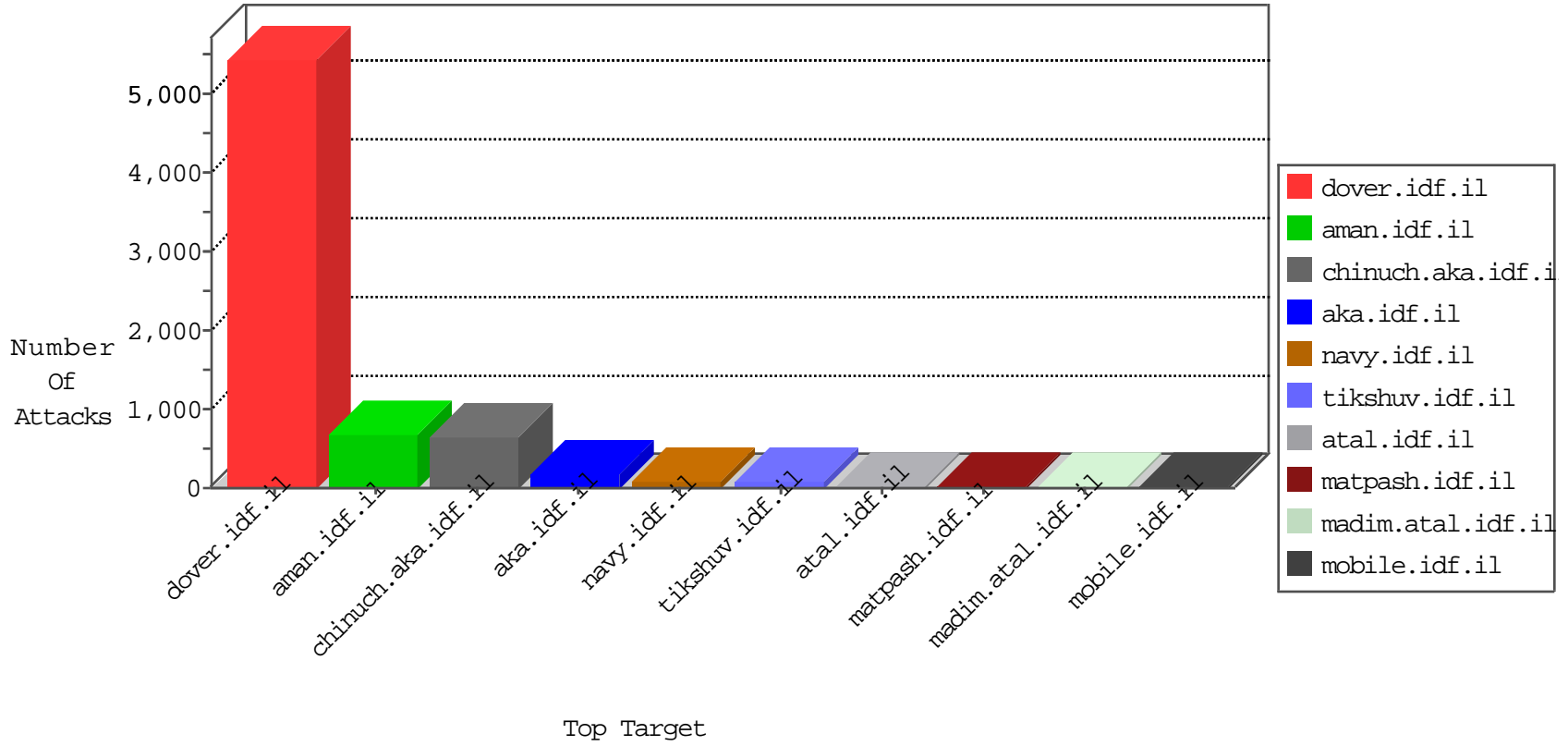


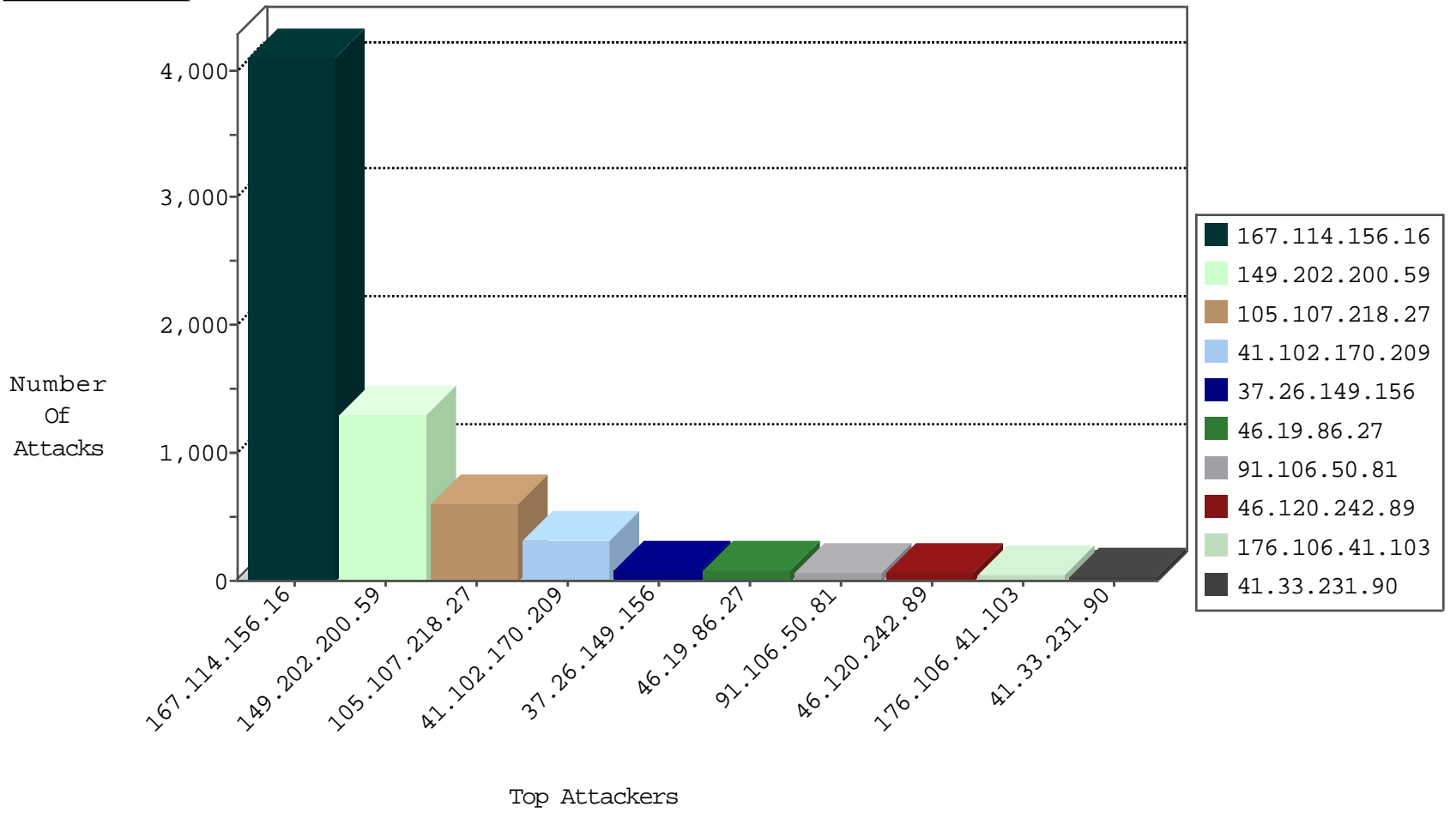
# IDF Under Attack Daily Report



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	4107
105.107.218.27	Algeria	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	653
91.106.50.81	Iraq	147.237.77.216	dover.idf.il	SQL-Inj-Pang-GMSSQLInt1	dest-reset	59
197.119.147.123	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	11
23.239.64.15	United States	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1
23.239.64.15	United States	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
158.85.253.245	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
61.135.189.114	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	3
69.30.215.26	United States	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.215.26	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.215.26	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.215.26	United States	147.237.76.31	nakchal.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.215.26	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	2
212.150.244.226	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
66.249.66.154	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
158.85.253.245	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	4
222.186.31.99	147.237.0.33	China	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
220.231.195.122	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.31.99	147.237.0.35	China	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
220.231.195.122	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
220.231.195.122	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -f -sS	1
46.19.85.237	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.202.200.59	France	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	638
149.202.200.59	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	632
105.107.218.27	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	547
41.102.170.209	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	307
46.19.86.27	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
46.120.242.89	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
176.106.41.103	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
176.106.41.103	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
63.141.204.186	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
37.26.149.156	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	15
176.13.17.30	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.28.164.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
109.253.159.97	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
37.26.149.156	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
37.26.149.156	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
176.13.19.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
87.70.38.27	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.149.156	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
37.26.149.156	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
105.107.218.27	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
109.67.178.56	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	8
31.210.186.240	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
176.106.41.103	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
109.67.178.56	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	6
79.180.177.165	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
80.246.136.12	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
149.78.196.165	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.178.233.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
95.86.122.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.65.105.166	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.106.41.103	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.180.21.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.36	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	6
2.55.61.212	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.219	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.219	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
