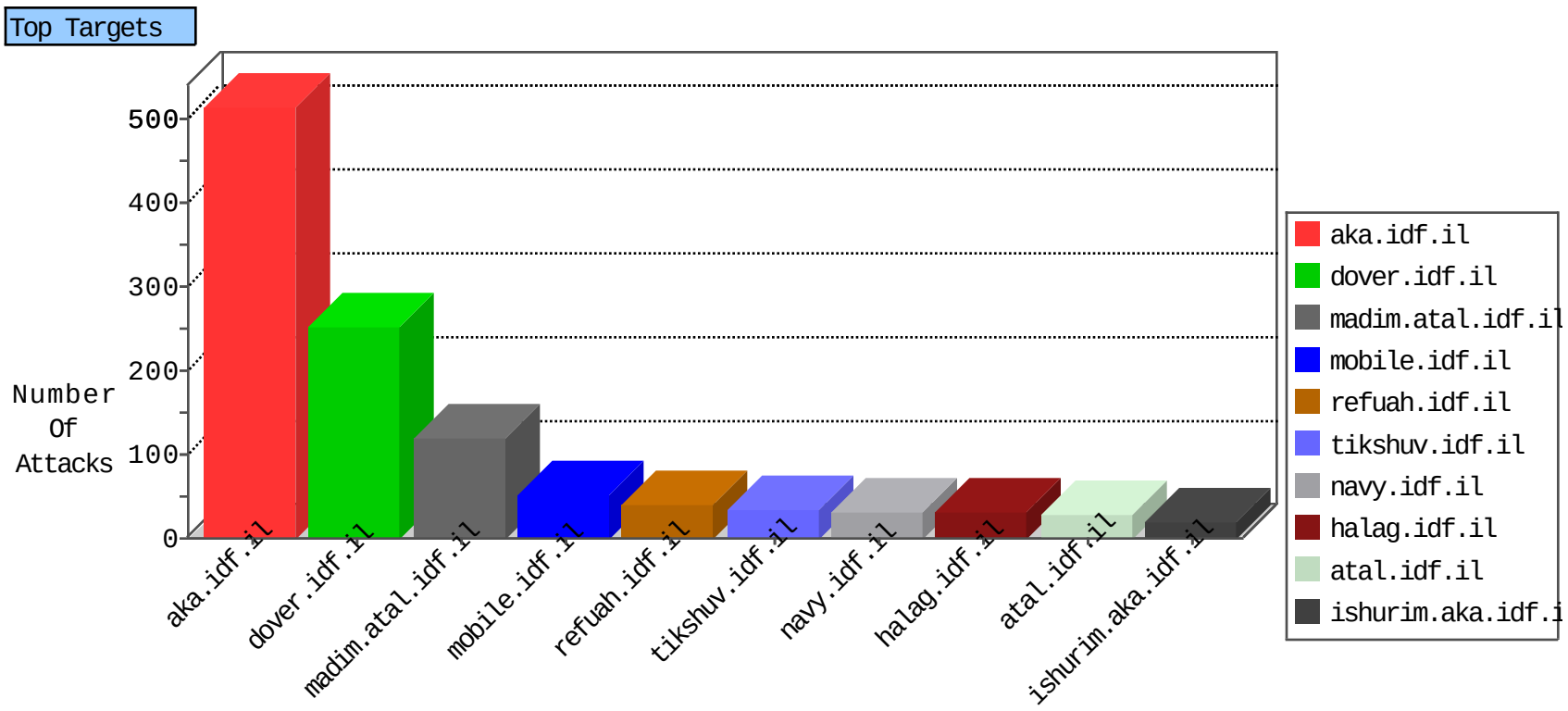
02-27-2016-19:04:05 to 02-27-2016-20:04:05

