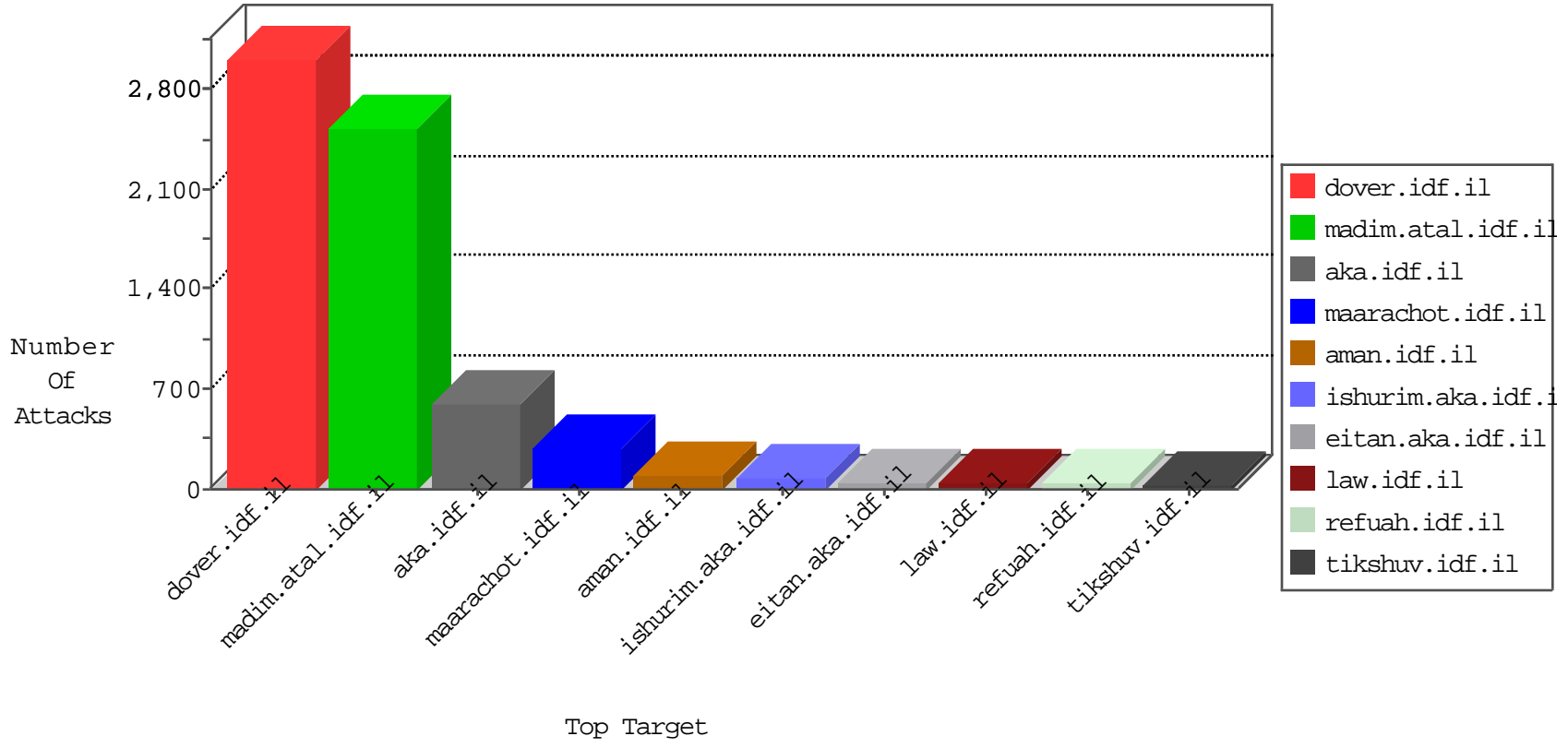


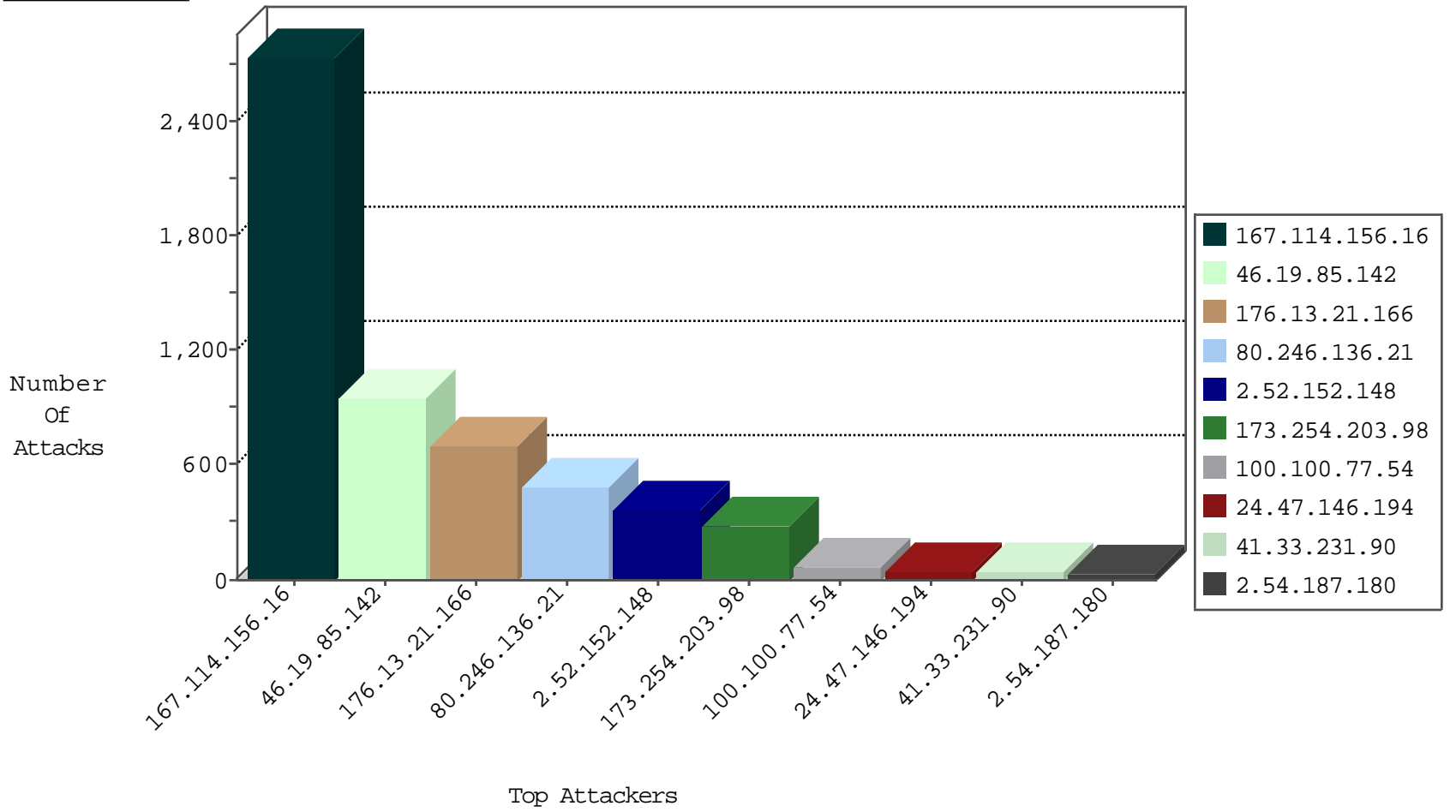
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.66.81	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3695
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3690
79.183.14.170	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
79.178.108.146	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
120.132.77.184	China	147.237.72.167	ishurim.aka.idf.il	block-sp-trafl	drop	1
31.168.171.81	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
93.174.93.151	Netherlands	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
120.132.77.184	China	147.237.72.156	aman.idf.il	block-sp-trafl	drop	1
120.132.77.184	China	147.237.72.166	aka.idf.il	block-sp-trafl	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
24.47.146.194	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
24.47.146.194	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
189.38.90.212	Brazil	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
24.47.146.194	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	26
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
91.201.236.113	147.237.72.14	Ukraine	dover.idf.il(old	ET DROP Spamhaus DROP Listed Traffic Inbound	1
80.246.136.21	147.237.0.19	Israel	madim.atal.idf.i	ET SCAN Possible SSL Brute Force attack or Site Crawl	1
50.204.188.142	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 4096	1
5.29.126.195	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.151.35.218	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
120.132.77.184	147.237.72.156	China	aman.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
94.242.239.40	147.237.77.216	Luxembourg	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.201.193	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.177.169.253	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.236.107.194	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
173.254.203.98	United States	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	285
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
5.29.119.254	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	32
199.203.196.245	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
100.100.77.54		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
100.100.47.100		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
100.100.90.168		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	20
100.100.77.54		147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	20
100.100.77.54		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
213.8.204.7	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
213.57.164.241	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
94.230.86.242	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
2.52.24.174	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.183.116.30	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.40.149		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
81.218.97.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.179.147.233	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
2.52.27.139	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
79.179.147.233	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
213.57.129.28	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
94.159.143.237	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
120.132.77.184	China	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	9
192.116.207.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
31.210.186.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
213.57.129.28	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
84.94.35.230	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.40	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
2.54.167.186	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	7
2.54.187.180	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
213.57.164.241	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
100.100.47.100		147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	7
5.102.254.176	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.46.39.101	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.187.180	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
