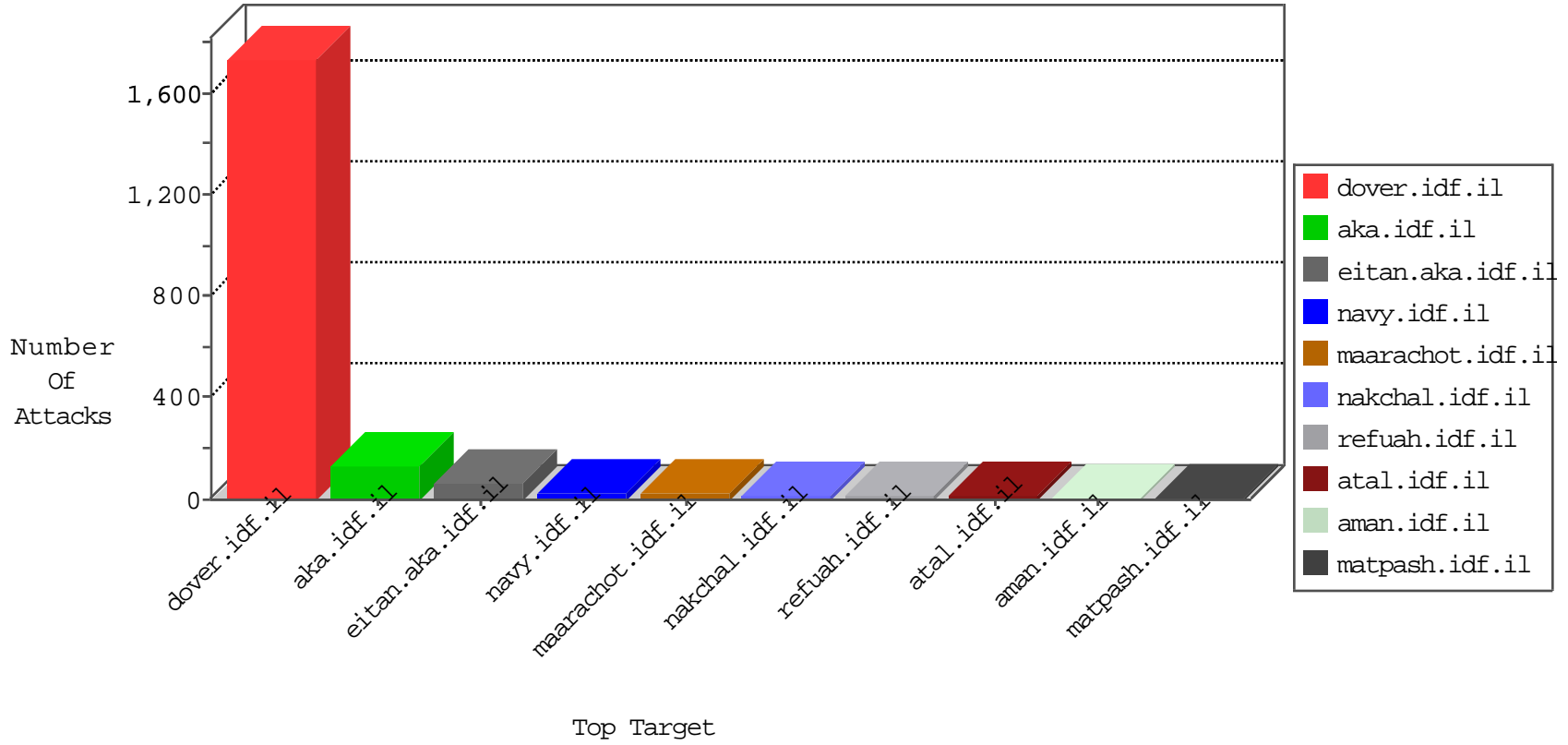


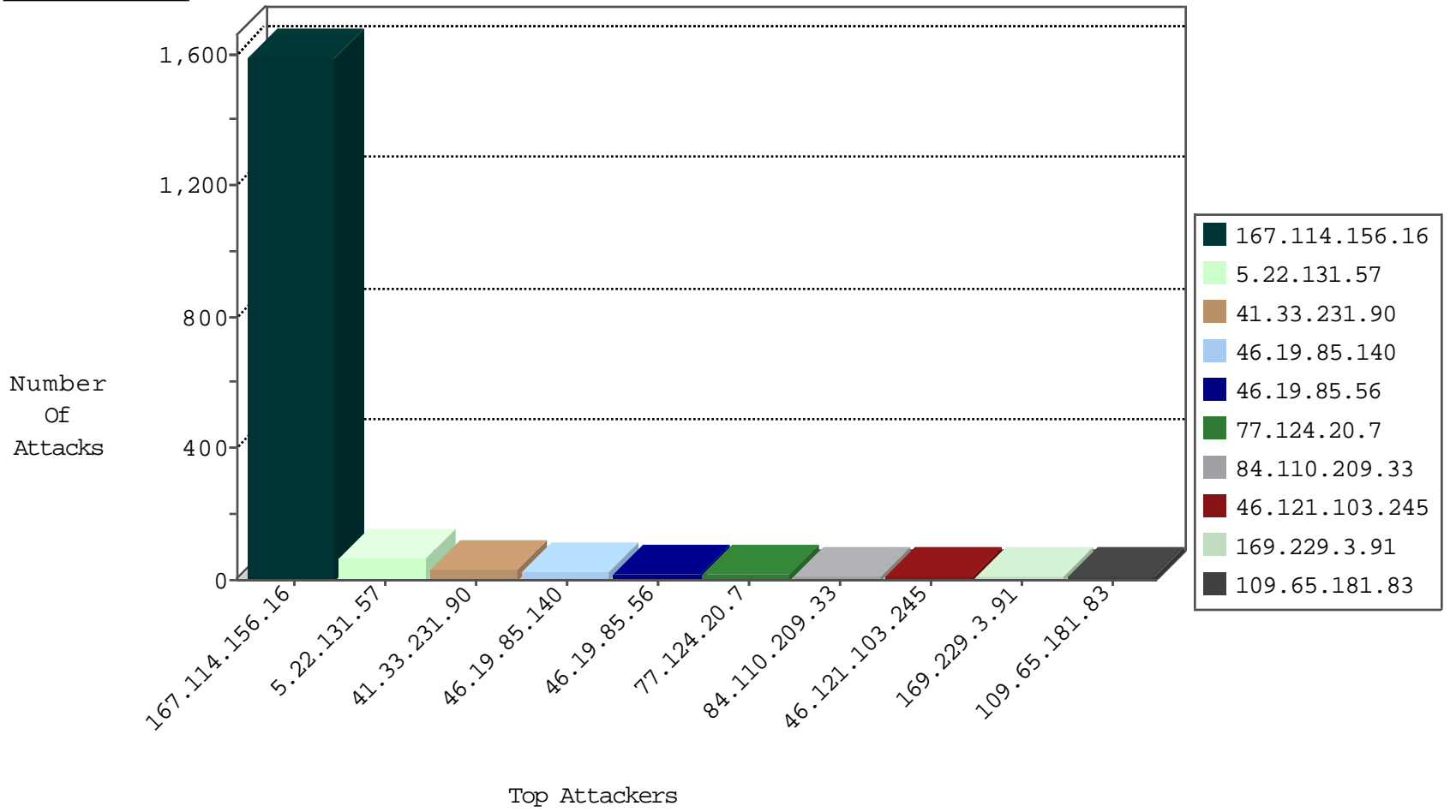
# IDF Under Attack Daily Report



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	Block_Ip_Web_In	drop	1593
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	6
84.108.174.55	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.2	United States	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
27.251.116.34	India	147.237.77.226	www.chamatz.aka.idf.il	12347: HTTP: PHP-CGI Query String Parameter Information Disclosure Vulnerability	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
27.251.116.34	India	147.237.77.233	atal.idf.il	12347: HTTP: PHP-CGI Query String Parameter Information Disclosure Vulnerability	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.158	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
109.127.71.39	Iraq	147.237.77.216	dover.idf.il	C1000125: HTTP: Block admin login to gov.il sites ?q=user	Block	1
27.251.116.34	India	147.237.0.15	kosher-kravi.idf.il	12347: HTTP: PHP-CGI Query String Parameter Information Disclosure Vulnerability	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
27.251.116.34	India	147.237.76.200	eitan.aka.idf.il	12347: HTTP: PHP-CGI Query String Parameter Information Disclosure Vulnerability	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
64.233.172.163	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
93.174.93.96	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
87.229.116.42	147.237.76.39	Hungary	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 4096	1
13.92.246.145	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
203.197.205.118	147.237.72.217	India	e.idf.il	ET SCAN NMAP -sS window 3072	1
175.123.98.240	147.237.0.34	Korea, Republic of	tikshuv.idf.il	SERVER-APACHE Apache Tomcat Web Application Manager access	1
104.128.144.131	147.237.77.226	Canada	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
96.127.95.44	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 4096	1
93.174.93.96	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.82.78.38	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 1024	1
13.92.246.145	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
203.197.205.118	147.237.72.217	India	e.idf.il	ET SCAN NMAP -sS window 1024	1
189.34.83.169	147.237.0.35	Brazil	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
175.123.98.240	147.237.0.19	Korea, Republic of	madim.atal.idf.il	SERVER-APACHE Apache Tomcat Web Application Manager access	1
104.128.144.131	147.237.77.205	Canada	prisha.idf.il	ET SCAN NMAP -sS window 4096	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.22.131.57	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
77.124.20.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
