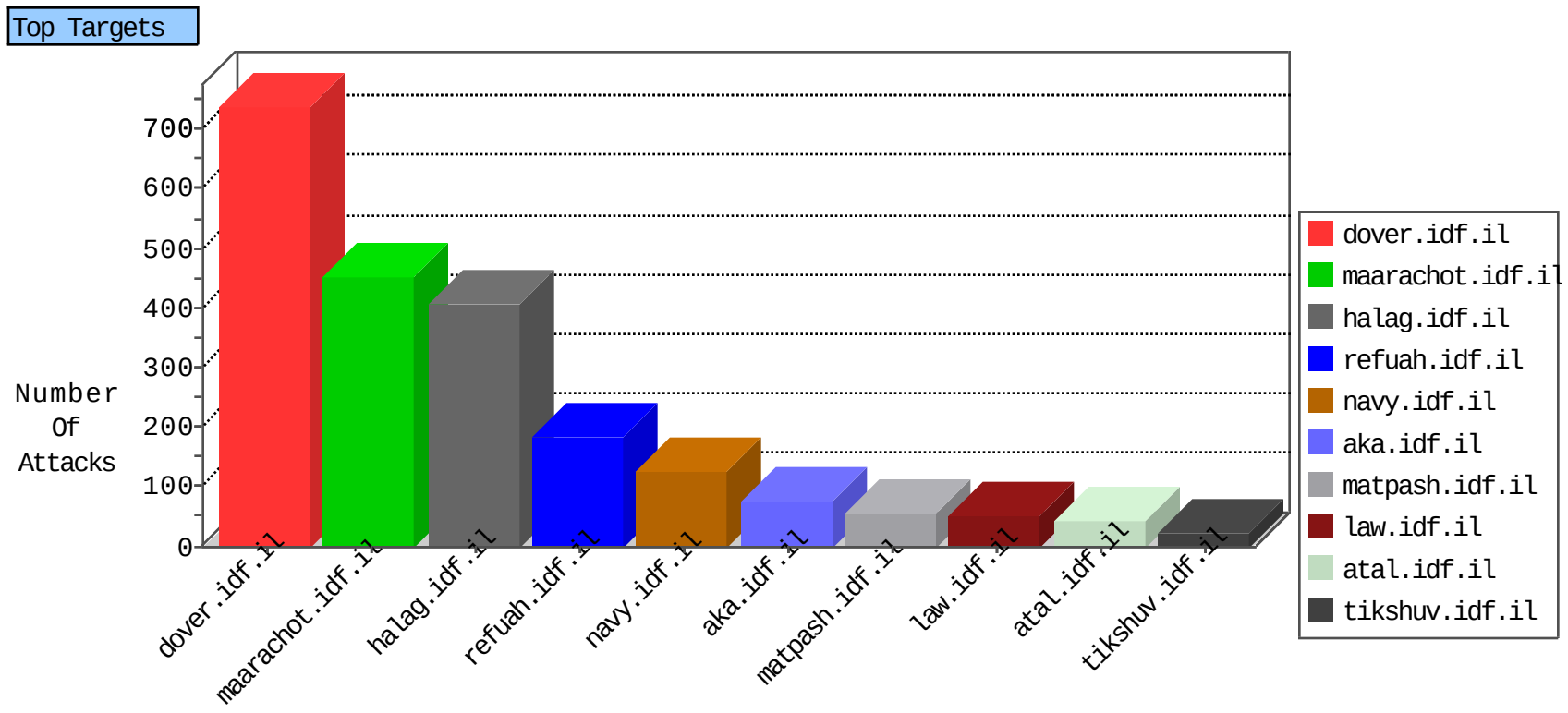
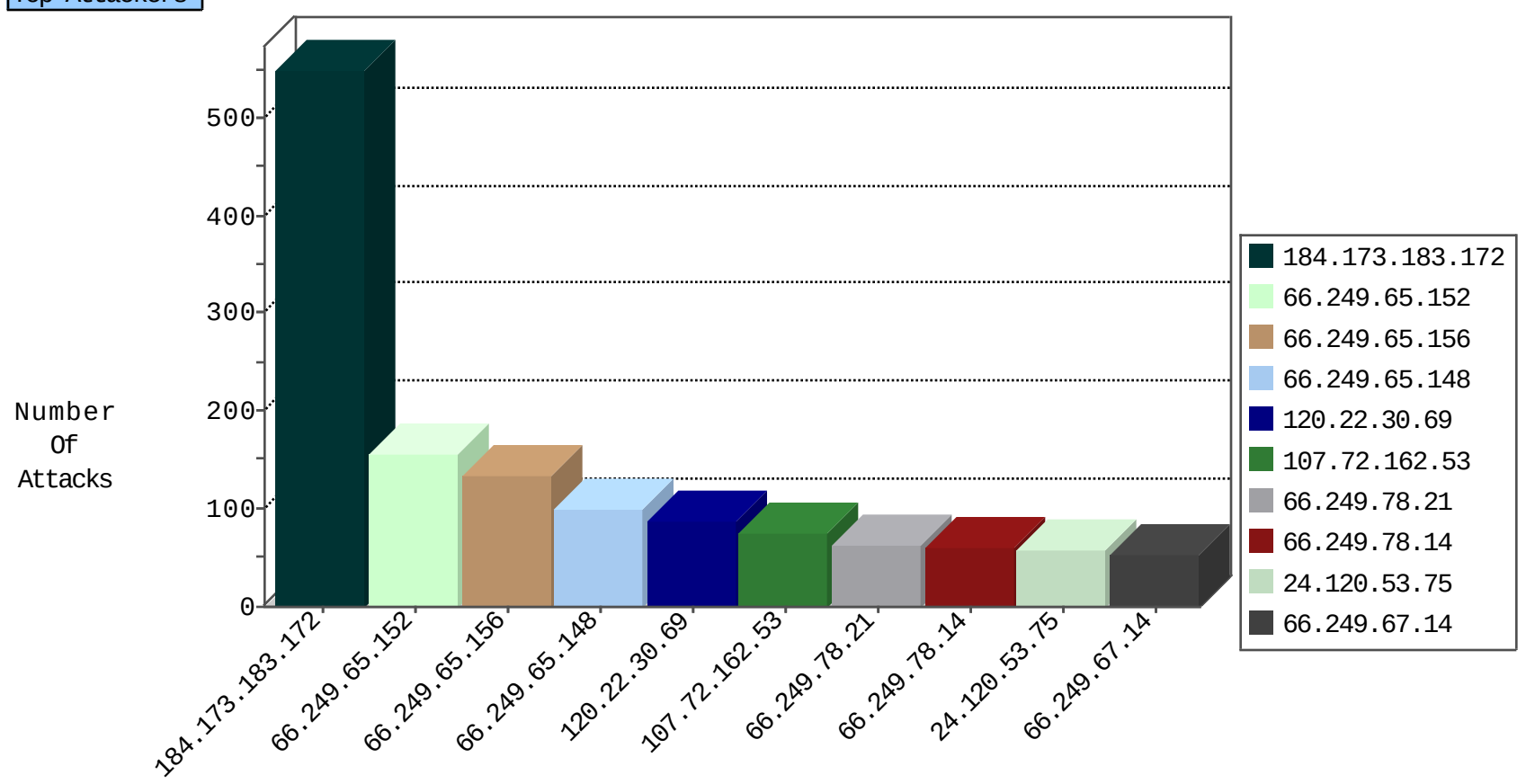
04-13-2015-05:03:06 to 04-13-2015-06:03:06

