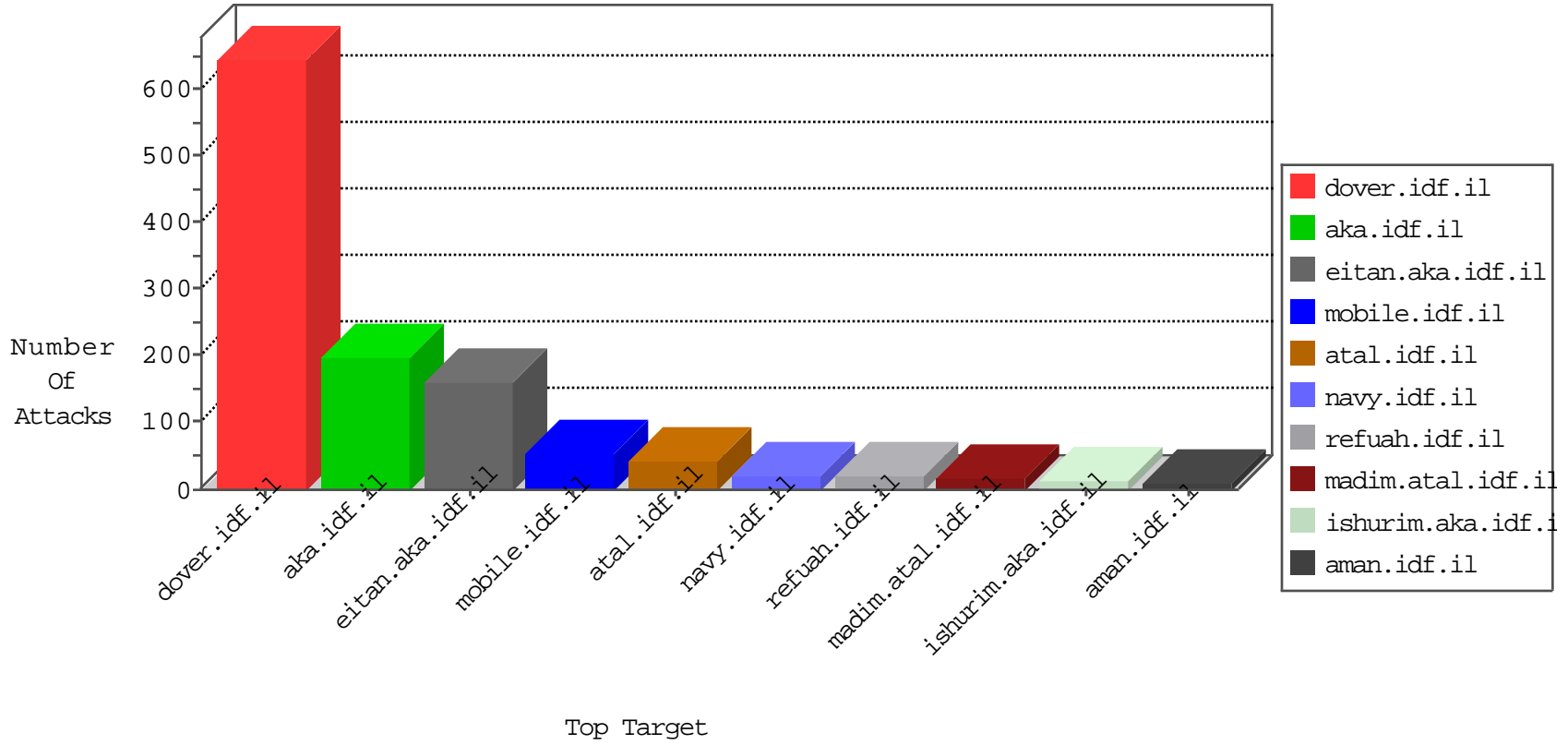


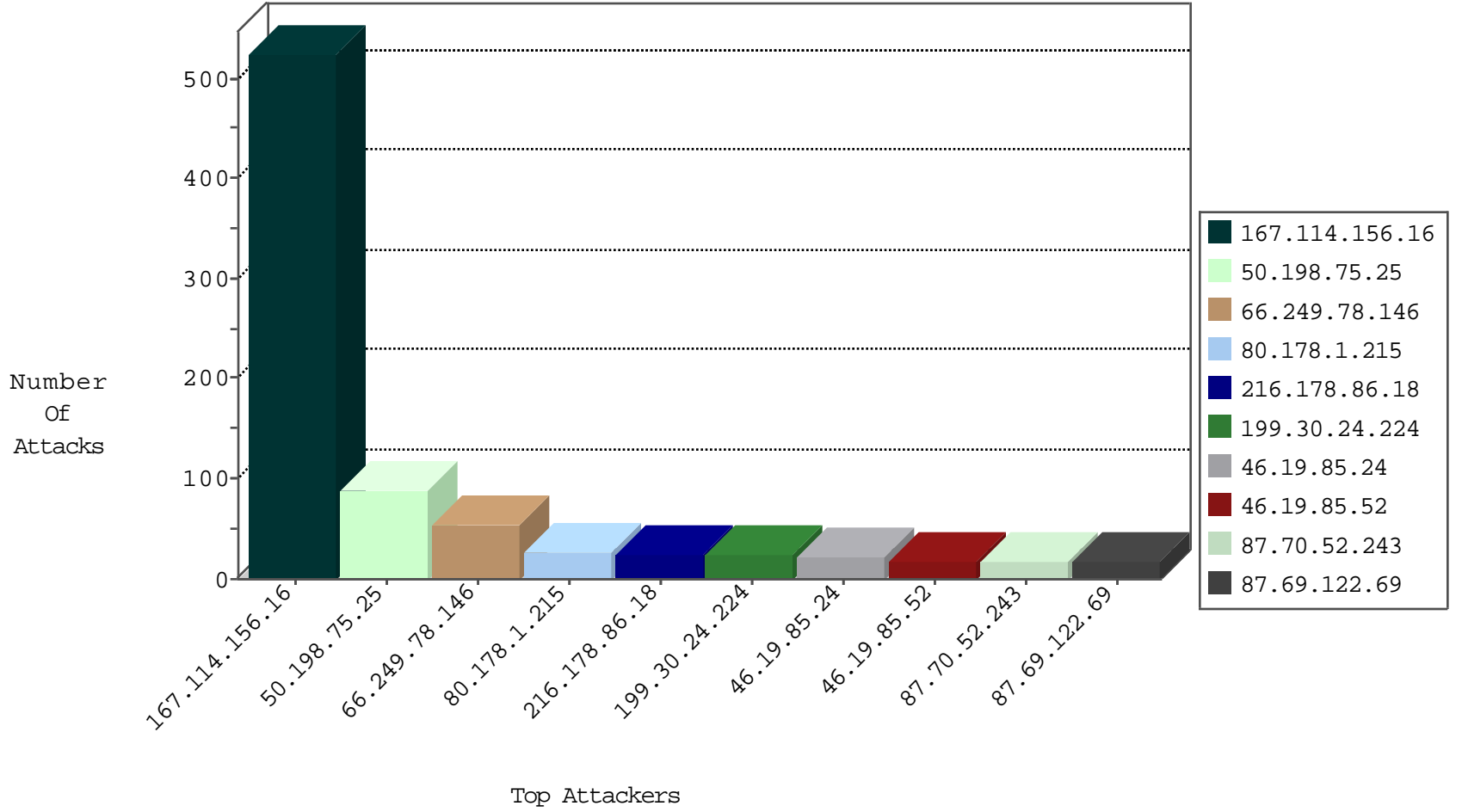
IDF Under Attack Daily Report



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	HTTP-POST-Segmented-DoS	dest-reset	23560
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2666
79.182.51.146	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	210
213.57.105.51	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	202
81.218.65.210	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	6
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
185.3.144.89	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
109.67.62.44	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
94.230.86.58	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1
58.221.46.246	China	147.237.76.30	himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
89.46.102.242	Romania	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
104.153.173.100	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
180.97.106.36	China	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.148	ggcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
45.63.20.231	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
180.97.106.36	China	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
46.120.230.43	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	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	3
66.102.9.17	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
61.161.130.241	147.237.0.34	China	tikshuv.idf.il	SERVER-APACHE Apache Tomcat Web Application Manager access	1
46.19.86.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
40.76.60.239	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
40.76.60.239	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
5.196.199.232	147.237.76.38	France	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.74	147.237.72.14	United States	dover.idf.il(old)	ET DROP Dshield Block Listed Source	1
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
61.161.130.241	147.237.0.17	China	m.my-kosher-kravi.idf.il	SERVER-APACHE Apache Tomcat Web Application Manager access	1
40.76.60.239	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1
40.76.60.239	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
40.76.60.239	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
5.100.253.185	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.59.148.210	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
93.174.93.50	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
50.198.75.25	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	88
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
216.178.86.18	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
199.30.24.224	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
80.178.1.215	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
46.19.85.24	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
5.22.131.120	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
