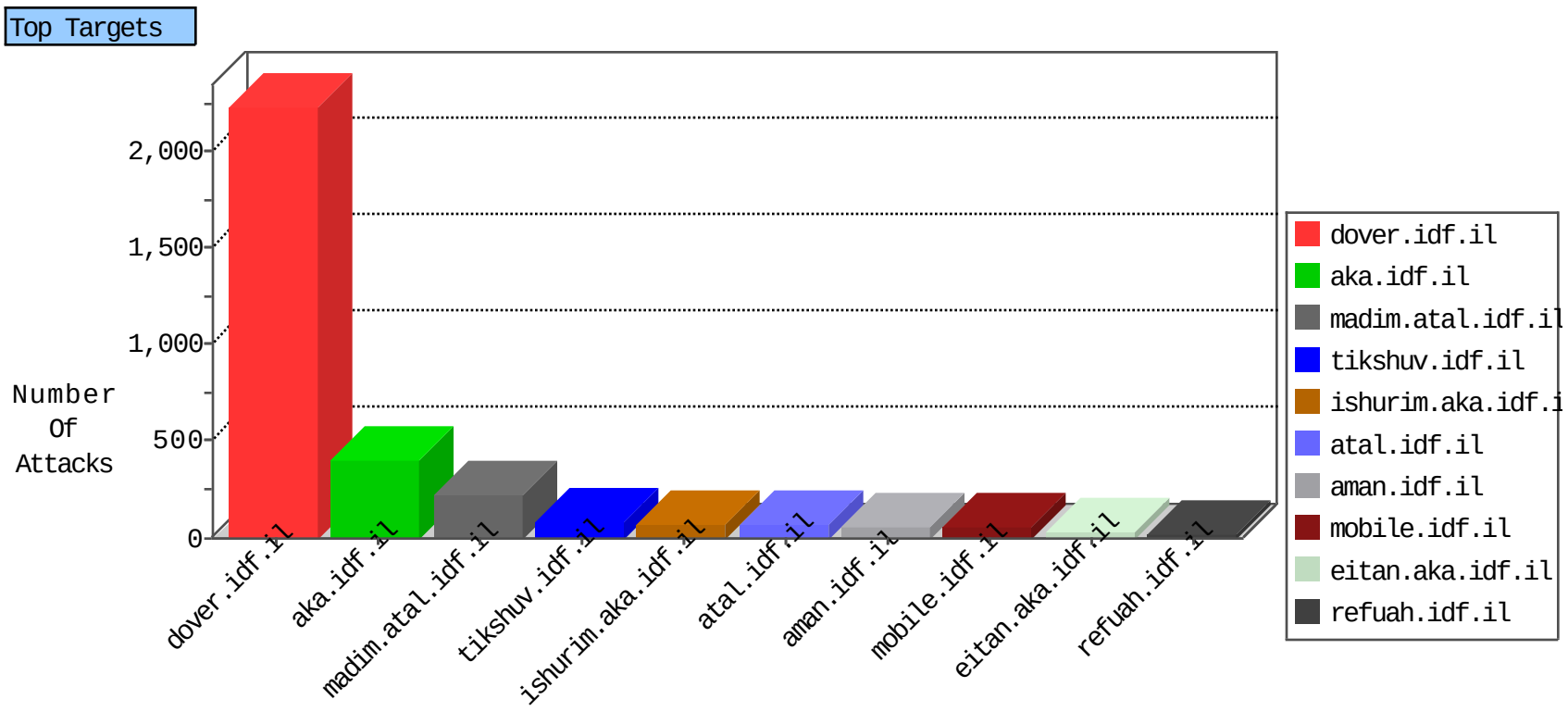
01-08-2016-10:04:07 to 01-08-2016-11:04:07

