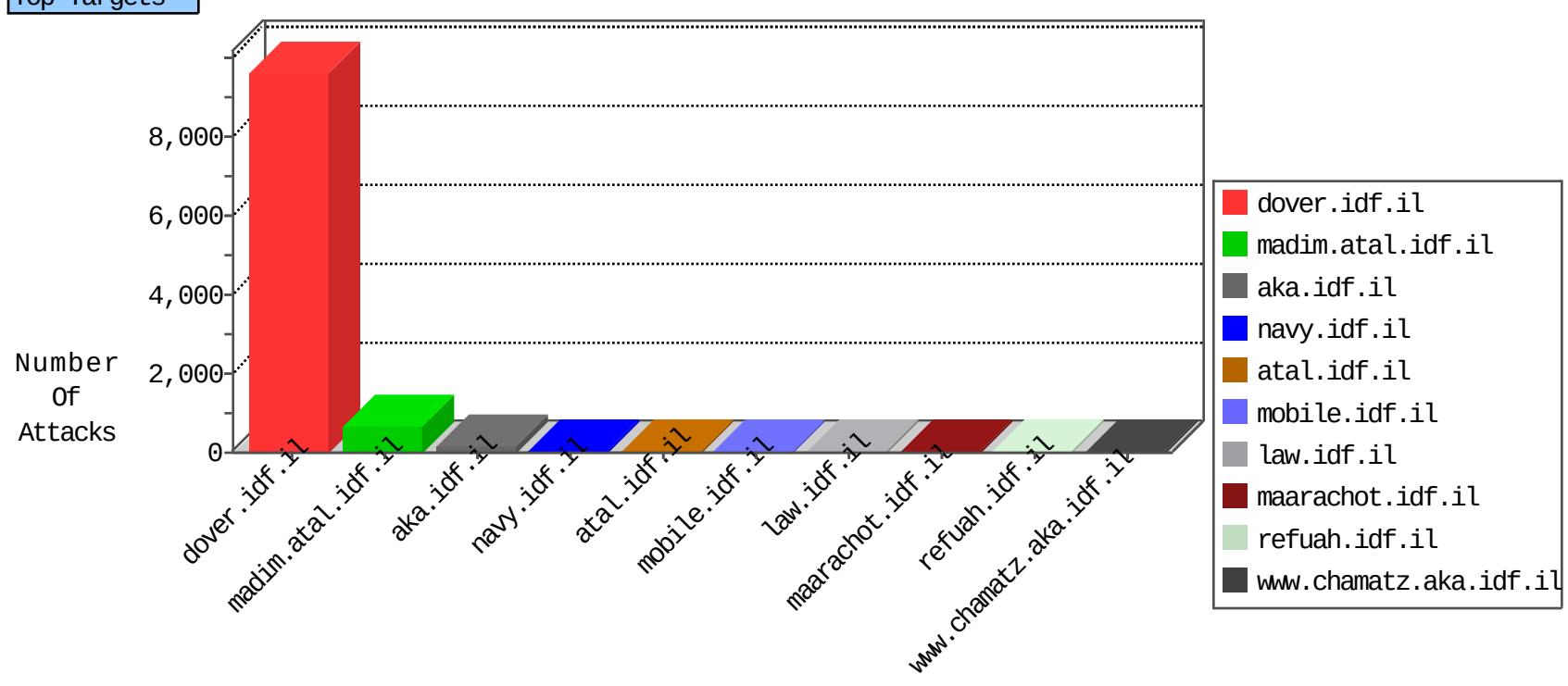
04-20-2015-21:03:06 to 04-20-2015-22:03:06

