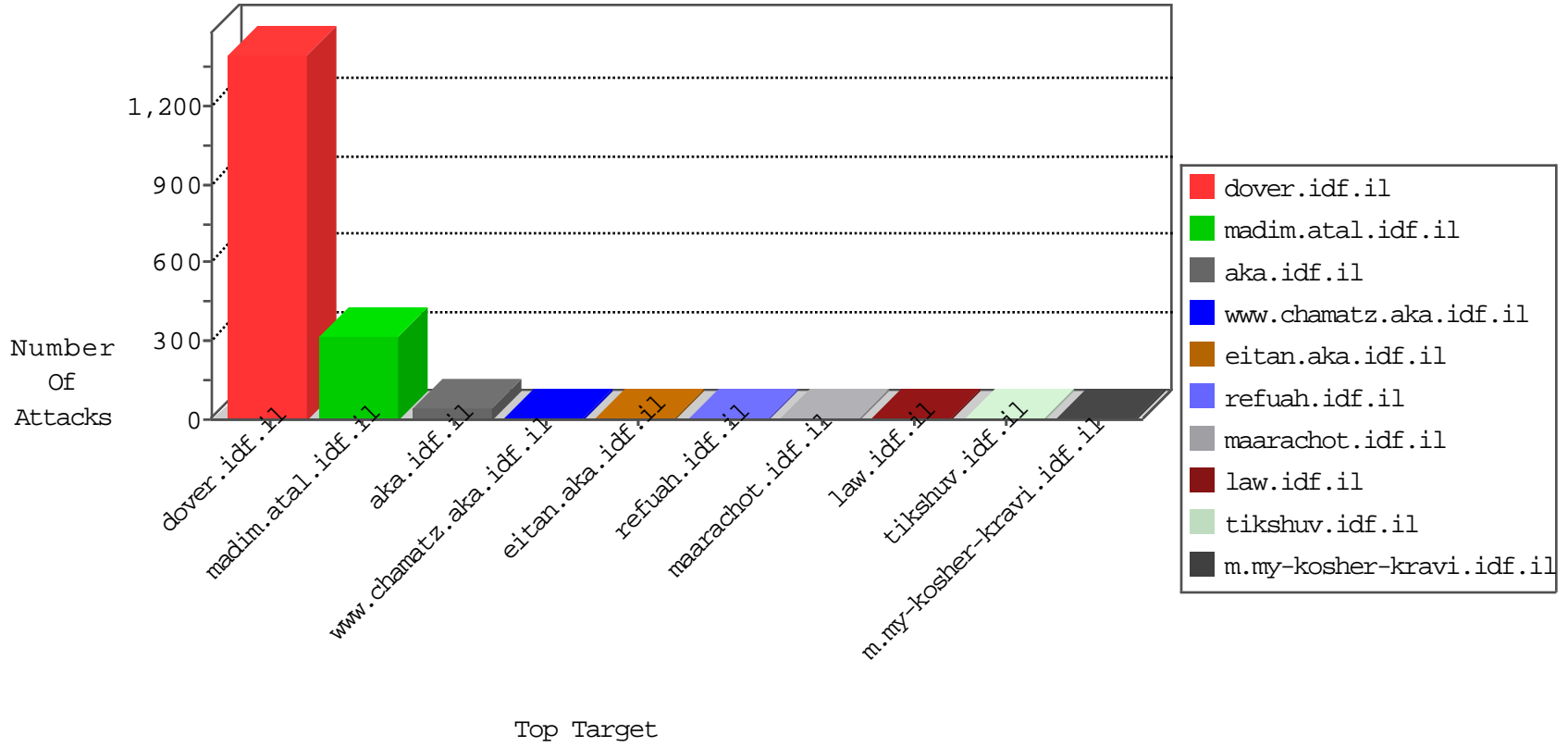


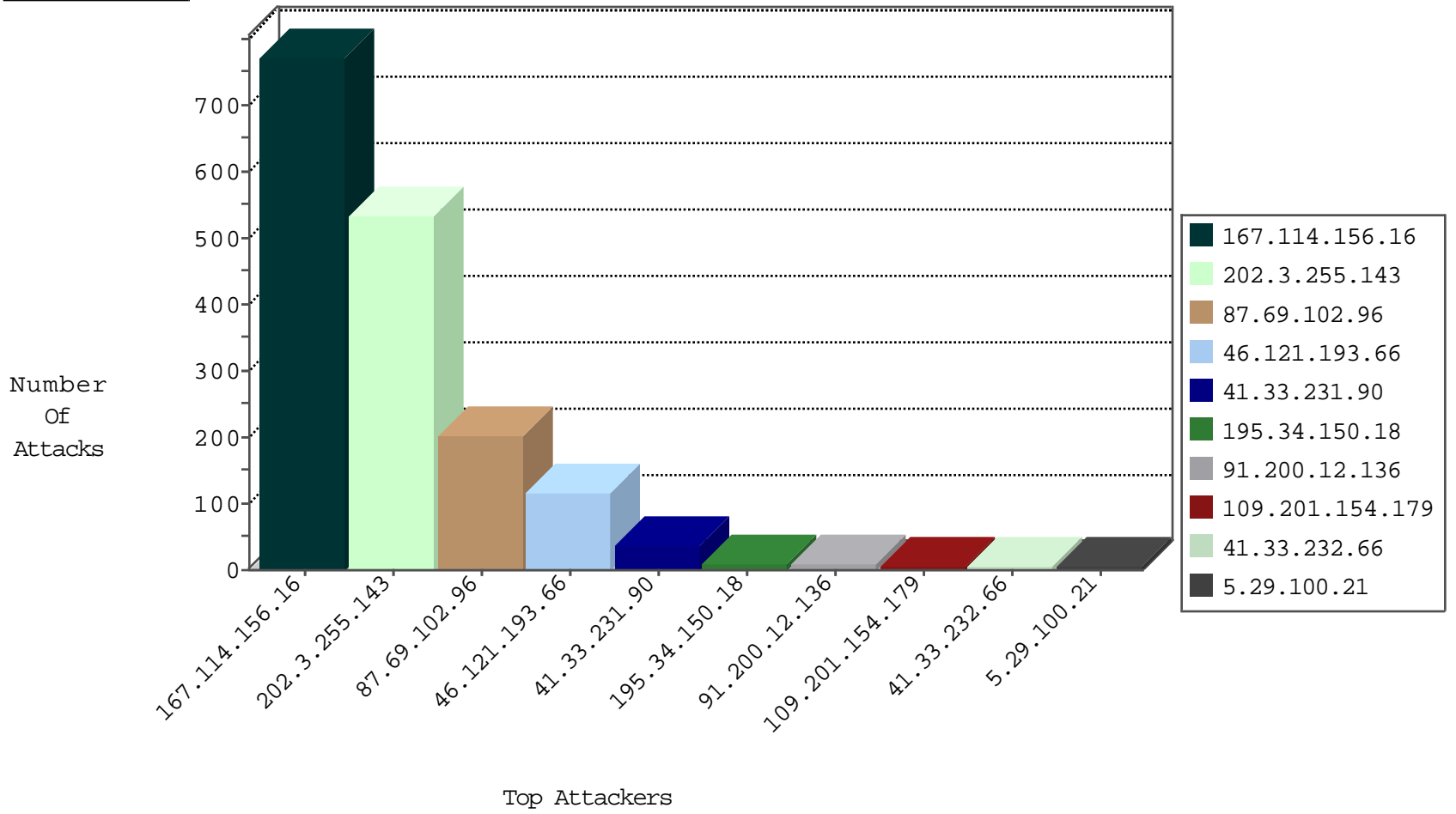
IDF Under Attack Daily Report



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
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	425
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
204.42.253.132	United States	147.237.76.148	ggcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
5.189.154.180	Germany	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
89.248.168.218	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
89.248.168.218	Netherlands	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
204.42.253.132	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
89.248.168.218	Netherlands	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	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
202.3.255.143	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	496
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
218.246.0.97	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.235.254.181	147.237.76.38	Turkey	e.e.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
78.182.33.126	147.237.76.198	Turkey	e.yochalan.idf.il	ET SCAN NMAP -sS window 1024	1
58.253.96.122	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.235.254.181	147.237.76.38	Turkey	e.e.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
58.253.96.122	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 4096	1
24.121.225.29	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1

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	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.121.193.66	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	13
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
109.201.154.179	Netherlands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
217.69.133.226	Russian Federation	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
169.0.177.135		147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
199.30.25.183	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
91.200.12.136	Ukraine	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
217.69.133.225	Russian Federation	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
91.200.12.136	Ukraine	147.237.77.226	www.chamatz.aka.idf.i l	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
109.67.22.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.90.235.154	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.222.139	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
157.55.39.98	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
128.232.110.28	United Kingdom	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
185.32.179.76	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
109.253.222.139	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
