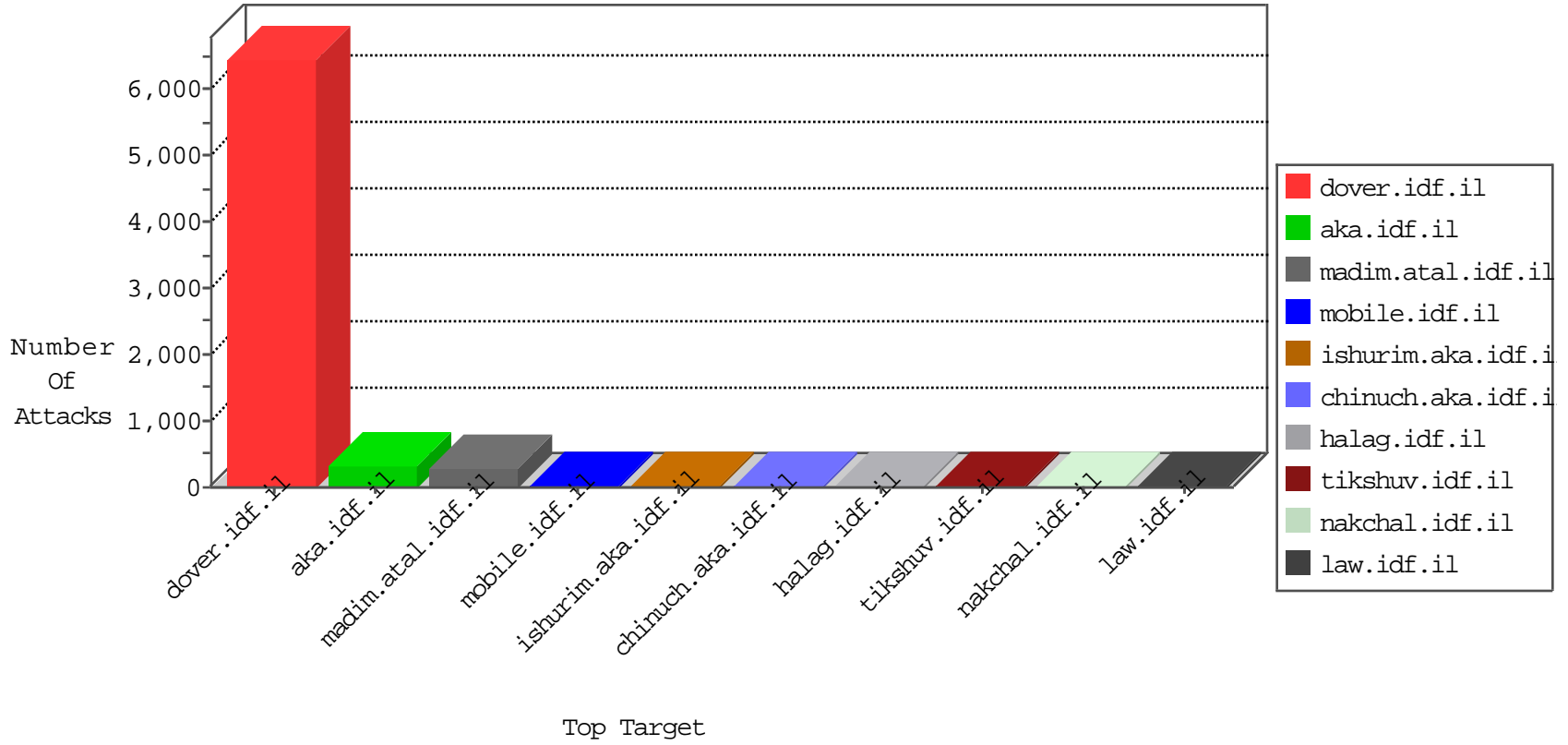


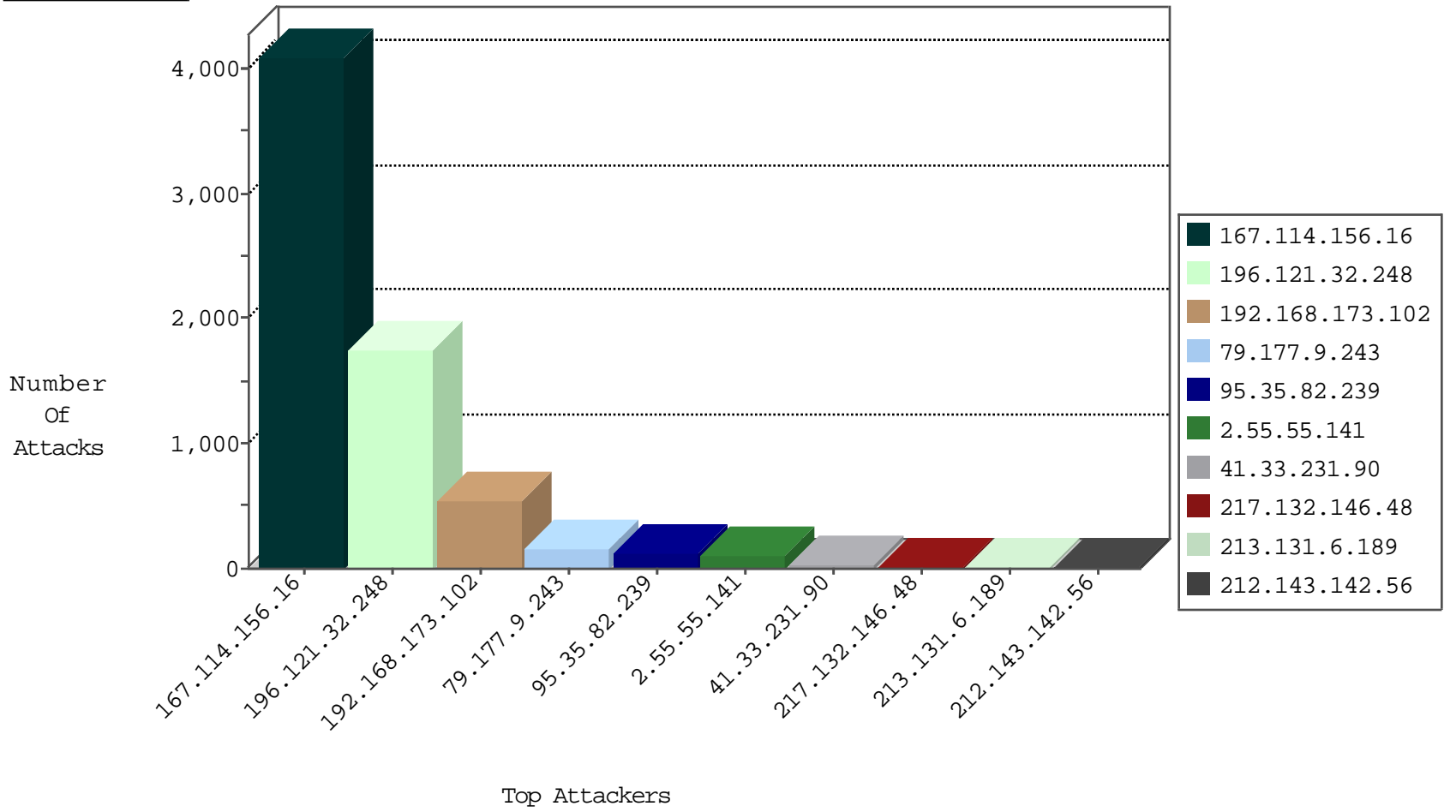
# IDF Under Attack Daily Report



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	4082
196.121.32.248	Morocco	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	16
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
192.96.201.142	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
115.159.150.148	China	147.237.8.45	e.eitan.idf.il	Invalid TCP Flags	drop	1
82.145.217.251	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	1
110.76.40.33	China	147.237.76.30	himush.idf.il	Invalid TCP Flags	drop	1
192.96.201.142	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
123.56.26.146	China	147.237.0.16	my-kosher-kravi.idf.il	I4 Source or Dest Port Zero	drop	1
91.15.199.144	Germany	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
179.43.144.50	Switzerland	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
115.159.150.148	China	147.237.0.19	madim.atal.idf.il	Invalid TCP Flags	drop	1
123.56.26.146	China	147.237.8.28	e.mobile-ks.idf.il	I4 Source or Dest Port Zero	drop	1
91.15.206.194	Germany	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
179.43.144.50	Switzerland	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
115.159.150.148	China	147.237.0.19	madim.atal.idf.il	I4 Source or Dest Port Zero	drop	1
219.232.243.28	China	147.237.0.33	idf.il	I4 Source or Dest Port Zero	drop	1
123.56.26.146	China	147.237.76.39	mobile.meitav.idf.il	Invalid TCP Flags	drop	1
91.15.206.194	Germany	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.142.245.132	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
51.255.162.164	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
144.76.8.132	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	2
51.255.162.164	France	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
176.13.11.20	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.78.96	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
183.60.48.25	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
141.101.178.137	147.237.8.45	Russian Federation	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 1024	1
213.131.6.189	147.237.76.147	Russian Federation	chinuch.aka.idf.il	ET WEB_SERVER Poison Null Byte	1
141.101.178.137	147.237.8.46	Russian Federation	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
122.52.127.9	147.237.76.44	Philippines	e.refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
50.60.153.98	147.237.77.234	United States	halag.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
196.121.32.248	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1733
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	337
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	195
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	14
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
5.22.129.233	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
95.10.213.250	Turkey	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
157.55.39.109	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.13.0	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
