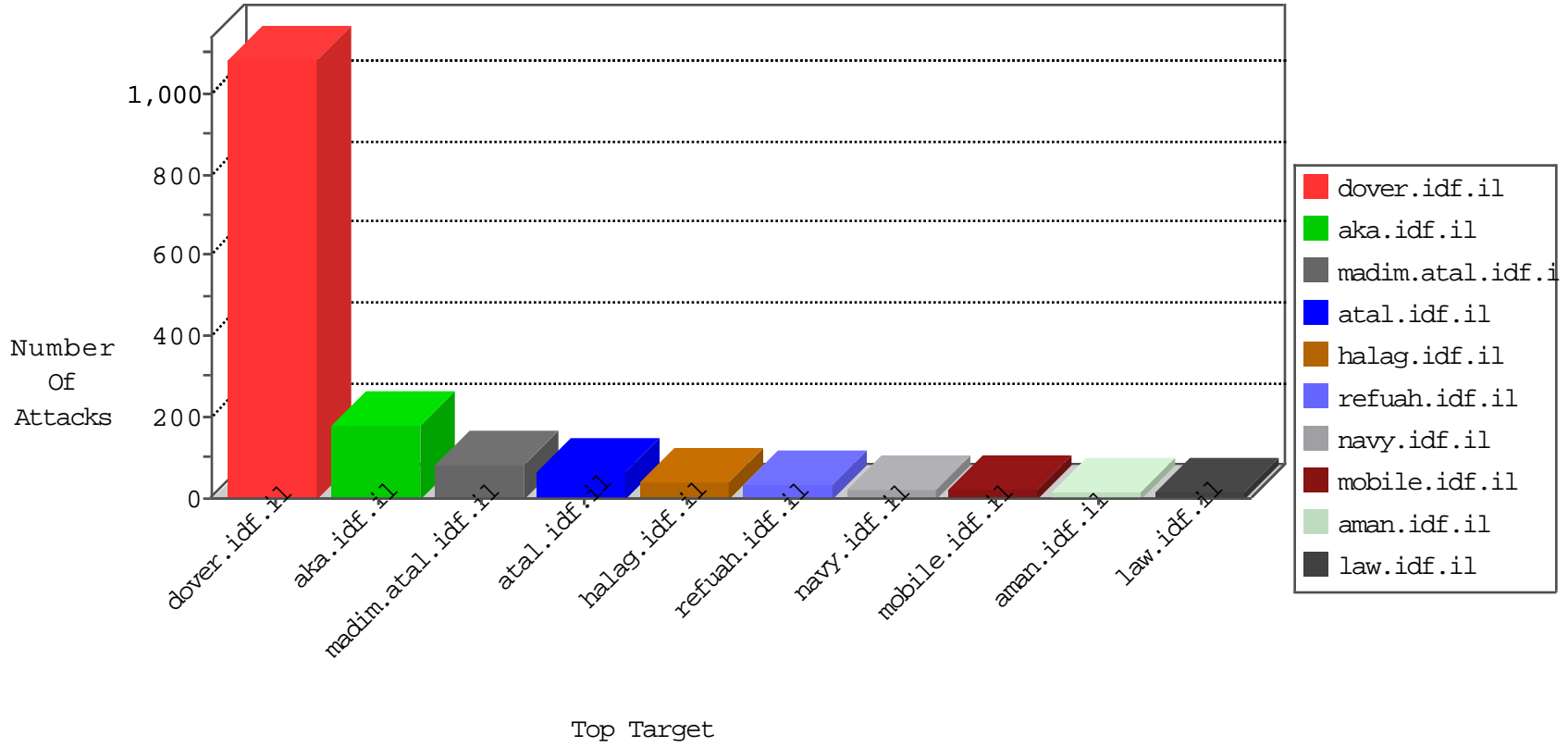




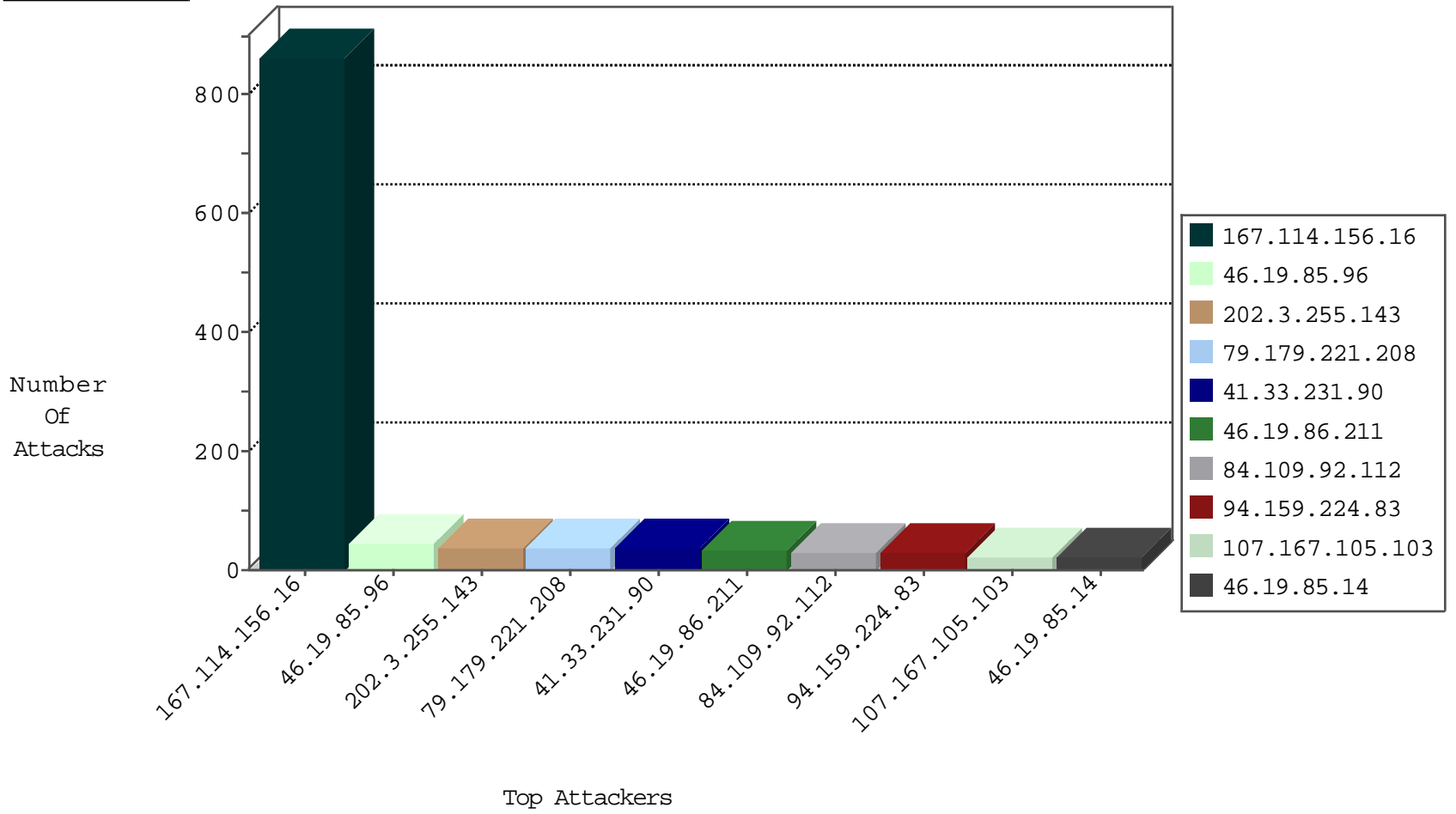
IDF Under Attack Daily Report



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	3000
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	2
74.91.28.58	United States	147.237.77.19	law-forum.idf.il	block-sp-traf1	drop	1
74.91.28.62	United States	147.237.72.166	aka.idf.il	block-sp-traf1	drop	1
185.130.5.224		147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
89.248.168.218	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
218.106.89.101	China	147.237.77.216	dover.idf.il	8479: HTTP: Suspicious HTTP Request	Block	2
60.173.236.84	China	147.237.77.216	dover.idf.il	8479: HTTP: Suspicious HTTP Request	Block	2
122.112.77.58	China	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
185.130.5.207		147.237.76.86	navy.idf.il	20085: HTTP: Mueblackcat Security Scanner Initial Request	Block	1
213.57.236.209	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

Top Attackers In IDS

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

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
84.109.92.112	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	29
107.167.105.103	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
79.179.221.208	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	18
79.179.221.208	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
46.19.85.14	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
94.159.224.83	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
94.159.224.83	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	13
79.181.133.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.28.177.21	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
79.181.29.116	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
87.69.32.107	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
87.69.32.107	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.211	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
46.19.86.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
51.39.165.250	United Kingdom	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
79.179.50.231	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.133.180	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
77.125.142.166	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.211	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
217.132.135.246	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.76	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
217.132.135.246	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.55.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.19.9	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.228.19.9	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
109.160.132.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
91.200.12.136	Ukraine	147.237.76.31	nakhchal.idf.il	drop	SAM rule	drop	4
79.176.217.117	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
217.69.133.226	Russian Federation	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
5.29.47.94	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
130.203.136.75	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
195.146.61.4	Iran, Islamic Republic of	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
91.200.12.136	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
37.46.39.13	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.64.146.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.154.156.117	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.211	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