61.135.190.200	China	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
141.212.122.185	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.111.68	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
94.242.228.108	Luxembourg	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
184.105.247.224	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
61.67.160.79	Taiwan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
2.54.155.69	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.181	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.113.89	United States	147.237.77.226	www.chamatz.aka.idf.i l	drop	SAM rule	drop	1
195.62.53.168	Russian Federation	147.237.0.17	m.my-kosher-kravi.id f.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.188	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
218.22.211.69	China	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
208.115.113.89	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
94.242.246.24	Luxembourg	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
184.105.247.228	United States	147.237.0.33	idf.il	drop		drop	1
61.67.160.88	Taiwan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
162.216.46.75	United States	147.237.0.17	m.my-kosher-kravi.id f.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.29.15.183	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.181	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
212.28.230.205	Lebanon	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
109.163.234.4	Romania	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
195.116.254.250	Poland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
74.82.47.56	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
173.161.52.213	United States	147.237.72.156	aman.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
49.183.185.234	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.189	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.176	United States	147.237.76.198	e.yochanan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
208.115.113.89	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1
95.38.61.199	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
61.67.160.89	Taiwan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
164.107.169.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.69.102.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	140
87.69.102.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
46.121.193.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
46.121.193.66	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.121.193.66	Block	45
5.29.100.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.238	Block	2
66.249.64.243	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.243	Block	2
