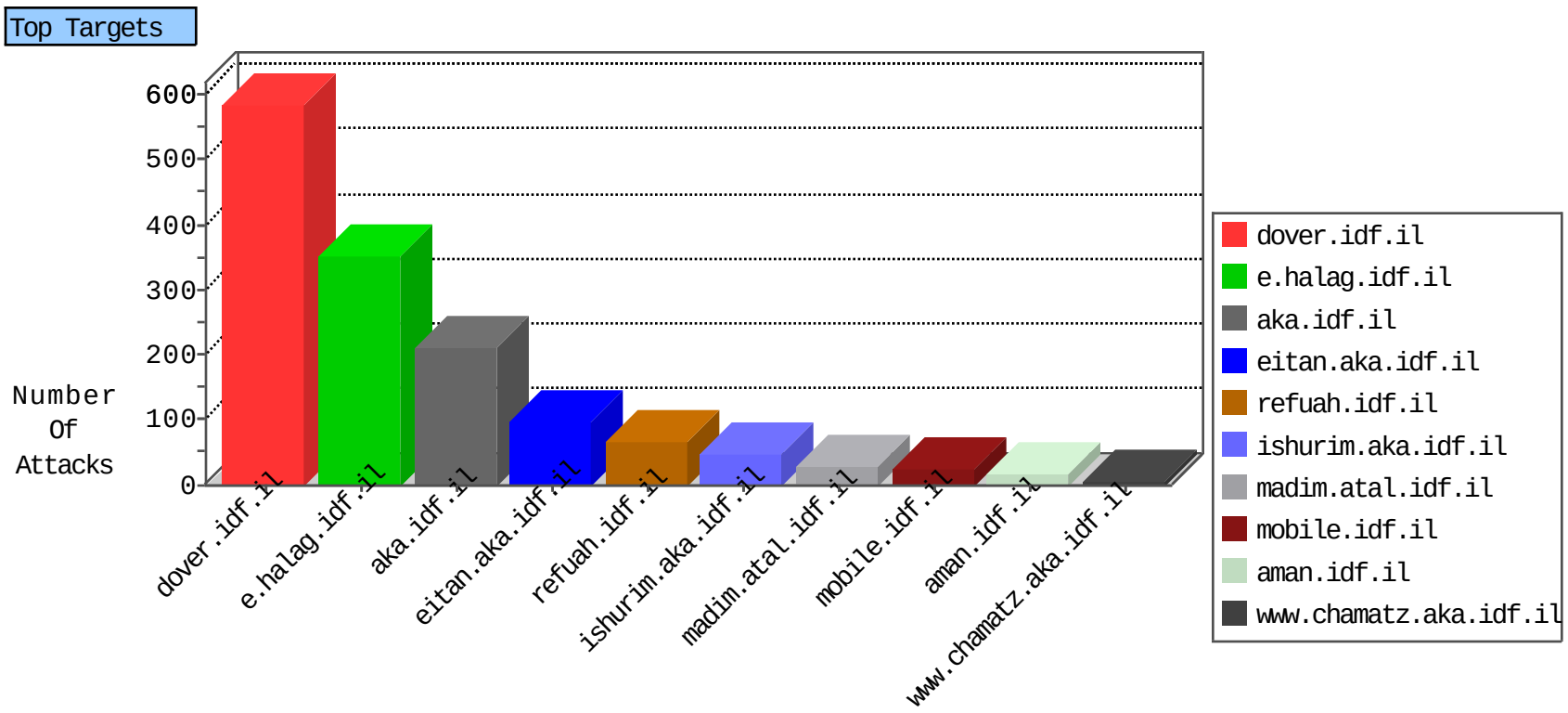
04-24-2016-20:04:07 to 04-24-2016-21:04:07