109.65.181.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
84.110.209.33	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
84.110.209.33	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.140	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.121.103.245	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.147.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.154.157.247	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
64.233.172.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.140	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.56	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
217.132.63.206	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.140	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
109.67.217.78	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.103	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.140	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.121.103.245	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
64.233.172.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.249.66.145	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.102.254.75	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.43.71.27	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.102.242.46	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.180.212.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.68.116	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.134.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
194.90.66.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
103.247.0.7	Australia	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.130.240.182	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.149.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.134.227	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.253.223.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.22.170	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.142.242.126	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.176.30.78	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
87.71.0.183	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.95.115.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.159.157.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.130.240.182	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.176.30.78	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
87.71.44.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.86.192	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.65.163.156	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.121.103.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.142.242.25	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.56	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 46.19.85.56	Block	14
79.183.182.24	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.183.182.24	Block	5
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	3
176.13.2.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.102.8.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
103.247.0.7	Australia	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.83.251	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.236.136.145	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19930-he/idfgdover.aspx	Block	1
200.73.17.115	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
5.28.179.224	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
103.247.0.7	Australia	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
66.249.83.254	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
217.69.136.210	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
184.105.247.195	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
79.183.182.24	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
66.249.66.141	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1
200.73.17.115	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/xmlrpc.php	Block	1
5.144.60.235	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
159.203.174.239	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17471-en/dover.aspx/feed/	Block	1
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
194.114.146.227	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.114.146.227	Block	1
80.246.130.62	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18551-he/dover.aspx	Block	1
207.241.229.32	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
37.113.91.120	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation FolderId in www.tikshuv.idf.il/modules/forums/searchresults.aspx	Block	1
175.123.98.240	Korea, Republic of	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/manager/html	Block	1
74.82.47.2	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
2.53.54.203	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
83.169.211.50	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/main/rabanut/general.aspx	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in tikshuv.idf.il/site/general.aspx	Block	1
37.142.68.96	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
175.123.98.240	Korea, Republic of	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/manager/html	Block	1
79.182.226.193	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/xbehvcsachar/default.aspx	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
2.53.156.36	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1