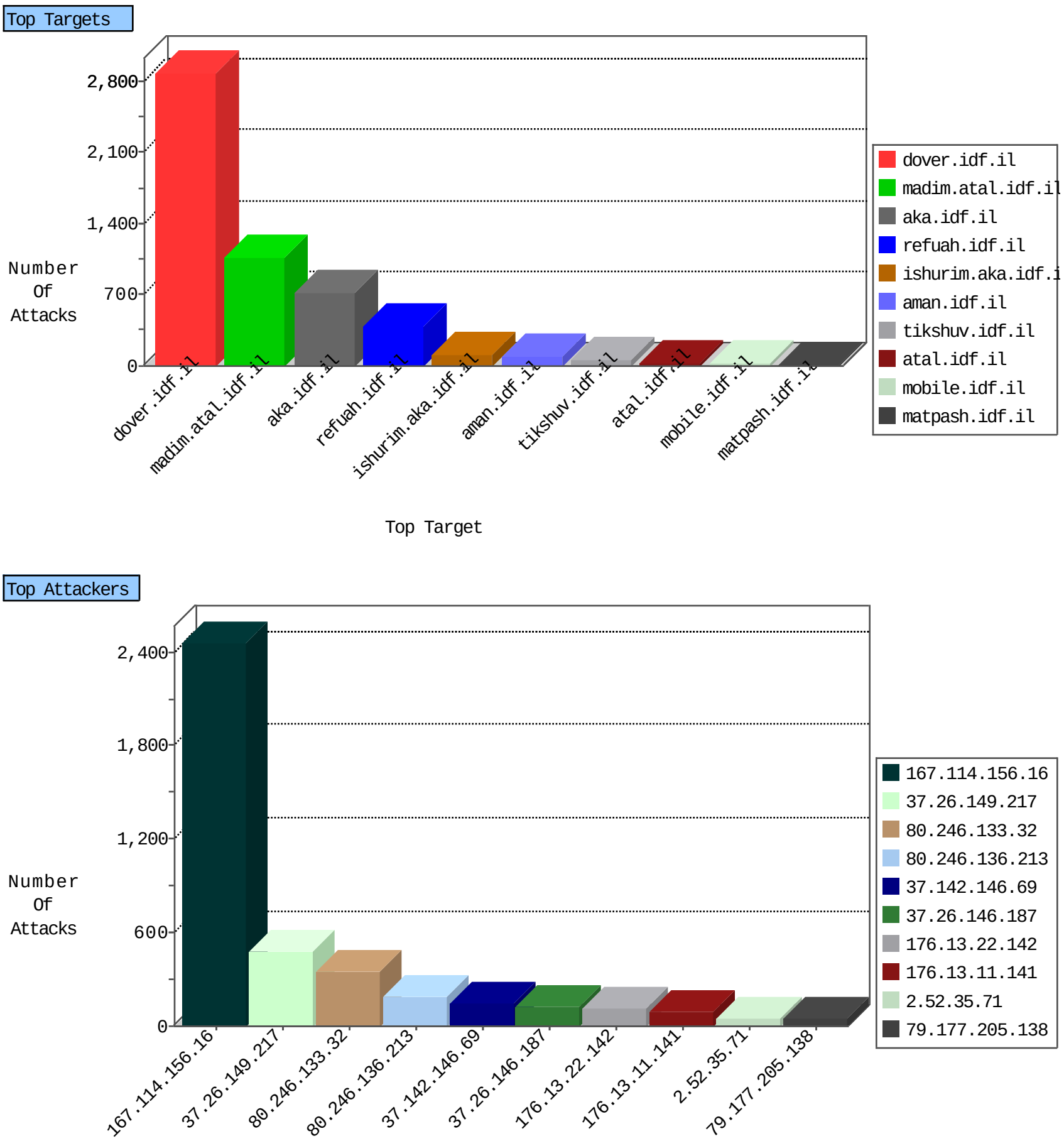
12-13-2015-12:04:03 to 12-13-2015-13:04:03