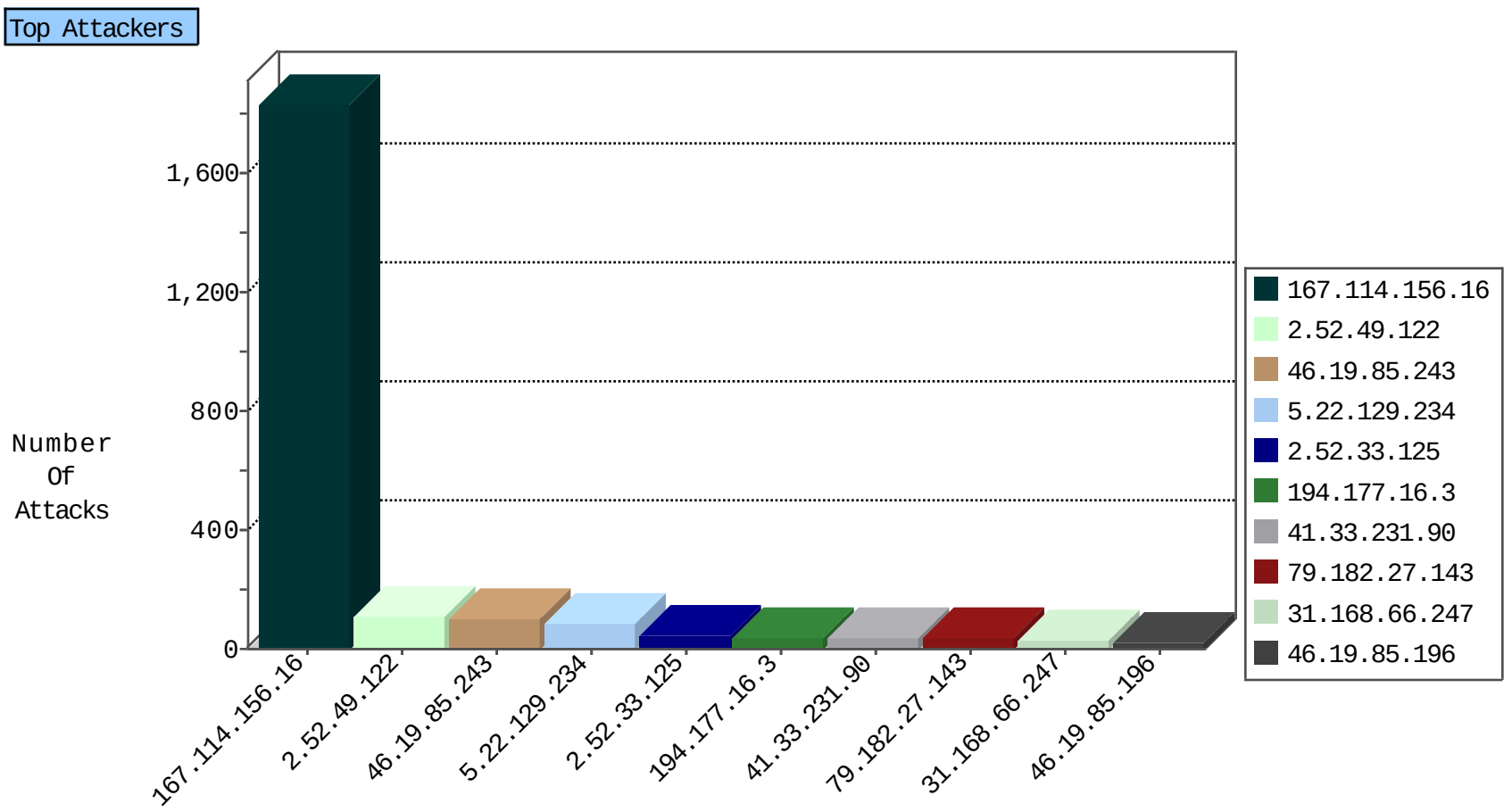
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-08-2016-10:04:07 to 01-08-2016-11:04:07

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	DOS-Tool-SwitchbladG	dest-reset	3036
5.22.129.234	Israel	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-RST	drop	5
31.168.66.247	Israel	147.237.0.19	madim.atal.idf.il	network flood IPv4 TCP-RST	drop	3
183.60.48.25	China	147.237.76.44	e.refuah.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
196.200.16.201	Kenya	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
109.65.29.32	Israel	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 TCP-RST	drop	1
180.97.106.36	China	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
46.19.86.194	Israel	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 TCP-RST	drop	1
196.200.16.202	Kenya	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
142.54.160.211	United States	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
10.0.0.17		147.237.72.166	aka.idf.il	network flood IPv4 TCP-RST	drop	1
77.125.127.21	Israel	147.237.72.156	aman.idf.il	network flood IPv4 TCP-RST	drop	1
2.54.10.76	Israel	147.237.72.166	aka.idf.il	network flood IPv4 TCP-RST	drop	1
196.200.16.203	Kenya	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
196.200.16.200	Kenya	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
107.150.55.213	United States	147.237.76.30	himush.idf.il	block-sp-traf1	drop	1
2.54.60.88	Israel	147.237.72.166	aka.idf.il	network flood IPv4 TCP-RST	drop	1
180.97.106.36	China	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
46.19.86.91	Israel	147.237.77.226	www.chamatz.aka.idf.il	network flood IPv4 TCP-RST	drop	1

