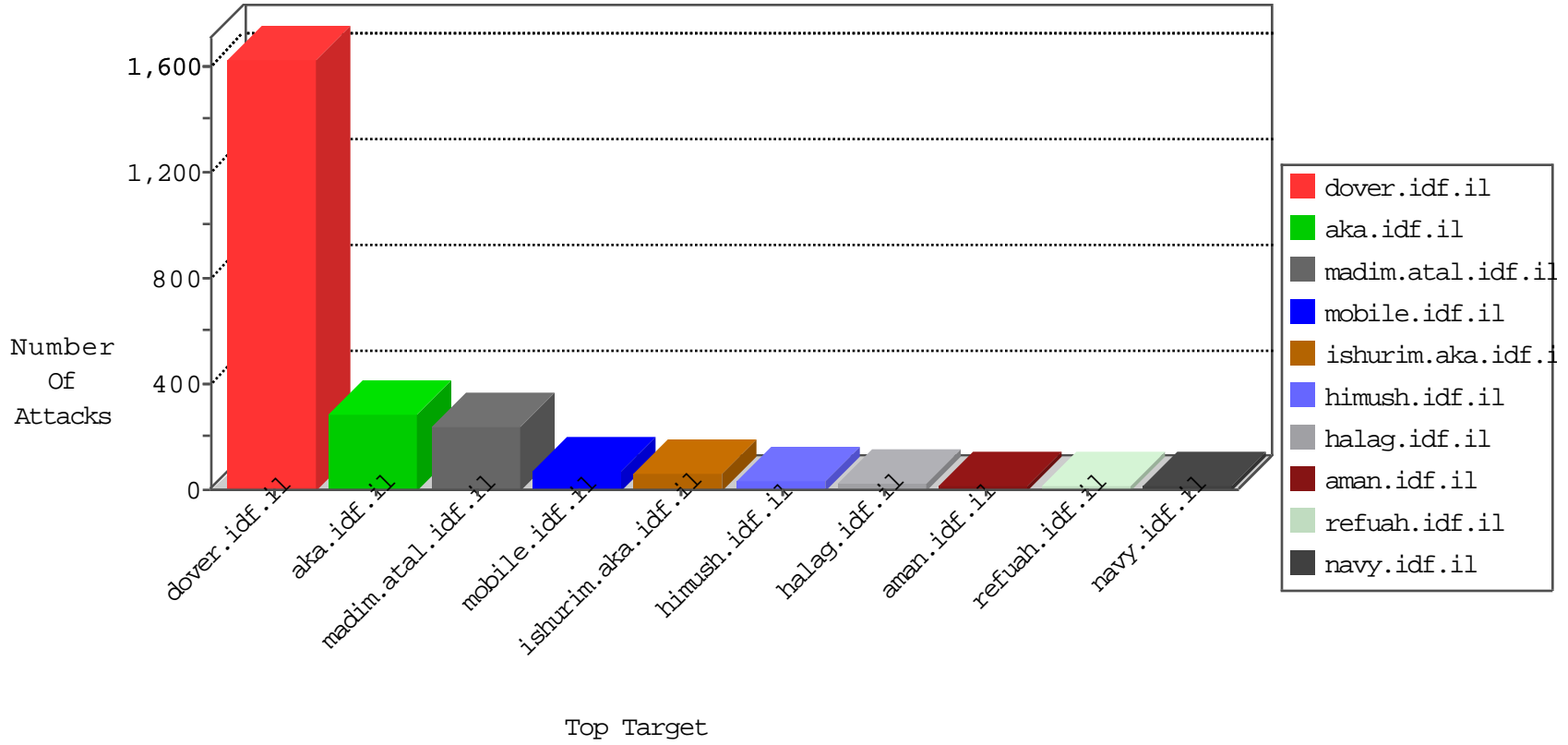


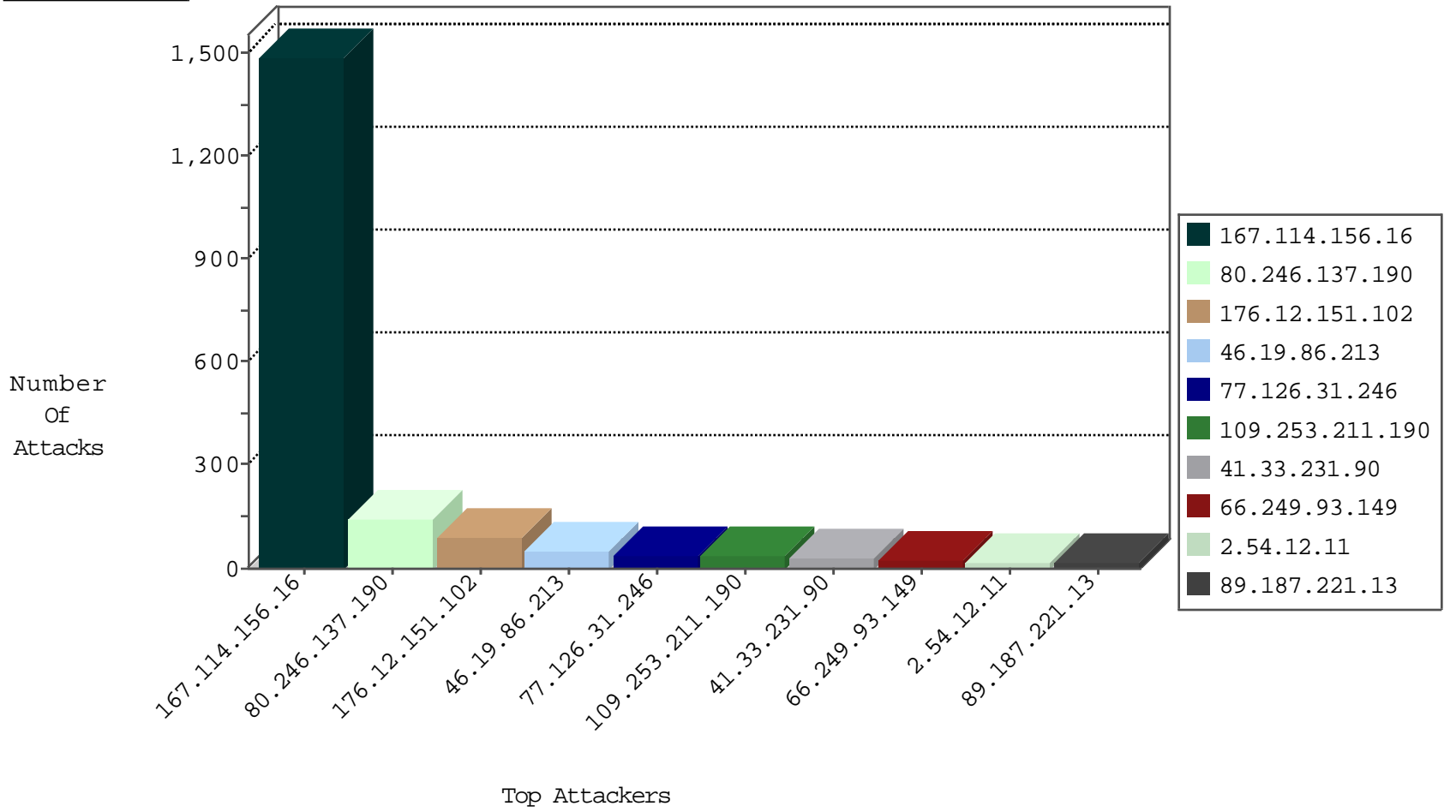
# IDF Under Attack Daily Report



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	3183
183.60.48.25	China	147.237.76.198	e.yohanan.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
66.240.236.119	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
67.79.13.53	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.187.221.13	Lebanon	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	3
89.187.221.13	Lebanon	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
185.63.188.120	Russian Federation	147.237.76.86	navy.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.253.211.190	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	19
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
89.187.221.13	147.237.77.216	Lebanon	dover.idf.il	GPL WEB_SERVER /etc/passwd	3
89.187.221.13	147.237.77.216	Lebanon	dover.idf.il	SQL Injection - Select From	3
89.231.153.168	147.237.77.178	Poland	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
80.246.137.190	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	1
89.231.153.168	147.237.76.202	Poland	e.halag.idf.il	ET SCAN Potential SSH Scan	1
79.180.50.86	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
223.4.174.30	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.231.153.168	147.237.76.196	Poland	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
73.17.14.46	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
89.231.153.168	147.237.76.31	Poland	nakchal.idf.il	ET SCAN Potential SSH Scan	1
23.96.213.135	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
168.62.174.240	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential SSH Scan	1
89.231.153.168	147.237.72.166	Poland	aka.idf.il	ET SCAN Potential SSH Scan	1
168.62.174.240	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential SSH Scan	1
89.231.153.168	147.237.0.16	Poland	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
89.187.221.14	147.237.77.216	Lebanon	dover.idf.il	GPL WEB_SERVER TRACE attempt	1
109.64.176.21	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.231.153.168	147.237.77.235	Poland	sviva.idf.il	ET SCAN Potential SSH Scan	1
84.108.58.125	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.231.153.168	147.237.77.19	Poland	law-forum.idf.il	ET SCAN Potential SSH Scan	1
80.230.18.88	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.231.153.168	147.237.76.197	Poland	e.himush.idf.il	ET SCAN Potential SSH Scan	1
79.178.34.209	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.239.242	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.231.153.168	147.237.76.39	Poland	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
37.142.64.117	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.115.90.26	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.231.153.168	147.237.72.217	Poland	e.idf.il	ET SCAN Potential SSH Scan	1
168.62.174.240	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
23.96.213.135	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
89.231.153.168	147.237.0.35	Poland	akaws.idf.il	ET SCAN Potential SSH Scan	1
147.235.236.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.187.221.14	147.237.77.216	Lebanon	dover.idf.il	SERVER-WEBAPP TRACE attempt	1