IDF Under Attack Daily Report



12-13-2015-12:04:03 to 12-13-2015-13:04:03

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	3441
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	84

12-13-2015-12:04:03 to 12-13-2015-13:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.120	Italy	147.237.76.200	eitan.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1

12-13-2015-12:04:03 to 12-13-2015-13:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.133.32	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
162.222.185.165	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential SSH Scan	1
96.22.224.103	147.237.72.14	Canada	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.76.198	Ukraine	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
84.95.86.191	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.147.23	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.117.174.114	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.177.148	147.237.72.166	Israel	aka.idf.il	ET WEB_SERVER Poison Null Byte	1
162.222.185.165	147.237.76.177	United States	ncore.idf.il	ET SCAN Potential SSH Scan	1
96.22.224.103	147.237.72.14	Canada	dover.idf.il(old)	ET SCAN NMAP -sS window 4096	1
95.86.66.129	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
88.249.106.23	147.237.76.196	Turkey	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.81.239	147.237.72.167	United States	ishurim.aka.idf.i	ET SCAN NMAP -sA (2)	1
46.19.85.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1

12-13-2015-12:04:03 to 12-13-2015-13:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.246.133.32	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	330
79.177.205.138	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	50
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
195.200.205.34	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	31
149.88.66.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
213.57.137.52	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	30
46.19.86.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
2.54.17.82	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
213.57.143.139	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	22
79.180.188.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
79.176.166.38	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
2.54.46.204	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
2.52.35.71	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack		reject	13
46.19.86.249	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	13
85.130.208.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.133.32	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
2.52.35.71	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	11
212.235.98.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	11
46.210.137.247	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
149.78.44.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
61.135.190.200	China	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	9
109.65.123.31	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
62.219.115.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
77.125.109.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.149.209	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
61.135.190.71	China	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	8
130.203.136.75	United States	147.237.77.74	law.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	8
185.112.102.222		147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.245	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.52.35.71	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	7
62.0.238.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.46	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
61.135.190.72	China	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	7
79.182.54.225	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.46.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.52.35.71	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence		monitor	7
2.52.35.71	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.54.46.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
79.180.168.34	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.69.243.141	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.2.87	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.12.30	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.168.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.137.52	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
2.54.15.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.178.187.155	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.219.137.44	Israel	147.237.72.166	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
37.26.149.217	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	293
37.26.146.187	Israel	147.237.72.166	aka.idf.il	Distributed Unknown HTTP Request Method	Block	122
80.246.136.213	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	113
176.13.22.142	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	112
37.26.149.217	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
37.142.146.69	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	99
37.26.149.217	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	82
80.246.136.213	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	74
176.13.11.141	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	73
37.142.146.69	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	48
176.13.11.141	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	18
185.32.179.79	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	16
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	15
37.26.147.203	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
37.26.149.192	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
176.13.4.193	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
46.19.85.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
2.54.169.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
93.173.10.204	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
37.26.148.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.12.122	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	3
176.13.23.86	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/tfasim.aspx.	Block	3
212.25.83.133	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	3
79.182.54.225	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	2
194.90.128.185	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	2
46.19.85.245	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.31.68	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.67.113.98	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/registrationwizard/undefined	Block	2
2.54.156.176	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
80.179.122.185	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/61998	Block	2
89.138.167.36	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.8.204.75	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
1.22.35.99	India	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
79.178.168.8	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.21.70	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.12.148.242	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.94.23.84	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.179.177.148	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL _Ö½×''[[#3]]Öµ@â€šÂ¦+sh8Ã¼u{Ãžâ€¦ÂŠÂ?,Ã–[[#25]]×•Ö·[[#30]]jrâ, ¬Â©g[[#27]][[#0]][[#22]][[#0]][[#4]][[#0]][[#5]][[#0]]	Block	1
66.249.66.31	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1
62.90.35.105	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
136.243.36.96	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 136.243.36.96	Block	1
5.29.139.90	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/giyus	Block	1
80.246.136.163	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
2.54.14.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.181.210.85	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.3.146.186	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.253	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1