IDF Under Attack
04-13-2015-05:03:06

Top Targets



Top Attackers



04-13-2015-05:03:06 to 04-13-2015-06:03:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.65.152	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	156
66.249.65.156	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	131
66.249.65.148	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	99
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	62
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	61
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	52
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	47
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	31
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	29
66.249.65.195	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	26
66.249.65.191	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	26
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	16
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	16
66.249.78.79	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	14
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	13
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	13
66.249.78.86	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	12
66.249.67.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	12
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	12
66.249.73.217	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	11
66.249.67.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	10
66.249.67.116	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	10
66.249.64.154	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	9
66.249.73.244	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	9
66.249.73.140	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	9
66.249.73.201	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.67.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	8
66.249.80.75	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	8
66.249.80.67	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	7
66.249.64.150	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	7
66.249.67.100	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	7
66.249.78.127	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	7
66.249.65.187	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	6
66.249.78.222	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ip_Web_In	drop	6
66.249.73.209	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.73.132	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.64.146	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	5
66.249.64.87	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	5
66.249.67.50	United States	147.237.72.14	dover.idf.il(old)	Block_Ip_Web_In	drop	5
66.249.78.67	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	5
66.249.64.121	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	4
66.249.67.34	United States	147.237.72.14	dover.idf.il(old)	Block_Ip_Web_In	drop	4
66.249.78.60	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	4
66.249.64.169	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	4
66.249.78.93	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	4
66.249.67.3	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	4
66.249.78.208	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ip_Web_In	drop	4
66.249.73.238	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	4
66.249.67.42	United States	147.237.72.14	dover.idf.il(old)	Block_Ip_Web_In	drop	4

04-13-2015-05:03:06 to 04-13-2015-06:03:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.234	halag.idf.il	DVRep_P-N_40-59	Permit	406
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	144
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	10
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	10

04-13-2015-05:03:06 to 04-13-2015-06:03:06

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
2.54.4.50	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.168	Japan	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
187.72.144.38	Brazil	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.128	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
61.160.223.70	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.223.70	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1

04-13-2015-05:03:06 to 04-13-2015-06:03:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
120.22.30.69	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	88
107.72.162.53	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	76
24.120.53.75	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	58
85.65.100.172	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
184.64.77.5	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
85.250.135.85	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
176.12.143.63	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
46.19.85.213	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
152.97.160.68	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
191.181.157.211	Brazil	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
24.251.56.86	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
24.176.106.237	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
5.29.164.155	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
203.127.58.231	Singapore	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
176.12.148.93	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
119.73.253.4	Singapore	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
82.80.25.221	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	6
203.127.58.229	Singapore	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
162.40.214.152	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
67.86.40.221	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
212.235.13.12	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
157.55.39.42	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
217.42.201.181	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
96.21.77.9	Canada	147.237.8.14	e.orchot.idf.i	Geo-location inbound enforcement	Geo-location enforcement	drop	3
207.46.13.89	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
79.181.254.220	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
61.135.190.68	China	147.237.0.200	m4u.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	2
159.224.160.225	Ukraine	147.237.72.166	aka.idf.il	SAM rule	drop	drop	2
80.246.130.131	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
192.114.91.213	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
159.224.160.225	Ukraine	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
203.127.96.220	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
159.224.160.225	Ukraine	147.237.77.216	dover.idf.il	SAM rule	drop	drop	2
207.46.13.82	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
73.191.195.126	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.42	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
14.216.27.145	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.171	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
176.12.140.184	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
212.174.166.140	Turkey	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
79.181.254.220	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
123.125.71.81	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
157.55.39.41	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1

04-13-2015-05:03:06 to 04-13-2015-06:03:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
173.254.24.43	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
46.4.13.87	Germany	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
207.46.13.89	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.89	Block	1
77.127.233.151	Israel	147.237.72.166	aka.idf.il	Unknown Parameter q in www.aka.idf.il/main/giyus/login.aspx	None	1
14.216.27.145	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 14.216.27.145	Block	1
157.55.39.172	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.4.68.142	Germany	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 46.4.68.142	Block	1
207.46.13.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/021904-1.stm	Block	1
109.65.119.93	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/payslips.aspx	None	1
31.44.135.1	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
173.254.24.43	United States	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
46.4.68.142	Germany	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1
157.55.39.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/kids.stm	Block	1
46.4.13.87	Germany	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
47.17.84.6	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
157.55.39.66	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//default.aspx	Block	1
207.46.13.82	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/download.stm	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/jump.stm	Block	1
14.216.27.145	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
157.55.39.171	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.4.68.142	Germany	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il//994-8613-he/navy.aspx.aspx	Block	1

04-13-2015-05:03:06 to 04-13-2015-06:03:06