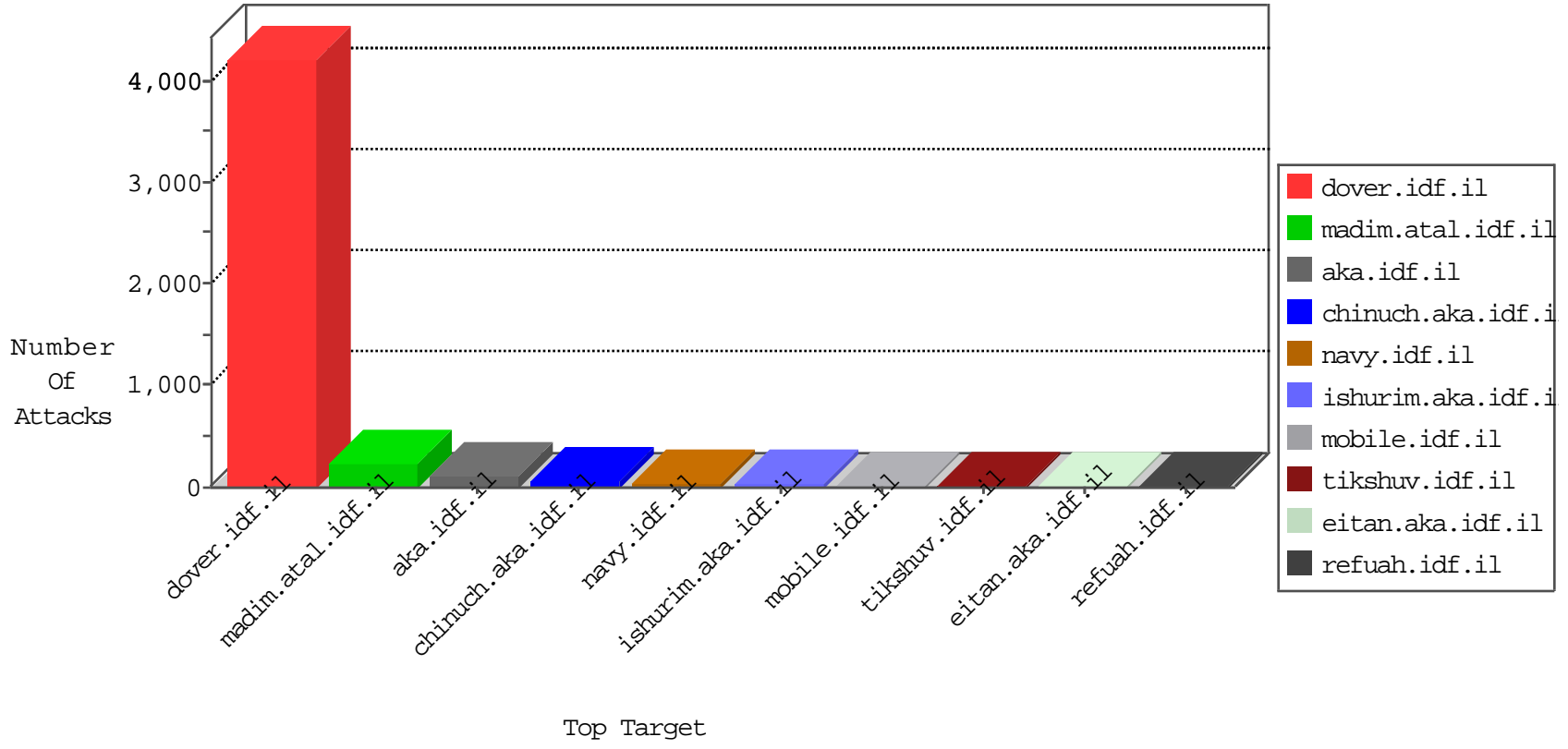


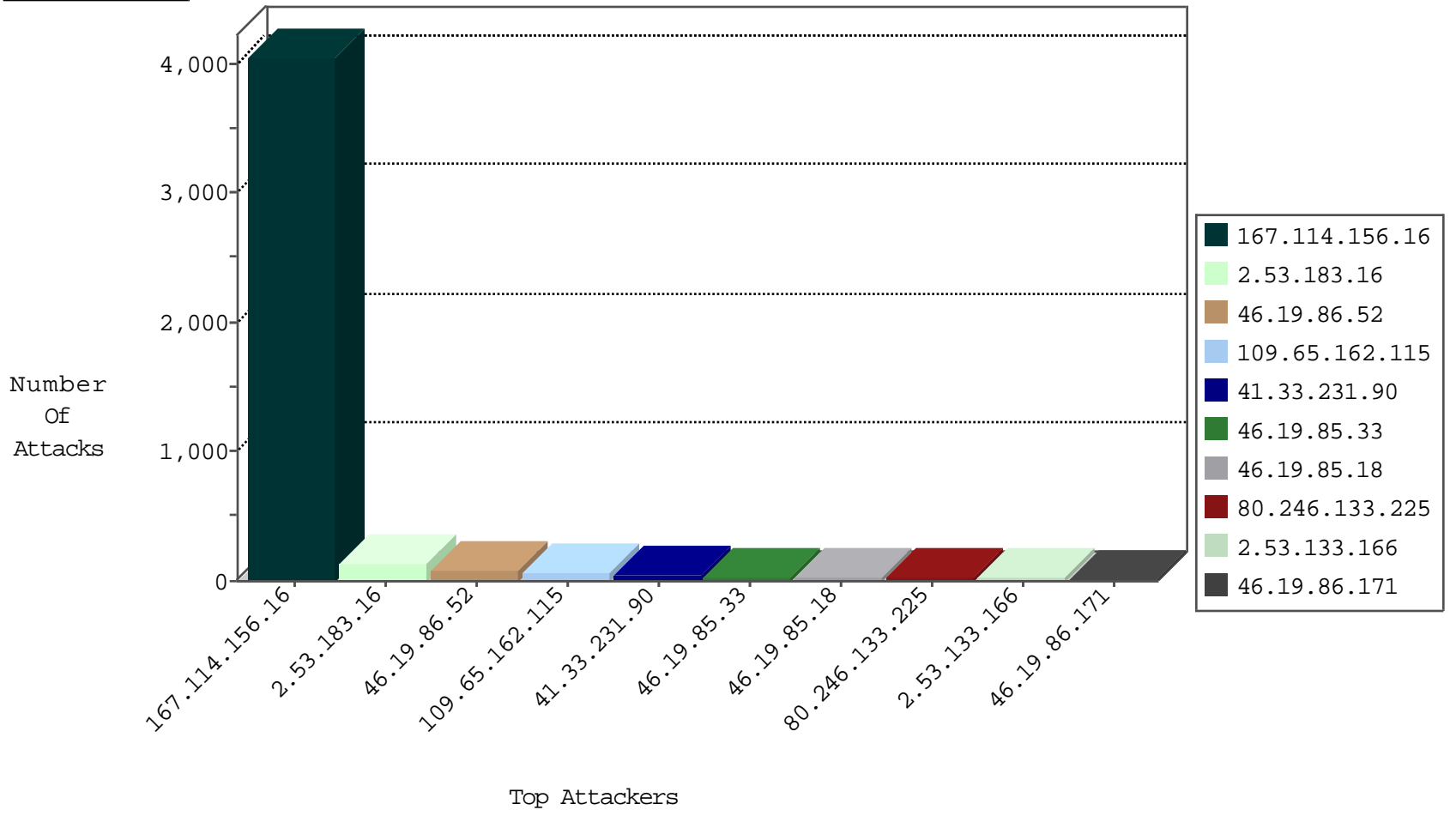
# IDF Under Attack Daily Report



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	4030
80.246.133.225	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	6
79.178.163.130	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	5
123.59.59.52	China	147.237.77.216	dover.idf.il	block-sp-trafl	forward	4
85.93.89.243	Germany	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
85.93.89.243	Germany	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
85.93.89.243	Germany	147.237.77.243	mobile.idf.il	Block_Udp_All_Nets	drop	1
85.93.89.243	Germany	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
109.186.49.99	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
85.93.89.243	Germany	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.57.205.145	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
109.253.215.206	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
199.30.24.125	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
199.58.86.209	United States	147.237.77.216	doover.idf.il	C1000074: HTTP: majestic bot	Block	2
40.77.167.92	United States	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
207.241.237.222	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
66.249.66.162	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
46.4.79.76	147.237.77.179	Germany	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
5.29.94.89	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.199.185.122	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
82.80.50.57	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
78.129.199.80	147.237.72.156	United Kingdom	aman.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.66.12	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
46.4.79.76	147.237.77.216	Germany	dover.idf.il	ET SCAN Potential SSH Scan	1
46.4.79.76	147.237.77.176	Germany	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
208.80.155.215	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
185.106.92.47	147.237.0.15	Russian Federation	kosher-kravi.idf.il	ET WEB_SERVER Muieblackcat scanner	1
79.177.18.173	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.158	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.65.162.115	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
2.53.133.166	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.86.171	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
176.13.5.205	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
80.246.133.225	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.33	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.18	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.210.8	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.64	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.33	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.64	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.154.155.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.27	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.18	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.18	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.33	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.18	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.33	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.253.128.112	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.117.143.250	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
2.53.148.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.52	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
95.35.51.169	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.19.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.32.19	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.137.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.232.28.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.160.168.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.48.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.53	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.178.163.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.208.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.139.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.23.169	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.117.143.250	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.53.137.220	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.80.177.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.14.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.0.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.39	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
