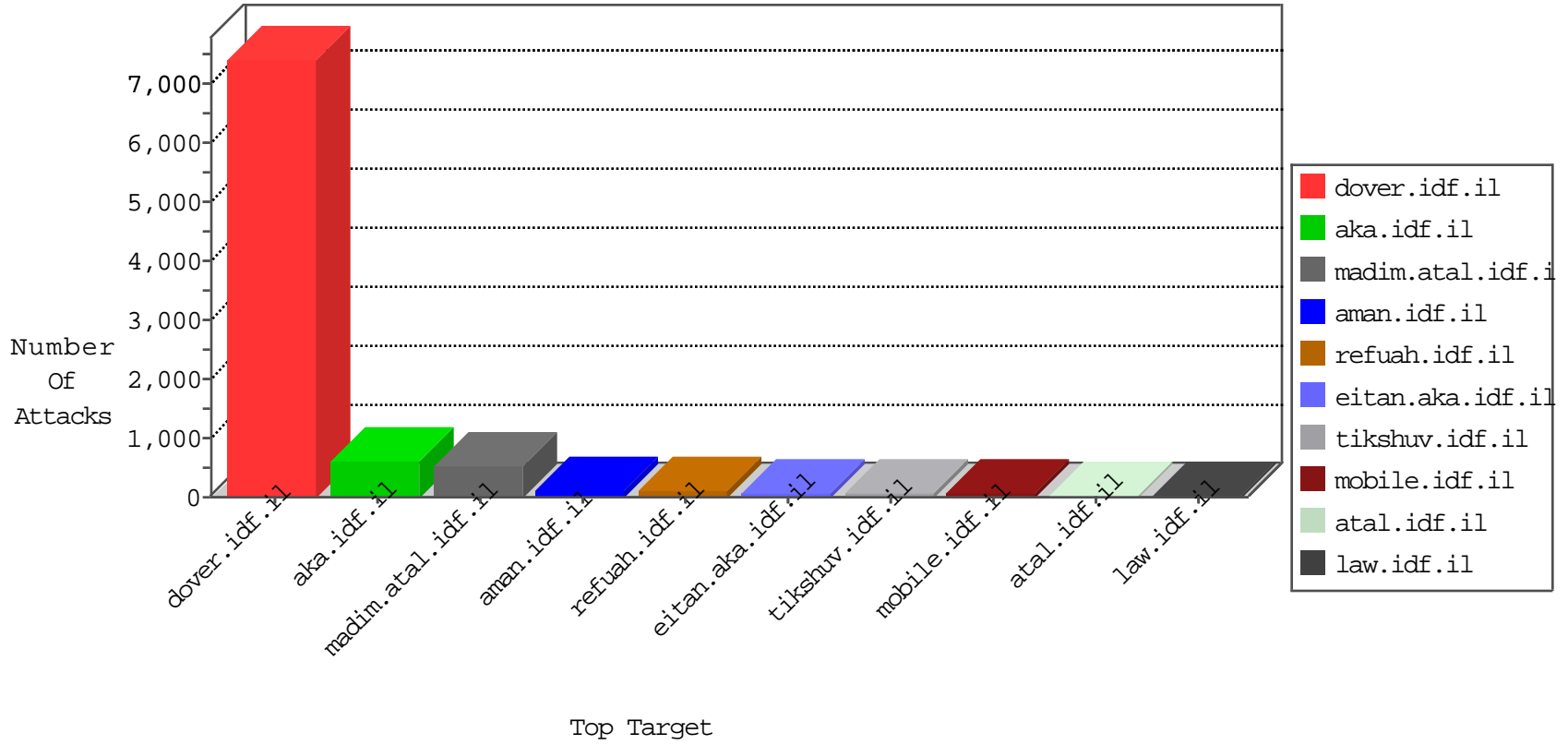


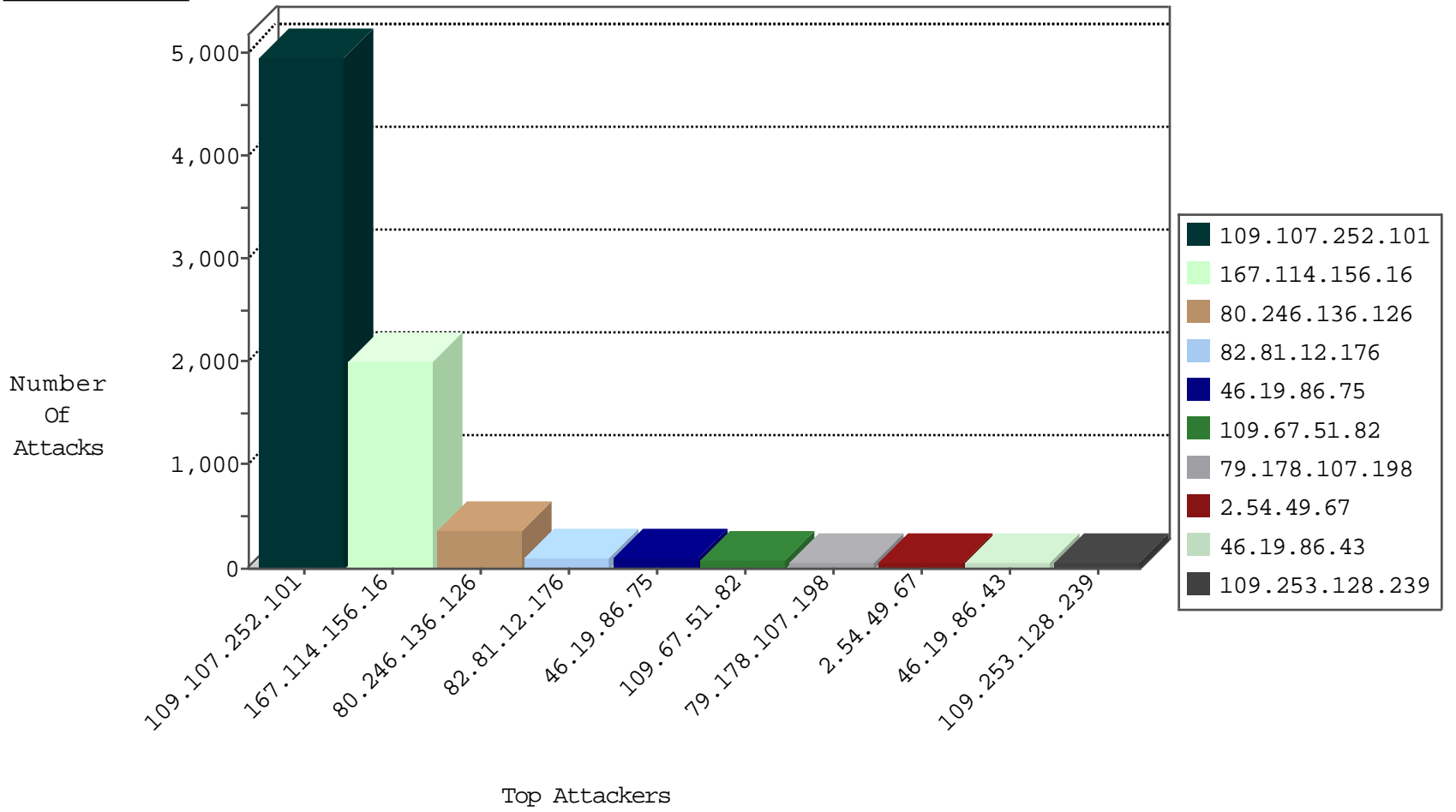
IDF Under Attack Daily Report



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	3130
109.107.252.101	Jordan	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	471
66.249.78.2	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	373
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	104
79.177.32.93	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
37.26.149.200	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
5.102.193.60	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
31.168.240.21	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
111.77.96.210	China	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
120.27.161.20	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
66.249.69.42	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
109.107.252.101	Jordan	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
45.217.19.171	Uruguay	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.130.35	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	18
213.57.187.181	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	8
37.26.149.165	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	6
2.54.35.192	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	2
213.8.204.20	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
111.77.96.210	China	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	C103: HTTP: User Agent Sogou+web+spider	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
109.107.252.101	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3590
109.107.252.101	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	426
109.107.252.101	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	318
109.107.252.101	Jordan	147.237.77.216	dover.idf.il	drop		drop	251
109.107.252.101	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	120
109.67.51.82	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	73
109.107.252.101	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence		alert	60
2.54.49.67	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
109.107.252.101	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	56
109.107.252.101	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	43
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
46.19.86.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	34
46.19.85.181	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
107.167.107.26	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	24
107.167.107.242	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	24
46.19.86.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	19
109.253.147.74	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
77.125.134.31	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
109.107.252.101	Jordan	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	15
46.19.86.75	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
79.180.222.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
87.68.51.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.142.215.25	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
46.19.86.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
5.28.161.58	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
197.47.99.67	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.54.17.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.52.19.159	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.117.157.200	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
37.46.39.176	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
45.217.19.171	Uruguay	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
194.114.146.227	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.86.75	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
5.28.161.58	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	6
149.78.226.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.65.138.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.65.168.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.28.161.58	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