77.125.158.135	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.78.160	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluum/templates/http://www.aka.idf.il/sip_storage/files/6/66556.pdf	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/print_bottom.asp	Block	1
40.77.167.43	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
157.55.39.103	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
79.178.112.131	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.75.6	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1631-he/refuah.aspx	Block	1
193.169.86.17	Ukraine	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
61.135.190.200	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
5.29.124.137	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 5.29.124.137	Block	1
105.107.193.104	Algeria	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/gyus/general.aspx	Block	1
157.55.39.245	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/228-he/faq.aspx	Block	1
80.246.136.118	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
66.249.75.15	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
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	1
66.249.64.137	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	1
23.97.233.72	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/sendtofriend/sendtofriend.aspx?&	Block	1
105.107.193.104	Algeria	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/gyus/forum/asp/showforum.asp	Block	1
66.249.64.239	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1234-he/atal.aspx	Block	1
158.69.172.227	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
83.169.10.185	Germany	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.75.127	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1236-he/refuah.aspx	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
66.249.64.229	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
37.205.0.65	Turkey	147.237.72.166	aka.idf.il	MSSQL Data Retrieval with Implicit Conversion Errors	None	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.180.229.173	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
173.161.52.213	United States	147.237.72.156	aman.idf.il	E-mail collector robots 14	Block	1
61.135.190.69	China	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pageNum in www.aka.idf.il/lomdim/forum/asp/showforum.asp	None	1
217.69.133.224	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gyus	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	1
37.205.0.65	Turkey	147.237.72.166	aka.idf.il	Multiple signatures from 37.205.0.65	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
66.249.66.64	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/2/111372.pdf	Block	1
173.161.52.213	United States	147.237.72.156	aman.idf.il	eMail Hoarding	Block	1
61.135.190.71	China	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1