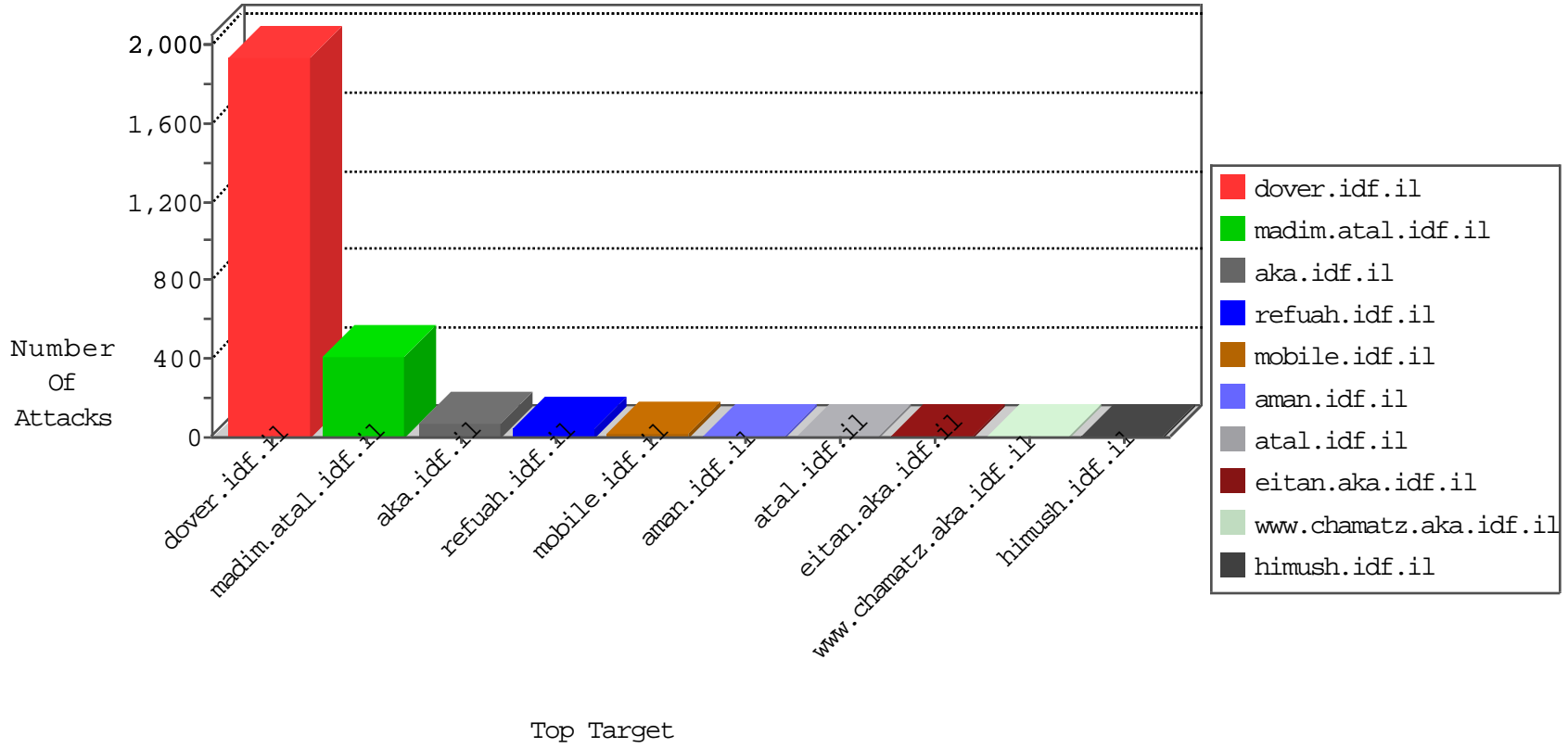


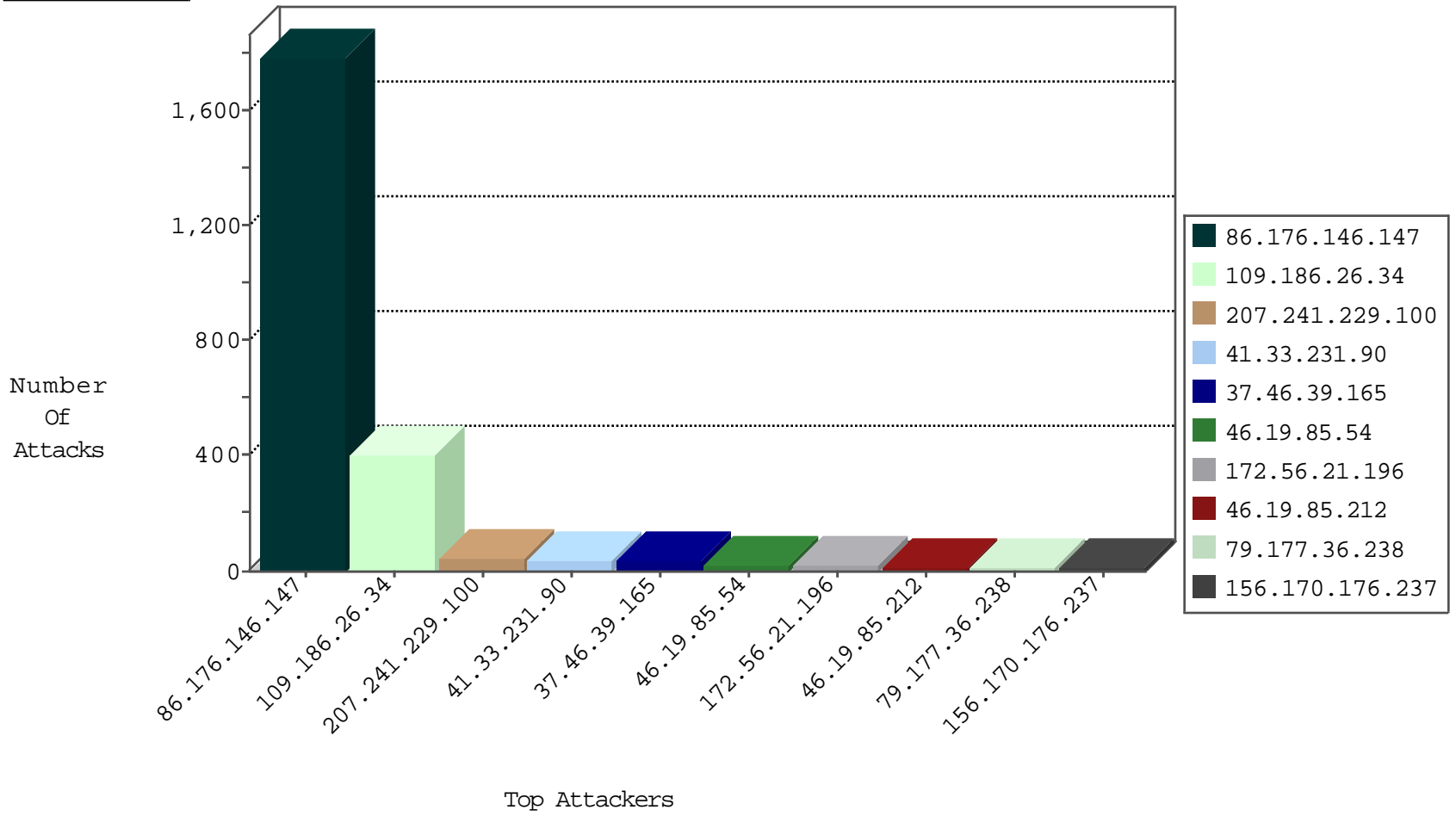
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
104.255.70.247		147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
142.54.160.213	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
153.188.176.67	Japan	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	1

Top Attackers In IPS

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

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
86.176.146.147	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	422
207.241.229.100	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
37.46.39.165	Israel	147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	28
86.176.146.147	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
172.56.21.196	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
156.170.176.237		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
79.177.36.238	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.115.177.203	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
89.139.1.110	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
46.19.85.54	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.180.19.230	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.212	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.54	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.212	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
80.179.14.94	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
85.64.206.122	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.54	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.46.39.165	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.54	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
93.158.152.49	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.80.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
105.90.179.21	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
77.127.193.91	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.76.127.44	Israel	147.237.77.234	halag.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
79.177.34.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.0.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
75.126.221.55	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
66.249.78.184	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
75.126.221.55	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
66.249.78.245	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
62.128.48.166	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
86.176.146.147	United Kingdom	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
