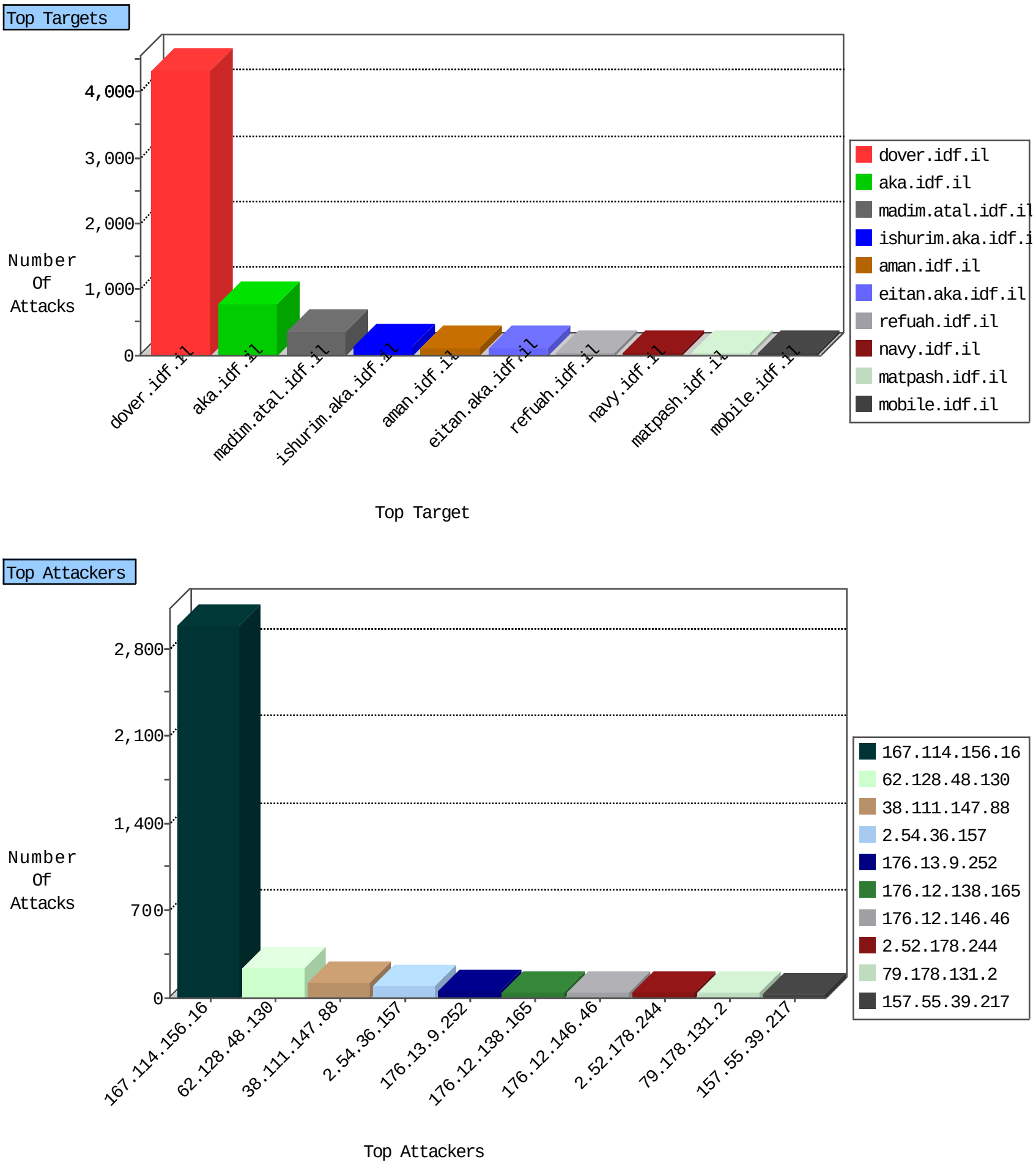
11-25-2015-11:04:03 to 11-25-2015-12:04:03

IDF Under Attack Daily Report



11-25-2015-11:04:03 to 11-25-2015-12:04:03

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	3078
66.249.66.97	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	370
81.218.5.130	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	21
82.145.219.134	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	8
176.13.16.180	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
46.158.35.236	Russian Federation	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
101.4.32.52	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
198.20.69.98	United States	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
104.192.0.226	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1

11-25-2015-11:04:03 to 11-25-2015-12:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
203.127.72.13	Singapore	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	8
212.235.62.200	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
188.165.15.99	France	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	1
194.114.146.227	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

11-25-2015-11:04:03 to 11-25-2015-12:04:03

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
132.72.55.86	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.250.81.22	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.193.236	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.181.56	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
104.243.16.122	147.237.8.14		e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.211.135	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.127.57.143	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.48.247	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

11-25-2015-11:04:03 to 11-25-2015-12:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	585
62.128.48.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	213
38.111.147.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	108
2.54.36.157	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	102
212.179.218.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
37.26.148.247	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
157.55.39.217	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
80.179.9.7	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
80.74.100.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
87.0.169.214	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
37.26.146.187	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
79.183.205.30	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	21
176.13.12.115	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
37.26.146.212	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
193.43.246.250	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
100.100.109.26		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
79.178.131.2	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
79.178.131.2	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	19
80.246.133.95	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.154	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
80.179.9.115	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
185.32.179.185	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
37.26.146.228	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
109.66.182.251	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
178.135.80.72	Lebanon	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
122.56.205.32	New Zealand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
62.128.48.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.252	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
212.179.71.70	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.252	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
2.52.178.244	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
46.19.85.154	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
176.12.145.185	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
66.249.81.218	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
193.43.245.250	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.86.119	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
173.252.88.244	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.13.94	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
66.249.81.218	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
77.125.101.231	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
185.32.179.185	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.5.201	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.86.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8

11-25-2015-11:04:03 to 11-25-2015-12:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.138.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	51
176.13.9.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	48
176.12.146.46	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	43
2.52.182.107	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
37.26.149.197	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	33
46.19.86.12	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	31
80.246.139.240	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
46.19.86.162	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
46.19.85.137	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
2.54.40.226	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
37.26.149.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
2.54.35.132	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
46.19.86.143	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.19.86.143	Block	5
109.64.5.53	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
109.65.181.59	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
80.246.136.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.137.85	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
185.32.179.173	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.124	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
38.111.147.88	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
2.54.170.213	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
203.127.72.13	Singapore	147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	2
93.173.226.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.108	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	2
46.19.86.143	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
46.19.86.45	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
80.246.137.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
68.180.229.173	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
196.29.104.35	Ghana	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
2.52.23.28	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.189	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
40.77.167.62	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.78.194	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/894-he/nakhal.aspx)	Block	1
37.26.147.190	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/halochamim	Block	1
46.19.86.84	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.111.36.20	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.19.85.239	Israel	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	1
5.175.193.232	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
62.219.163.146	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 62.219.163.146	Block	1
157.55.39.121	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/captcha.ashx	Block	1
46.19.85.14	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.126.102.100	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

11-25-2015-11:04:03 to 11-25-2015-12:04:03