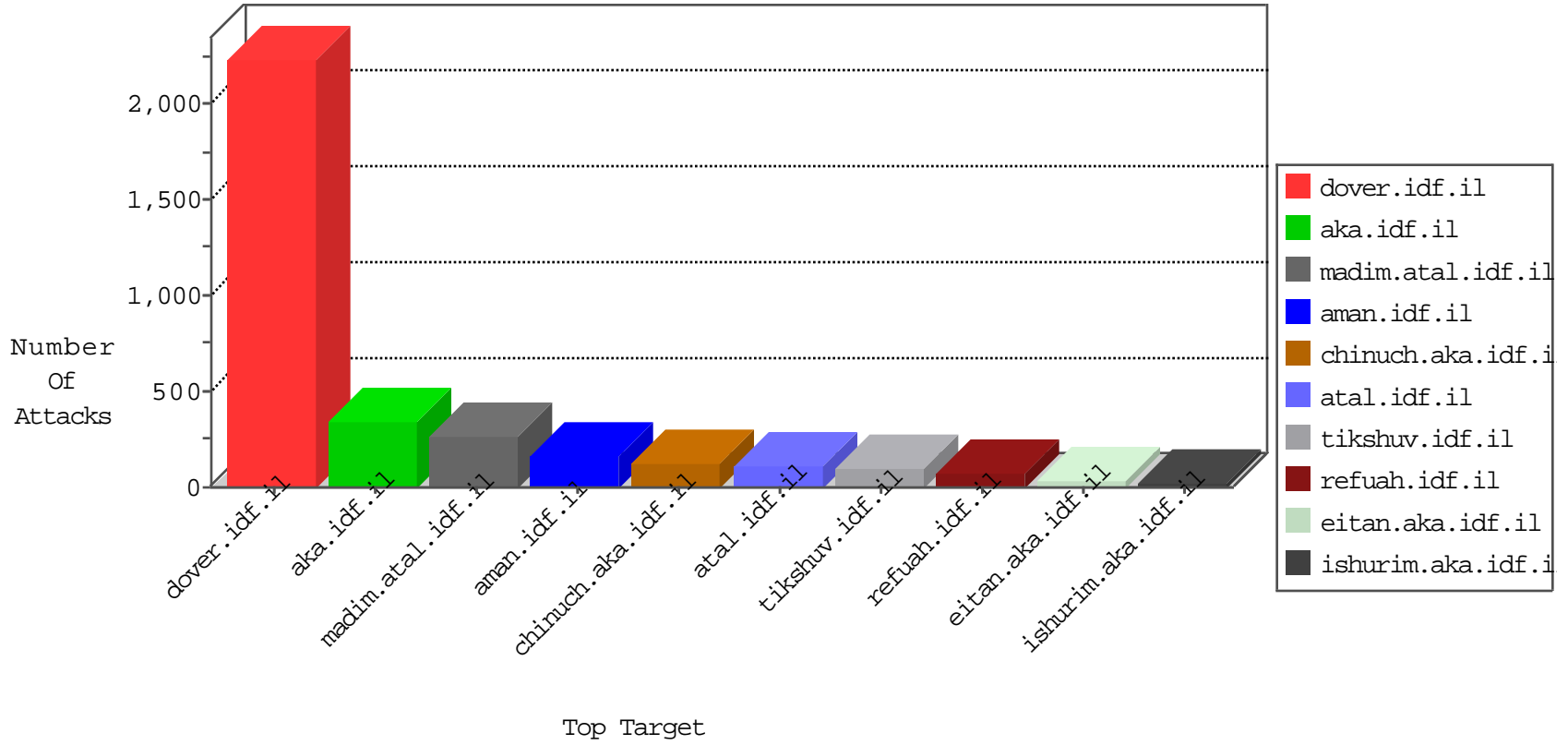


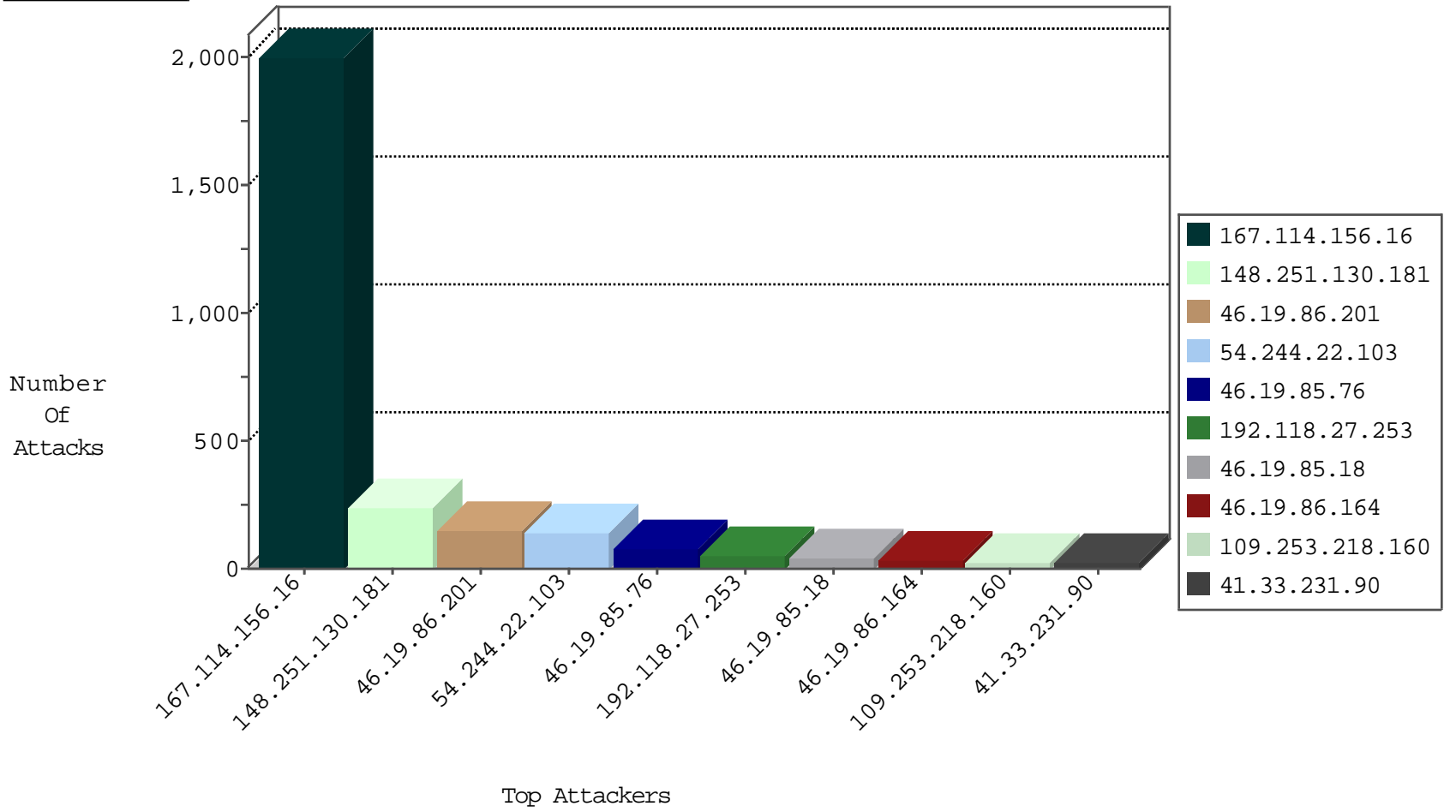
IDF Under Attack Daily Report



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	3018
82.80.136.93	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	12
79.182.186.220	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
175.136.191.119	Malaysia	147.237.76.34	ychalan.idf.il	Block_Udp_All_Nets	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
188.168.17.185	Russian Federation	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
23.95.50.58	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	1
194.90.131.82	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
185.81.158.41		147.237.76.148	ggcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
23.95.50.58	United States	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
114.214.191.242	China	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.254.32.63	United Kingdom	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	1
198.20.69.77	United States	147.237.76.176	test.ncore.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
148.251.130.181	Germany	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	117
148.251.130.181	Germany	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	117
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	72
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	70
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	23
176.13.13.30	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
46.19.85.16	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
46.19.86.164	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
192.118.27.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
109.253.218.160	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
46.19.86.218	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
192.118.27.253	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.18	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.164	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
149.78.243.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.65.23.249	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	11
46.19.86.237	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.18	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
176.65.6.96	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
2.54.148.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.118.27.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.18	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.18	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
176.13.6.38	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
37.26.146.198	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
82.81.17.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.179.13.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.94.111.58	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.137.175	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.64.30.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.114.118.30	Palestinian Territory, Occupied	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.118.27.253	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.3.144.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.148	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.24	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.24	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.253.218.160	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
37.26.146.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
109.253.218.160	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.146.214	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.86.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
65.55.210.28	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
157.55.39.197	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.54.44.234	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
