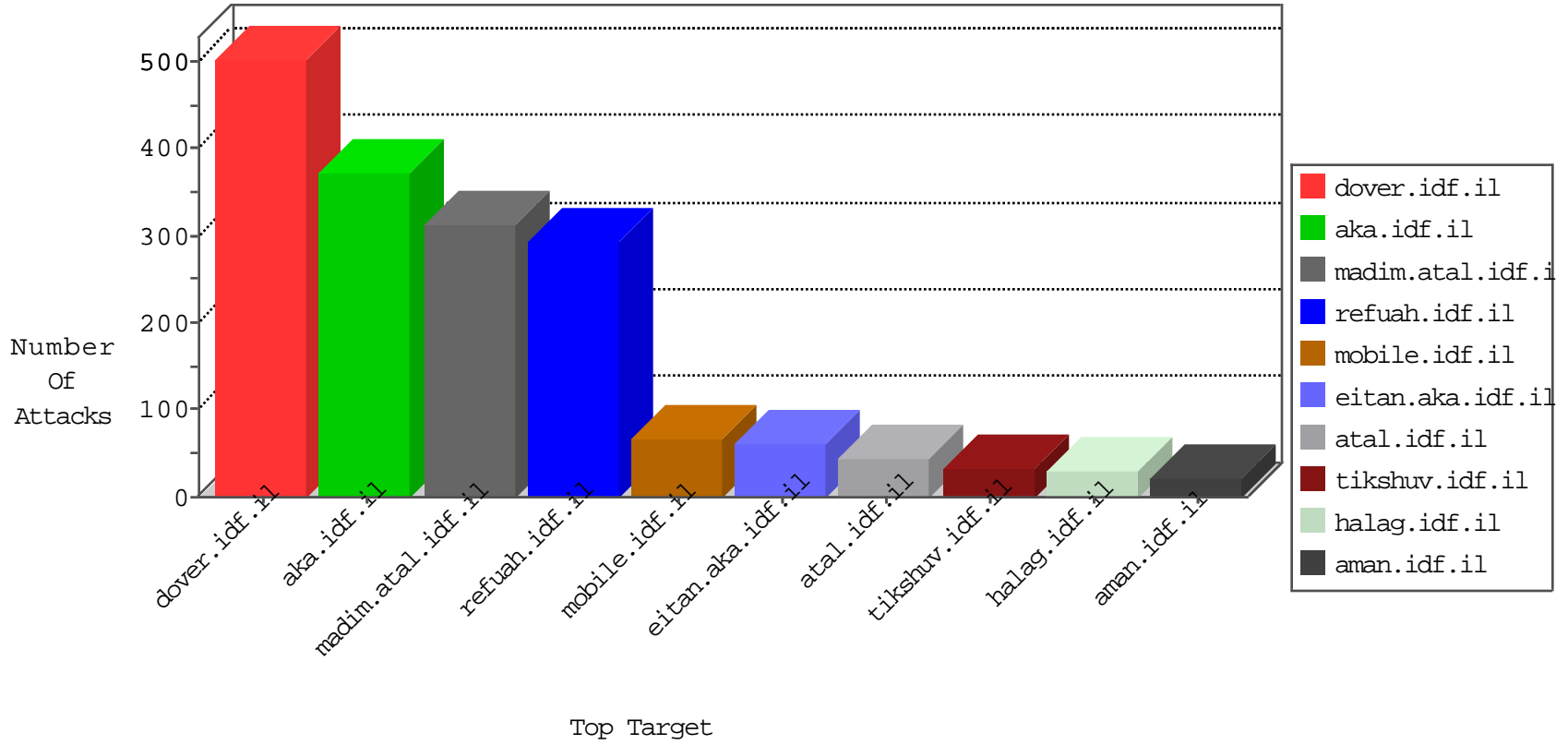


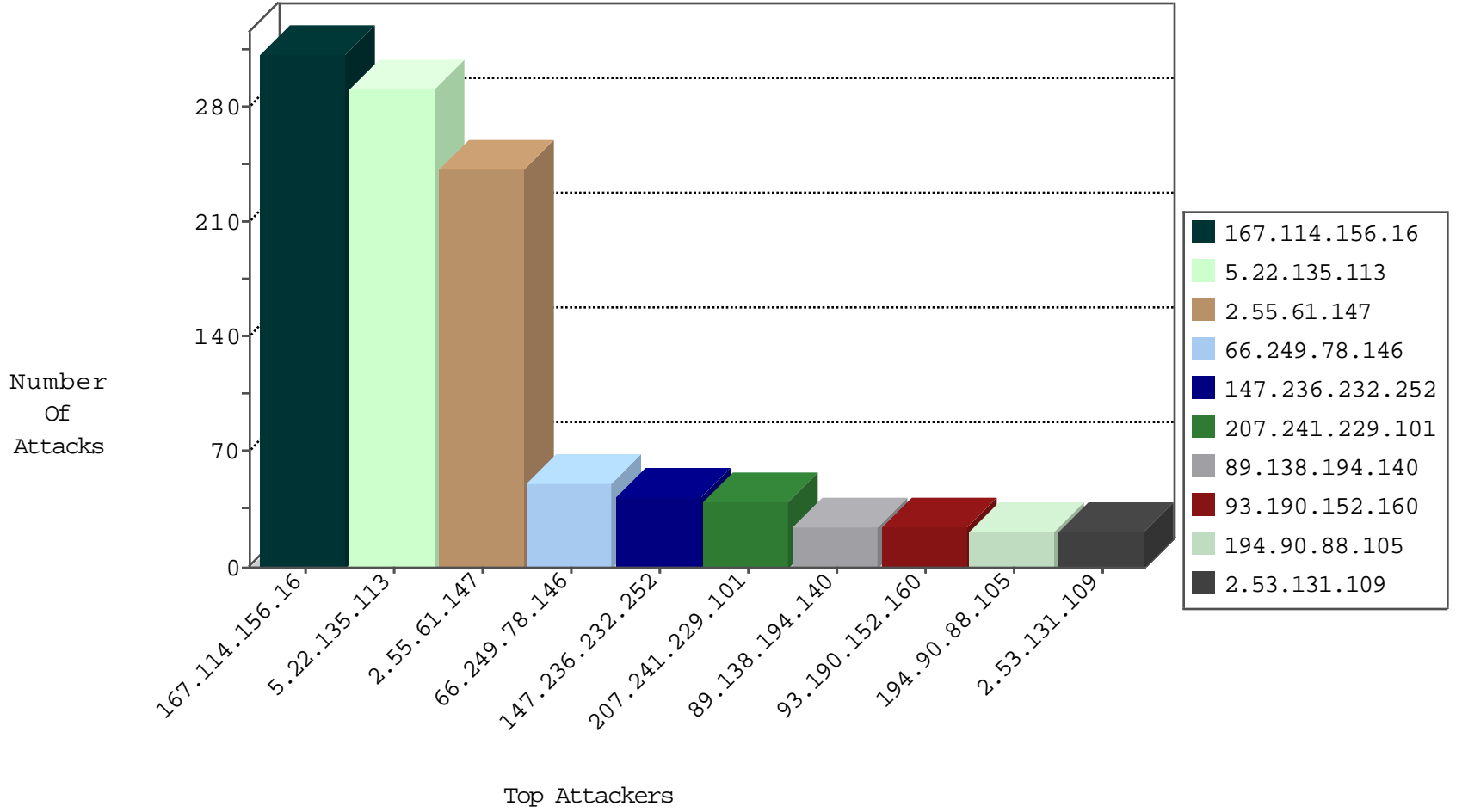
IDF Under Attack Daily Report



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	18506
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6314
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	4607
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	61
79.179.187.22	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
192.118.132.185	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	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
134.147.203.115	Germany	147.237.76.176	test.ncore.idf.i	Block_Ntp_All_Net	drop	2
71.6.135.131	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
67.228.38.74	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
67.228.38.74	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
133.242.52.175	147.237.72.166	Japan	aka.idf.il	ET WEB_SERVER Poison Null Byte	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.22.135.113	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	283
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
207.241.229.101	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	40
93.190.152.160	Europe	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
194.90.88.105	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
2.53.131.109	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
146.185.56.202	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
37.26.149.142	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
212.117.151.42	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
194.90.217.102	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
87.70.130.74	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.53.58.0	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.209	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
89.138.194.140	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
80.179.225.42	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
85.130.216.127	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
89.138.194.140	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
89.138.194.140	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
31.168.101.163	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
62.90.99.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.93.245	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.250.152.92	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.86.131	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.12	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
5.28.150.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.139.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.176	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.22.135.113	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
54.86.207.189	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.65.114.53	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
193.104.77.4	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.176	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.93.182	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.14.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
212.106.78.71	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.130.216.127	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
147.236.232.252	Israel	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.53.28.88	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.100	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
109.253.227.81	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	4
82.205.90.29	Palestinian Territory, Occupied	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.102	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.61.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	242
