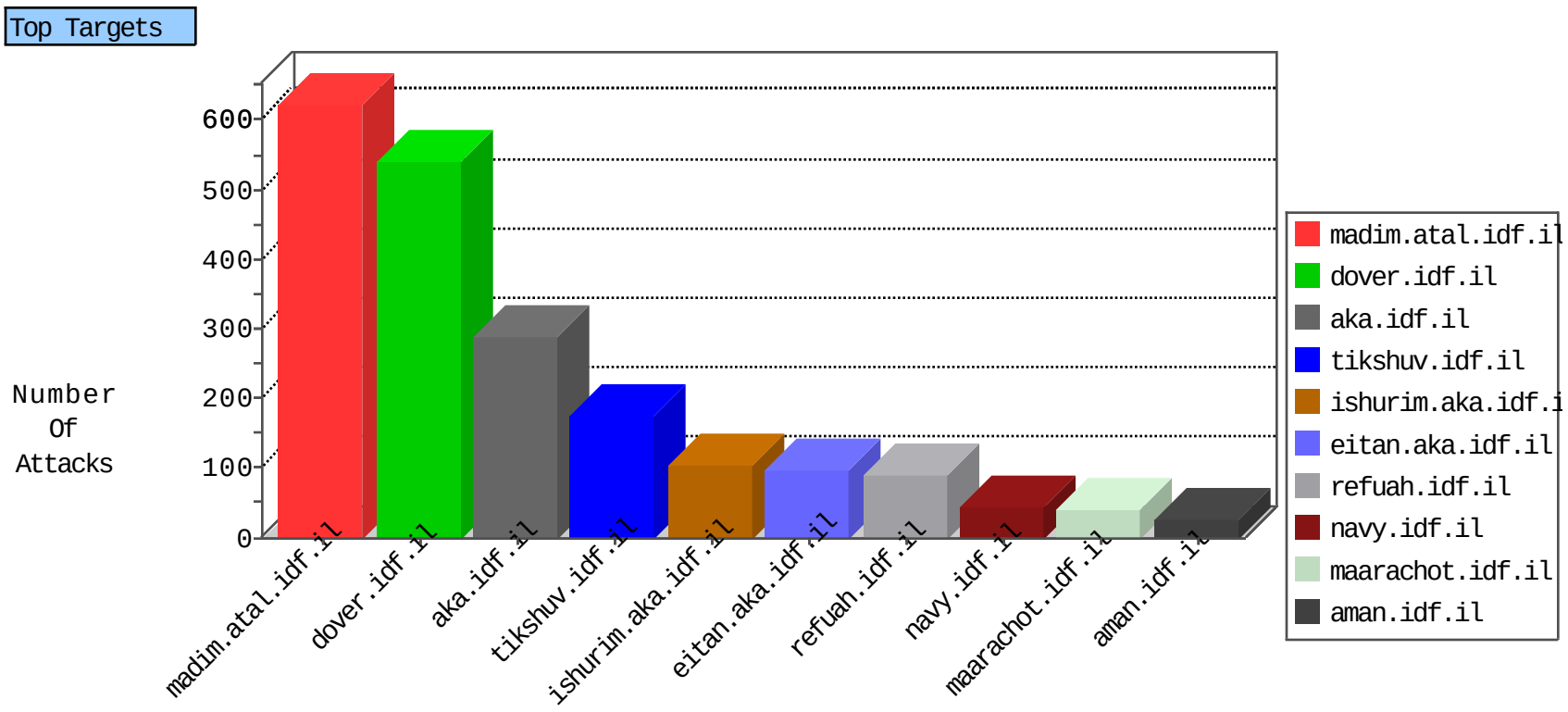
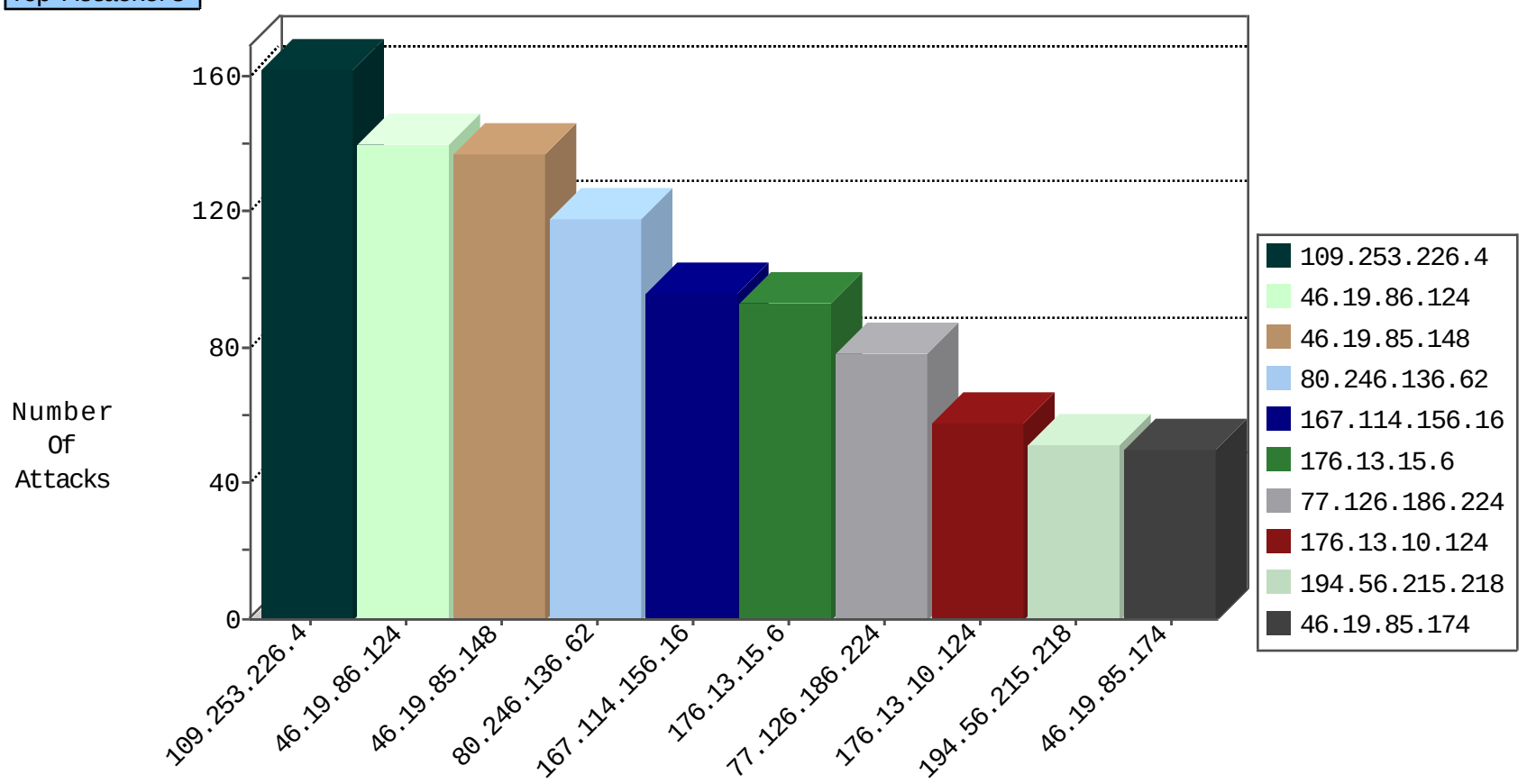
05-03-2016-12:04:05 to 05-03-2016-13:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



