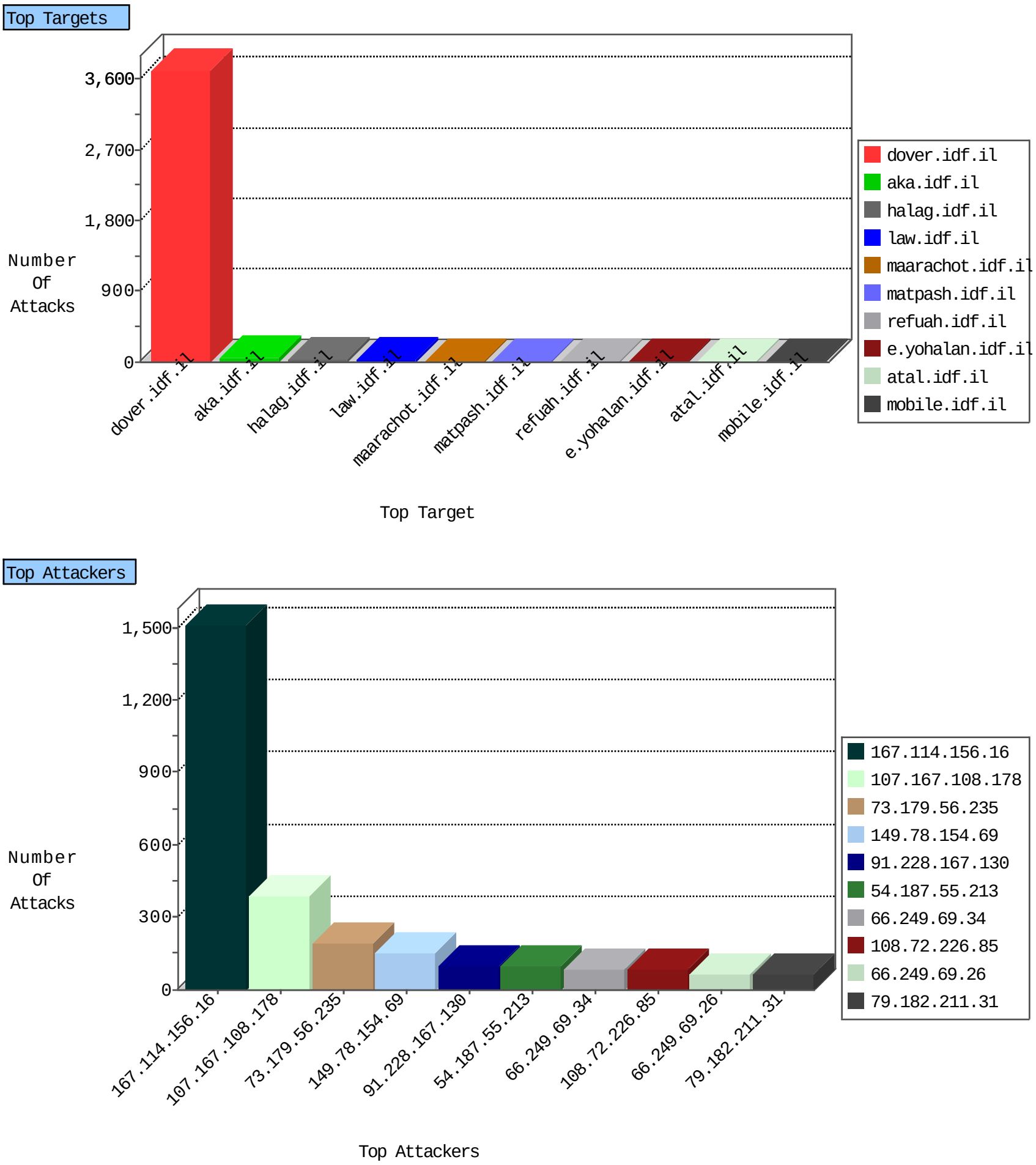
11-04-2015-05:04:09 to 11-04-2015-06:04:09

IDF Under Attack Daily Report



11-04-2015-05:04:09 to 11-04-2015-06:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.122	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3402
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2619
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1013
54.187.55.213	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	645
66.249.67.79	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	605
66.249.67.6	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	414
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	349
66.249.67.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	35
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	9
66.249.79.41	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	7
66.249.79.43	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	6
101.95.129.11	China	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	2
108.59.253.71	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
66.249.69.34	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
91.228.167.130	Slovakia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
205.203.135.1	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
220.111.56.160	Japan	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
46.19.141.25	Switzerland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
180.49.109.223	Japan	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
71.6.216.40	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
66.249.69.42	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
183.195.151.2	China	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1

11-04-2015-05:04:09 to 11-04-2015-06:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.44.115	Italy	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1

11-04-2015-05:04:09 to 11-04-2015-06:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	5
66.249.79.43	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
119.73.228.136	147.237.77.178	Singapore	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.160.155	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential SSH Scan	1
5.39.222.253	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential SSH Scan	1
218.161.68.246	147.237.8.28	Taiwan	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.193.22.122	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
119.10.8.133	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
5.39.222.253	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential SSH Scan	1

11-04-2015-05:04:09 to 11-04-2015-06:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
107.167.108.178	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	389
73.179.56.235	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	191
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	154
91.228.167.130	Slovakia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	96
54.187.55.213	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	92
108.72.226.85	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	85
66.249.69.34	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
79.182.211.31	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	63
205.203.135.1	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	52
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	50
66.249.69.26	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
68.97.113.152	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	39
138.163.160.42	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
66.249.69.42	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	31
212.199.182.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
76.110.98.182	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
68.4.93.63	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
2.52.161.207	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
184.32.13.142	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
67.168.45.6	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
212.179.90.106	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
91.228.167.109	Slovakia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
66.249.69.26	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
66.249.69.42	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
122.56.102.94	New Zealand	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
85.250.158.44	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
108.31.182.147	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
66.249.69.34	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
101.180.99.106	Australia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
66.249.78.44	United States	147.237.77.234	halag.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
50.45.196.198	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
109.66.119.46	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
198.58.103.158	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
66.249.69.26	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
108.59.253.71	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
100.100.124.215		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
201.103.192.22	Mexico	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
66.249.78.51	United States	147.237.77.234	halag.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
108.18.223.140	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
157.55.39.32	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	SAM rule	drop	9
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
66.249.93.196	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
46.19.86.156	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9

11-04-2015-05:04:09 to 11-04-2015-06:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/undefined/	Block	2
198.20.69.74	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-ar/cogat.aspx	Block	1
66.249.67.60	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
162.216.46.9	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list20050529.htm	Block	1
66.249.74.108	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/1/112921.pdf	Block	1
66.249.65.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/3481.jpg	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1073-he/nakhal.aspx	Block	1
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/8/71098.doc	Block	1
23.21.144.29	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
162.254.149.38	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.65.118	Block	1
104.33.97.119	United States	147.237.77.233	atal.idf.il	E-mail collector robots 14	Block	1
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/6/70246.pdf	Block	1
37.140.188.112	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter DocID in www.aka.idf.il/giyus/atuda/	None	1
176.13.2.206	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx	Block	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
104.33.97.119	United States	147.237.77.233	atal.idf.il	eMail Hoarding	Block	1
66.249.69.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/scriptresource.axd	Block	1
45.35.71.181		147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
191.252.44.242	Brazil	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
157.55.39.117	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
66.249.74.104	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/1/112221.pdf	Block	1
64.210.232.73	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1

11-04-2015-05:04:09 to 11-04-2015-06:04:09