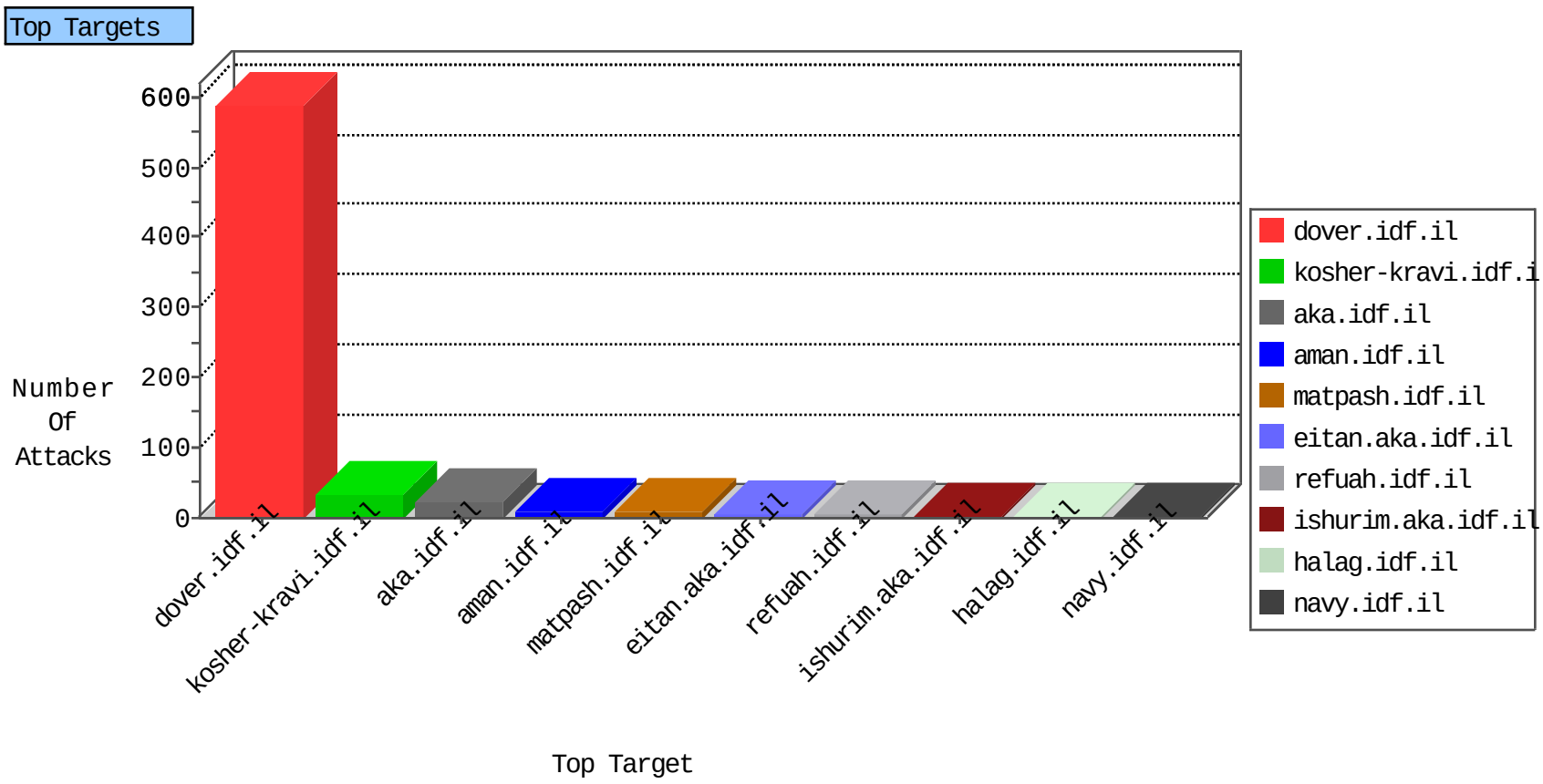
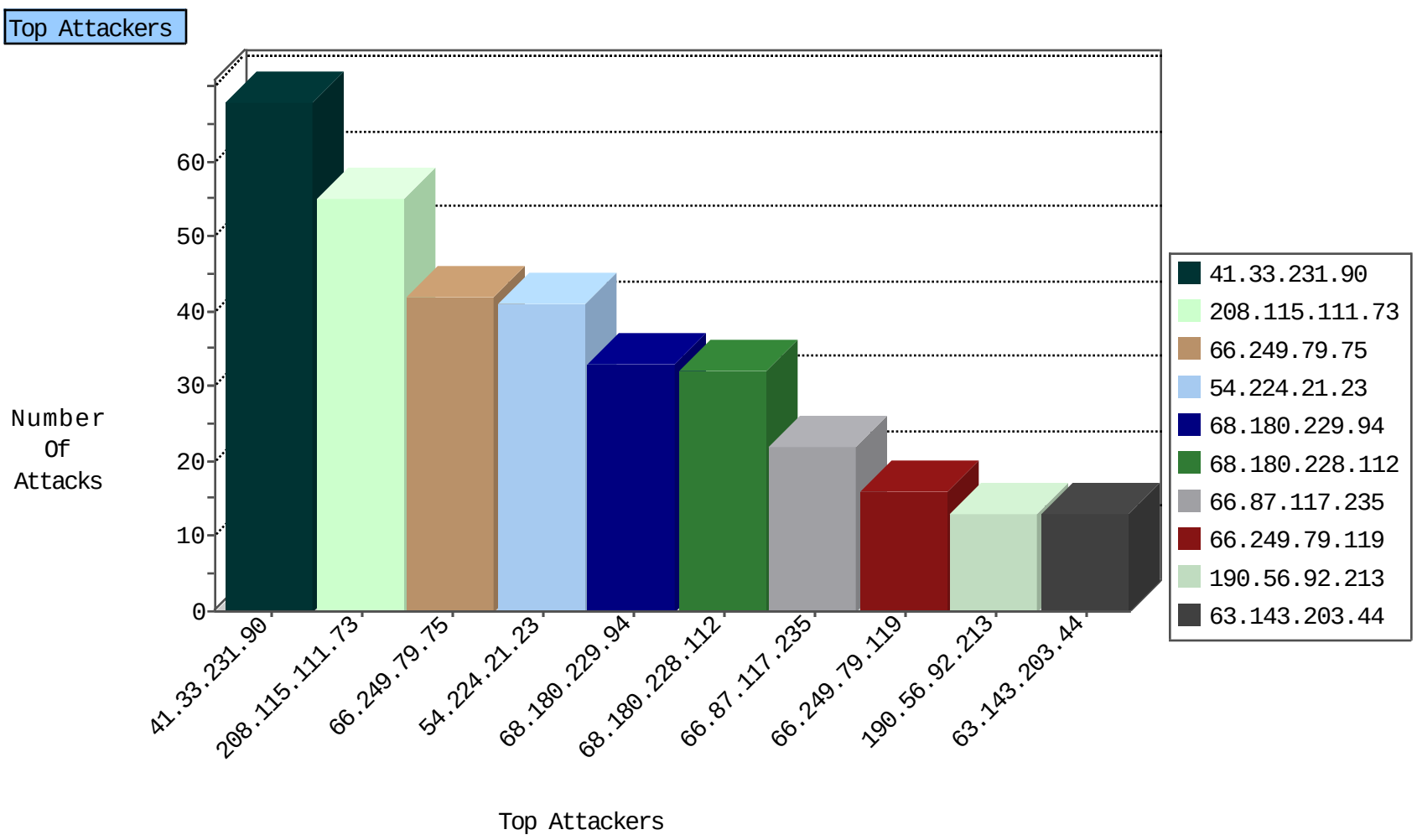
11-24-2015-04:04:02 to 11-24-2015-05:04:02

