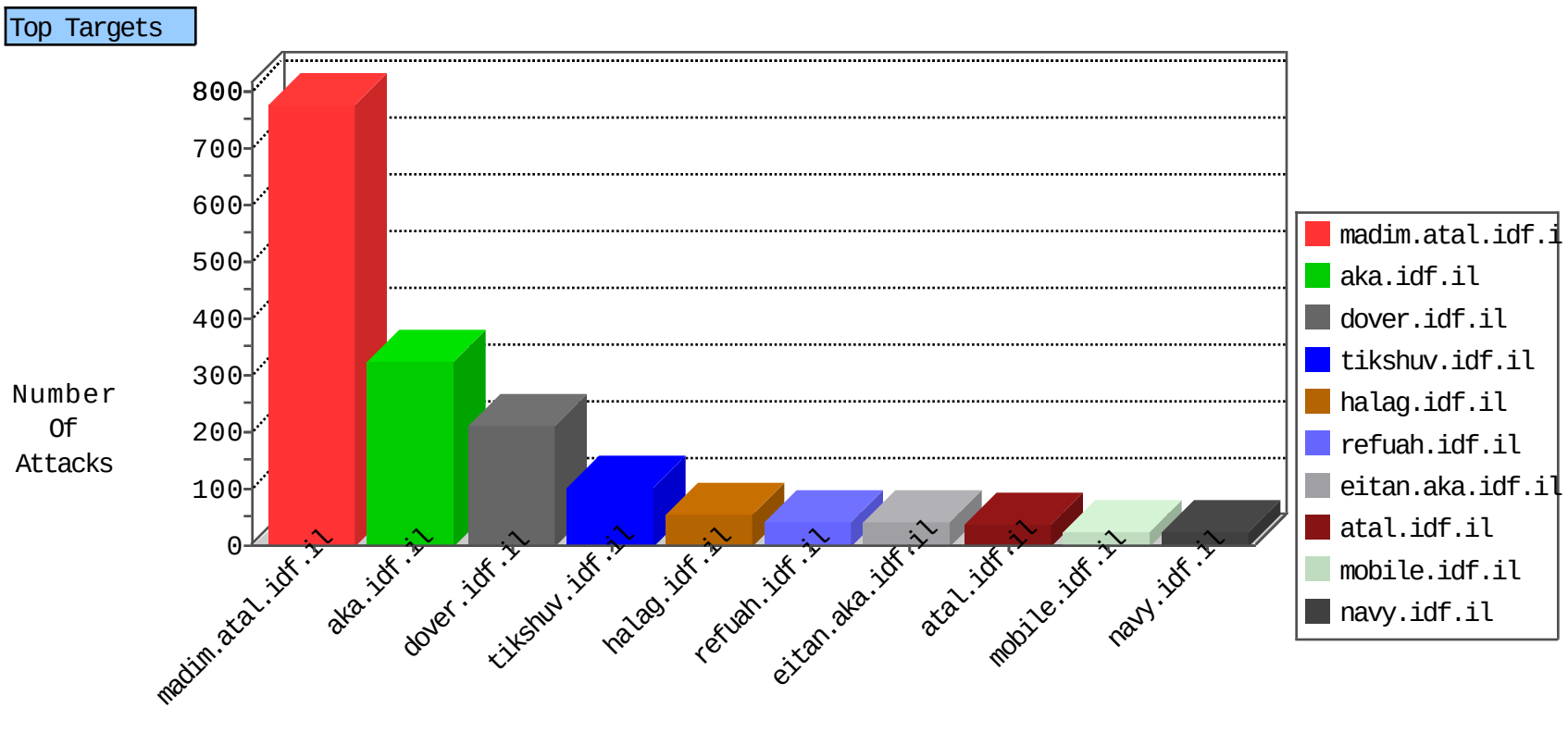
02-07-2016-10:04:09 to 02-07-2016-11:04:09

