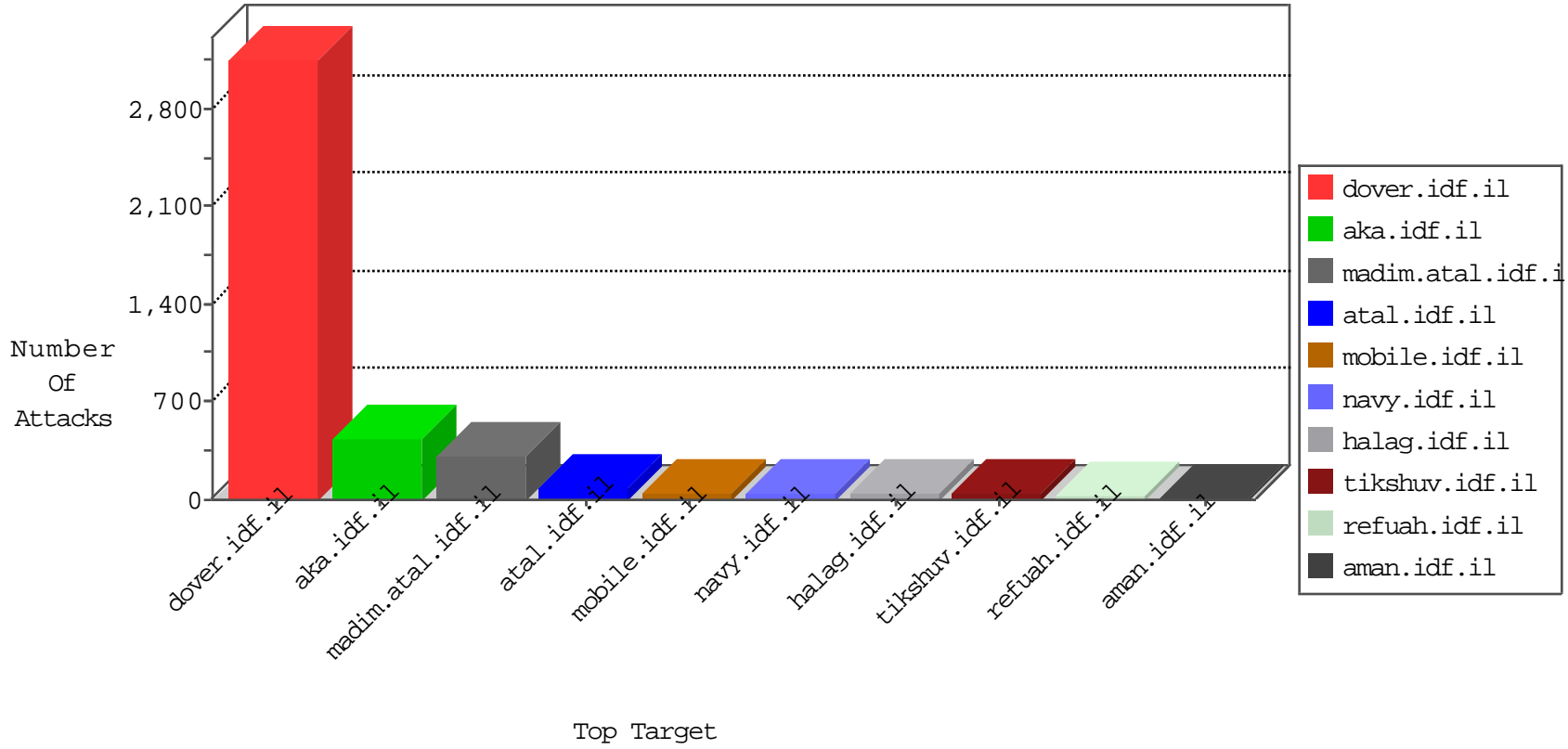


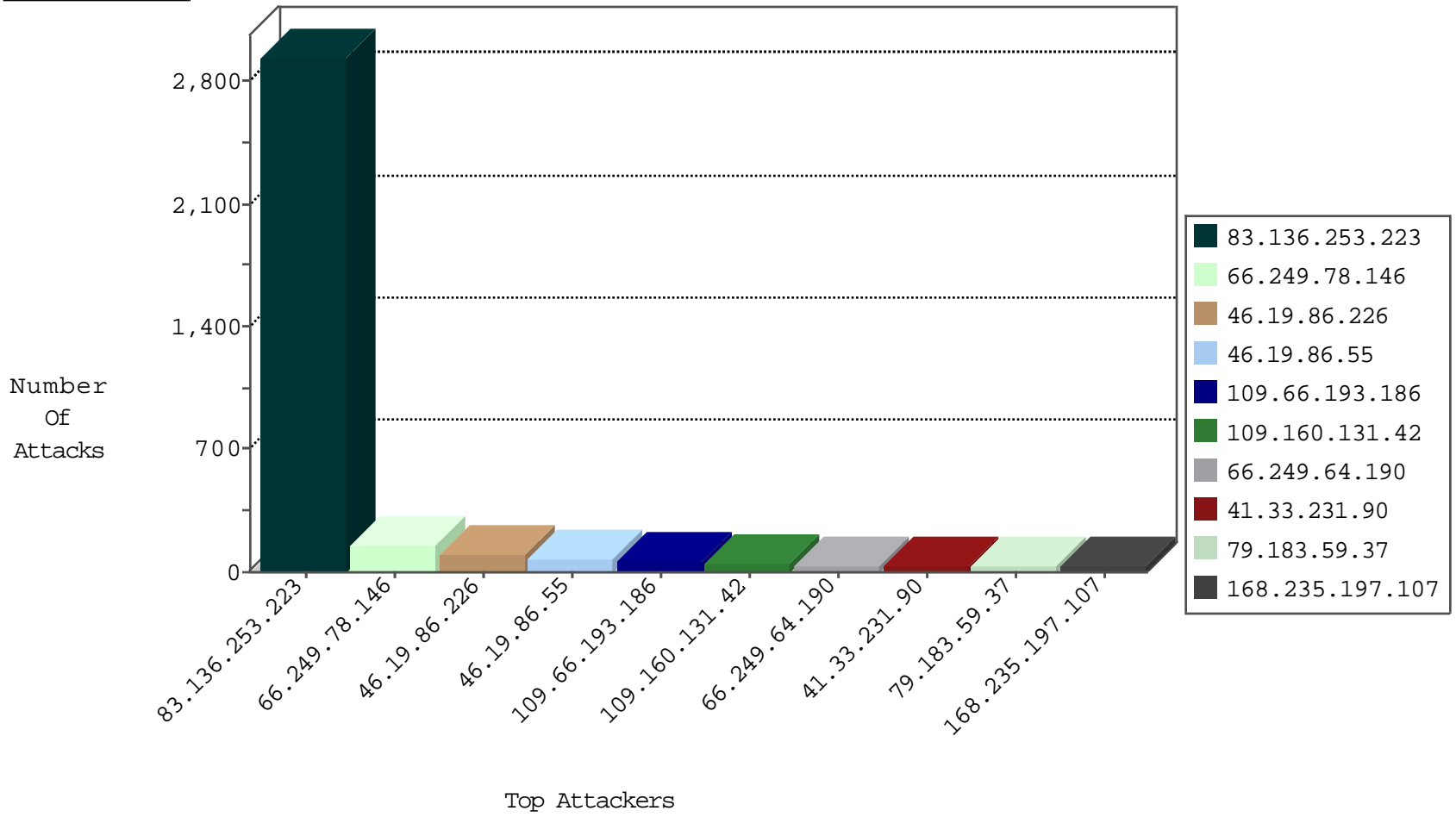
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
83.136.253.223	United Kingdom	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	85
83.136.253.223	United Kingdom	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
168.235.197.107	United States	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
168.235.197.107	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
123.130.244.58	China	147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
200.160.6.137	Brazil	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	2
83.136.253.223	United Kingdom	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
205.209.185.11	United States	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1
188.138.102.50	Germany	147.237.8.45	e.eitan.idf.il	Block_Udp_All_Nets	drop	1
151.225.249.172	United Kingdom	147.237.77.19	law-forum.idf.il	Block_Udp_All_Nets	drop	1
188.138.102.50	Germany	147.237.8.46	e.chinuch.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.121.63.115	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
185.3.147.63	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
46.19.86.196	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
46.19.86.6	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
213.57.155.171	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
109.65.192.38	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.165.197.141	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
134.249.53.96	Ukraine	147.237.76.147	chinuch.aka.idf.il	C1000016: HTTP: administrator in URI	Block	1
157.55.39.92	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
40.77.167.26	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	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
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
82.117.208.243	147.237.72.167		ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
198.180.198.185	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
186.114.17.231	147.237.76.31	Colombia	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
113.53.106.72	147.237.76.86	Thailand	navy.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
112.196.49.101	147.237.77.243	India	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
89.255.21.58	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential SSH Scan	1
60.153.108.23	147.237.0.33	Japan	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
198.180.198.185	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 3072	1
183.56.166.188	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
112.196.49.101	147.237.77.243	India	mobile.idf.il	ET SCAN NMAP -sS window 2048	1
112.196.49.101	147.237.77.243	India	mobile.idf.il	ET SCAN NMAP -f -sS	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
83.136.253.223	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2915
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	98
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
79.183.59.37	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
109.64.16.105	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	31
