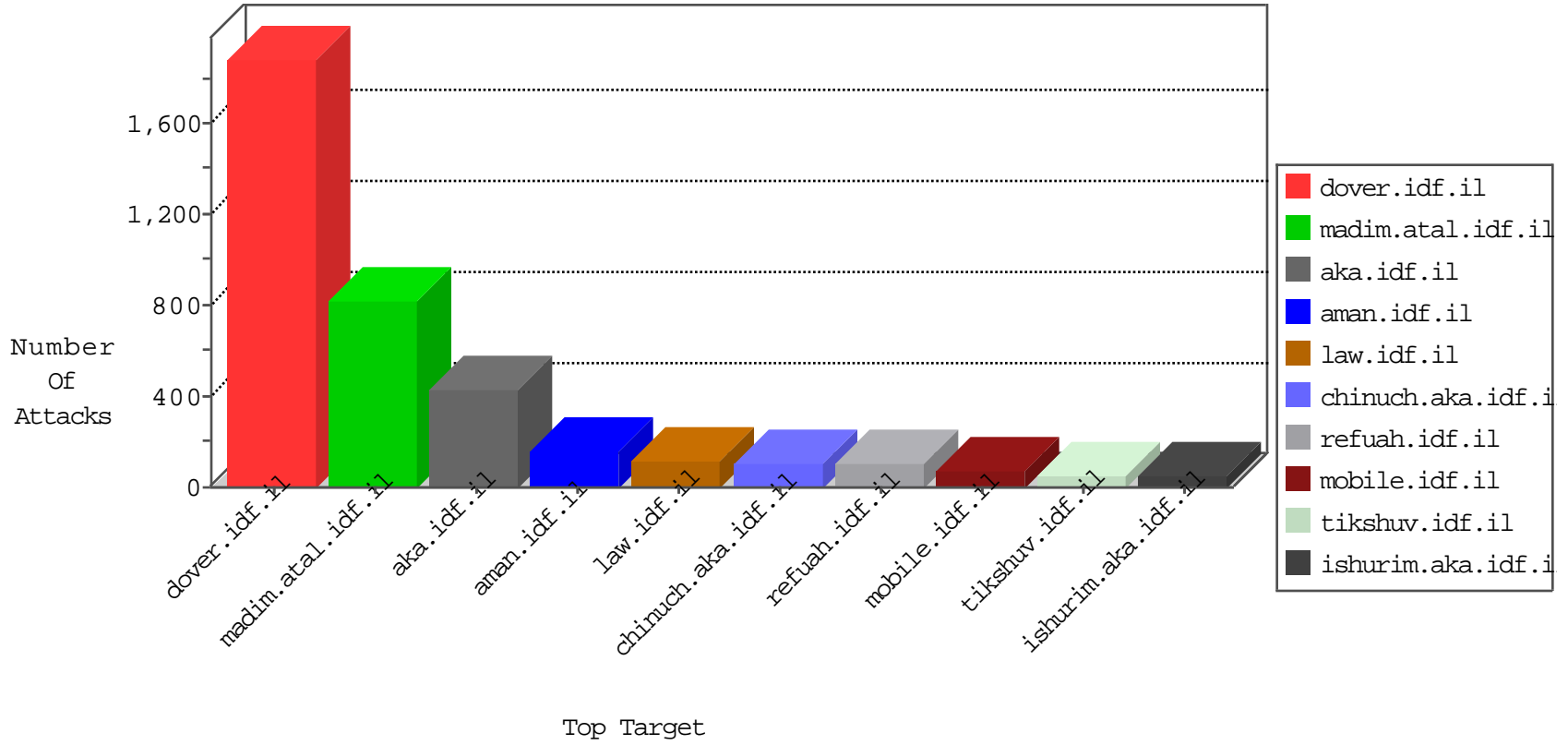


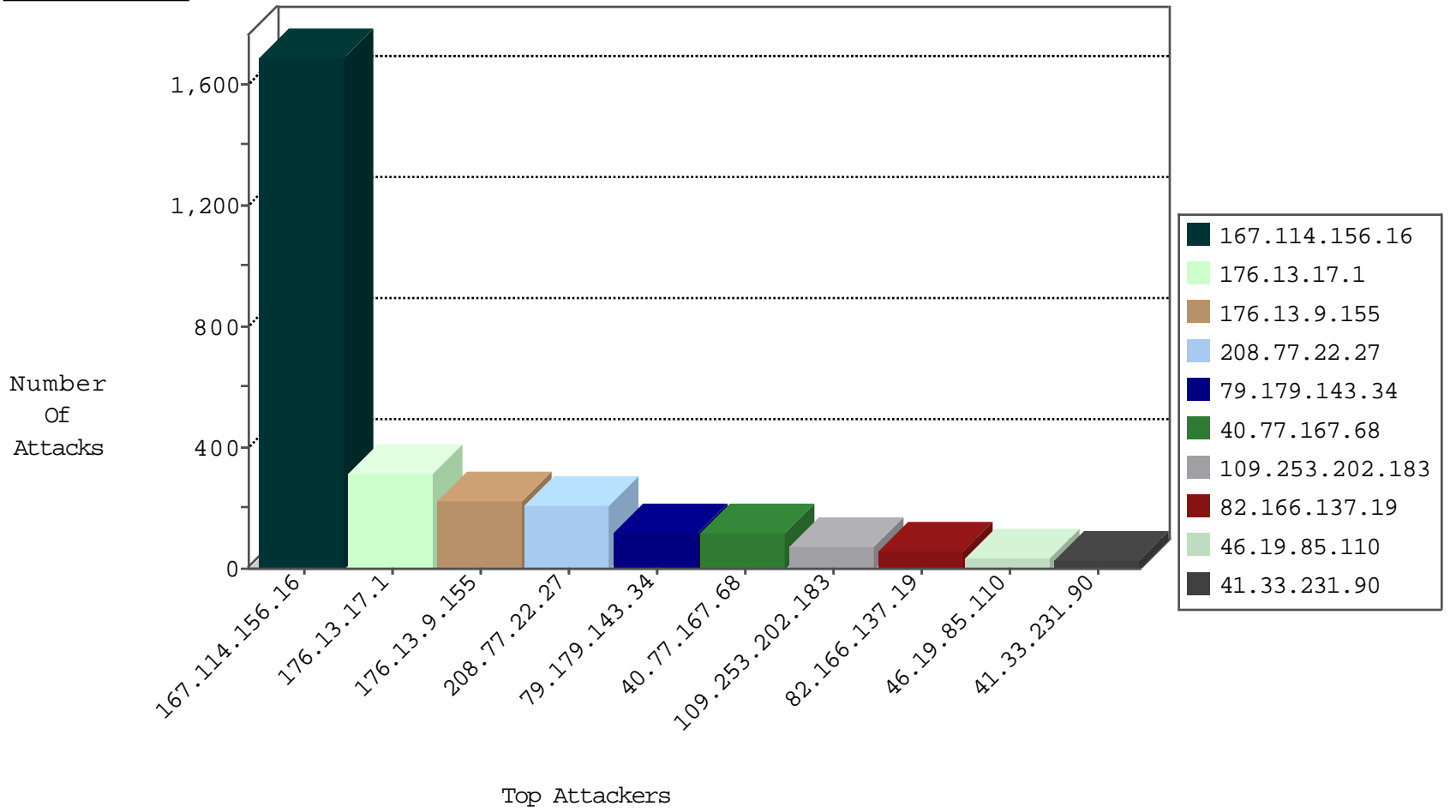
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	2592
82.166.137.19	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	522
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	87
85.130.251.227	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	6

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

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	1
176.13.19.77	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.105.72	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.135	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.95.121	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
220.231.195.122	147.237.8.45	China	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
185.3.146.199	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.137.189	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.176.19.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
23.251.49.125	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.42.156	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
40.77.167.68	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	109
208.77.22.27	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	100
208.77.22.27	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	85
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
2.54.155.142	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.86.77	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	20
208.77.22.27	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack		reject	18
185.120.126.25		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
109.253.136.244	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
80.246.130.153	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
46.19.86.44	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.86.67	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
79.177.212.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.121	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.110	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
149.78.43.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.110	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
109.186.27.174	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
132.66.30.157	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
46.19.86.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.148.214	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	8
185.120.125.32		147.237.72.156	aman.idf.il	drop	SAM rule	drop	8
40.77.167.68	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	7
192.114.23.210	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
37.26.148.214	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
212.179.21.194	Israel	147.237.8.27	e.madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.114.23.210	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.85.239	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
31.168.154.80	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.46	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.176.19.40	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.25	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.183.177.74	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.5	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.161.181	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.155.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.120.125.32		147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
46.19.85.249	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
