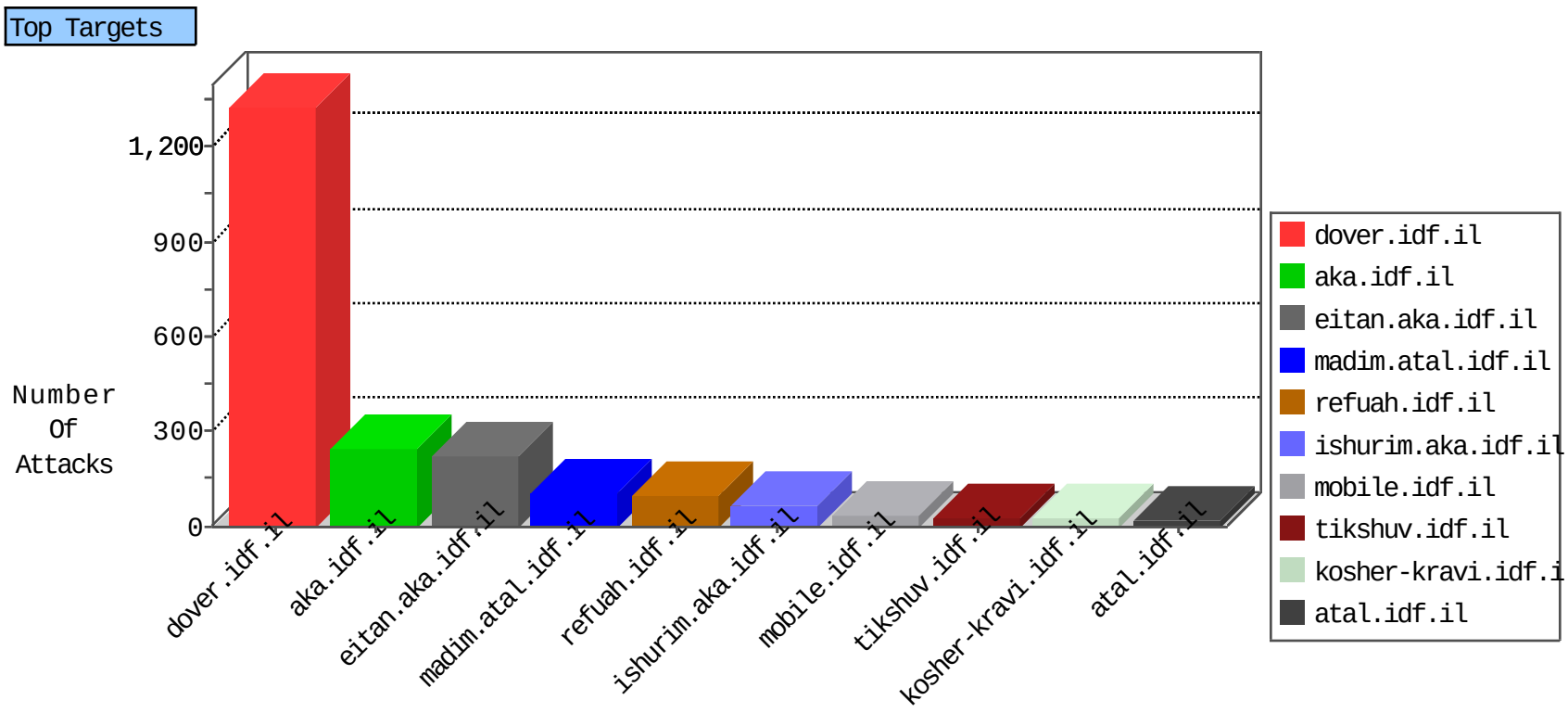
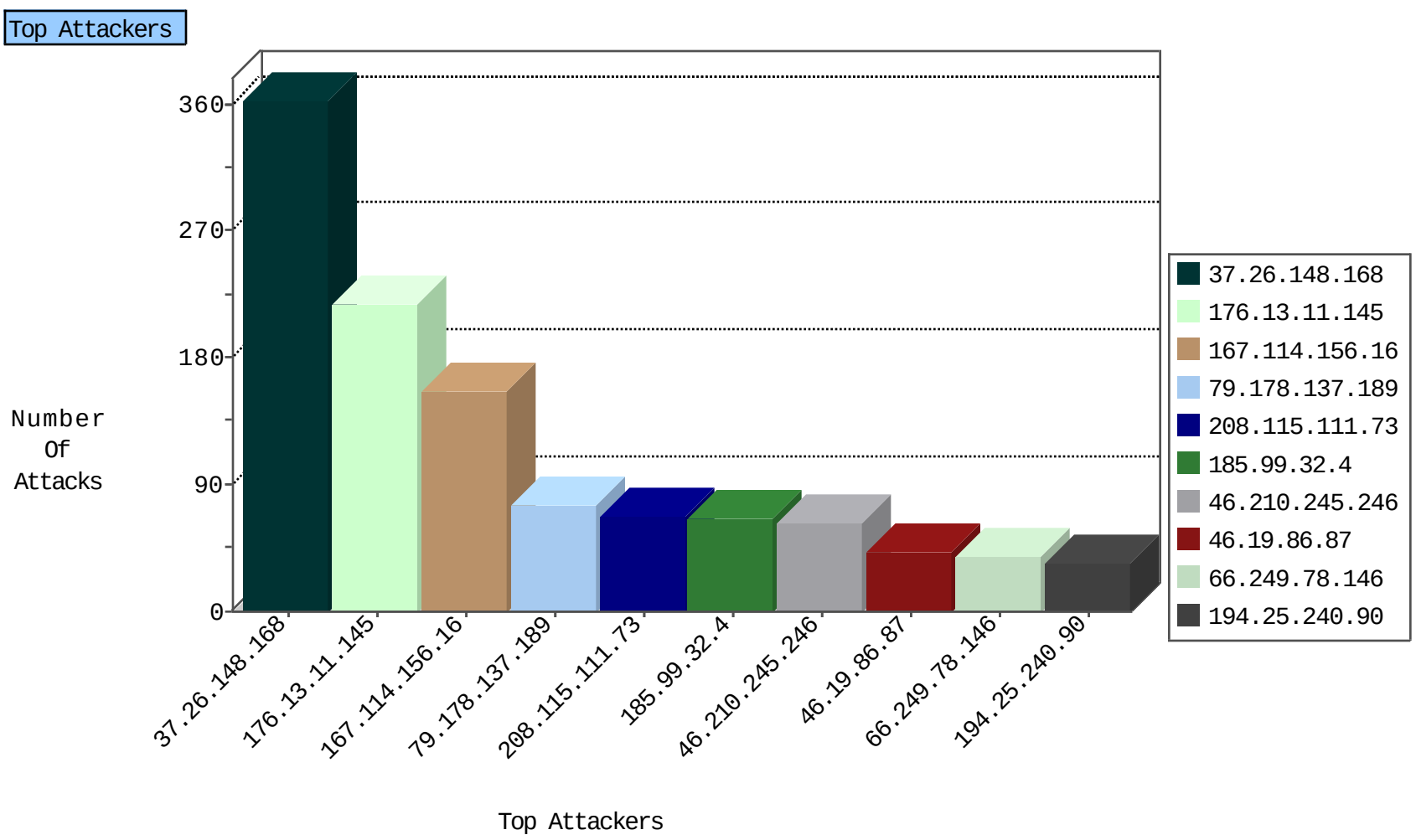
05-03-2016-14:04:05 to 05-03-2016-15:04:05

