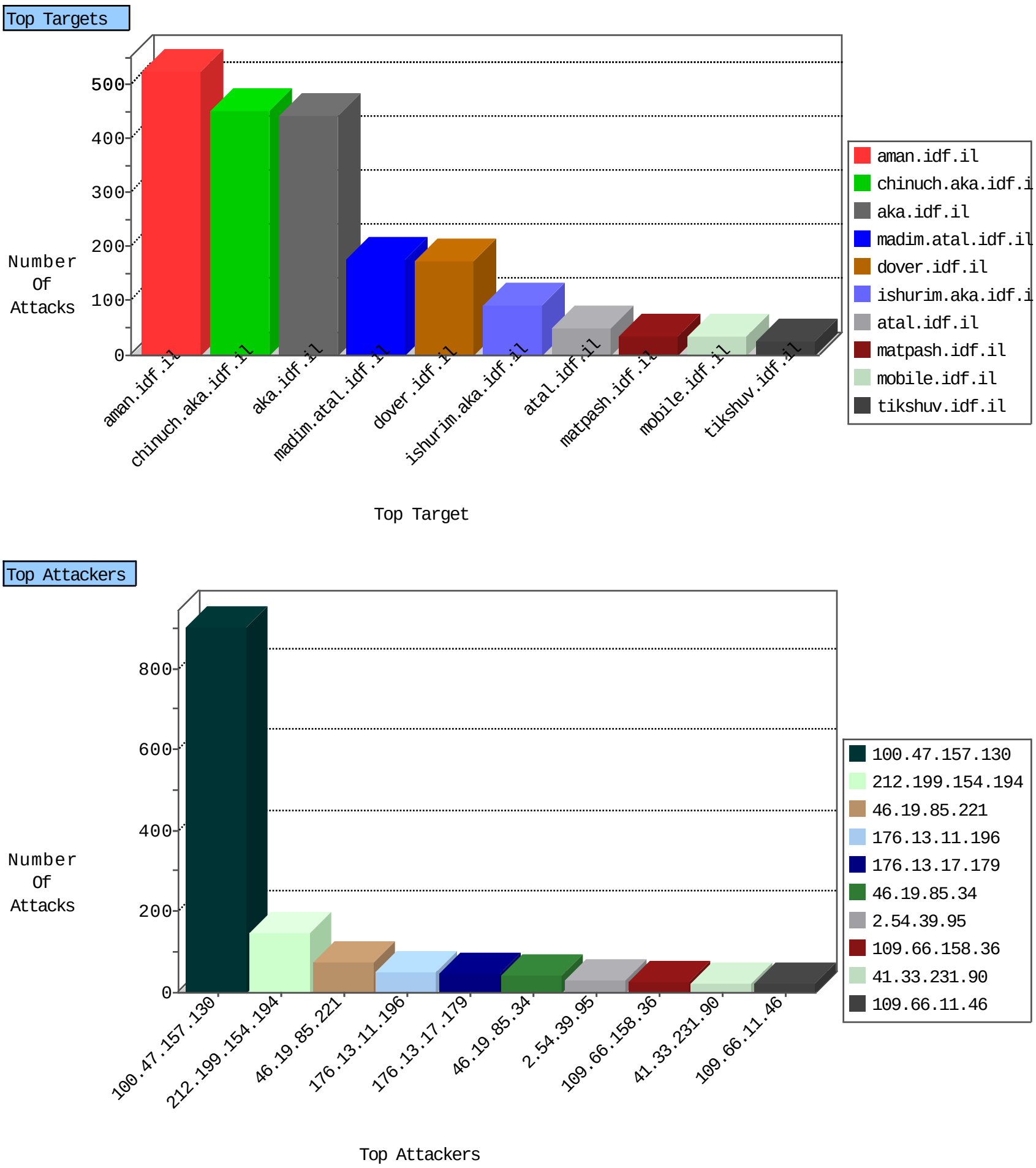
02-10-2016-14:04:05 to 02-10-2016-15:04:05