82.81.14.58	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.25	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.59	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.21	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.176.155.178	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.110	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.159.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.17	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.121	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.102.224	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.17.1	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	155
176.13.9.155	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	126
176.13.17.1	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	115
176.13.9.155	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	98
79.179.143.34	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	86
109.253.202.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	71
176.13.17.1	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 176.13.17.1	Block	45
79.179.143.34	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	30
46.19.85.234	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	26
46.19.86.209	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	25
176.13.7.200	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	24
77.126.51.58	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
2.52.25.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
109.186.12.62	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.156.17	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.12.155.140	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.14.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.176.155.178	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	3
79.183.209.213	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.151	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.21	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.65.26.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
80.246.139.95	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.7.139	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
192.114.23.211	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.67.157.34	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	2
149.50.75.42	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	2
2.54.8.64	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
207.46.13.14	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/chamatz/klali/default.asp	None	1
46.19.85.90	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.220.222	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.158	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.176.227.65	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct113 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
192.240.174.105	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on refua.atal.idf.il/test/wp-admin/	Block	1
2.54.134.250	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
94.230.93.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
64.233.172.230	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/36546.pdf	Block	1
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/shared/home.png	Block	1
212.143.187.73	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
46.19.85.239	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
149.78.136.147	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.168.144.247	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
195.154.226.90	France	147.237.77.74	law.idf.il	Illegal HTTP Version HTTP/	Block	1
2.54.35.224	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
72.29.127.17	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on refua.atal.idf.il/wp/wp-admin/	Block	1
85.250.182.247	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
217.194.203.41	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.139.60	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1