IDF Under Attack
Daily Report





11-24-2015-04:04:02 to 11-24-2015-05:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	491
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	9
93.174.93.151	Netherlands	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
185.106.94.28		147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
146.185.239.100	Russian Federation	147.237.72.156	aman.idf.il	block-sp-traf1	drop	1
185.106.94.28		147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
188.138.1.218	Germany	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1

11-24-2015-04:04:02 to 11-24-2015-05:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-24-2015-04:04:02 to 11-24-2015-05:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.78.82	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
178.79.182.42	147.237.8.24	United Kingdom	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
141.105.71.68	147.237.76.197	Russian Federation	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
141.105.71.68	147.237.72.14	Russian Federation	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
74.117.209.136	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
31.6.71.154	147.237.72.14	Poland	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
178.79.182.42	147.237.0.17	United Kingdom	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
141.105.71.68	147.237.76.176	Russian Federation	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
141.105.71.68	147.237.8.45	Russian Federation	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
85.90.247.26	147.237.77.170	United Kingdom	maarachot.idf.il	ET SCAN Potential SSH Scan	1
23.95.248.139	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1

11-24-2015-04:04:02 to 11-24-2015-05:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
66.249.79.75	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
68.180.229.94	United States	147.237.0.15	kosher-kravi.idf.i	drop	SAM rule	drop	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
66.87.117.235	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
190.56.92.213	Guatemala	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
128.242.249.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.69.172	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
1.127.48.73	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
95.108.158.171	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	9
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
63.143.203.44	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
95.108.158.152	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
5.255.253.158	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
5.255.253.168	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
5.255.253.150	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
172.56.29.8	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.249.66.96	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.46.13.17	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.140.141.2	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.255.253.170	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.79.79	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
40.77.167.0	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
141.8.142.11	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
81.216.205.40	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
165.123.68.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
70.190.211.27	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
157.55.39.128	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
52.33.66.29	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.79.75	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.79.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
128.242.249.12	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.79.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.79.75	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
168.63.12.166	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
79.180.24.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.129	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.79.119	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.69.105.83	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.12.142.0	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.66.96	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
66.249.79.75	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
46.166.188.250	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
141.212.122.96	United States	147.237.72.167	ishurim.aka.idf.il	Multiple Malformed URL from 141.212.122.96	Block	1
5.144.60.251	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.65.220.87	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	1
66.249.66.96	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
168.63.12.166	United States	147.237.72.156	aman.idf.il	Multiple signatures from 168.63.12.166	Block	1
46.19.85.125	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.79.119	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1153-he/dover.aspx	Block	1
46.166.190.162	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
141.212.122.96	United States	147.237.76.86	navy.idf.il	Multiple Malformed URL from 141.212.122.96	Block	1
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
46.19.85.125	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method essionId=cdlnsvesuays3j45znkndjb2 in URL	Block	1
110.92.98.1	Singapore	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.65.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/size100x0/2764.jpg	Block	1
141.212.122.96	United States	147.237.77.234	halag.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
5.255.253.158	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.170	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
111.206.116.217	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/home	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9043-he/refuah.aspx	Block	1
149.202.98.161	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
5.255.253.170	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.184	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/opevent/opevent.in.aspx	Block	1
46.19.86.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
111.206.116.217	China	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/home	Block	1
68.180.229.173	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.96	Israel	147.237.72.166	aka.idf.il	Unknown Parameter p in www.aka.idf.il/giyus/forum/asp/showforum.asp	None	1
168.63.12.166	United States	147.237.72.156	aman.idf.il	MSSQL Data Retrieval with Implicit Conversion Errors	None	1
46.19.85.125	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1