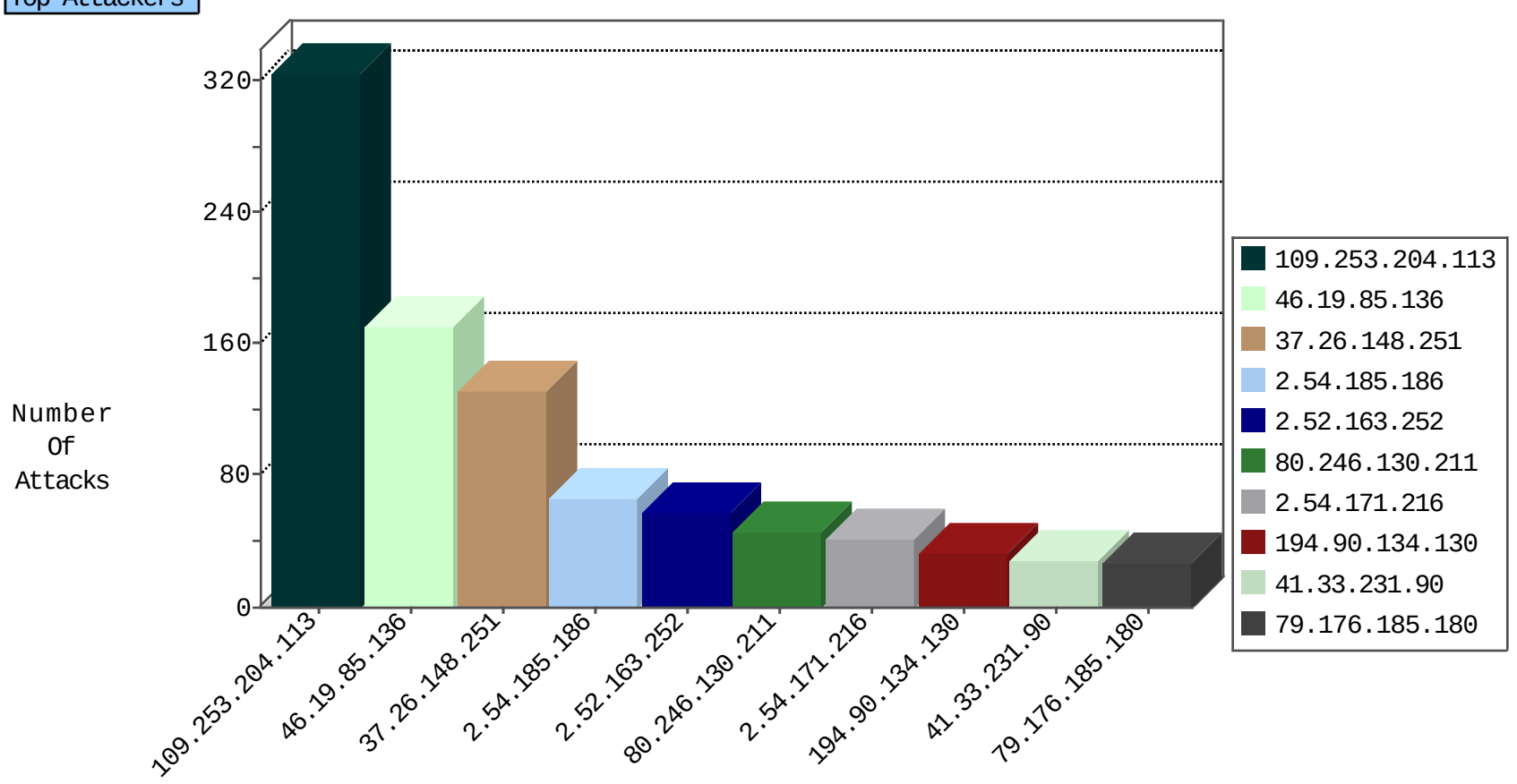
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-07-2016-10:04:09 to 02-07-2016-11:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	4
81.218.206.82	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
79.176.57.137	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
136.0.99.222	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
79.176.57.137	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
45.32.229.187		147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
85.64.2.166	Israel	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

02-07-2016-10:04:09 to 02-07-2016-11:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.26.251.210	Vietnam	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

