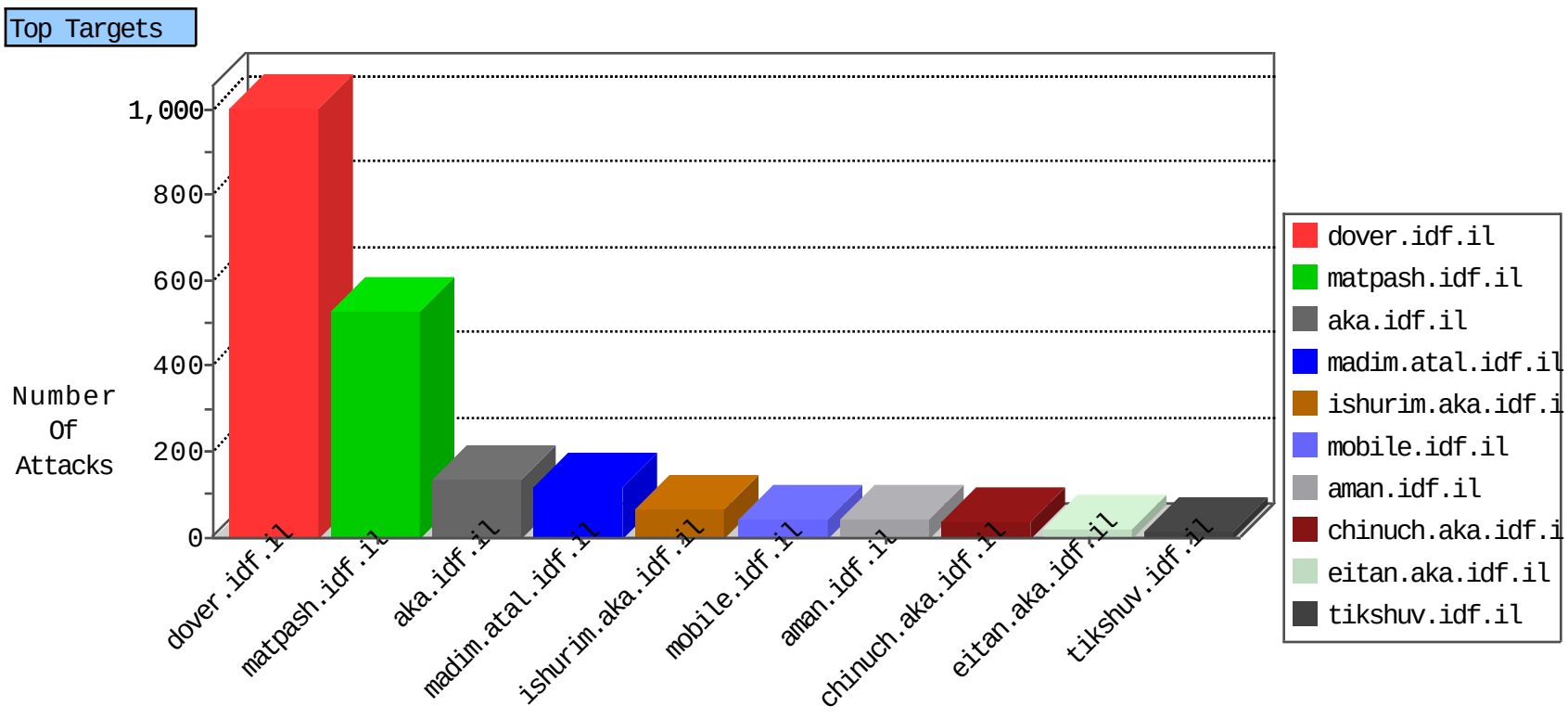
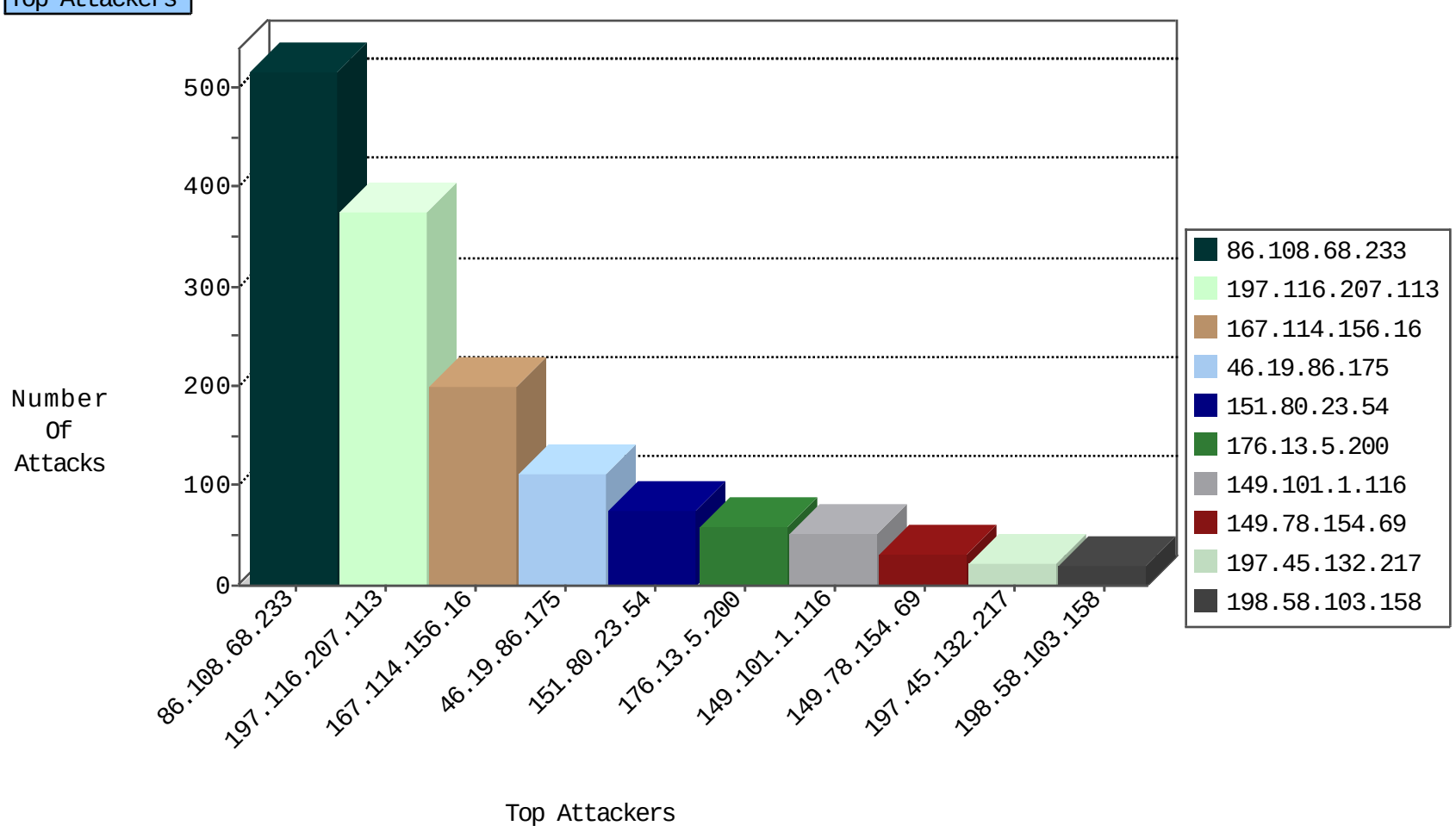
04-27-2016-23:04:09 to 04-28-2016-00:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-27-2016-23:04:09 to 04-28-2016-00:04:09