79.178.147.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.75	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
85.65.138.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.102.254.188	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.127.237.185	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.134.31	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.52.136.225	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
5.22.135.127	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	199
80.246.136.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	112
79.178.107.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
80.246.136.126	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 80.246.136.126	Block	47
109.253.128.239	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	43
46.19.86.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
46.19.86.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15
79.178.107.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
77.126.96.55	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	5
2.54.41.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
81.218.136.85	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/0/	Block	3
109.253.128.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
52.34.80.78	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	2
109.253.199.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.69.42	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.42	Block	2
79.179.182.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.125.242.175	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/9/2479.jpg	Block	1
207.46.13.148	United States	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31/	Block	1
37.26.146.186	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
87.69.48.241	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.69.34	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
185.32.179.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.210	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.181.37.13	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.244	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.217.45	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.112	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.107.252.101	Jordan	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
79.178.28.115	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.9.106.81	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
84.111.158.37	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.125.72.232	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.30	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
157.55.39.15	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/62312	Block	1
2.51.22.96	United Arab Emirates	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
80.246.136.108	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.178.203.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.8.204.67	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1
37.26.147.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
91.214.201.107	Moldova, Republic of	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
2.54.133.235	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
187.189.195.40	Mexico	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/a2billing/customer/iridium_threed.php	Block	1
79.182.11.98	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$LoginControl\$captcha\$captchaText in www.aka.idf.il/main/gyus/default.aspx	None	1
46.117.96.121	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
141.212.122.177	United States	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31/	Block	1
46.19.85.114	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.22.134.209	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.65.0.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.125.81.179	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 77.125.81.179	Block	1