02-07-2016-10:04:09 to 02-07-2016-11:04:09

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
80.74.100.131	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.196	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.86	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.78.222.186	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
147.236.33.66	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
128.139.19.171	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.212.27	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.63.202	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.197.61.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.158.224	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.179.18.61	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.127.10.42	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
37.46.38.29	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.15.74	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.78.183.172	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
136.0.99.222	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
114.112.90.54	147.237.72.156	China	aman.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.145.121	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.13.208	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-07-2016-10:04:09 to 02-07-2016-11:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.185.186	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
80.246.130.211	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	45
194.90.134.130	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	29
79.176.185.180	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
2.54.19.109	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
46.19.85.136	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.86.91	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	18
109.66.99.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
82.81.31.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
136.0.99.222	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.117.3.254	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.54.151.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.53	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
176.14.13.57	Russian Federation	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.86.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.117.3.254	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
85.64.2.166	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.23	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.168.249	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.127.215.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.7.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.81.183	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.67.234.83	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
176.13.9.231	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.147.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.218.203.202	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.29.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.24.206.38	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.26.149.230	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.169.97	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
141.0.13.59	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
85.64.2.166	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.39	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.125	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
192.116.95.240	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
81.218.116.129	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.150	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.78.233	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.78.239	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
62.90.161.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.103	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.253.156.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.178.128	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.65.107.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.4.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.230	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	3

02-07-2016-10:04:09 to 02-07-2016-11:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.204.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	172
37.26.148.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	94
46.19.85.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	85
109.253.204.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	81
109.253.204.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	71
46.19.85.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
2.52.163.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
2.54.171.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
37.26.148.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	38
46.19.85.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
176.13.11.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
212.179.140.133	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	5
46.19.86.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.22.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.27.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.144.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.10.99.200	Switzerland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-ar	Block	3
31.168.23.60	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.168.23.60	Block	3
80.246.130.145	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	2
37.26.149.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.17.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.80.196.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
31.154.19.5	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/secure/default.aspx	Block	2
2.52.163.109	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1381	Block	2
176.13.2.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	2
217.194.198.104	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
213.57.42.252	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/www.tikshuv.idf.il	Block	1
94.242.228.108	Luxembourg	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	1
171.25.193.78	Sweden	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/article/watch	Block	1
109.253.131.117	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method ÃŸzÂ″3[[#6]]ÂŠ+Â‹ [[#15]]Â±Ã¯[[#19]][[#31]]Â‡c[[#12]]	Block	1
84.228.175.102	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.168.23.60	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/titlecap.png	Block	1
192.116.95.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.179.13.253	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method ÃŸzÂ″3[[#6]]ÂŠ+Â‹ [[#15]]Â±Ã¯[[#19]][[#31]]Â‡c[[#12]] in URL Ö½Ã¿×¦×³_×§Â-v×¦â€?g×€ [[#0]]Ëœ×?×˜×¦â‚¬×™[[#31]]ÃŸÃ·Ãž×¦	Block	1
62.0.102.190	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
216.72.40.185	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$1 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
95.86.88.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/&sa=u&ved=0ahukewi6zmwdnexkahwr8xikhvqobsyqfggcmac&usg=afqjcnh4ucr3bqpmkvh4yz9t7jscutsloq	Block	1
80.246.130.211	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
2.54.174.222	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/miyun	Block	1
184.168.200.74	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/wordpress/wp-admin/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1414-he/dover.aspx	Block	1
174.136.50.3	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/wp/wp-admin/	Block	1
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version Ã?Ã‹Â‡#Ã™Hk;j*{Y4[[#1]]aoÂšzÂˆzÂ’$Ã·{Â³Ã– Â,Â—\ÃŽ#Â§UÃ,Ã«[[#18]] *&Â¼EÃ–Ã²d[[#26]]<Â¶gÃŸÃ¾%ÂƒÃ?Ã‡ÃžÃ«~Ã–YÃ¦Ã‹Â¦Ã NÂ’Ã¤[[#16]]{Ã¹8Â°_uwÃ¬[[#8]]-R^Â•Â JÃ—UÂ˜Ã§Ã,Ã¨/)-Â¯sÃ¿[[#0]]Ã²pPÂŽ\Â“Ã”Â˜:aÂ¼gÃ¶mnÃ¹[[#3]]=[[#15]]uÂŽ [[#12]]>'R*Ã?UÃŸ	Block	1
212.150.189.2	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
85.64.2.166	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1

02-07-2016-10:04:09 to 02-07-2016-11:04:09