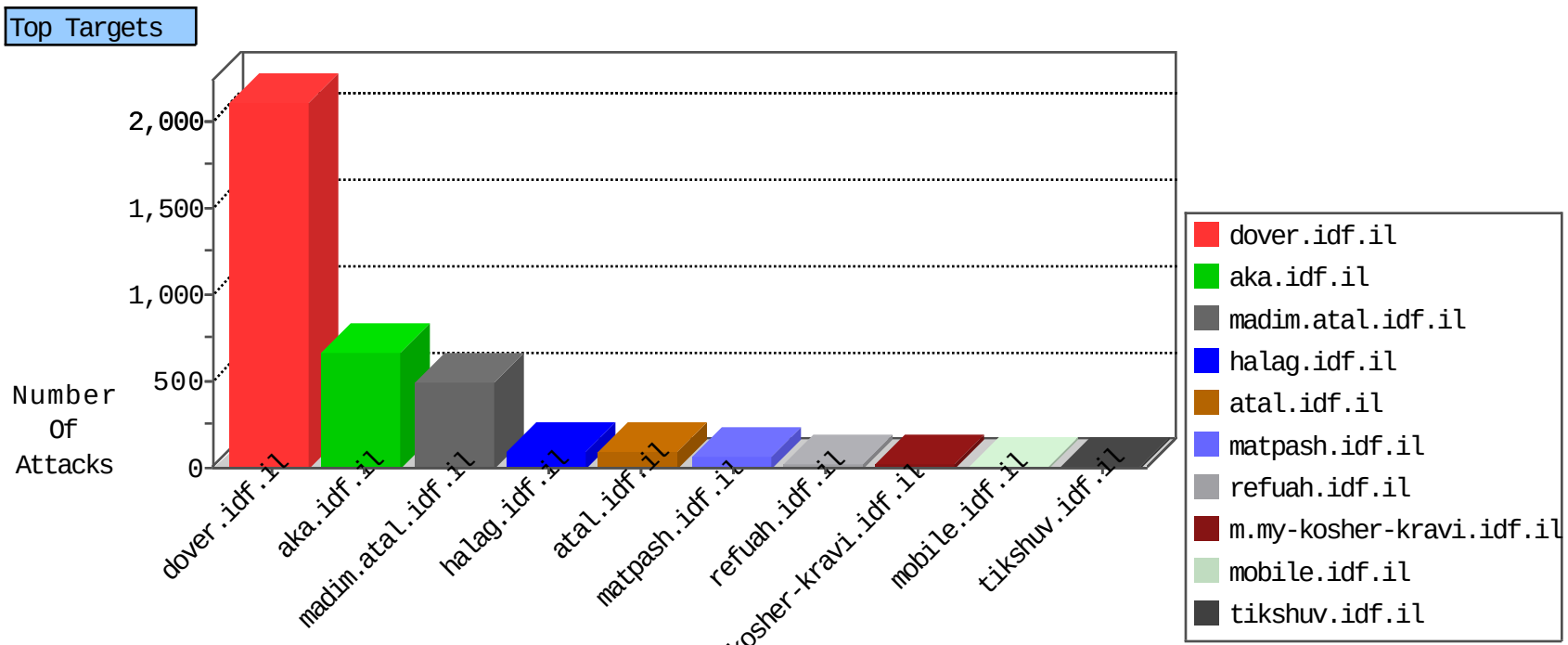
11-20-2015-14:04:04 to 11-20-2015-15:04:04