40.77.167.105	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.118.27.253	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	4
213.244.84.242	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
207.46.13.108	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
165.225.72.80	United States	147.237.76.31	nakchal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	99
46.19.85.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	75
46.19.86.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	43
149.88.48.164	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 149.88.48.164	Block	22
46.117.233.201	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 46.117.233.201	Block	14
46.19.85.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	10
149.88.224.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
37.26.149.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
165.225.72.80	United States	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	4
46.19.86.201	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ct100\$ContentPlaceholder1\$txtMobile in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	4
81.218.70.243	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 81.218.70.243	Block	4
37.26.147.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.213.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.140.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	3
85.250.199.42	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	3
165.225.72.80	United States	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 165.225.72.80	Block	3
212.76.102.250	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
132.70.66.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
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	2
109.253.213.100	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 109.253.213.100	Block	2
109.253.199.215	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
109.253.213.100	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	2
46.19.85.74	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	2
213.151.38.209	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/iturim/resources/images/body/images/main.jpg	Block	2
192.116.239.196	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	2
46.19.85.74	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	2
61.216.2.14	Taiwan	147.237.76.86	navy.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
176.13.14.237	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
40.77.167.105	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/faq/	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
31.13.110.106	Ireland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.228.145.174	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
46.121.194.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.88.71.227	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
2.52.154.204	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
79.182.13.146	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.76.102.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/adguard-ajax-api/api	Block	1
109.253.218.160	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
46.19.85.74	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version __atuvc=1%7C3; __atuvs=569f6c5987870b8f000; __atssc=facebook%3B5	Block	1
109.253.138.237	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/	Block	1
66.249.93.102	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
185.127.10.40		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/main/home/default.aspx	Block	1
86.145.136.179	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
54.153.32.246	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
149.78.136.147	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.39.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.12.149	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
73.136.215.236	United States	147.237.77.176	matpash.idf.il	eMail Hoarding	Block	1