38.111.147.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
168.235.197.107	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
46.116.251.77	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
79.181.30.187	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
2.54.177.46	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
83.136.253.223	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
109.253.128.250	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.180.198.66	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
5.102.254.88	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.176.134.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.177.22.93	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.66.16.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.121.73.117	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.16	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.76	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
109.253.144.246	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.10.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.89.217.229		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
109.67.114.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.202.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.142.68.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.142.87	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
81.227.21.246	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
194.30.134.180	Cyprus	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
2.54.132.89	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.67.101.204	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.102	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.89.217.230		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
5.102.254.19	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.94.126.249	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
188.120.154.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.89.217.228		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
149.88.205.189	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
188.120.148.137	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.178.6.123	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.181.30.187	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
2.54.185.190	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
168.235.197.107	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
149.88.205.189	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
5.22.131.123	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.245.232	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	96
46.19.86.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
109.160.131.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
109.66.193.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
66.249.78.146	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.146	Block	40
46.19.86.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
66.249.64.190	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.190	Block	14
109.253.146.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
217.132.48.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.144.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.194.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.108.49.199	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
62.90.251.110	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/	Block	2
149.88.205.189	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.253.128.250	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
89.138.36.110	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	2
132.76.50.5	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/7/size338x0/1877.jpg	Block	2
185.3.144.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.66.193.186	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	2
5.102.254.88	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
37.26.148.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.78.146	United States	147.237.72.166	aka.idf.il	Unknown Parameter newsItem in www.aka.idf.il/megurim/news/	None	1
109.253.217.170	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.69.143	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
95.43.241.10	Bulgaria	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
40.77.167.28	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.127.161.91	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/	Block	1
66.249.78.146	United States	147.237.72.166	aka.idf.il	Unknown Parameter doc in www.aka.idf.il/kamlar/klali/default.asp	None	1
24.154.163.183	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.176	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/1321-he/asp.aspx.	Block	1
84.108.175.1	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
37.26.148.175	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.79.75	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
128.30.52.90	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/portalmiluim/templates/home.asp	Block	1
66.249.64.98	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluim/hebrew/asp/default.asp	Block	1
109.65.117.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.180.198.66	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.78.146	United States	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/shalishut/site/contactus.aspx	None	1
31.154.248.181	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
149.88.205.189	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.142.64.97	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
68.180.228.95	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakchal.idf.il/1100-he/nakchal.aspx	Block	1
66.249.78.146	United States	147.237.72.166	aka.idf.il	Unknown Parameter Do... in www.aka.idf.il/giyus/kadatz/	None	1
66.249.64.166	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
79.183.59.37	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	United States	147.237.72.166	aka.idf.il	Unknown Parameter gt; in www.aka.idf.il/main/rabanut/general.aspx	None	1
31.168.218.69	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mivtza	Block	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/kamlar/klali/default.asp	None	1