IDF Under Attack Daily Report



02-10-2016-14:04:05 to 02-10-2016-15:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.199.154.194	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	752
199.203.53.3	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
79.179.199.234	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
82.81.12.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
115.230.124.164	China	147.237.76.39	mobile.meitav.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
45.63.8.39		147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1

02-10-2016-14:04:05 to 02-10-2016-15:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-10-2016-14:04:05 to 02-10-2016-15:04:05

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	3
79.178.182.137	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.160.102	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.61.32.19	147.237.8.28	Russian Federation	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.114.146.227	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.84.245	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.228.216.141	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.139.11.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.111.30.88	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.179.33.148	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.42.153	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.61.32.19	147.237.8.46	Russian Federation	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
46.37.217.14	147.237.77.216	Ukraine	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.133.7	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.120.126.59	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.211.149	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.130.246.228	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.249.182	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-10-2016-14:04:05 to 02-10-2016-15:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
100.47.157.130	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	451
100.47.157.130	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	449
212.199.154.194	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	76
46.19.85.221	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	70
2.54.39.95	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
46.19.85.34	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
109.66.11.46	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
192.0.81.57	United States	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	19
176.13.1.180	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
31.168.88.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
81.218.70.243	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	11
147.236.34.10	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
79.181.119.54	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.240	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
82.166.184.137	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
31.210.186.84	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.54.164.191	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
2.54.174.198	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.180.141.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.252.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.3.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.214.155	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.155	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	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
46.116.83.165	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.14.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.1.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.117.137.115	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence		monitor	6
79.179.38.249	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.246.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.200.162	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
86.47.85.234	Ireland	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
188.120.154.82	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.98	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
50.18.94.121	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
80.246.139.225	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.52.9.132	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
209.88.198.1	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.0.80.167	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.183	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
87.68.144.123	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
149.78.204.185	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
193.202.110.189	Netherlands	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.34	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
37.26.149.237	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.63.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.19.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-10-2016-14:04:05 to 02-10-2016-15:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.11.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
176.13.17.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
109.66.158.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
109.253.221.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
85.65.77.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	15
176.13.15.207	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 176.13.15.207	Block	9
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	6
212.199.152.166	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on aka.idf.il/	Block	4
2.54.133.7	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	4
2.54.134.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.9.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.201.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
89.138.250.197	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 89.138.250.197	Block	3
109.253.219.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.12.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.145.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.156.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.181.1.147	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.34	Israel	147.237.77.216	dover.idf.il	Multiple Malformed URL from 46.19.85.34	Block	2
217.194.202.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.54.132.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.34	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.34	Block	2
85.65.44.215	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
46.19.85.34	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method 6,en;q=0.4 in URL	Block	1
207.46.13.177	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/size220x0/sip_storage	Block	1
79.172.211.136	Hungary	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-login.php	Block	1
128.232.110.28	United Kingdom	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
46.19.85.34	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
213.8.204.47	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
93.172.227.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
82.166.184.137	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
192.115.130.253	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/3/111843.pdf	Block	1
157.55.39.247	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/imagevideogallerylobby/imagevideogallerylobby.aspx	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
46.19.85.34	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
31.154.41.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sacar	Block	1
87.69.54.80	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
176.13.15.207	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m	Block	1
79.177.52.72	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$20 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.121.70.100	Israel	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	1
138.134.102.15	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
46.19.85.34	Israel	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 46.19.85.34	Block	1
213.8.204.47	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
95.86.77.185	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-21570-he/idfgdover.aspx&sa=u&ved=0ahukewjqomctmo3kahwlhhokhs_ga64qfggomai&usg=afqjcngkxkptobpol8pgxzxftd95sstiiw	Block	1
84.109.114.230	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
195.74.38.160	Sweden	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
167.114.229.242	Canada	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1

02-10-2016-14:04:05 to 02-10-2016-15:04:05