05-03-2016-12:04:05 to 05-03-2016-13:04:05

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	3068
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1399
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	166
109.65.30.6	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
81.218.56.245	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
81.218.56.245	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	3
204.42.253.130	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	2
204.42.253.130	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	2
204.42.253.130	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	2
37.26.146.151	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
204.42.253.130	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
66.240.236.119	United States	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	DOS-Tool-SwitchbladG	dest-reset	1

05-03-2016-12:04:05 to 05-03-2016-13:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-03-2016-12:04:05 to 05-03-2016-13:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
209.66.70.253	147.237.77.176	United States	matpash.idf.il	Tehila - Perl LWP with fake user agent	4
79.180.179.22	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	2
79.182.21.216	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.74.119	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.3.202.115	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
62.128.48.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.3.202.115	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.144	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.142.150	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.197	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.169.65.152	147.237.0.33	United Kingdom	idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potentia Scan or Infection	1
43.231.240.156	147.237.0.34	India	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
85.65.200.207	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.192.159	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.61.172	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.179.96.90	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.235.67.47	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.179.22	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	1
212.25.69.210	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.145.28	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
77.126.27.110	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.3.202.115	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
51.36.188.42	147.237.77.216	United Kingdom	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.140.23	147.237.76.148	United Kingdom	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 1024	1
46.19.86.59	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.140.235	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.170	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.69.11.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.141.195	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.103.119	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

05-03-2016-12:04:05 to 05-03-2016-13:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.253.226.4	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	162
77.126.186.224	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	78
194.56.215.218	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	50
176.13.10.124	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
37.237.184.143	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
136.0.99.167	United States	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	26
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
176.13.23.138	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
197.45.132.217	Egypt	147.237.77.216	dover.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
198.58.102.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
41.68.167.10	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
31.168.136.9	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
192.117.12.65	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
104.131.63.222	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.4.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.103.102	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
31.168.136.9	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
212.25.84.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
176.13.10.124	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
213.8.96.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
62.128.48.130	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
85.158.138.21	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.117.12.65	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.178.207.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.227	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.91.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	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
2.53.186.255	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.121.249.113	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.11.242	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.78.252	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
95.35.209.55	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.232	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.202.65.93	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
109.253.214.159	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.133.248	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.55.180.103	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.44	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
85.130.205.150	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

05-03-2016-12:04:05 to 05-03-2016-13:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.148	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	137
46.19.86.124	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	137
80.246.136.62	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	118
176.13.15.6	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	93
46.19.85.174	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	50
176.13.16.82	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	16
176.13.13.73	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	13
37.26.148.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
2.55.150.172	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
109.253.214.200	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
62.90.234.249	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/general/mobile	Block	5
46.19.85.141	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
84.95.211.153	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized HTTP Method	Block	4
81.218.251.251	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	4
81.218.251.251	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/resources/content/images/mainpage/	Block	4
178.137.83.178	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1556-en/	Block	4
109.253.192.204	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.124	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.119	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
194.114.146.227	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.114.146.227	Block	3
84.95.211.153	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/sip_storage/files/4/	Block	3
176.13.5.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
216.72.41.193	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/homepage/mobile	Block	3
216.72.41.193	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 216.72.41.193	Block	3
66.249.69.39	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/mas	Block	2
199.30.25.67	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
87.69.51.39	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
104.131.63.222	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 104.131.63.222	Block	2
109.253.223.238	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.11.242	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
31.168.136.9	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	NULL Character in URL	Block	1
77.124.46.195	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.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
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	1
197.77.205.1	South Africa	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/wp-login.php	Block	1
79.181.161.64	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized HTTP Method	Block	1
138.134.102.16	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1
216.72.41.193	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/general/mobile	Block	1
209.88.198.1	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	1
85.250.254.229	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
31.168.136.9	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
194.56.215.218	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
79.176.52.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Unknown HTTP Request Method â in URL	Block	1
213.8.204.46	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
84.95.211.153	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 84.95.211.153	Block	1
79.181.161.64	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/9/113339.pdf	Block	1

05-03-2016-12:04:05 to 05-03-2016-13:04:05