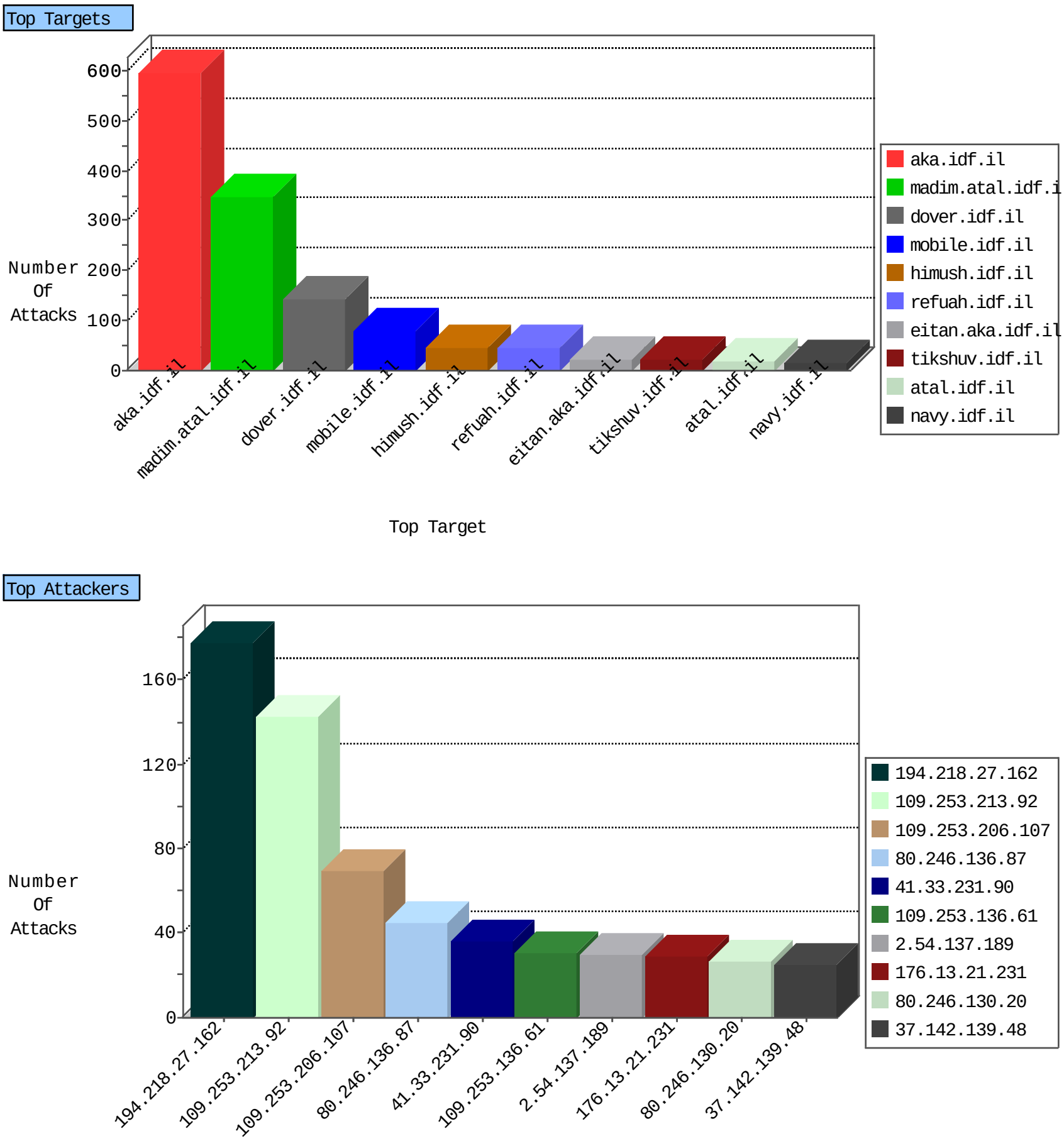
02-29-2016-08:04:05 to 02-29-2016-09:04:05

IDF Under Attack
Daily Report



02-29-2016-08:04:05 to 02-29-2016-09:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.23.141.210	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	1
198.23.141.210	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
198.23.141.210	United States	147.237.77.235	sviva.idf.il	Block_Ntp_All_Net	drop	1
184.105.247.211	United States	147.237.72.217	e.idf.il	Block_Udp_All_Nets	drop	1
198.23.141.210	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
208.67.1.130	United States	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	1
184.105.247.211	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
198.23.141.210	United States	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.201		147.237.77.226	www.chamatz.aka.idf.il	Block_Udp_All_Nets	drop	1