01-08-2016-10:04:07 to 01-08-2016-11:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-08-2016-10:04:07 to 01-08-2016-11:04:07

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	4
66.249.93.107	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.249.69.34	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
91.231.192.149	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.248.146.42	147.237.76.31	Russian Federation	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.64.122	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN Potential SSH Scan	1
80.82.64.122	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
177.239.212.65	147.237.77.74	Mexico	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
121.201.27.61	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
5.102.253.64	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
121.201.27.61	147.237.0.15	China	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
109.65.193.158	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.172.33.89	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.65.73.84	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.82.64.122	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
217.132.32.163	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.82.64.122	147.237.0.33	Netherlands	idf.il	ET SCAN Potential SSH Scan	1
177.239.212.65	147.237.77.176	Mexico	matpash.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
77.126.91.205	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
173.199.74.136	147.237.8.46	United Kingdom	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
121.201.27.61	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
109.67.18.141	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.176.141	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

01-08-2016-10:04:07 to 01-08-2016-11:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.52.49.122	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	52
194.177.16.3	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	37
79.182.27.143	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
109.253.207.199	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
80.178.101.40	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	19
2.52.49.122	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
2.52.49.122	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
5.34.164.84	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	13
46.19.86.58	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
2.52.49.122	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	13
2.54.30.132	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.9	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.129.80	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
192.116.102.64	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
46.19.85.196	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.52.49.122	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	9
37.26.149.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
46.19.85.196	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
5.22.131.42	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
84.94.33.27	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
109.66.56.223	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.221	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
109.253.139.97	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
79.183.225.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
176.13.19.58	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.176	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.77	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.77	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.162.37	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
133.130.98.204	Japan	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.22.131.42	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.219.195.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.188.24	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.152.206	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
80.246.140.69	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
216.72.40.185	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.141	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.249	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
133.130.98.204	Japan	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
176.13.5.175	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
45.35.64.142		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.58	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.253.158.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.193	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.116.175.102	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5

01-08-2016-10:04:07 to 01-08-2016-11:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	90
5.22.129.234	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 5.22.129.234	Block	75
2.52.33.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
31.168.66.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
81.218.170.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
79.183.164.221	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	7
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	6
37.142.177.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.142.185.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.206.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.68.146.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.29.84.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.3.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.180.103.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.181.201.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.196	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
79.178.184.176	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 79.178.184.176	Block	2
84.108.90.87	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
192.243.55.129	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.129	Block	2
137.95.1.11	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 137.95.1.11	Block	2
46.19.85.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.109.215.167	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
62.219.195.78	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version [[#29]]mIyÂ³Ã¿^Ã‡Ã²Â¤Â™Ã‌[[#7]]eJÂŠÂ²Ã§Ã§XLÃ, Ã±fÃ?Â'7-	Block	1
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/getfile.aspx?filename=xgf5b3nolwrvy3ncdghpa2fcdhphdmltxdewodcuzg9j&infocenteritem=true	Block	1
157.55.39.27	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/captcha.ashx	Block	1
80.72.9.5	Sweden	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 80.72.9.5	Block	1
79.177.20.149	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
109.253.139.97	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.95	Block	1
204.85.191.30	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
2.54.162.37	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
89.139.236.184	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
62.219.195.78	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
192.243.55.129	Dominica	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	1
116.199.118.118	China	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
5.102.241.98	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/giyus/general.aspx	None	1
213.151.36.20	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
62.219.195.78	Israel	147.237.72.166	aka.idf.il	Malformed URL [[#29]]-Â³Â?	Block	1
192.243.55.136	Dominica	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	1
84.111.52.183	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.169	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.75	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.72.9.5	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1526	Block	1
109.253.192.247	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid\u003d59336 in www.aka.idf.il/main/giyus/general.aspx	None	1

01-08-2016-10:04:07 to 01-08-2016-11:04:07