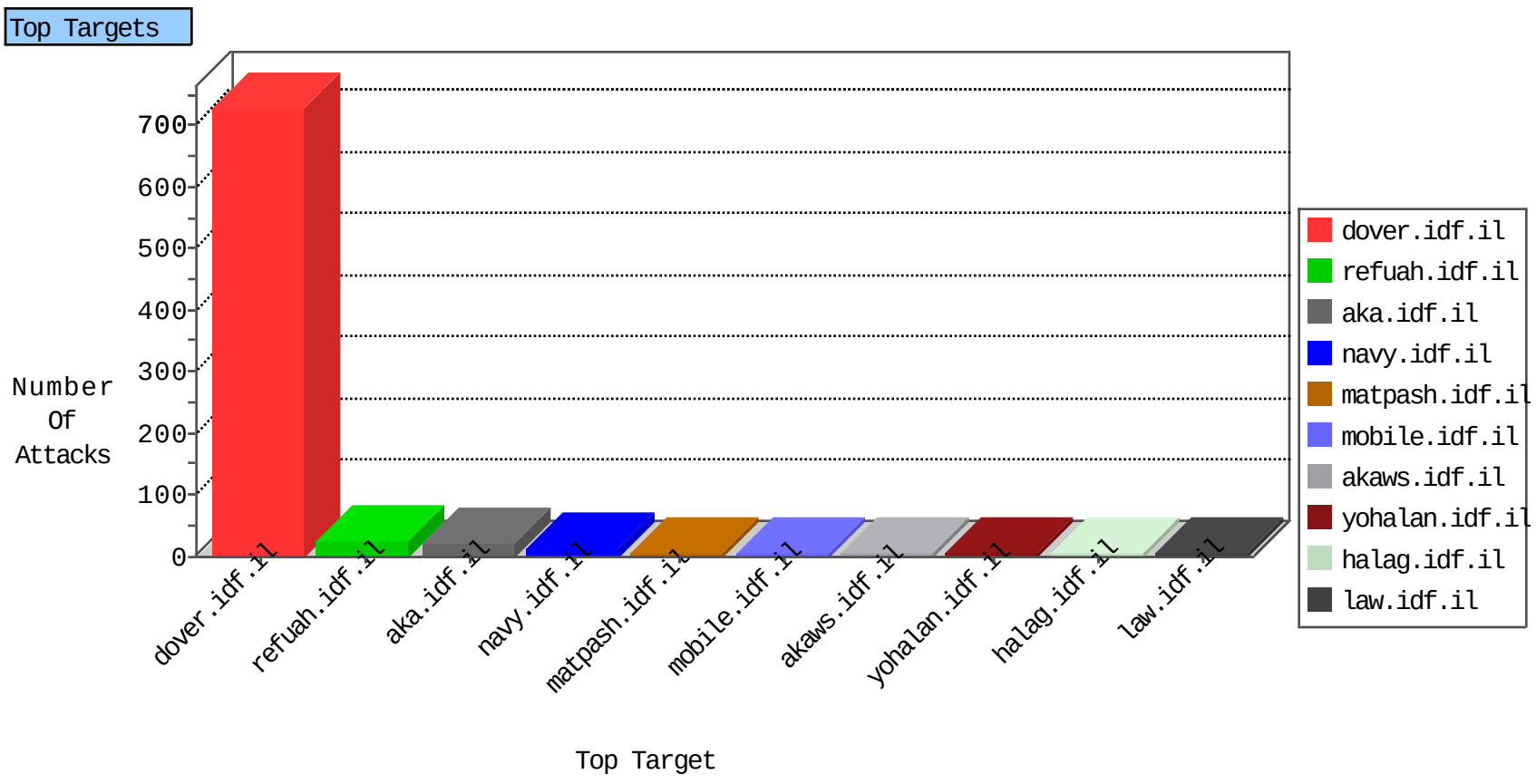
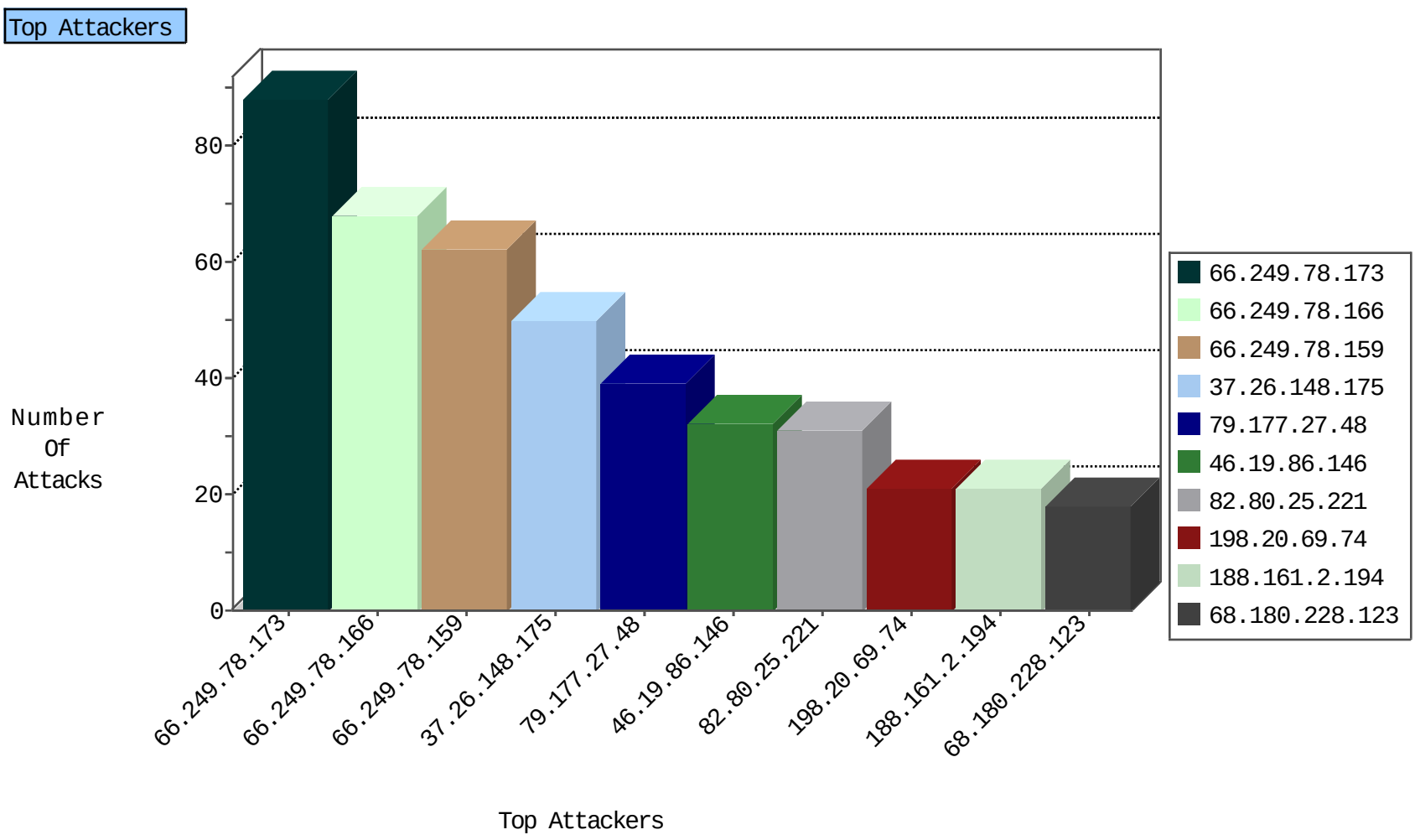
04-15-2015-03:03:02 to 04-15-2015-04:03:02

