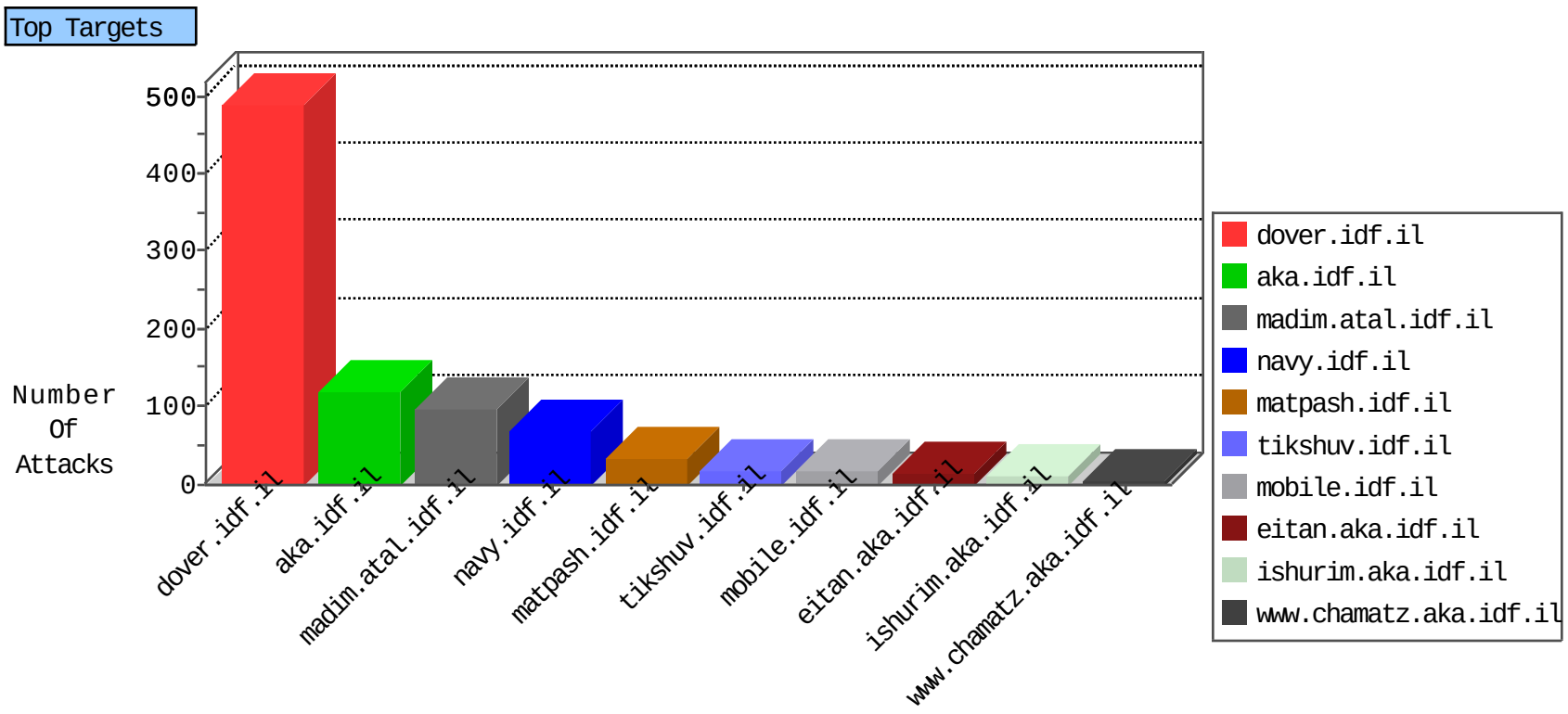
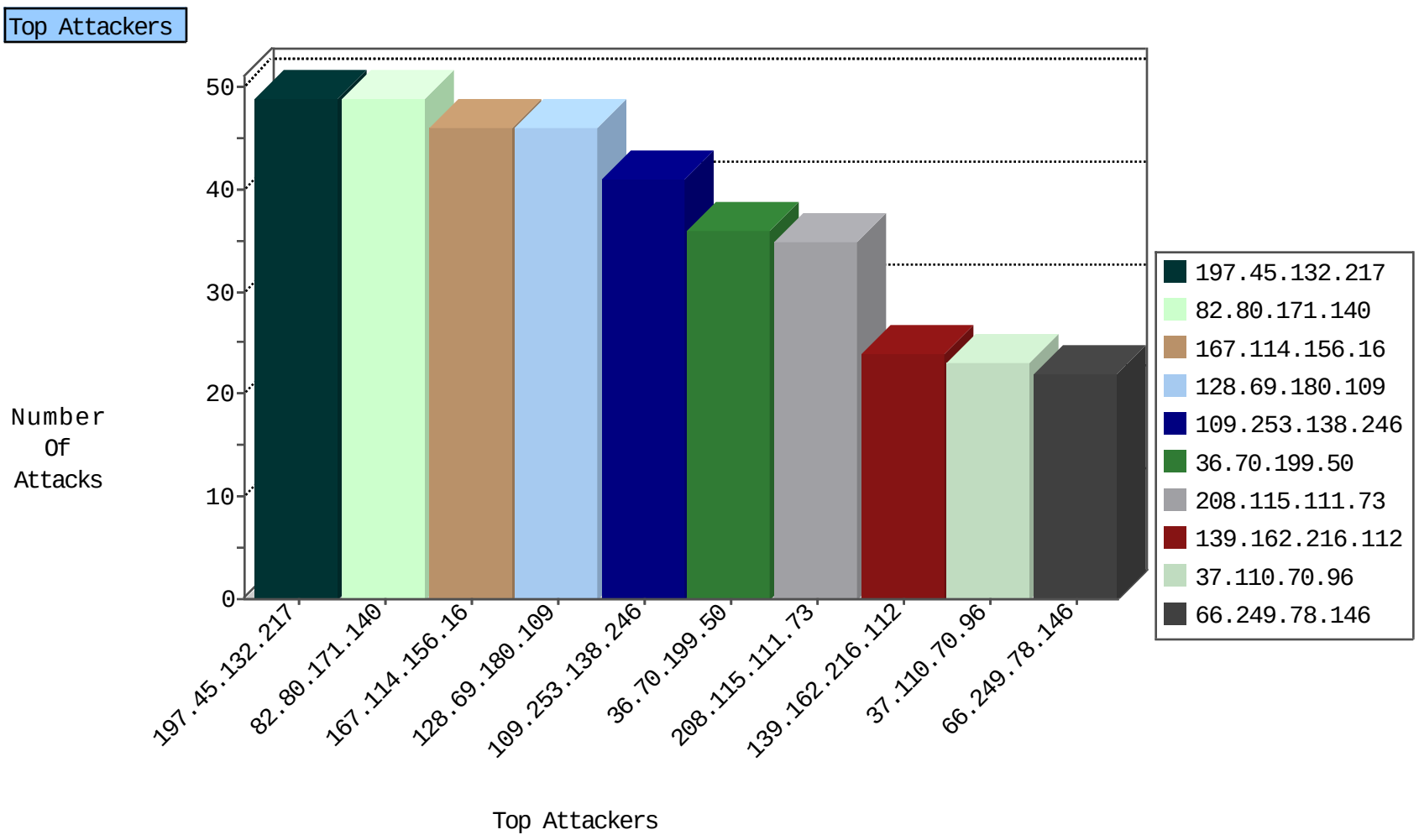
04-27-2016-08:04:02 to 04-27-2016-09:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-27-2016-08:04:02 to 04-27-2016-09:04:02