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	8724
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2167
197.116.207.113	Algeria	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	10
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
79.183.13.169	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
185.130.5.48	Lithuania	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.48	Lithuania	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
113.17.184.25	China	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.48	Lithuania	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
71.6.167.142	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
123.59.59.52	China	147.237.77.233	atal.idf.il	block-sp-traf1	drop	1
185.130.5.48	Lithuania	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1

04-27-2016-23:04:09 to 04-28-2016-00:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-27-2016-23:04:09 to 04-28-2016-00:04:09

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
193.227.34.78	147.237.76.202	Egypt	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
169.45.138.6	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
169.45.138.6	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
104.156.230.199	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.230.74	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
193.227.34.78	147.237.76.202	Egypt	e.halag.idf.il	ET SCAN NMAP -sS window 4096	1
169.45.138.6	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN Potential SSH Scan	1
169.45.138.6	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
107.158.255.194	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.79.104	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1

04-27-2016-23:04:09 to 04-28-2016-00:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
86.108.68.233	Jordan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	504
197.116.207.113	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	281
176.13.5.200	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
197.116.207.113	Algeria	147.237.77.216	dover.idf.il	drop		drop	46
149.101.1.116	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
151.80.23.54	France	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	39
151.80.23.54	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	36
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
198.58.103.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
197.116.207.113	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
166.137.10.52	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
37.26.146.229	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
208.115.113.89	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	12
31.154.165.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.99.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
178.39.157.212	Switzerland	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.103.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
86.108.68.233	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
213.57.185.89	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
197.116.207.113	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	9
46.19.86.175	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
113.95.44.143	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
113.95.44.143	China	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
79.178.201.67	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.26.148.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.94	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.159.169.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.66.184	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.175	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.76.106.9	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
40.77.167.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.177.16.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.111.80.2	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.46.13.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
185.32.179.179	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.102.242.214	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
82.69.27.238	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.121.196.141	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
31.38.188.103	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
178.39.157.212	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

04-27-2016-23:04:09 to 04-28-2016-00:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	85
109.65.208.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
213.57.185.89	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
5.248.253.133	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1556-en/	Block	3
93.172.159.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
131.253.25.190	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.53.163.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.175	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	2
106.38.241.106	China	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 106.38.241.106	Block	2
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/listpage/	Block	1
46.116.52.238	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1275-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.0.16	my-kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
113.95.44.143	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/usercontrols/headerupper/	Block	1
84.228.63.150	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 84.228.63.150	Block	1
207.46.13.15	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/yohalan/main/asp	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
141.212.122.161	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
17.142.156.171	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/apple-app-site-association	Block	1
106.38.241.106	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/main/giyus/giyus/general.aspx	Block	1
77.126.40.212	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.116.215.5	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
117.78.13.29	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/robots.txt	Block	1
5.29.11.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
84.228.63.150	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
66.249.64.243	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
149.78.195.125	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.46.38.107	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
109.65.0.22	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
79.178.201.67	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/960.css	Block	1
46.117.37.24	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
185.32.179.94	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
130.185.155.10	Sweden	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
5.29.179.244	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	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/9/2689.jpg	Block	1
153.129.11.252	Japan	147.237.72.166	aka.idf.il	Unknown Parameter amp;catId in www.aka.idf.il/rights/asp/info.asp	None	1
109.65.176.23	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1
80.179.109.2	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
46.120.156.131	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
194.187.168.220	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
130.185.155.10	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/resources/images/inservice.jpg	Block	1
157.55.39.128	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19149-he/dover...	Block	1
84.111.80.2	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
197.116.207.113	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
17.142.155.123	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/apple-app-site-association	Block	1

04-27-2016-23:04:09 to 04-28-2016-00:04:09