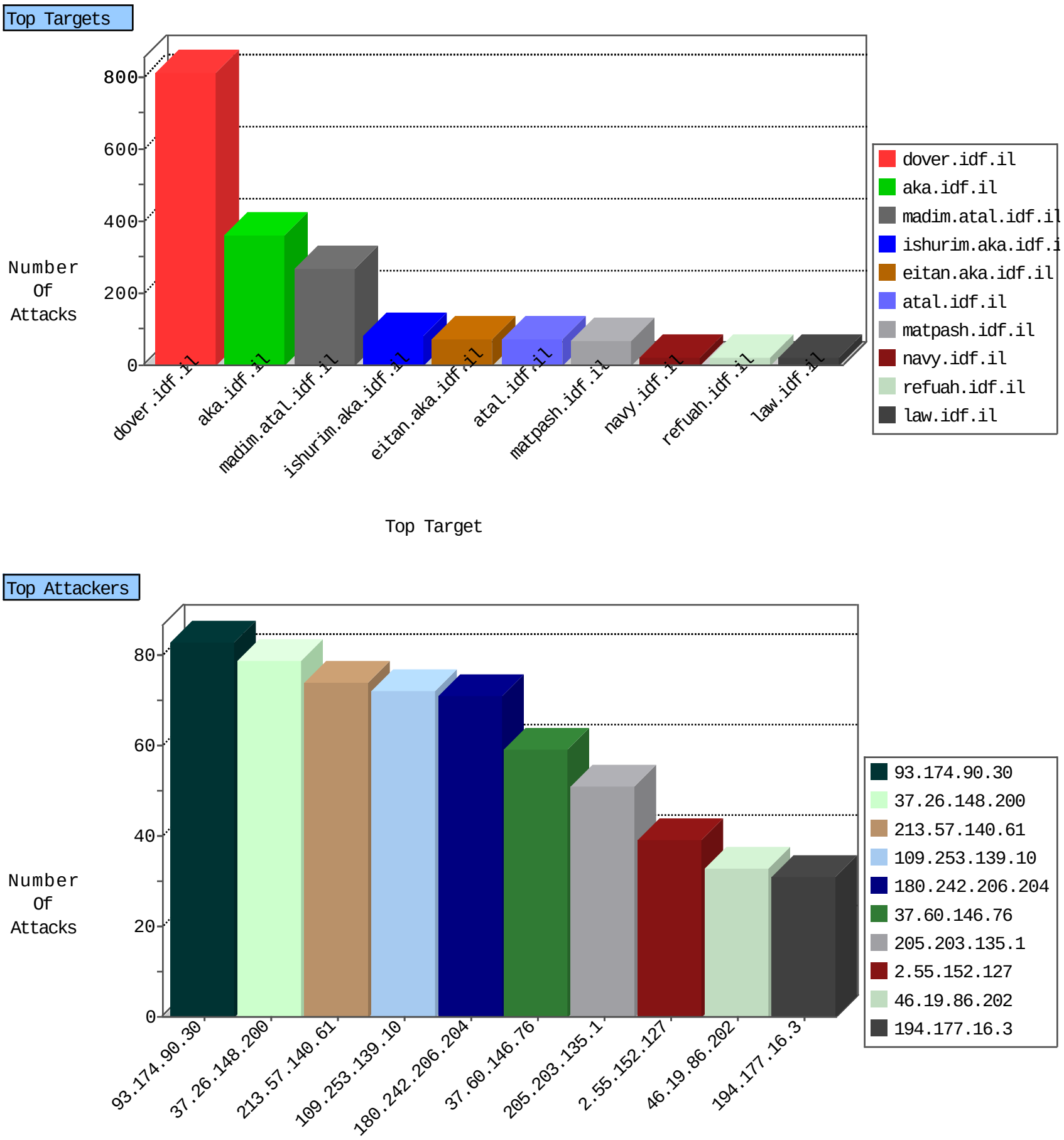
05-03-2016-10:04:07 to 05-03-2016-11:04:07

IDF Under Attack Daily Report



05-03-2016-10:04:07 to 05-03-2016-11:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	241
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	61
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
71.6.216.56	United States	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
24.78.101.185	Canada	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
94.102.52.10	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
45.32.79.225	Netherlands	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
71.6.216.43	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1