178.255.215.87	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-14-2016-08:04:02 to 04-14-2016-09:04:02

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.102.195.176	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.46.38.155	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.179.190.84	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.183.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	138
46.19.86.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	74
109.253.221.168	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	7
75.17.232.116	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtEmail in www.idf.il/1038-en/dover.aspx	Block	3
2.53.175.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.81.75.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.21.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.147.184	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gyus	Block	2
46.19.85.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.55.38.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
123.59.59.52	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.qyer.com/894-he/dover.aspx	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/homepage/div.item	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
207.46.13.81	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-he	Block	1
149.50.20.226	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	1
109.160.168.47	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Cookie Tampering on cookie wb48617274: Expected AC95F956, Observed 001D4B51	None	1
176.13.23.63	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
66.249.73.147	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
2.53.129.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
124.73.11.78	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1281-ar/cogat.aspx/trackback/	Block	1
87.70.134.99	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
212.199.151.160	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gius	Block	1
157.55.39.54	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
38.102.226.16	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
109.253.210.8	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
66.249.75.35	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/page.asp	Block	1
176.58.75.113	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/163-	Block	1
91.38.223.136	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
77.237.138.202	Czech Republic	147.237.77.176	matpash.idf.il	Unauthorized URL Access to /	Block	1
219.74.180.192	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.199	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/sachar/klali.aspx	None	1
40.77.167.16	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/ishurim	Block	1
66.249.78.111	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
185.77.91.113	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/index.php	Block	1
132.72.65.183	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ctl100\$cphMain\$cphSachar\$ctl155 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
94.188.161.145	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	1
79.177.231.228	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 106 cookies	Block	1
157.55.39.199	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
110.86.186.223	China	147.237.77.176	matpash.idf.il	Unauthorized HTTP Method	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.249.78.158	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
203.127.96.217	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
94.188.161.145	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew	Block	1
80.179.7.171	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyas	Block	1