02-29-2016-08:04:05 to 02-29-2016-09:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.183.152.62	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	16
66.249.64.180	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.216	dover.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
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

02-29-2016-08:04:05 to 02-29-2016-09:04:05

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	3
80.246.130.20	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
46.120.167.182	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.84	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.211.102.129	147.237.0.16	Russian Federation	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
212.179.90.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.3.144.45	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.78.224.174	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.198.164	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.178.234.99	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.196	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.130	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
176.13.22.112	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
88.35.115.118	147.237.76.148	Italy	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1

02-29-2016-08:04:05 to 02-29-2016-09:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	116
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	60
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
109.253.136.61	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
185.99.32.3		147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
176.13.15.172	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.16.9	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.130.20	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
109.65.33.86	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
80.246.130.20	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.17	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
109.253.159.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.210.220.51	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.253.136.61	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
5.102.254.176	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
157.55.39.58	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
217.194.204.3	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
81.218.173.126	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
37.26.146.155	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
185.99.32.3		147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.49.62	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.204.113	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.150	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.217.94	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.166.114	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.35.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.55.93	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.139.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.33.86	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
217.194.199.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.8.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.150	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.53.66	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
40.77.167.23	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.139.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.177	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.124	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
207.46.13.110	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.93.248	Israel	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
37.26.149.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.176.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.23.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.172.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.131.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.23.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-29-2016-08:04:05 to 02-29-2016-09:04:05

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
79.177.48.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-29-2016-08:04:05 to 02-29-2016-09:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.213.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	143
109.253.206.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	70
80.246.136.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
2.54.137.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
176.13.21.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
176.13.4.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	7
46.121.75.164	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/shchar	Block	6
37.26.149.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.4.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
176.13.6.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
176.13.15.172	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
66.249.69.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	3
2.52.166.114	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.253.143.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.16.9	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
31.154.80.209	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	2
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.205	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
37.142.139.48	Israel	147.237.72.166	aka.idf.il	Too Many Headers per Request - 65 Headers	Block	1
37.26.146.148	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.136.61	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
37.142.139.48	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 37.142.139.48	Block	1
37.142.139.48	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL sע1[[ע$:#2[[]]#16[[!]]#4[[»‡]]#22ת]];i˙[[#25]]®'[[#8]]z¬ty˛1[[#6]]ƒm¦%т	Block	1
195.191.233.220	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/dover.aspx/	Block	1
66.249.78.87	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
37.26.148.188	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.35	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1
37.142.139.48	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 37.142.139.48	Block	1
37.142.139.48	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 37.142.139.48	Block	1
66.249.66.15	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1727	Block	1
37.142.139.48	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
180.76.15.163	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9757-he/refuah.aspx	Block	1
37.26.146.155	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 37.26.146.155 (Open Mode)	None	1
162.217.230.109	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.142.139.48	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method ^ŒK´¦¾WÂÉs%[[#0]]S=¾[[#7]]·Ú#Vñ*?•ERwßWžm…ð[[#15]]“D1ÛÂ•û'ú¤ in URL sע1[[ע$:#2[[]]#16[[!]]#4[[»‡]]#22ת]]	Block	1
37.142.139.48	Israel	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 37.142.139.48	Block	1
37.142.139.48	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version ª>õí[[#23]]Ëñ[[#5]]lJÄ•Cs}Ræ[[#8]]"[[#30]]³[[#8]]ÖuÜžj[[#25]]]î-[[#23]]&Ÿý÷%[[#8]]Rì¯·9Òånl«ã«ù…)5[[#8]]h<Àn¨ÚOãAh–{Þ¢@ˆVÙoþ÷[[#26]]æë[[#30]]Ç–þ=ñP[[#7]]ß9•i÷ÂN¾[[#22]][[#8]]õ{ÅÌÌ	Block	1
68.180.228.95	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakhal.idf.il/1108-he/nakhal.aspx	Block	1
37.26.148.219	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.195	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
37.142.139.48	Israel	147.237.72.166	aka.idf.il	NULL Character in Header Name at	Block	1
2.54.189.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
91.199.69.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter sbredirect in www.aka.idf.il/main/sachar/	None	1
37.142.139.48	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 37.142.139.48	Block	1
66.249.66.33	United States	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
37.142.139.48	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name	Block	1
184.105.247.195	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
37.26.146.155	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - 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

02-29-2016-08:04:05 to 02-29-2016-09:04:05