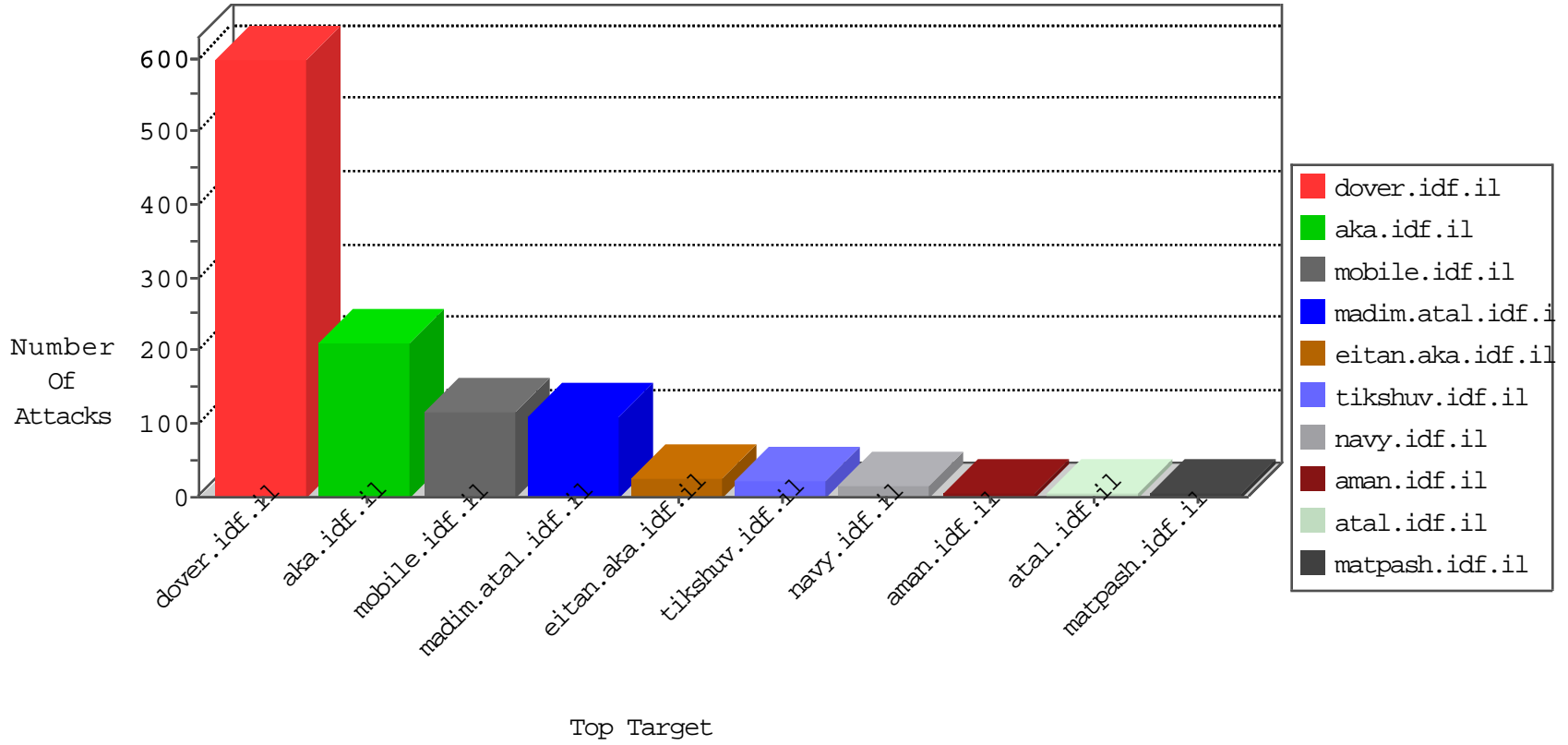


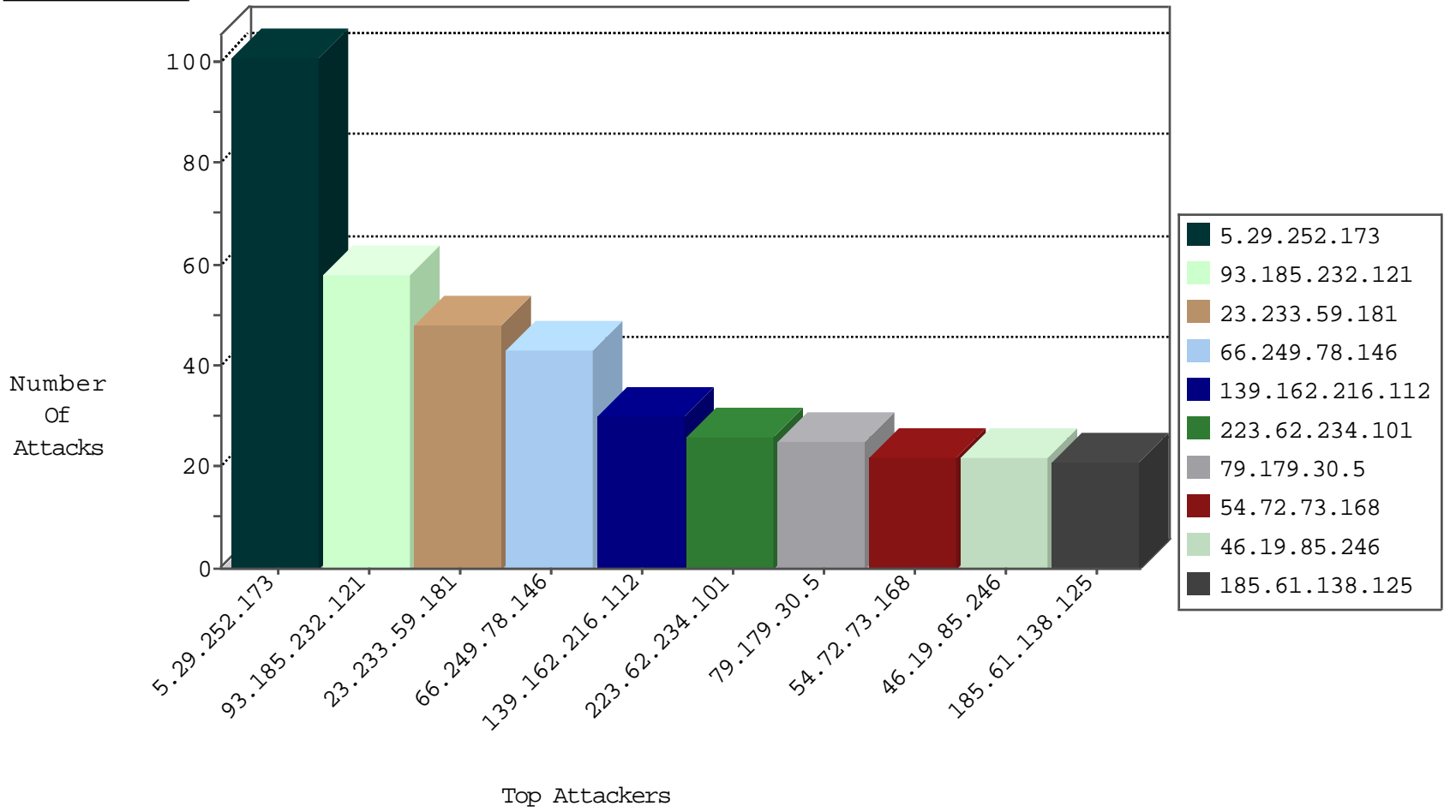
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3
204.42.253.2	United States	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.148	ggcenter.aka.idf.il	Block_Ntp_All_Net	drop	2
66.240.236.119	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

## 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	4
79.178.173.79	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
66.249.64.191	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
188.136.144.104	147.237.77.61	Iran, Islamic Republic of	e.cogat.idf.il	ET SCAN NMAP -f -sS	1
161.202.120.149	147.237.0.34	Japan	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
161.202.120.149	147.237.0.19	Japan	madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
109.64.55.100	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
188.136.144.104	147.237.77.61	Iran, Islamic Republic of	e.cogat.idf.il	ET SCAN NMAP -sS window 2048	1
161.202.120.149	147.237.0.35	Japan	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
161.202.120.149	147.237.0.19	Japan	madim.atal.idf.i	ET SCAN Potential SSH Scan	1
124.122.240.13	147.237.0.35	Thailand	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
80.82.78.38	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -sS window 1024	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
46.17.100.16	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
188.136.144.104	147.237.77.61	Iran, Islamic Republic of	e.cogat.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
93.185.232.121	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
23.233.59.181	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
223.62.234.101	Korea, Republic of	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	26
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
79.179.30.5	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
185.61.138.125	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
94.230.86.252	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
213.57.63.143	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	15
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
175.157.55.9	Sri Lanka	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
207.46.13.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
66.249.93.119	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
79.176.38.48	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.147.239	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.64.134.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.144.62.154	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.103.160	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.102.6.131	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
85.248.227.164	Slovakia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.43.89.114	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
86.165.226.209	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.93.115	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
171.25.193.77	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
37.26.146.195	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.26.148.248	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.246	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.53.16.210	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.246	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.66.184	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.144.240	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.3.59	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
91.143.235.191	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
217.132.151.80	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.66.47	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