81.169.237.146	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	2
66.249.65.82	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
172.56.39.84	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
66.249.78.177	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
62.0.117.82	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
213.57.171.164	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.13.19.74	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.19.86.31	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
80.246.130.169	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
195.60.232.57	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
62.0.117.82	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
172.56.21.196	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
176.13.19.74	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
86.176.146.147	United Kingdom	147.237.77.216	dover.idf.il	Automated Vulnerability Scanning	Block	1305
109.186.26.34	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.186.26.34	Block	202
109.186.26.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
109.186.26.34	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 109.186.26.34	Block	92
109.65.111.23	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	4
46.19.85.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
149.78.26.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.177.36.238	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
62.219.208.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.29.93.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
216.218.207.138	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
81.106.46.80	United Kingdom	147.237.76.30	himush.idf.il	Illegal Byte Code Character in Header Name p/ÃŽ&š&A,8&?Ã™Ã Ã¶Ã Ä"Ã²&Ã~	Block	1
66.249.78.233	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.233	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/view_pictures.asp	Block	1
89.139.1.110	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
81.106.46.80	United Kingdom	147.237.76.30	himush.idf.il	Unknown HTTP Request Method Ã~[[#0]][[#0]][[#0]]CÃ£[[#11]]Ã"ÃœÃe a[RÃ-P[[#27]][[#30]]Ã;Ã Ã¿[[#3]]Ã?/Ã.ÃÝÃ?d[[#7]]Ã'Ã&Ã'[[#19]]Ã?Ã' Zy[[#16]][[#27]]:Ã 2[[#8]]•Ã?Ã?Ã&Ã~Ã;ÃšÃ?mÃfÃ-ÃÄ"Ã~Ã"Ã~ÃÝÃ Ã<1Ã" Ã£Ã&Ã"Ã*Ãª+[[#20]]RÃ~W_ÃœÃ,Ã„[[#7]]Ã¥(Ã&=1ÃœÃ„	Block	1
67.52.46.10	United States	147.237.77.233	atal.idf.il	Distributed eMail Hoarding	Block	1
162.243.175.80	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
109.66.157.218	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Question\$74 in aka.idf.il/main/gyus/questionnaire.aspx	None	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1381-16313-he/dover.aspx	Block	1