37.142.64.106	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.71.168.236	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.137.59	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.41.128.34	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.117.152.29	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
95.210.108.138	Spain	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
112.198.242.65	Philippines	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
64.233.172.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.181.222.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.41.52	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.27.105.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.44.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.39.26	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.182.166.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.21.217	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.125.125.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.64.122.199	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
5.22.135.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.117.34	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
196.121.32.248	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
2.52.128.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.95.252.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.164.46	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.9.243	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.114.23.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.39.97	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
85.64.122.199	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
5.28.164.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.178.17.30	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.224.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.64.122.199	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
2.53.44.26	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
185.27.105.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.237.209	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.197	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
84.109.118.211	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.19.85.62	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
31.210.187.82	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.147.126	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.19.85.175	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.9.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	153
95.35.82.239	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.35.82.239	Block	118
2.55.55.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	92
217.132.146.48	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	16
5.29.191.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.253.136.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
66.102.8.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
79.182.185.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
157.55.39.49	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
66.102.8.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
79.183.117.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
95.52.122.236	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ https://twitter.com/	Block	2
109.64.6.19	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	2
109.253.132.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.55.16.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
41.107.213.186	Algeria	147.237.77.216	dover.idf.il	Parameter Type Violation ID in ww.idf.il/1294-ar/dover.aspx	Block	2
196.121.32.248	Morocco	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	2
41.226.169.145	Tunisia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
217.69.133.243	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gyius/hebrew	Block	1
157.55.39.109	United States	147.237.72.166	aka.idf.il	Unknown Parameter KEY in www.aka.idf.il/ishurim/cityofficers/	None	1
5.10.229.226	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
213.131.6.189	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Illegal Byte Code Character in Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]][[#3]][[#3]][[#8]]•δç%úêDr çL.UùQîpyi•V7"*èÏc;o80y[[#0]][[#0]][[#28]]Ä/Ä+Ä0Ä,Ä[[#19]]Ä	Block	1
199.167.129.140	Canada	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
176.111.109.155	Portugal	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
114.97.56.215	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1043-11784-ar/cogat.aspx/trackback/	Block	1
5.157.57.45	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
213.131.6.189	Russian Federation	147.237.76.147	chinuch.aka.idf.il	NULL Character in Header Name at [[#0]]æ[[#0]]•[[#0]]/[[#0]]5Ä[[#18]][[#0]]	Block	1
212.14.228.126	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
91.224.13.64	Latvia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
192.40.57.129	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/gyius/general.aspx	Block	1
46.121.221.12	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
157.55.39.194	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/valtam/main/personalentrance.asp	Block	1
213.131.6.189	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Illegal Byte Code Character in URL [[#20]]	Block	1
204.79.180.163	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
177.98.5.225	Brazil	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
141.212.122.129	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to /x	Block	1
37.235.53.238	Spain	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
213.131.6.189	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Illegal Byte Code Character in Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]][[#3]][[#3]][[#8]]•δç%úêDr çL.UùQîpyi•V7"*èÏc;o80y[[#0]][[#0]][[#28]]Ä/Ä+Ä0Ä,Ä[[#19]]Ä	Block	1
2.54.164.145	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.57.128.53	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
93.172.135.82	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
66.249.93.78	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
193.182.144.142	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
46.246.89.243	Sweden	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
217.148.44.140	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
158.255.208.29	Hong Kong	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
5.34.183.55	Ukraine	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
213.131.6.189	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Illegal HTTP Version	Block	1