66.249.93.148	Europe	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	5
37.26.149.156	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
2.55.59.143	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.26.149.156	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
191.176.23.111	Brazil	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.120.22.123	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.26.149.156	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
37.26.149.156	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.149.156	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.26.149.156	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
5.29.112.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
46.19.85.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.24.206.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
95.86.111.217	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	2
46.19.85.183	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.183	Block	2
37.201.192.154	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	2
46.19.85.183	Israel	147.237.77.216	dover.idf.il	Multiple Malformed URL from 46.19.85.183	Block	2
190.214.173.129	Ecuador	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
5.22.134.194	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
213.254.241.4	France	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$btnSearch in www.aka.idf.il/main/sachar/default.aspx	None	1
37.26.149.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.42	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;amp in www.aka.idf.il/	None	1
79.181.116.108	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
2.53.43.240	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
190.214.173.129	Ecuador	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
46.19.85.183	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
5.29.97.140	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
46.19.85.183	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method : in URL he-il,he	Block	1
163.172.13.21	United Kingdom	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
79.182.126.190	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
2.53.131.16	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
66.249.64.103	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluilml/maind9ea.html	Block	1
197.119.147.123	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
46.19.85.183	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
149.88.56.188	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/<html><head><title>502 bad gateway</title></head><body bgcolor=	Block	1
68.180.230.184	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
46.19.85.237	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
40.77.167.78	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
163.172.13.21	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
91.106.50.81	Iraq	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 91.106.50.81	Block	1
2.53.131.16	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 2.53.131.16	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/daily	Block	1
207.46.13.144	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/319,	Block	1
46.19.85.183	Israel	147.237.77.216	dover.idf.il	Malformed URL he-il,he;q=0.8,en-us;q=0.6,en;q=0.4	Block	1
31.210.186.240	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
149.88.171.218	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.75.79.95	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/31/	Block	1
46.121.70.206	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
94.123.192.152	Turkey	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 94.123.192.152	Block	1
2.55.61.212	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-9241-he/dover.aspx	Block	1
213.8.204.21	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
37.26.149.152	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.30	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.30	Block	1
2.53.43.240	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 2.53.43.240 (Open Mode)	None	1