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	HTTP-POST-Segmented-DoS	dest-reset	2459
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1052
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
128.69.180.109	Russian Federation	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
185.103.252.96	Russian Federation	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
128.69.180.109	Russian Federation	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	1
204.42.253.2	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
123.59.59.52	China	147.237.77.234	halag.idf.il	block-sp-traf1	drop	1

04-27-2016-08:04:02 to 04-27-2016-09:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-27-2016-08:04:02 to 04-27-2016-09:04:02

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	4
109.253.207.188	147.237.77.216	Israel	dover.idf.il	INDICATOR-SCAN myscan	2
109.253.207.188	147.237.77.216	Israel	dover.idf.il	GPL SCAN myscan	2
183.60.48.25	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
163.172.140.23	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
63.221.141.195	147.237.76.197	United States	e.himush.idf.il	ET SCAN Potential SSH Scan	1
46.166.138.157	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
13.82.25.17	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
163.172.140.23	147.237.72.217	United Kingdom	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
114.215.150.44	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
46.166.190.204	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
13.82.25.17	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 4096	1
203.86.29.220	147.237.76.176	China	test.ncore.idf.il	ET SCAN NMAP -sS window 3072	1
187.22.126.154	147.237.0.33	Brazil	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

04-27-2016-08:04:02 to 04-27-2016-09:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
128.69.180.109	Russian Federation	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	42
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
36.70.199.50	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
37.110.70.96	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	23
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
54.72.0.55	Ireland	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	12
198.58.103.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
40.77.167.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
91.197.61.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.181.6.217	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
76.11.27.79	Canada	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
203.81.85.2	Myanmar	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
207.46.13.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
40.77.167.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.94	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.94	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.99.32.7	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.160.184.203	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.36.65.117	Oman	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.87.142.238	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
98.232.163.119	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.64.122.129	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
108.5.51.7	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.64.122.129	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.178.107.59	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	4
149.50.122.75	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.142.205.32	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
31.168.86.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.239.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.253.143.31	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.64.167	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.46.13.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
31.168.116.85	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-27-2016-08:04:02 to 04-27-2016-09:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.171.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
109.253.138.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
93.85.57.2	Belarus	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
79.181.1.231	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.181.1.231	Block	5
93.85.57.2	Belarus	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 93.85.57.2	Block	5
194.90.128.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.90.128.185	Block	4
77.126.142.239	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
185.24.233.175	Ireland	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 185.24.233.175	Block	2
149.88.213.64	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	2
79.181.1.231	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/3/	Block	2
185.32.179.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	2
71.60.180.200	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1407-he/atal.aspx	Block	1
66.249.66.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/mobile/	Block	1
157.55.39.27	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gius	Block	1
85.113.45.191	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/daily'a=0	Block	1
66.249.78.146	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
65.208.151.116	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/4/	Block	1
66.249.66.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/contactus/contactus.aspx	Block	1
88.86.99.166	Czech Republic	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in tikshuv.idf.il/site/general.aspx	Block	1
68.180.230.108	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1117-he/nakhal.aspx	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
149.50.122.75	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.50	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
5.39.222.159	Netherlands	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
185.24.233.175	Ireland	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/news/news.in.aspx	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	1
66.249.64.229	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/896	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/3249.jpg	Block	1
31.168.115.189	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
150.70.173.8	Japan	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1407-he/atal.aspx	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/5/2975.jpg	Block	1
51.255.65.49	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/doctrine/doctrine.stm"	Block	1
192.117.110.40	Israel	147.237.72.166	aka.idf.il	Unauthorized Method GET for www.aka.idf.il/iturim/asp/searchresults.asp	Block	1
93.85.57.2	Belarus	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1

04-27-2016-08:04:02 to 04-27-2016-09:04:02