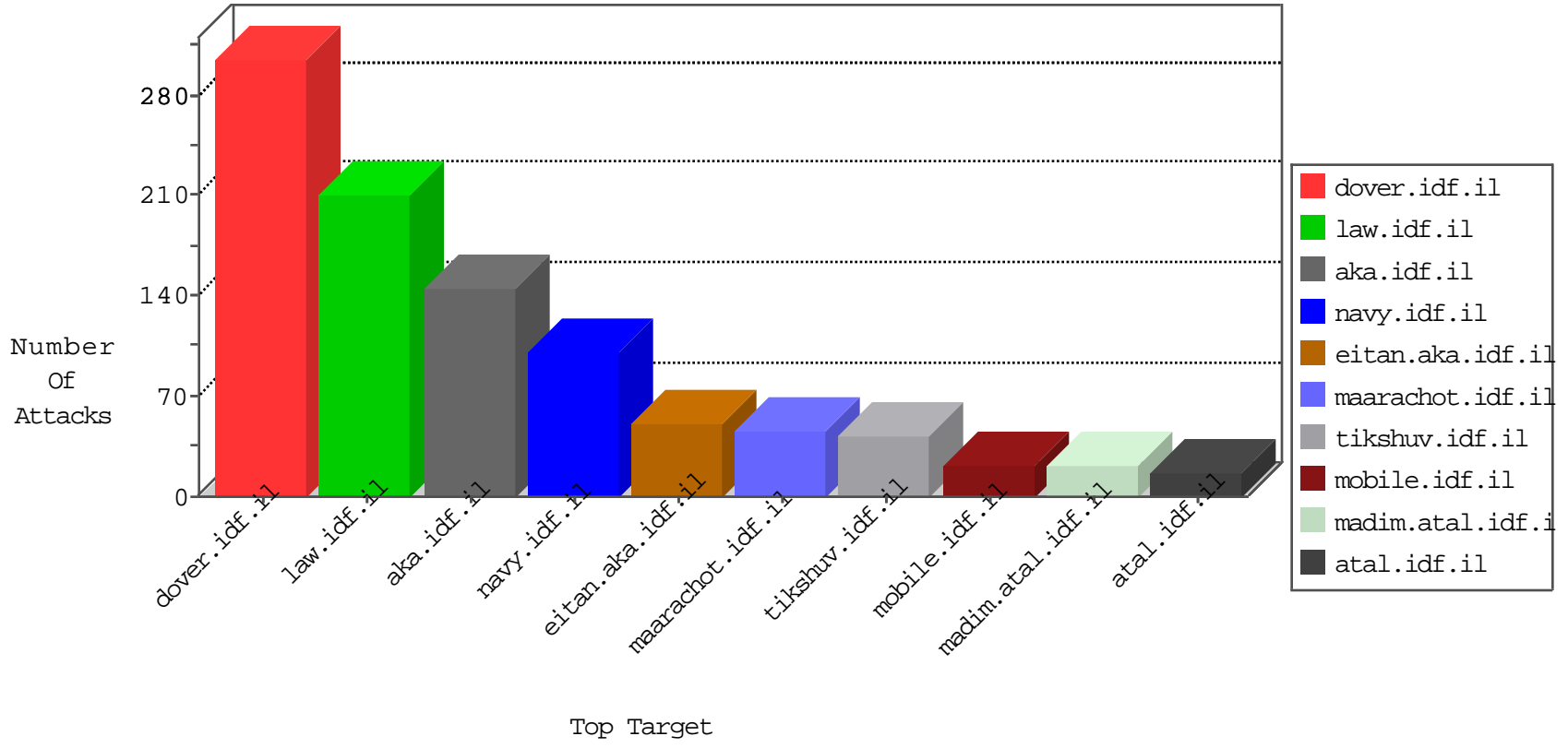


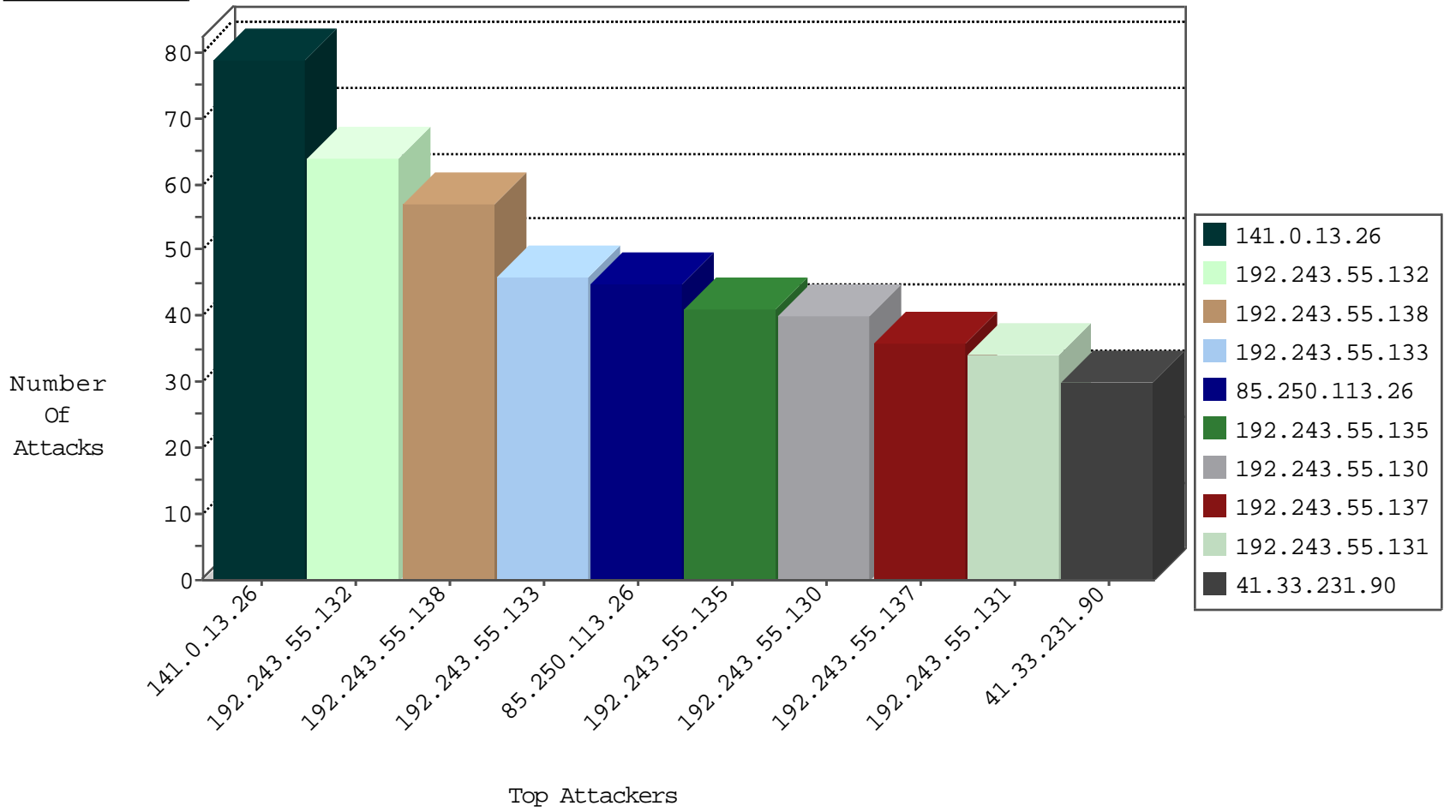
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.178.147.33	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
71.6.135.131	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.224		147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.94.48.202	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
64.87.23.55	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
79.182.207.81	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	2
2.54.167.81	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1
46.19.85.43	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1
207.46.13.4	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
64.87.23.55	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.102.9.91	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
103.53.84.13	147.237.0.15		kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.200.165.32	147.237.76.196	Russian Federation	e.sviva.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
85.65.103.88	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.108.68.226	147.237.0.34	Denmark	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
128.199.164.55	147.237.76.42	Singapore	refuah.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
88.249.106.23	147.237.76.39	Turkey	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
46.101.93.164	147.237.77.19	Russian Federation	law-forum.idf.il	ET SCAN Potential SSH Scan	1
2.108.68.226	147.237.0.19	Denmark	madim.atal.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.0.13.26	Norway	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	74
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
84.111.78.88	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
79.182.197.129	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.86.240	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
85.250.113.26	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
85.250.113.26	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
66.249.66.63	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
185.3.147.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.180.57.201	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.183.117.53	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.1.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.46.13.78	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.133	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
185.32.179.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	6
85.250.113.26	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	6
87.68.42.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.150	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.210.186.65	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.179.188.234	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.132	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.86.48	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.96.230	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.177.96.230	Block	12
46.19.86.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
79.176.179.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.59	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
87.71.34.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.8.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
38.111.147.88	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
38.111.147.88	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 38.111.147.88	Block	2