188.165.250.173	France	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
2.54.187.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
185.3.144.152	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
213.57.164.241	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
2.54.187.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.187.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
93.173.134.225	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.30	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
100.100.104.89		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
199.203.147.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.177.248	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.30	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	615
176.13.21.166	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.21.166	Block	296
80.246.136.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	267
176.13.21.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	233
80.246.136.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	204
46.19.85.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	190
2.52.152.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	179
176.13.21.166	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 176.13.21.166	Block	163
46.19.85.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	149
2.52.152.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	114
2.52.152.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	70
37.26.148.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
80.246.136.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	13
81.218.97.114	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 81.218.97.114	Block	6
104.236.107.194		147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 104.236.107.194	Block	4
37.26.147.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.183.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.40.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.121.121.220	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
37.26.146.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
167.220.196.251	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	2
176.13.12.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.66.81	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.66.81	Block	2
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.66.61	Block	2
46.19.85.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.148.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.177.133.136	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/1/109241.pdf	Block	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
41.69.251.43	Egypt	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/xmlrpc.php	Block	1
94.159.149.93	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.154.91.227	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
84.110.109.27	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	1
66.249.66.75	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/giyus/general.aspx	None	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/size100x0/3467.jpg	Block	1
149.78.166.151	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.19	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
80.246.133.183	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
188.165.250.173	France	147.237.72.167	ishurim.aka.idf.il	MSSQL Data Retrieval with Implicit Conversion Errors	None	1
89.138.249.8	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.75.102	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/links.aspx	Block	1
66.249.66.31	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/idf_in_pictures/2002/april/	Block	1
176.12.149.33	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.108.34.55	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	1
2.52.0.31	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.248	Israel	147.237.0.19	madim.atal.idf.il	Multiple Untraceable SSL Sessions from 80.246.136.248 (Unknown SSL Session)	None	1
46.120.170.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.186.26.19	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.177.211.58	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.95	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/	Block	1