87.69.122.69	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.52	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.183.6.107	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.250.25.183	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.52	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.149.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.176.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.69.122.69	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.52	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.131.5	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
208.115.113.89	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
37.26.148.240	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
37.239.68.34	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.39.177	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
91.200.12.85	Ukraine	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
192.241.189.66	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
41.102.19.249	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
65.55.210.190	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.93.249	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.109.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.30.76	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.178.145.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.142.149	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.144.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.89	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.210.163	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.11.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.186.50	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.53.61.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
122.3.171.66	Philippines	147.237.0.15	kosher-kravi.idf.il	drop	First packet isn't SYN	drop	3
66.249.78.153	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.23.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
208.54.36.169	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.206	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.242.14	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.65.229.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.154.189.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.153	Israel	147.237.72.166	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
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.146	Block	10
82.166.247.200	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 82.166.247.200	Block	9
46.19.86.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.66.83.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.24	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
109.253.227.103	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
2.53.171.132	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
23.250.3.10	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	2
109.253.131.5	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	2
46.19.85.111	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
82.166.247.200	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to ww.navy.idf.il/templates/faq/mobile	Block	2
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to ww.aka.idf.il/sip_storage/files/0/6	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
85.250.25.183	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/login.aspx?moduleto goto=0	Block	1
163.172.13.244	United Kingdom	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/atal1/izkor/view_img.asp	Block	1
80.178.1.215	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in www.aka.idf.il/chanatz/klali/default.asp	None	1
143.160.252.27	South Africa	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4616.jpg	Block	1
46.116.109.6	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/general/mobile	Block	1
85.250.25.183	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	1
68.180.229.89	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to ww.aka.idf.il/valtam	Block	1
199.59.148.210	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/8/size220x0/16838.jpg	Block	1
66.249.66.156	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
109.253.131.5	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
80.246.139.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in www.aka.idf.il/kamlar/kishur/default.asp	None	1
148.251.176.212	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
46.121.209.57	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/57056.pdf&ved=0ahukewj88mpmt6f mahuc_iwkhwtar4qfggdmai&usg=afqjcnf1yolugsboijblzxiye0gplabog&sig2=sljt3vnb9hu32rwugzqe5w	Block	1
87.71.84.165	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1115-ar/dover.aspx	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
213.8.204.50	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gius	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docid in www.aka.idf.il/giyus/yahash/login/	None	1
157.55.39.119	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
61.161.130.241	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/manager/html	Block	1
109.64.131.147	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/https://mobile.idf.il/	Block	1
71.6.146.185	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
213.113.202.189	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/894-en/idfgdover.aspx	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.254	Block	1
163.172.13.244	United Kingdom	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 163.172.13.244	Block	1
61.161.130.241	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/manager/html	Block	1
2.53.9.71	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
109.65.229.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
80.178.1.215	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/https://www.idf.il/	Block	1