46.19.86.196	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
84.111.180.47	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.243.55.136	Block	2
5.29.245.65	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
85.64.115.69	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Question\$23 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
79.179.48.188	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.179.48.188	Block	1
46.161.63.161	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter amp;catid in www.aka.idf.il/rights/asp/info.asp	None	1
95.30.43.206	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation FolderId in www.tikshuv.idf.il/modules/forums/forum.aspx	Block	1
37.238.128.6	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
79.179.48.188	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
207.46.13.78	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9710-he/refuah.aspx	Block	1
109.64.112.120	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
85.64.115.69	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Question\$78 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
5.189.205.200	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/chinuch/home/default.asp'	Block	1
79.179.48.188	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
178.24.114.144	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/video http://www.youtube.com/v/tv4zoxi3kn	Block	1
66.249.64.223	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.chimush.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
95.30.43.206	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation ForumId in www.tikshuv.idf.il/modules/forums/forum.aspx	Block	1
79.179.151.22	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.176.39.172	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Question\$112 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
207.46.13.193	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/kamlar/newspaper.asp	Block	1
157.55.39.146	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.9.46.135	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter amp;catId in www.aka.idf.il/rights/asp/info.asp	None	1
79.179.48.188	Israel	147.237.76.147	chinuch.aka.idf.il	PHP Attempt	Block	1
178.255.87.242	United Kingdom	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/robots.txt	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
95.30.43.206	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation lang in www.tikshuv.idf.il/modules/forums/forum.aspx	Block	1
84.111.65.82	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash	Block	1
166.78.134.156	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
93.186.31.98	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.39.40.84	Kuwait	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
79.179.48.188	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/xmlrpc.php	Block	1
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
38.111.147.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
98.175.103.108	United States	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
46.120.142.4	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
166.78.134.156	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
93.186.31.114	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.39.40.84	Kuwait	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
79.179.48.188	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1