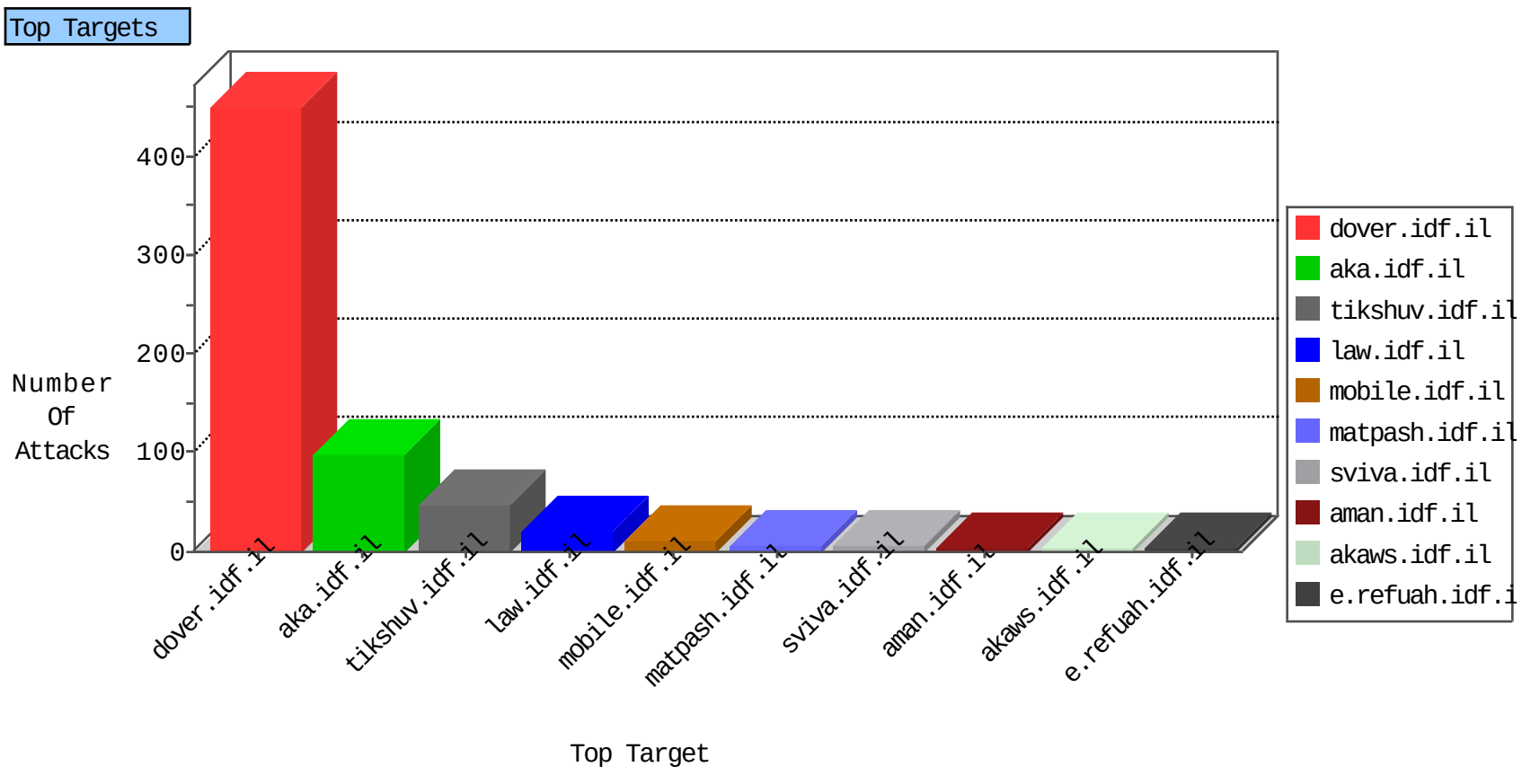
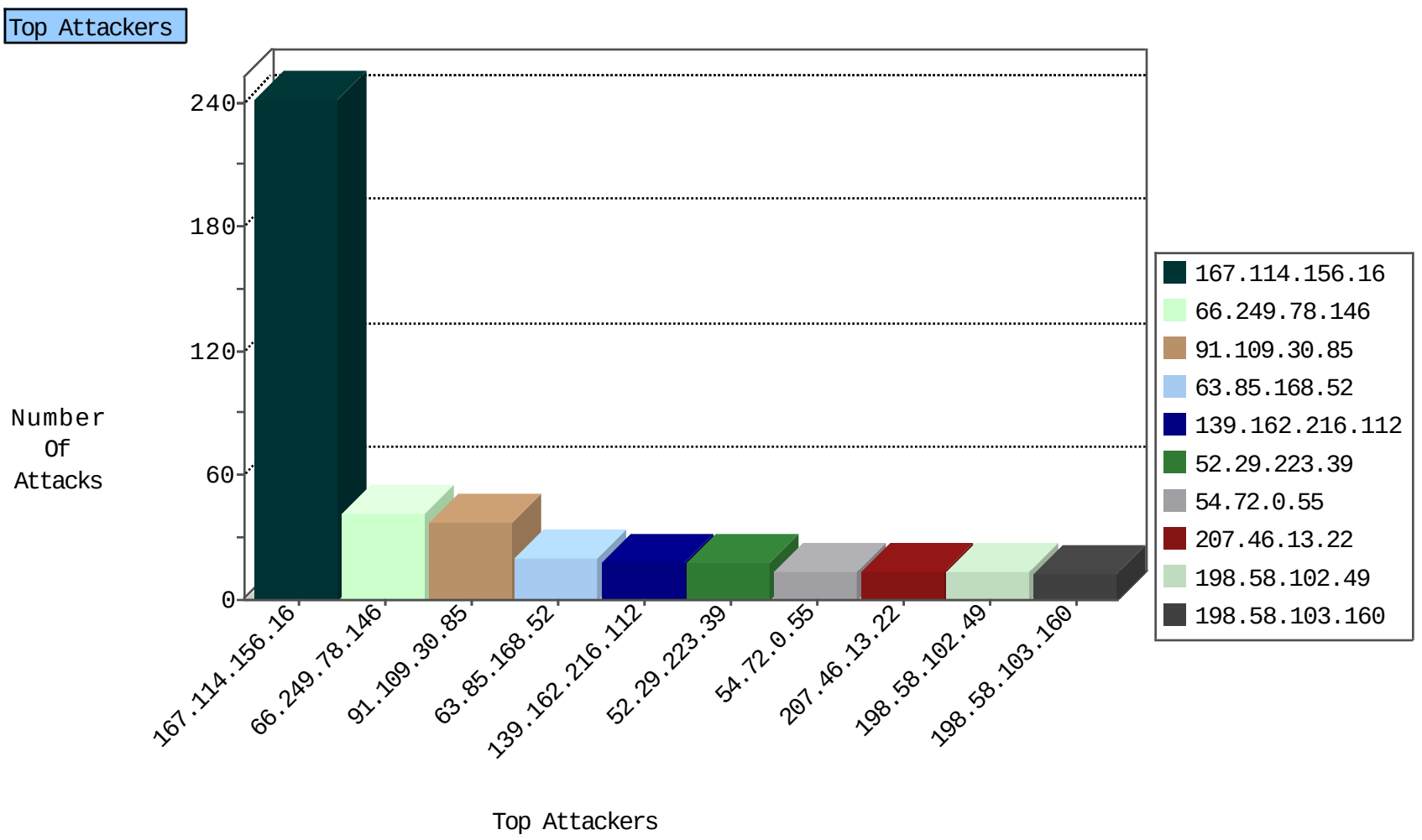
04-29-2016-07:04:09 to 04-29-2016-08:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-29-2016-07:04:09 to 04-29-2016-08:04:09