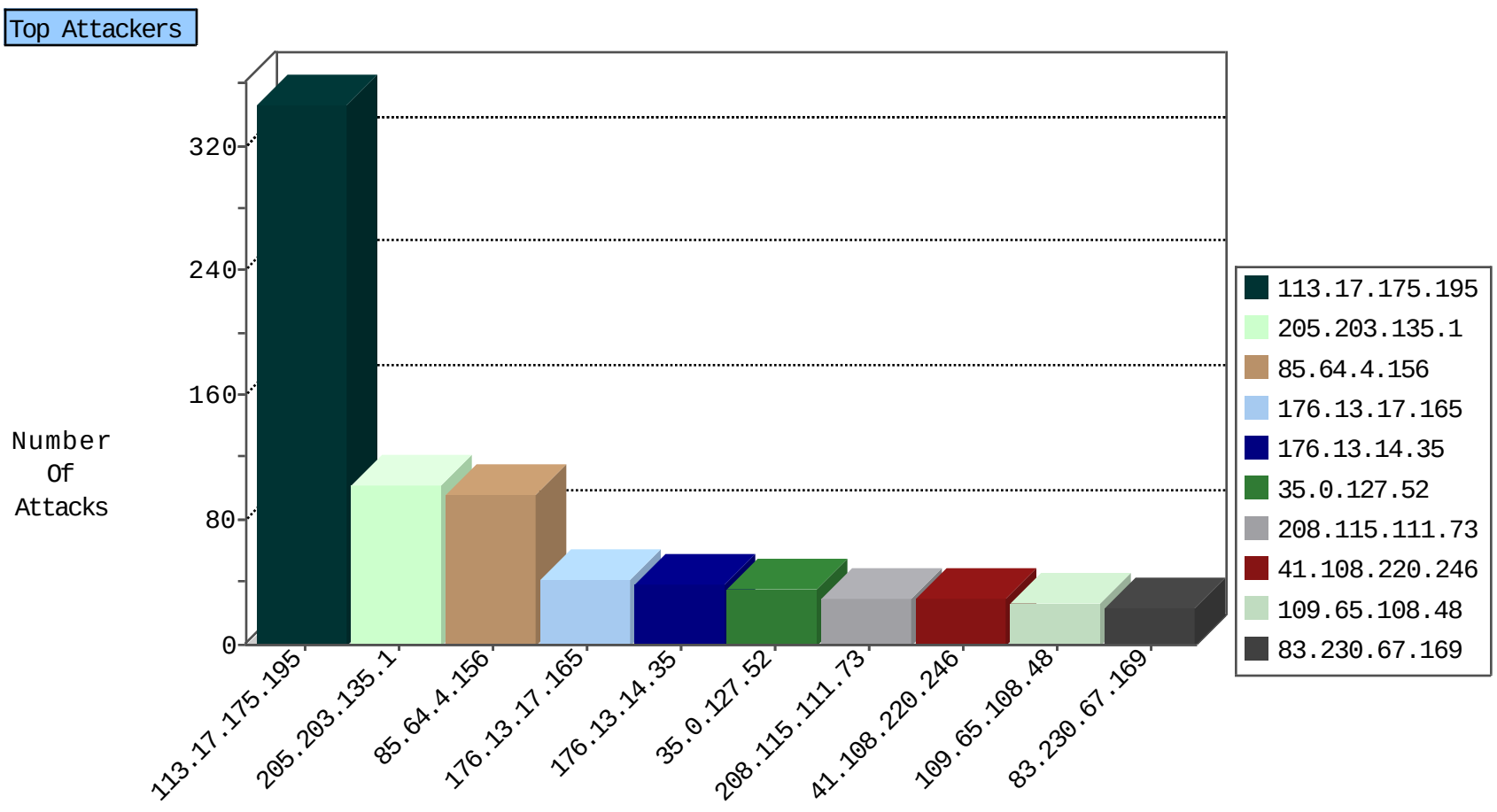
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

04-24-2016-20:04:07 to 04-24-2016-21:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
113.17.175.195	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	347
81.218.65.210	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	6
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
109.66.70.135	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	2
74.91.20.198	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
52.70.97.105	United States	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
69.197.185.19	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1
107.150.46.35	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	drop	1
169.54.233.125	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
173.208.197.253	United States	147.237.77.205	prisha.idf.il	block-sp-traf1	drop	1
188.138.17.205	France	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

04-24-2016-20:04:07 to 04-24-2016-21:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-24-2016-20:04:07 to 04-24-2016-21:04:07

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

04-24-2016-20:04:07 to 04-24-2016-21:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
85.64.4.156	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	96
176.13.17.165	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
176.13.14.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
83.230.67.169	Poland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
41.108.220.246	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
41.108.220.246	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
109.65.108.48	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
66.102.9.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
109.65.108.48	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	13
162.243.116.152	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.99.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.28	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.238.136.135	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.92	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
87.70.73.3	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
207.46.13.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
85.130.178.143	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
124.178.66.22	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
87.70.71.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
35.0.127.52	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
35.0.127.52	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
35.0.127.52	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
35.0.127.52	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
37.26.148.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.60	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
208.54.80.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
94.43.247.101	Georgia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
185.3.147.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.14.35	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
87.71.48.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.101.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.178.36.249	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
37.26.148.189	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
72.167.232.160	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.60	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.180.169.254	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.26.148.141	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.26.149.168	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4

04-24-2016-20:04:07 to 04-24-2016-21:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.148.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
213.233.84.136	Romania	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.53.40.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
95.86.81.56	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	4
95.86.82.85	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	4
109.64.10.187	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 109.64.10.187	Block	4
79.181.200.30	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	3
2.53.149.94	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	2
79.181.200.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	2
66.220.145.246	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
74.91.20.198	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to www.178tx.com/	Block	1
207.46.13.173	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.225	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
46.19.85.145	Israel	147.237.76.42	refuah.idf.il	Malformed URL	Block	1
141.212.122.129	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to /x	Block	1
84.228.155.9	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
185.120.125.129	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
65.55.218.48	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.253.215.76	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.53.162.20	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.178.36.249	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Parameter Type Violation searchText in www.idf.il/1497-en/dover.aspx	Block	1
46.19.85.145	Israel	147.237.76.42	refuah.idf.il	Multiple Malformed URL from 46.19.85.145	Block	1
149.78.27.229	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/ 2002/july/hamas.stm>.	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
185.120.125.129	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 185.120.125.129	Block	1
66.220.145.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
131.253.26.224	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.55.40.201	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
46.19.85.145	Israel	147.237.76.42	refuah.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.145	Block	1
157.55.39.69	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-ar/cogat.aspx	Block	1
199.30.24.85	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.220.145.245	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
31.61.137.30	Poland	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout2.css	Block	1
141.212.122.129	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to /x	Block	1
46.19.85.145	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method gav in URL	Block	1
157.55.39.224	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
69.197.185.19	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.fc376.com/	Block	1
207.46.13.164	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
141.212.122.129	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /x	Block	1
83.230.67.169	Poland	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/listpage/	Block	1
176.52.56.16	Russian Federation	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/404.aspx'	Block	1
46.19.86.154	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
109.64.10.187	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/mobile	Block	1

04-24-2016-20:04:07 to 04-24-2016-21:04:07