IDF Under Attack Daily Report





05-03-2016-14:04:05 to 05-03-2016-15:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.125.82.55	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2582
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	41
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	12
109.65.30.6	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	10
109.65.30.6	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
194.54.168.65	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
194.54.168.65	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
222.186.55.215	China	147.237.76.199	e.nakchal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
71.6.216.47	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
203.100.186.131	Korea, Republic of	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
45.32.79.225	Netherlands	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1

05-03-2016-14:04:05 to 05-03-2016-15:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	Block	1

05-03-2016-14:04:05 to 05-03-2016-15:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	**Signature**	**Count**

05-03-2016-14:04:05 to 05-03-2016-15:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.148.168	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	360
176.13.11.145	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	219
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	142
79.178.137.189	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	71
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
185.99.32.4	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
46.210.245.246	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
194.25.240.90	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
74.6.254.127	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
66.249.78.95	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
83.130.98.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
106.193.5.171	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
83.244.55.38	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
162.243.97.21	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
82.81.46.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	11
192.116.239.196	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	11
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
37.26.148.157	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
94.195.125.73	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.179.36.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.64.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
84.108.147.12	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
198.58.103.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.116.239.196	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	7
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
8.37.227.81	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	6
5.28.171.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.222.215	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.5.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.114.23.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
89.145.95.42	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
222.110.71.107	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.53.26.185	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.210.210.98	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.86.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.178.1.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

05-03-2016-14:04:05 to 05-03-2016-15:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
176.13.15.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
80.246.136.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
46.19.86.53	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 46.19.86.53	Block	8
84.108.76.111	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	7
194.90.99.193	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.90.99.193	Block	4
94.188.161.145	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	4
131.253.25.204	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
94.188.161.145	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew	Block	4
81.218.251.250	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	4
81.218.251.250	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/resources/content/images/mainpage/	Block	4
212.199.118.19	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 212.199.118.19	Block	3
176.13.1.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.57.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.177.19.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	3
46.120.160.61	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/	Block	3
80.246.133.86	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	3
2.55.5.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.178.137.189	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 79.178.137.189	Block	3
46.19.85.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.146.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.179.21.194	Block	2
81.16.160.45	Sweden	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
2.53.155.91	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
81.16.160.45	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index/.php	Block	2
79.177.216.149	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 79.177.216.149	Block	2
176.13.19.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.21.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.176.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.57.40.169	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	2
213.57.40.169	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/	Block	2
2.53.33.55	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
149.88.59.65	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.93.111	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
89.138.96.115	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 89.138.96.115	Block	1
52.21.178.185	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17207-en/dover.aspx#.vyinv9eihyq.twitter	Block	1
79.177.19.6	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.177.19.6	Block	1
2.55.50.84	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
82.102.136.66	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.117.62.227	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
184.105.247.196	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
79.178.137.189	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/1765-he/	Block	1
46.19.85.133	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl17 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.i	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1397-en/dover.aspx	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	1
89.138.96.115	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/1/112901.pdf	Block	1
46.19.86.87	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/mobile/login.aspx	Block	1

05-03-2016-14:04:05 to 05-03-2016-15:04:05