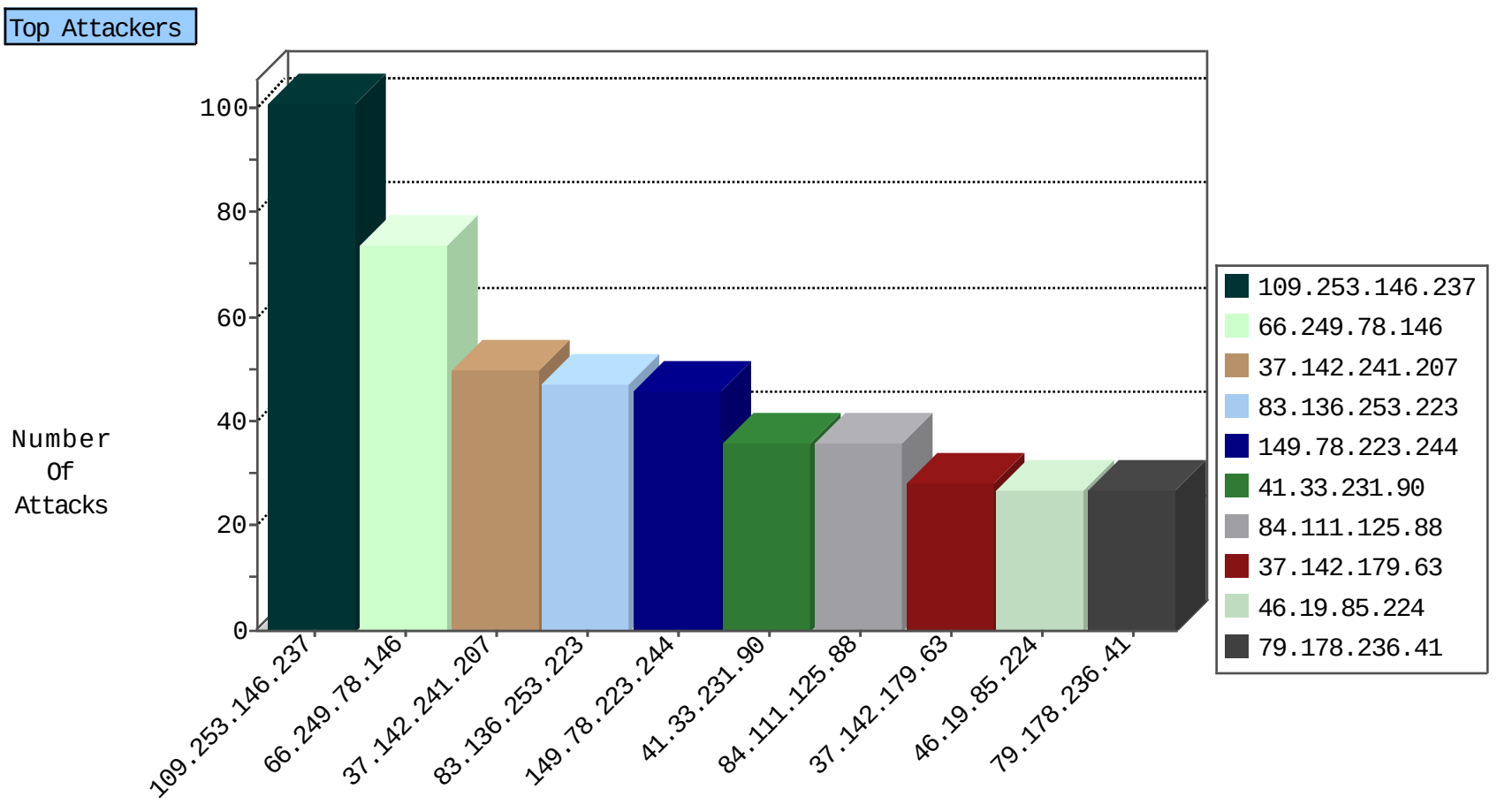
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-27-2016-19:04:05 to 02-27-2016-20:04:05

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	82
84.111.125.88	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	36
83.136.253.223	United Kingdom	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
79.177.230.247	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
83.136.253.223	United Kingdom	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
134.147.203.115	Germany	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	2
85.105.108.6	Turkey	147.237.77.205	prisha.idf.il	Block_Udp_All_Nets	drop	1
205.209.185.11	United States	147.237.77.61	e.cogat.idf.il	Block_Ntp_All_Net	drop	1
114.222.91.99	China	147.237.77.74	law.idf.il	Block_Udp_All_Nets	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
198.20.70.114	United States	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	1

