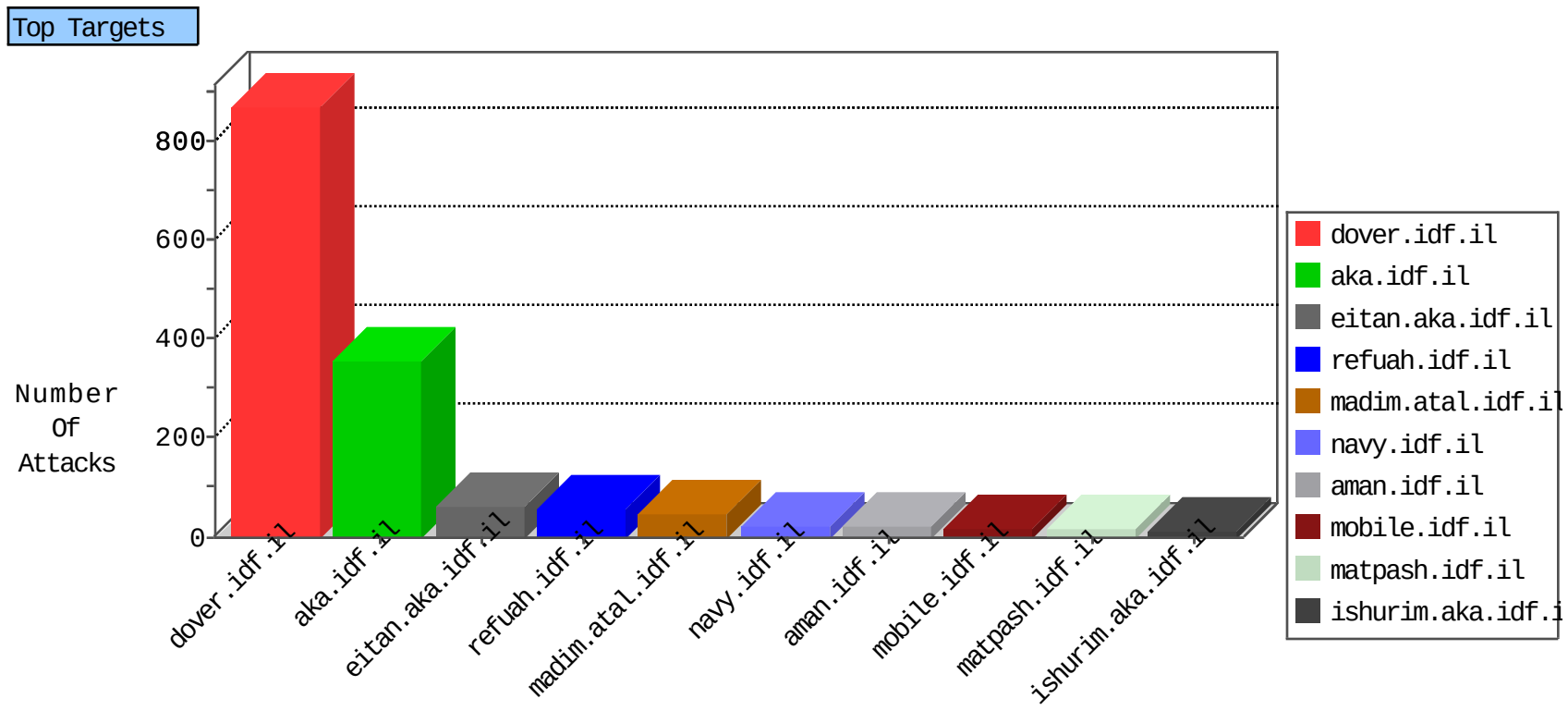
05-04-2016-17:04:08 to 05-04-2016-18:04:08

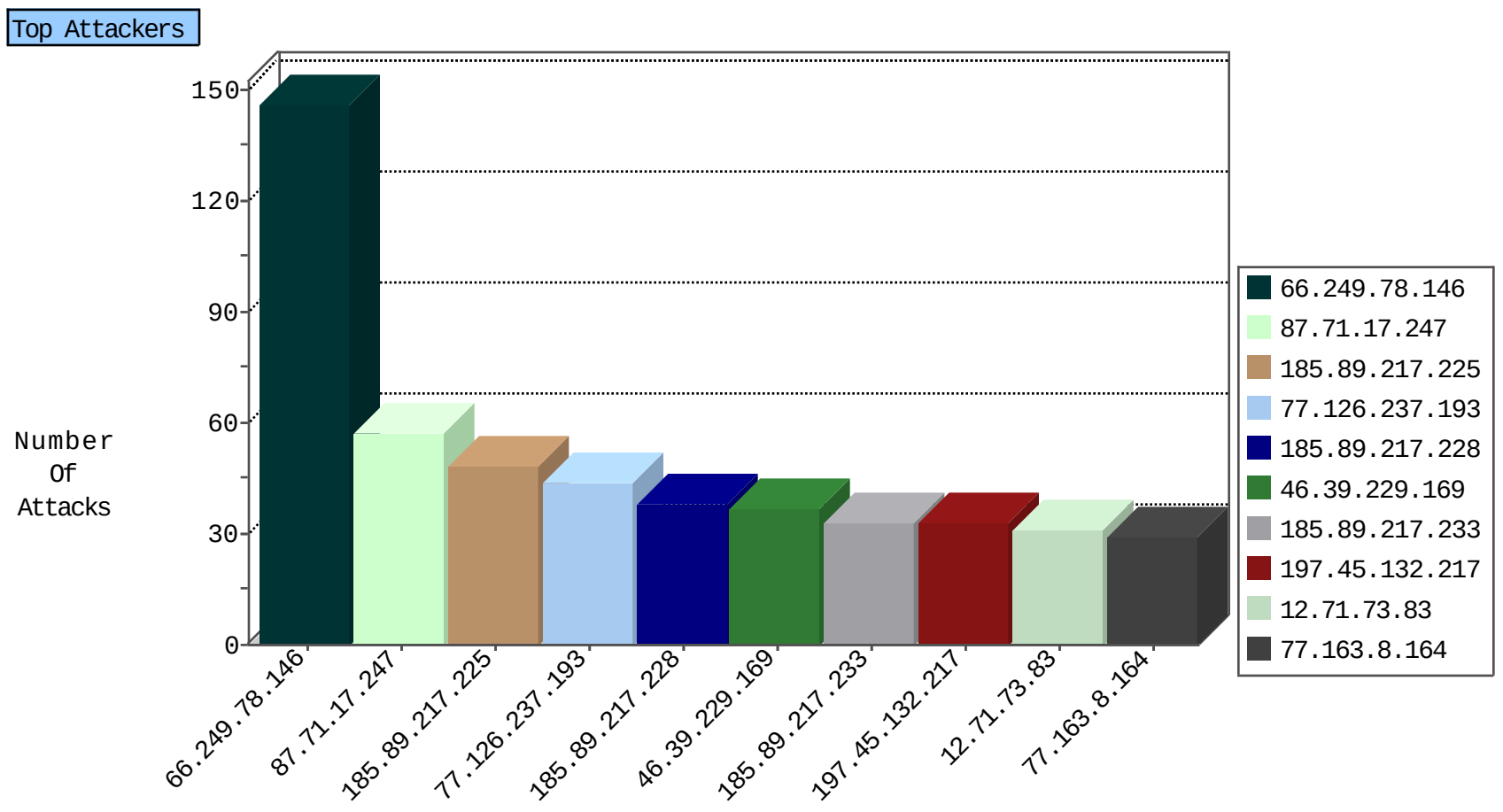
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