88.254.110.197	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.252.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	101
46.118.156.3	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1556-en/	Block	6
79.179.30.5	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
199.30.25.128	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
217.132.151.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.176.38.48	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
150.129.184.71	Malaysia	147.237.77.233	atal.idf.il	PHP Attempt	Block	2
144.76.90.230	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 144.76.90.230	Block	2
5.22.135.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.220.182	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
199.30.24.237	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
85.65.127.79	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.65.127.79	Block	2
37.26.147.239	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
144.76.90.230	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.53.16.210	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
207.241.229.225	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/oprolescategory/oprolescategory.in.aspx	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
40.77.167.96	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/eitan/listpage/	Block	1
93.109.218.123	Cyprus	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.79.107	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
66.249.75.16	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/size100x0/2690.jpg	Block	1
176.10.99.206	Switzerland	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
79.179.144.240	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
212.91.120.154	Croatia	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/9/60929.pdf	Block	1
150.129.184.71	Malaysia	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/wp-login.php	Block	1
109.226.28.77	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ctl00\$cphMain\$cphSachar\$ctl199 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/signals/atar/	Block	1
66.249.75.24	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/size100x0/3403.jpg	Block	1
176.13.3.59	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
149.78.148.86	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.64.113.145	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/booklets.aspx	Block	1
66.249.64.143	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
151.80.31.108	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp	Block	1
77.237.138.202	Czech Republic	147.237.77.235	sviva.idf.il	Unauthorized Method HEAD for /	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
150.129.184.71	Malaysia	147.237.77.233	atal.idf.il	Admin Blocking	Block	1
5.102.195.152	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ctl00\$cphMain\$cphSachar\$ctl167 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
217.132.151.80	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter d in www.aka.idf.il/milum/templates/inner.asp	None	1
151.80.31.109	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/nahal.stm.	Block	1
141.212.122.161	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId\u003d58624 in www.aka.idf.il/main/giyus/general.aspx	None	1
150.129.184.71	Malaysia	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 150.129.184.71	Block	1
85.65.127.79	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
220.181.108.152	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.79.89	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/elram	Block	1
66.249.66.5	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/fhgffgdgd646465.aspx	Block	1