147.236.232.252	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 147.236.232.252	Block	26
185.120.125.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
84.109.115.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
147.236.232.252	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 147.236.232.252	Block	9
46.19.86.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
2.53.17.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
46.19.85.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.53.131.109	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.75	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	4
2.53.26.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.216.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.179.114.27	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	3
37.26.149.142	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.205	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/general/mobile	Block	2
134.191.232.68	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
2.53.55.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
147.236.232.252	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/templates/general/mobile	Block	2
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.176.2.84	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.176.2.84	Block	2
2.53.15.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.102.6.191	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.86.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.67.17.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
133.242.52.175	Japan	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name [[#0]]e[[#0]]•[[#0]]/[[#0]]5Å[[#18]][[#0]]	Block	1
46.120.242.60	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct109 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
212.76.115.141	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
87.69.100.176	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1440-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Abnormally Long Request method	Block	1
79.177.14.5	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
133.242.52.175	Japan	147.237.72.166	aka.idf.il	NULL Character in Header Name at	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
46.19.86.60	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
84.110.53.213	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
151.80.31.104	France	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
133.242.52.175	Japan	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]][[#3]][[#3]]86İ+PÜCñf-svëY[[#30]]!Rj•D@[[#26]] Æ:B*ò*Ql[[#0]][[#0]][[#28]]Å/Å+À0À,Å[[#19]]Å	Block	1
62.219.21.55	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.70.130.74	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Illegal Byte Code Character in Method ÄYË'<'5n?•#;_gòr*v³¤<€; [[#27]]É+#ÉÜhùL{çRÚ[[#8]]PZ*Ó"Öjà	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/listpage/	Block	1
133.242.52.175	Japan	147.237.72.166	aka.idf.il	NULL Character in Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]][[#3]][[#3]]86İ+PÜCñf-svëY[[#30]]!Rj•D@[[#26]] Æ:B*ò*Ql[[#0]][[#0]][[#28]]Å/Å+À0À,Å[[#19]]Å	Block	1
46.19.86.75	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.19.86.75	Block	1
195.112.235.59	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/894-he/chinuch.aspx	Block	1
118.193.163.150	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
84.110.53.213	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.44	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/894-he/atal.aspx	Block	1
68.180.229.89	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/yohalan/main/faq.asp	Block	1
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1