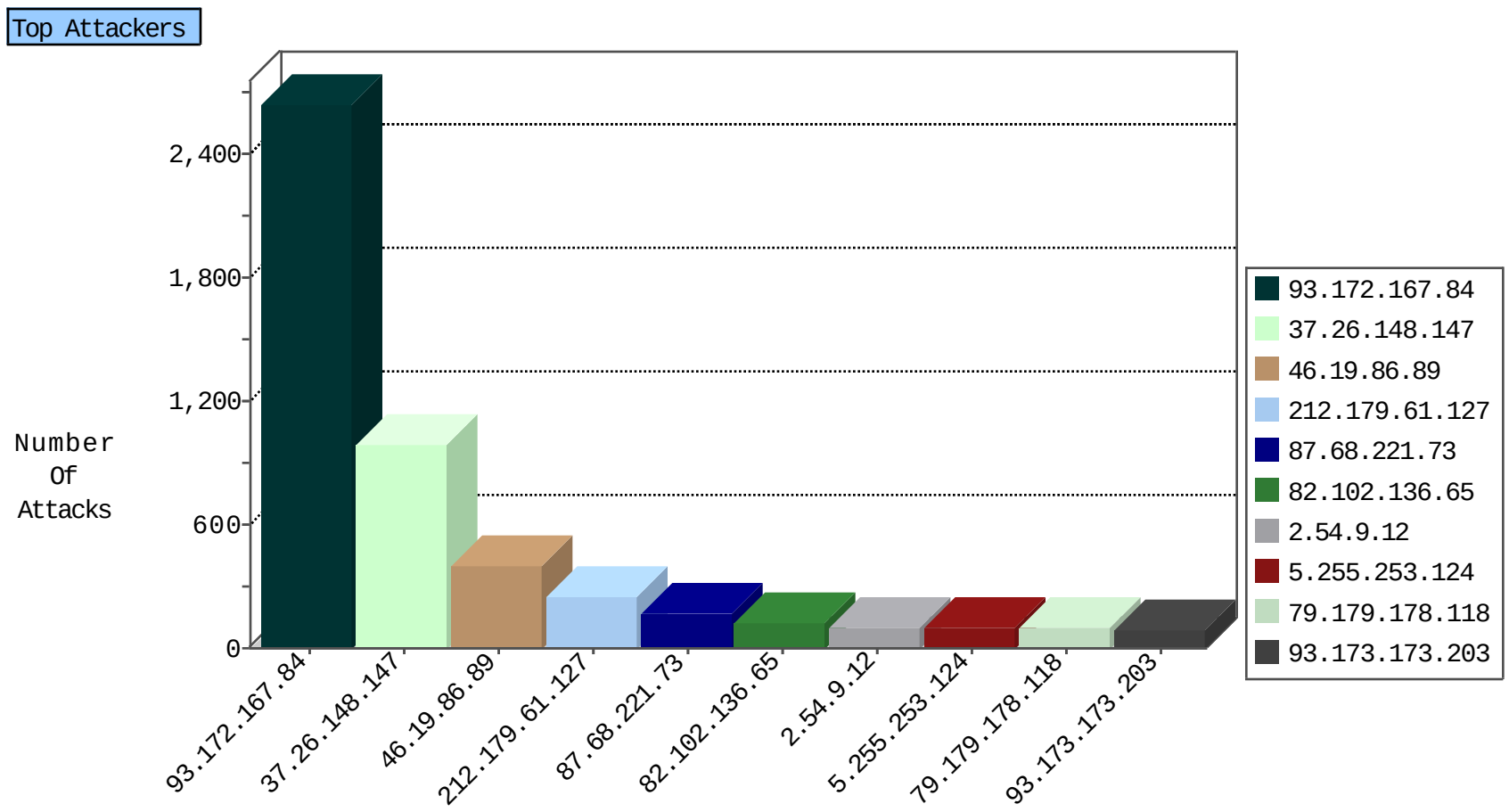
IDF Under Attack
04-20-2015-21:03:06

Top Targets



Top Target

Top Attackers



Top Attackers

04-20-2015-21:03:06 to 04-20-2015-22:03:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.157	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	2922
2.54.144.221	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	17
149.88.20.101	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	9
109.64.2.97	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
82.102.141.250	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	2
77.126.18.9	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
46.19.86.146	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
89.138.220.60	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
71.6.216.55	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
87.69.193.226	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
177.10.234.14	Brazil	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
80.178.195.9	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.121.111.195	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
188.120.148.144	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
80.246.138.222	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

04-20-2015-21:03:06 to 04-20-2015-22:03:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
93.172.148.7	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	2
71.6.165.200	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
2.54.143.68	Israel	147.237.0.19	madim.atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
50.7.159.11	Germany	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
77.126.18.9	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-20-2015-21:03:06 to 04-20-2015-22:03:06

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
66.249.67.39	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
66.249.73.211	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.67.24	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.26	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
109.64.32.17	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.190	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.32	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
122.228.207.76	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
43.255.190.60	Japan	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
122.228.207.76	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.98	United States	147.237.72.156	aman.idf.il	ET DROP Dshield Block Listed Source	1
122.228.207.76	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
193.104.41.53	Moldova, Republic of	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
193.104.41.53	Moldova, Republic of	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
43.255.190.60	Japan	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.190.60	Japan	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
116.121.137.2	Korea, Republic of	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
193.104.41.53	Moldova, Republic of	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
84.228.21.173	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
122.228.207.76	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1