IDF Under Attack
04-15-2015-03:03:02

Top Targets



Top Attackers



04-15-2015-03:03:02 to 04-15-2015-04:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.73.217	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	649
82.145.221.20	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	5
72.181.121.41	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	2
204.8.154.50	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
121.54.54.153	Philippines	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
71.6.216.40	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
192.3.207.90	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1

04-15-2015-03:03:02 to 04-15-2015-04:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
188.161.2.194	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
74.71.49.139	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
198.20.69.98	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.148	gqcenter.aka.idf.i	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.202	e.halag.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
41.105.82.195	Algeria	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
74.71.49.139	United States	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1

04-15-2015-03:03:02 to 04-15-2015-04:03:02

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	29
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
193.105.134.32	Sweden	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
37.75.232.25	United Kingdom	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
223.5.20.21	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
104.167.117.197		147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 4096	1
222.77.190.33	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
104.167.117.197		147.237.77.234	halag.idf.il	ET SCAN NMAP -f -sS	1
197.203.43.56	Algeria	147.237.77.216	dover.idf.il	SQL 1 = 1 - possible sql injection attempt	1
101.226.2.99	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.65	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
37.75.232.25	United Kingdom	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
222.77.190.33	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
104.167.117.197		147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 2048	1
222.77.190.33	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
101.226.2.99	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 2048	1
197.203.43.56	Algeria	147.237.77.216	dover.idf.il	SQL 1 = 0 - possible sql injection attempt	1