02-27-2016-19:04:05 to 02-27-2016-20:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.135.127	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
199.30.24.72	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
84.94.41.65	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
31.168.211.194	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
37.142.68.121	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
36.110.147.106	China	147.237.77.216	dover.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
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

02-27-2016-19:04:05 to 02-27-2016-20:04:05

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
132.74.95.19	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
213.238.176.44	147.237.76.39	Turkey	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.76.34	China	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
114.112.90.54	147.237.77.74	China	law.idf.il	SERVER-APACHE Apache SSI error page cross-site scripting	1

02-27-2016-19:04:05 to 02-27-2016-20:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
79.178.236.41	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
37.142.241.207	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
37.142.241.207	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	25
79.176.4.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
2.54.165.197	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
83.136.253.223	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
83.136.253.223	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
37.142.179.63	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
37.142.179.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
109.64.16.105	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
37.142.242.226	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
176.13.17.50	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.130.75	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
79.177.121.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.224	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.72	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.173	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.9	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
217.132.111.142	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.173	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
77.125.240.161	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.178.134.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.84	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.6.63	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.54.58.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.248	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
31.210.179.115	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.179.167.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.248	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.67.114.28	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
41.47.17.249	Egypt	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.224	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
5.102.242.164	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
185.89.217.234		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
217.132.36.234	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.134.190.239	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.3.147.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
77.125.6.63	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4

02-27-2016-19:04:05 to 02-27-2016-20:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.146.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	101
66.249.78.146	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.146	Block	32
66.249.64.190	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.190	Block	7
109.253.216.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
149.78.223.244	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 149.78.223.244	Block	4
149.78.223.244	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 149.78.223.244	Block	4
149.78.223.244	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 149.78.223.244	Block	4
176.13.17.50	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
149.78.223.244	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 149.78.223.244	Block	4
149.78.223.244	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 149.78.223.244	Block	4
149.78.223.244	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 149.78.223.244	Block	3
149.78.223.244	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 149.78.223.244	Block	3
109.65.153.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
149.78.223.244	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 149.78.223.244	Block	3
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
2.52.147.149	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
82.166.22.37	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 82.166.22.37	Block	2
66.249.79.75	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.75	Block	2
172.98.85.253		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
149.78.223.244	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 149.78.223.244	Block	2
37.26.146.156	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.65.124.249	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
5.102.242.195	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
109.253.211.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
149.78.223.244	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Method from 149.78.223.244	Block	2
37.26.146.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.181.241.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/controls/atuda/	Block	2
46.116.253.102	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
31.154.248.181	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
149.78.223.244	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL o´cb[[#7]]•[[#24]]§Ÿ•=¥Ê[[#30]]mÙ;[[#30]]‹no&ℸn[[#1]][[ℸ#26λ]]¡„	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/jenin.stm)	Block	1
178.255.215.87	France	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
114.112.90.54	China	147.237.77.74	law.idf.il	Illegal Host Name	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/faq.aspx	None	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unauthorized Method GET for www.aka.idf.il/navy/navy/crafttab/technicalparameters.aspx	Block	1
149.78.223.244	Israel	147.237.72.166	aka.idf.il	NULL Character in Header Name at [[#0]]y[[#19]]•[[#20]]®ÉhÌ£v¸q¼[[#18]]S~®Ž¥iPÖÒ[[#4]] ~8è…ç	Block	1
105.155.141.240	Morocco	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.178.134.53	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
37.142.68.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.79.20	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/general/general.aspx	Block	1
5.22.129.234	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/1132-8953-he/navy.aspx#.vtbcmnea2x8.facebook	Block	1
149.78.223.244	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
109.160.206.179	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/home.aspx	Block	1
172.98.85.79		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
93.173.1.220	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.117.61.166	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1
31.210.179.115	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
149.78.223.244	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version	Block	1
66.249.78.146	United States	147.237.72.166	aka.idf.il	Unknown Parameter docId91 in www.aka.idf.il/patzar/klali/default.asp	None	1
199.30.24.198	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

02-27-2016-19:04:05 to 02-27-2016-20:04:05