109.64.198.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.164.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.200.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.211	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.126.69.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.119.76	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
176.13.1.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
109.64.166.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	6
2.54.173.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
178.137.85.67	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 178.137.85.67	Block	3
109.253.146.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.187.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.228.19.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.181.29.116	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
46.19.85.54	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.179.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
217.132.135.246	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.176.53.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
144.76.182.149	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 144.76.182.149	Block	2
178.137.85.67	Ukraine	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
74.82.47.4	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
46.19.86.64	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.66.119.76	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.146.226	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
84.109.92.112	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
79.180.35.48	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1
188.138.1.218	Germany	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
144.76.182.149	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1158-he/404.aspx	Block	1
107.178.194.87	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	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31/	Block	1
2.52.145.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/eitan/kishurim/	Block	1
81.220.95.14	France	147.237.77.74	law.idf.il	PHP Attempt	Block	1
77.125.142.166	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.105.60.176	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
109.228.113.106		147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
37.142.64.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
195.146.61.5	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
157.55.39.98	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/58457.pd	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp/docid in www.aka.idf.il/main/gyus/general.aspx	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.19.85.14	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
217.132.123.12	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyus/controls/atuda/Å	Block	1
81.220.95.14	France	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
178.137.85.67	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
77.127.196.170	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
46.117.237.195	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.228.113.106		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
87.69.32.107	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.190.206	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.181.201.219	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.102	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/61998	Block	1