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	9930
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	12
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	5
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
204.42.253.2	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	2
113.75.84.72	China	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
183.18.64.125	China	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
113.116.251.73	China	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.116	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1

04-29-2016-07:04:09 to 04-29-2016-08:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-29-2016-07:04:09 to 04-29-2016-08:04:09

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
163.172.140.23	147.237.0.200	United Kingdom	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
123.249.0.183	147.237.76.42	China	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
123.249.0.183	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
63.85.168.52	147.237.77.74	United States	law.idf.il	ET WEB_SERVER Poison Null Byte	1
190.124.35.115	147.237.77.205	Nicaragua	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
161.202.120.149	147.237.0.33	Japan	idf.il	ET SCAN NMAP -sS window 1024	1
123.249.0.183	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
68.116.21.226	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
14.185.66.237	147.237.8.28	Vietnam	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
210.15.242.7	147.237.76.39	Australia	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
190.124.35.115	147.237.77.205	Nicaragua	prisha.idf.il	ET SCAN NMAP -sS window 4096	1

04-29-2016-07:04:09 to 04-29-2016-08:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
91.109.30.85	Germany	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	35
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
198.58.102.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
198.58.103.160	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.181.58.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
162.243.125.185	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.126.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
207.46.13.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
63.85.168.52	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
157.55.39.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.28.225	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.245	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.246.11	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.3.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.15	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.66.47	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.190	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.148.155	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
173.252.90.109	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
52.91.40.35	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
91.109.30.85	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
162.243.37.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
89.138.78.133	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
157.55.39.133	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
112.207.236.162	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.53.167.220	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.109.147.56	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
164.132.161.49	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
142.4.217.162	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.115	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.142.243.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.247.238	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.50	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.198	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.94	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.117.197.244	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.65.183.235	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	3
46.119.127.129	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.119.127.129	Block	3
85.65.183.235	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.65.183.235	Block	3
80.178.157.211	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 80.178.157.211	Block	2
148.251.176.212	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
79.180.123.76	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.180.123.76	Block	1
63.85.168.52	United States	147.237.77.74	law.idf.il	NULL Character in Header Name at	Block	1
46.119.127.129	Ukraine	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
63.85.168.52	United States	147.237.77.74	law.idf.il	Illegal Byte Code Character in URL ¸[[#20]]¸	Block	1
176.13.12.24	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
79.180.123.76	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/3	Block	1
63.85.168.52	United States	147.237.77.74	law.idf.il	NULL Character in Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]][[#21]]Ml©ºEA&_ €šû¯º[[#2]][[#31]]•FNãojGSØ–4Êù¶[[#2]]™[[#0]][[#0]][[#28]]À/À+À0À, À[[#19]]À	Block	1
54.189.255.26	United States	147.237.0.34	tikshuv.idf.il	Distributed Parameter Type Violation on www.tikshuv.idf.il/modules/forums/forum.aspx parameter ForumId	Block	1
94.159.245.199	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/sachar	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	1
63.85.168.52	United States	147.237.77.74	law.idf.il	Illegal HTTP Version	Block	1
188.120.148.155	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
63.85.168.52	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
63.85.168.52	United States	147.237.77.74	law.idf.il	Abnormally Long Request method	Block	1
94.230.95.97	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 94.230.95.97	Block	1
74.82.47.2	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
63.85.168.52	United States	147.237.77.74	law.idf.il	Malformed HTTP Header Line 1	Block	1
207.46.13.22	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.22	Block	1
80.178.157.211	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
63.85.168.52	United States	147.237.77.74	law.idf.il	Unknown HTTP Request Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]][[#21]]Ml©ºEA&_ €šû¯º[[#2]][[#31]]•FNãojGSØ–4Êù¶[[#2]]™[[#0]][[#0]][[#28]]À/À+À0À, À[[#19]]À in URL ¸[[#20]]¸	Block	1
63.85.168.52	United States	147.237.77.74	law.idf.il	Illegal Byte Code Character in Header Name	Block	1
94.230.95.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/resources/images/common/hrhorizontal.gif"	Block	1
79.177.89.67	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in aka.idf.il/main/sachar/markiveysachar.aspx	None	1
63.85.168.52	United States	147.237.77.74	law.idf.il	Malformed URL ¸[[#20]]¸	Block	1
207.46.13.22	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-14322-he/dover.aspx′½¸¿¸¯¸′½¸¿¸¯¸′×′₪	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/size100x0/2400.jpg	Block	1
63.85.168.52	United States	147.237.77.74	law.idf.il	Illegal Byte Code Character in Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]][[#21]]Ml©ºEA&_ €šû¯º[[#2]][[#31]]•FNãojGSØ–4Êù¶[[#2]]™[[#0]][[#0]][[#28]]À/À+À0À, À[[#19]]À	Block	1

04-29-2016-07:04:09 to 04-29-2016-08:04:09