04-20-2015-21:03:06 to 04-20-2015-22:03:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
93.172.167.84	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2648
37.26.148.147	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	986
212.179.61.127	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	252
87.68.221.73	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	166
82.102.136.65	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	126
2.54.9.12	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	99
79.179.178.118	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	94
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	93
93.173.173.203	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	89
177.6.247.163	Brazil	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	82
46.19.86.44	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	82
79.181.142.215	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	81
109.66.111.54	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	78
77.243.189.211	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	71
46.19.85.200	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	69
2.54.189.136	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	65
87.68.252.7	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	63
84.94.46.46	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	63
46.19.85.46	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	62
66.249.93.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	60
84.109.127.37	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	57
79.180.2.4	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	56
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	54
109.67.199.231	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	51
149.78.114.239	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50
5.144.60.134	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	48
66.249.93.164	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	46
176.12.139.47	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	45
93.172.106.29	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	45
162.157.124.12	Canada	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	44
37.26.147.139	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	43
93.173.240.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
2.52.0.183	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
109.253.134.158	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
46.19.86.139	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
46.121.64.180	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
81.218.28.58	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
109.160.243.215	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
84.108.162.122	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
79.182.135.14	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
46.19.85.55	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
79.178.113.129	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
31.154.3.195	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
46.19.85.58	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
66.249.79.74	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
84.94.175.65	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
109.253.157.125	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
176.12.146.106	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.86.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	395
109.253.134.195	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	61
109.253.128.73	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	54
109.253.128.44	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	52
2.54.143.68	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	37
109.253.146.139	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	28
2.54.1.1	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	16
84.109.105.223	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.109.105.223	Block	16
85.65.46.95	Israel	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	6
149.88.43.20	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	6
85.65.46.95	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 85.65.46.95	Block	5
85.65.46.95	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 85.65.46.95	Block	5
85.65.46.95	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 85.65.46.95	Block	5
31.168.207.236	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
85.65.46.95	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 85.65.46.95	Block	5
85.65.46.95	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 85.65.46.95	Block	5
109.253.134.63	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	4
85.65.46.95	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 85.65.46.95	Block	4
85.65.46.95	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 85.65.46.95	Block	4
134.249.53.8	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/	Block	4
109.253.133.106	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	4
85.65.46.95	Israel	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 85.65.46.95	Block	3
149.78.48.122	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
85.65.46.95	Israel	147.237.72.166	aka.idf.il	Distributed Illegal URL Path Encoding	Block	3
109.253.156.85	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	3
46.120.209.105	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	3
85.65.46.95	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 85.65.46.95	Block	3
85.65.46.95	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Method from 85.65.46.95	Block	2
66.249.79.58	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.58	Block	2
149.78.48.122	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 149.78.48.122	Block	2
46.121.73.15	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	2
84.95.60.196	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.253.128.181	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
5.22.130.179	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.253.144.206	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	2
85.65.46.95	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 85.65.46.95	Block	2
109.253.145.88	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	2
5.29.219.229	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
109.65.187.209	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
216.244.83.168	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
185.32.177.182	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
85.65.46.95	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method [[#27]]ÂœÂ¶Ãœ>B[[#29]]	Block	1
66.249.64.64	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8727-he/refuah.aspx	Block	1
109.253.146.54	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/requestpayslipexplanation.aspx	None	1
85.65.46.95	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL d[[#20]]$Ö»Ë†Â¿×£% $iÂ¿×©â€“Â¢/d)[[#18]]Â ×€{q%ËœfÂ¥4Âµâ„¢^[[#17]]@wg×€tÂœÆ’×€ ;1[[#11]][[#31]]	Block	1
46.19.86.89	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/mobile/shared/ajax/updatemakatqauntity.aspx	Block	1
95.86.122.146	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
84.111.30.66	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
209.183.183.253	United States	147.237.76.86	navy.idf.il	Illegal Byte Code Character in URL dÂ±[[#27]]"Â?×£Â½â€°Ö¶Â´×š [[#1]]×¦u[[#16]]hÂŒi6zÂ¡![[#4]]Â¨×±5Â?Â¿[[#23]]ÂžÂµ×ž×˜[[#31]]â€¦Ã™×’ Â-×•Â´z[[#14]][[#8]]Ã—â€¹[k^l•Ã¼Ö¹q×£Â·ÃŠ-qcË†×’pn6Â¼[[#28]]Â»v<va	Block	1

04-20-2015-21:03:06 to 04-20-2015-22:03:06