05-03-2016-10:04:07 to 05-03-2016-11:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-03-2016-10:04:07 to 05-03-2016-11:04:07

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
116.212.253.27	147.237.77.216	Australia	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.98.35	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.151.53.59	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.52.47	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.7.167	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.0.67.217	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.55	147.237.77.216	Ukraine	dover.idf.il	ET SCAN Potential SSH Scan	1
37.142.242.56	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.55	147.237.76.38	Ukraine	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
31.168.29.239	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.143.102	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.78.18.138	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.161.14	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
95.86.64.211	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.206.178	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
207.232.36.181	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.124.95	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.55	147.237.77.233	Ukraine	atal.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.121	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.55	147.237.76.42	Ukraine	refuah.idf.il	ET SCAN Potential SSH Scan	1
37.26.147.211	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.55	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN Potential SSH Scan	1
31.168.13.78	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.78.92.139	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1

05-03-2016-10:04:07 to 05-03-2016-11:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.148.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	79
93.174.90.30	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	79
180.242.206.204	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
37.60.146.76	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	59
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
194.177.16.3	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	31
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
185.99.32.7	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
95.86.102.48	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
37.26.148.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
81.218.251.252	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
66.249.93.79	Europe	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	21
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
54.72.0.55	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
2.53.158.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
66.249.93.74	Europe	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	16
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
62.219.137.44	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
109.253.139.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.85.139	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.104.237	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.26.148.175	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
66.249.93.115	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
62.219.254.97	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
62.210.143.245	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
58.222.232.198	China	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
62.16.73.143	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
37.26.148.197	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
199.203.215.1	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
199.203.215.1	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
176.13.3.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.253.156.6	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
81.218.251.250	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.93.87	Europe	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	8
37.26.148.247	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
171.76.105.158	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.246.139.60	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
2.55.190.188	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
66.249.69.93	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.139.10	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	72
213.57.140.61	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	54
2.55.152.127	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	39
46.19.86.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	33
81.218.203.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	16
89.139.169.168	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 89.139.169.168	Block	11
109.253.193.154	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
109.253.131.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
192.116.232.69	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	5
176.13.6.170	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
81.218.251.250	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	4
84.95.211.153	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized HTTP Method	Block	4
46.19.86.155	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
180.242.206.204	Indonesia	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 180.242.206.204	Block	3
109.253.224.96	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.53.151.105	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.53.182.137	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.64.12.183	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	2
37.26.147.200	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.23.51	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
171.76.105.158	India	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	2
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 208.115.113.82	Block	2
37.26.147.199	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
77.124.5.6	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
212.117.143.250	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	1
108.26.200.209	United States	147.237.76.200	eitan.aka.idf.il	Malformed URL	Block	1
88.198.44.46	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
192.114.105.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
149.78.106.62	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
109.64.12.183	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 109.64.12.183	Block	1
62.219.254.97	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
108.26.200.209	United States	147.237.76.200	eitan.aka.idf.il	Abnormally Long Request method	Block	1
37.26.147.199	Israel	147.237.0.19	madim.atal.idf.i	SSL Untraceable Connection - Open Mode	None	1
197.77.205.1	South Africa	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
176.13.15.72	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.95.211.153	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/sip_storage/files/4/	Block	1
77.158.88.40	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	1
108.26.200.209	United States	147.237.76.200	eitan.aka.idf.il	NULL Character in Header Name at [[#0]][[#0]][[#28]]À/À+À0À,À[[#19]]À#011À[[#20]]À	Block	1
149.88.195.82	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
66.249.69.124	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
108.26.200.209	United States	147.237.76.200	eitan.aka.idf.il	Illegal Byte Code Character in Header Name [[#0]]œ[[#0]]•[[#0]]/[[#0]]5À[[#18]][[#0]]	Block	1
84.108.62.107	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$cb14737250 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
77.158.88.41	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.253.139.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/def	Block	1
46.120.106.173	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/default.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
108.26.200.209	United States	147.237.76.200	eitan.aka.idf.il	NULL Character in Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]]C4U[[#12]]#012Ýªa $'ð-–…æá¨6šÊùè•J}Æ¿LÛHW	Block	1
89.139.169.168	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/general/mobile	Block	1

05-03-2016-10:04:07 to 05-03-2016-11:04:07