04-15-2015-03:03:02 to 04-15-2015-04:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	80
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	62
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	54
37.26.148.175	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
79.177.27.48	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
46.19.86.146	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
188.161.2.194	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
68.180.228.123	United States	147.237.76.42	refuah.idf.i	SAM rule	drop	drop	18
198.20.69.74	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
66.249.83.194	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
66.249.64.142	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
74.71.49.139	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
66.249.64.150	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
220.255.1.145	Singapore	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
70.196.195.57	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
66.249.64.146	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
70.196.195.57	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
178.162.193.233	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
2.52.7.164	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
220.255.1.121	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
109.253.143.155	Israel	147.237.77.243	mobile.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
203.127.58.237	Singapore	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
220.255.1.30	Singapore	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
220.255.1.161	Singapore	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
207.46.13.89	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
66.249.78.159	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
68.180.228.117	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
71.172.48.205	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
201.37.117.193	Brazil	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
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
220.181.108.187	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
220.181.108.140	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.19.85.40	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
72.19.139.36	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
98.118.10.246	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
66.249.83.182	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
98.226.103.99	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
188.165.15.78	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
220.255.1.151	Singapore	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	3
220.255.1.115	Singapore	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	3
66.249.73.193	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
50.97.52.131	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
80.246.130.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
207.46.13.31	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
198.20.69.74	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	6
66.249.78.173	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	6
66.249.78.159	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	3
85.250.1.27	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/profs.asp	Block	3
46.19.85.49	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	3
85.214.16.223	Germany	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
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
77.237.138.202	Czech Republic	147.237.77.74	law.idf.il	Unauthorized URL Access to /	Block	1
66.249.73.217	United States	147.237.72.166	aka.idf.il	Unknown Parameter docI in www.aka.idf.il/main/giyus/general.aspx	None	1
207.46.13.133	United States	147.237.72.166	aka.idf.il	Unknown Parameter 6683f660 in www.aka.idf.il/main/home/default.aspx	None	1
190.47.58.166	Chile	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.65.41	United States	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam.	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	1
66.249.65.161	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1250-he/atal.aspx	Block	1
197.203.43.56	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/+and+1=1--	Block	1
62.210.182.43	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
188.138.17.205	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
85.214.16.223	Germany	147.237.72.166	aka.idf.il	Admin Blocking	Block	1
66.249.78.102	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1065-he/dover.aspx	Block	1
209.200.244.57	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
190.124.140.167	Argentina	147.237.72.166	aka.idf.il	Unknown Parameter in www.aka.idf.il/brothers/skira/default.asp	None	1
66.249.65.56	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/937-he/navy.aspx	Block	1
162.231.164.247	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il./	Block	1
5.141.213.104	Russian Federation	147.237.77.216	dover.idf.il	Unknown HTTP Request Method COOK in URL www.idf.il/1116-en/dover.aspx	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/0225-1.stm	Block	1
66.249.67.111	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/edim/yoman/enlarge.asp	Block	1
198.20.69.74	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.65.10	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
188.143.232.40	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.40	Block	1
192.99.15.227	Canada	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
66.249.65.58	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/1156-he/navy.aspx	Block	1
31.44.133.246	Israel	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1381-12200-he/kkkkkkk=ff5c52b5kkkkkkk_ff5c52b5	Block	1
66.249.73.201	United States	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
199.47.81.11	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/351-	Block	1
66.249.65.39	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/edim	Block	1
188.143.232.40	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/searchresults/searchresults.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
195.144.11.46	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
66.249.65.60	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/938-he/navy.aspx	Block	1
46.19.85.49	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.19.85.49	Block	1
180.76.4.140	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
74.208.16.178	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
66.249.73.211	United States	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
207.46.13.60	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-10770-en	Block	1
188.165.15.78	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/0225-1.stm	Block	1
66.249.65.41	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/rights/asp/faq.asp	None	1
112.111.173.26	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/2/2792.ppt/trackback/	Block	1
197.203.43.56	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.203.43.56	Block	1
66.249.65.157	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1234-he/atal.aspx	Block	1