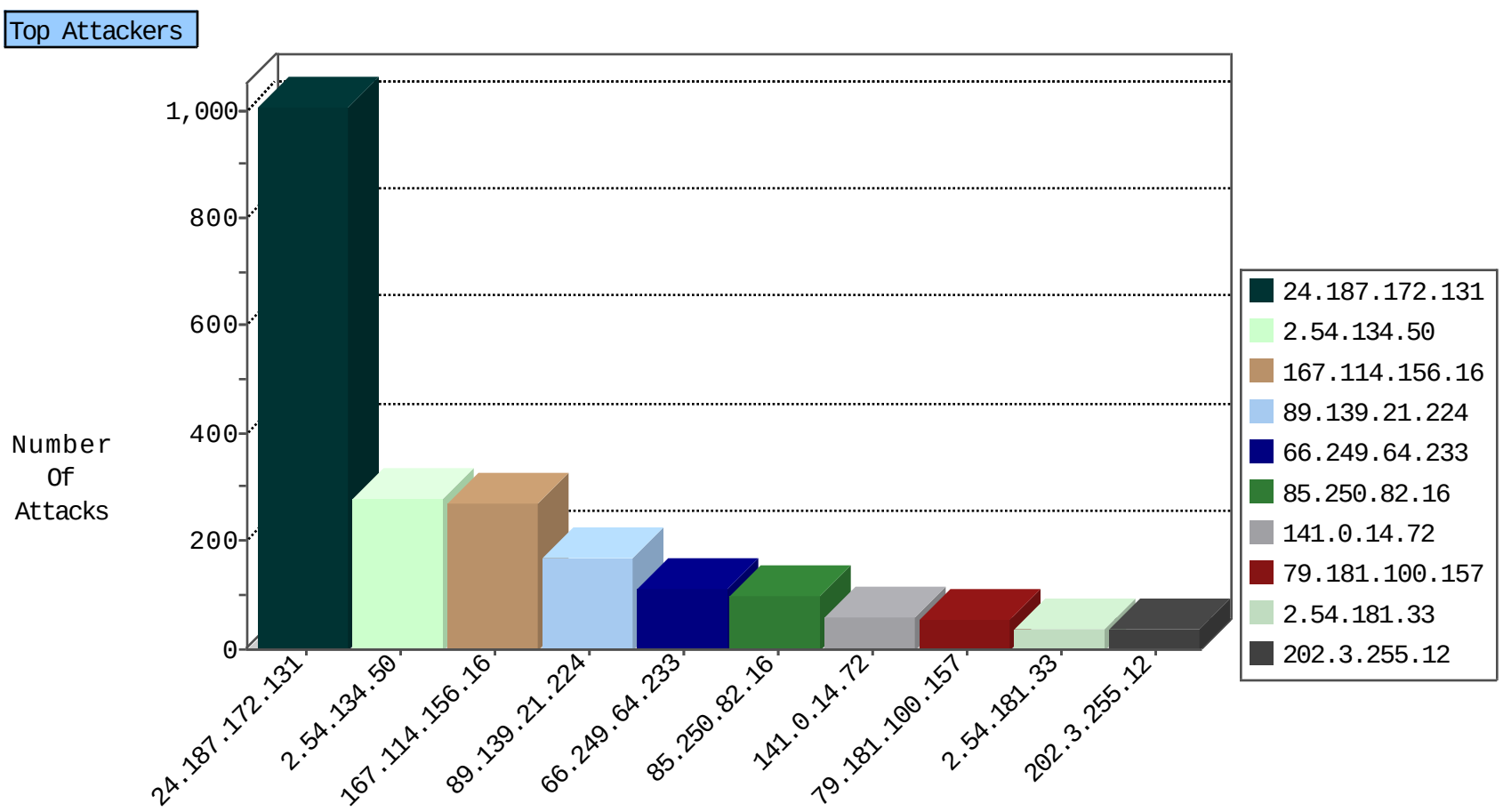
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-20-2015-14:04:04 to 11-20-2015-15:04:04

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	16457
66.249.67.122	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1095
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	275
84.108.251.57	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
79.179.171.121	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
176.13.12.177	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
105.108.232.48	Algeria	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
117.194.57.208	India	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
141.212.121.199	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
37.46.39.183	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
198.20.70.114	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1

11-20-2015-14:04:04 to 11-20-2015-15:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.85	France	147.237.77.226	www.chamatz.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
151.80.31.147	Italy	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-20-2015-14:04:04 to 11-20-2015-15:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	**Signature**	**Count**

11-20-2015-14:04:04 to 11-20-2015-15:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
24.187.172.131	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1008
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	112
89.139.21.224	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	93
89.139.21.224	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	75
141.0.14.72	Europe	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	60
79.181.100.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
202.3.255.12	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
31.186.228.57	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	31
100.100.111.22		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	28
46.19.86.67	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
31.186.228.96	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	22
31.186.228.60	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	22
31.186.228.58	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
31.186.228.95	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
95.86.110.57	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
100.100.48.159		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
31.186.228.29	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
100.100.34.100		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
77.126.95.110	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
31.186.228.31	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
46.19.86.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
37.26.148.167	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
31.186.228.30	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
31.186.228.93	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
100.100.82.133		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
217.175.54.60	Italy	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.64.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
217.175.54.62	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
220.255.148.20	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	11
100.100.96.42		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
31.186.228.32	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
100.100.126.142		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.72	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
77.125.79.131	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
37.26.147.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
84.108.251.57	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
66.249.66.75	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
149.78.35.28	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
79.181.111.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.52.134.209	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
80.246.133.229	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
216.223.27.22	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
84.228.137.144	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
31.186.228.59	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.120.240.178	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
87.69.158.121	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
5.29.36.234	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7

11-20-2015-14:04:04 to 11-20-2015-15:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.134.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	153
2.54.134.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	104
85.250.82.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
2.54.181.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
2.54.4.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
85.250.82.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	29
37.142.222.233	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 37.142.222.233	Block	25
2.54.134.50	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.54.134.50	Block	23
87.68.156.42	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	15
46.120.229.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
79.182.221.25	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	5
37.142.222.233	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	5
213.57.211.9	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	4
213.57.211.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/pages/fan_status.php	Block	4
2.52.152.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
95.86.105.184	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 95.86.105.184	Block	4
176.13.1.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.9.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.66.155.238	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	3
109.66.155.238	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/pages/fan_status.php	Block	3
2.52.167.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.12.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
89.138.23.222	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
5.28.162.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.250.178.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.228.151.143	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
46.116.198.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.12.140.108	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
82.81.7.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.146.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
149.88.143.163	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 149.88.143.163	Block	2
46.19.86.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.130.224.21	Netherlands	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.130.224.21	Block	2
66.249.67.52	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
149.88.143.163	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/sachar/payslips.aspx	Block	1
84.111.155.140	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.67.55.93	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.125.72.14	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/nahal.stm.	Block	1
95.86.105.184	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/kiosk/kiosk.aspx&sa=u&ved=0ahukewjr_76d_57jahwf-w4khx0iankqfgggmaa&usg=afqjcngyomaz3tdlraodkcl0huqlbg9rpa	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
149.78.35.28	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 149.78.35.28	Block	1
84.94.179.178	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.116.99.24	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.130.224.21	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1524	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.180.38.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
176.228.188.214	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1

11-20-2015-14:04:04 to 11-20-2015-15:04:04