109.65.213.223	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
95.175.95.24	147.237.76.34	Kuwait	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
85.64.72.197	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
46.19.86.213	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	48
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
77.126.31.246	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
66.249.93.149	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
109.253.211.190	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
79.176.36.14	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
176.13.21.24	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.178.203.50	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.12.11	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.176.18.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.21.110	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.12.11	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
93.172.191.123	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.183.129	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.150.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.12.11	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
109.64.23.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.95.210.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.211.190	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.178.203.50	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.180.58.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.254.48	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.120.125.42		147.237.72.156	aman.idf.il	drop	SAM rule	drop	5
80.246.140.3	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
37.46.39.2	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.142.156.205	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
5.28.149.236	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
81.218.170.183	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
79.181.70.145	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
84.108.217.72	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
213.57.129.222	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
2.54.6.0	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.41.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.213.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.30.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.250.236.99	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.180.104.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.176.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
128.127.107.81	Netherlands	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.191	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.211.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.81	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.5.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.154.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

12-23-2015-19:04:05 to 12-23-2015-20:04:05

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.178.32.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.137.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	98
176.12.151.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	92
80.246.137.190	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 80.246.137.190	Block	41
89.187.221.13	Lebanon	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 89.187.221.13	Block	4
79.179.152.139	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.179.152.139	Block	4
79.179.152.139	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	3
128.127.107.81	Netherlands	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
80.246.136.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.145.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.0.158	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	2
109.66.48.8	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
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	2
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	2
176.13.1.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.177.134.212	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
185.32.179.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
94.230.82.143	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
50.7.124.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
176.12.140.196	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.250.86.77	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
46.19.85.100	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.223.79	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.146.217	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
207.241.229.37	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized Method HEAD for eitan.aka.idf.il/	None	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
176.13.21.24	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
46.19.86.152	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/login.aspx	None	1
150.70.173.59	Japan	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
84.109.178.110	Israel	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
37.26.146.137	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.186.69.135	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/home.aspx	Block	1
80.246.136.23	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.8.204.19	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.178.34.209	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.49.14.190	Poland	147.237.77.176	matpash.idf.il	Unauthorized URL Access to testp2.czar.bielawa.pl/testproxy.php	Block	1
95.215.45.187	Sweden	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
85.250.236.99	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
62.128.48.122	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.246.137.207	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.167	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
5.28.154.222	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.66.19.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.180.150.46	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.29.215.141	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
89.187.221.14	Lebanon	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
77.125.98.120	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.21.24	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.117.41.131	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
157.55.39.131	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1