05-04-2016-17:04:08 to 05-04-2016-18:04:08

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	DOS-Tool-SwitchbladG	dest-reset	3
14.29.32.135	China	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	1
177.54.156.23	Brazil	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
185.118.222.1	Lebanon	147.237.0.16	my-kosher-kravi.idf.il	L4 Source or Dest Port Zero	drop	1

05-04-2016-17:04:08 to 05-04-2016-18:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-04-2016-17:04:08 to 05-04-2016-18:04:08

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	2
109.253.217.140	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.230.86.226	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.111.226.190	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.62.170	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.219.163.73	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.117.35.160	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
40.76.60.239	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -f -sS	1
2.53.188.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.2.119	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.219.238.10	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
85.64.102.16	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.111.190.20	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.64.190	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
62.219.141.85	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
40.76.60.239	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
13.82.55.149	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 3072	1

05-04-2016-17:04:08 to 05-04-2016-18:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
87.71.17.247	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
185.89.217.225	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
77.126.237.193	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	43
185.89.217.228	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
46.39.229.169	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
185.89.217.233	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
12.71.73.83	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
77.163.8.164	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
108.27.241.29	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
185.89.217.232	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
185.89.217.234	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
185.89.217.231	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
185.89.217.229	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
185.89.217.227	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
37.26.148.143	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
185.89.217.224	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
162.243.126.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
185.89.217.226	Netherlands	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
196.145.62.14	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.55.164.88	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
88.168.145.185	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
5.22.129.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.53.186.6	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.93.115	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
188.227.234.166	Palestinian Territory, Occupied	147.237.77.176	matpash.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
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.73.137	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.117.94.29	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.67	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.55.164.88	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
37.26.148.167	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.73.208	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.104	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.65.237.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.55.164.88	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.8.42.81	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

05-04-2016-17:04:08 to 05-04-2016-18:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.215.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
80.246.136.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
131.253.25.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
2.53.130.184	Israel	147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	4
2.53.130.184	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/1/	Block	3
2.53.172.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.186.6	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.12.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.8.42.81	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	2
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
131.253.25.253	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
149.78.123.151	United States	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.201.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.78.248	Block	1
46.19.86.102	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Illegal Byte Code Character in Header Name	Block	1
72.229.58.64	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.73.146	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/templates/sendtofriend/sendtofriend.aspx	Block	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	Distributed Abnormally Long Request	Block	1
46.19.85.23	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
89.139.131.156	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/smalim.aspx	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Malformed URL	Block	1
77.126.237.193	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.78.13	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Method	Block	1
46.19.85.24	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
89.139.131.156	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 10.100.102.4/upnpcp/notify/event	Block	1
66.249.66.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/3294.jpg	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Unknown HTTP Request Method) in URL	Block	1
77.237.138.202	Czech Republic	147.237.77.234	halag.idf.il	Unauthorized URL Access to /	Block	1
66.249.78.20	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	NULL Character in Method	Block	1
2.53.130.184	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 2.53.130.184	Block	1
94.159.168.80	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1810-he/	Block	1
66.249.93.184	Israel	147.237.72.166	aka.idf.il	URL is Above Root Directory www.aka.idf.il/../images/innerpage/right-side-shadow.gif	Block	1
66.249.69.7	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list20050529.htm	Block	1
5.22.129.121	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/69056.pdf	Block	1
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-9481-he/cogat.asp	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Abnormally Long Header Line request header name	Block	1
67.175.153.18	United States	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
66.249.73.137	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1361-he/dover.aspx	Block	1
185.27.105.101	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.157	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/smalim/html/13.asp	Block	1
5.102.216.7	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
85.64.229.221	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/general/mobile	Block	1

05-04-2016-17:04:08 to 05-04-2016-18:04:08