37.142.190.63	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Question\$67 in aka.idf.il/main/gyus/questionnaire.aspx	None	1
81.106.46.80	United Kingdom	147.237.76.30	himush.idf.il	Illegal Byte Code Character in Method Ã~[[#0]][[#0]][[#0]]CÃ£[[#11]]Ã"ÃœÃe a[RÃ-P[[#27]][[#30]]Ã;Ã Ã¿[[#3]]Ã?/Ã.ÃÝÃ?d[[#7]]Ã'Ã&Ã'[[#19]]Ã?Ã' Zy[[#16]][[#27]]:Ã 2[[#8]]•Ã?Ã?Ã&Ã~Ã;ÃšÃ?mÃfÃ-ÃÄ"Ã~Ã"Ã~ÃÝÃ Ã<1Ã" Ã£Ã&Ã"Ã*Ãª+[[#20]]RÃ~W_ÃœÃ,Ã„[[#7]]Ã¥(Ã&=1ÃœÃ„	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/2974.jpg	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-15044-he/dover.aspx	Block	1
91.109.247.173	United Kingdom	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 91.109.247.173	Block	1
84.229.173.130	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$btnAtudaBack in www.aka.idf.il/main/gyus/atuda/asmachta.aspx	None	1
172.56.21.196	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training/	Block	1
86.176.146.147	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
81.106.46.80	United Kingdom	147.237.76.30	himush.idf.il	Malformed HTTP Header Line 1	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2828.jpg	Block	1
66.249.74.104	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 66.249.74.104	Block	1
91.109.247.173	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-21915-ar/idfgdover.aspx	Block	1
85.65.43.172	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.65.43.172	Block	1
192.243.55.133	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.133	Block	1
109.186.26.34	Israel	147.237.0.19	madim.atal.idf.il	Too Many 403: Response Code per Session	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/view_img.asp	Block	1
87.68.150.51	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
81.106.46.80	United Kingdom	147.237.76.30	himush.idf.il	Malformed URL	Block	1
66.249.78.245	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
157.55.39.100	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/bamachane/	Block	1
66.249.74.106	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/3/112243.pdf	Block	1
85.65.43.172	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
2.54.185.57	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	1
192.254.204.106	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
81.106.46.80	United Kingdom	147.237.76.30	himush.idf.il	Abnormally Long Request method	Block	1
109.186.26.34	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
66.249.78.223	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1774	Block	1
66.249.65.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/5/3295.jpg	Block	1