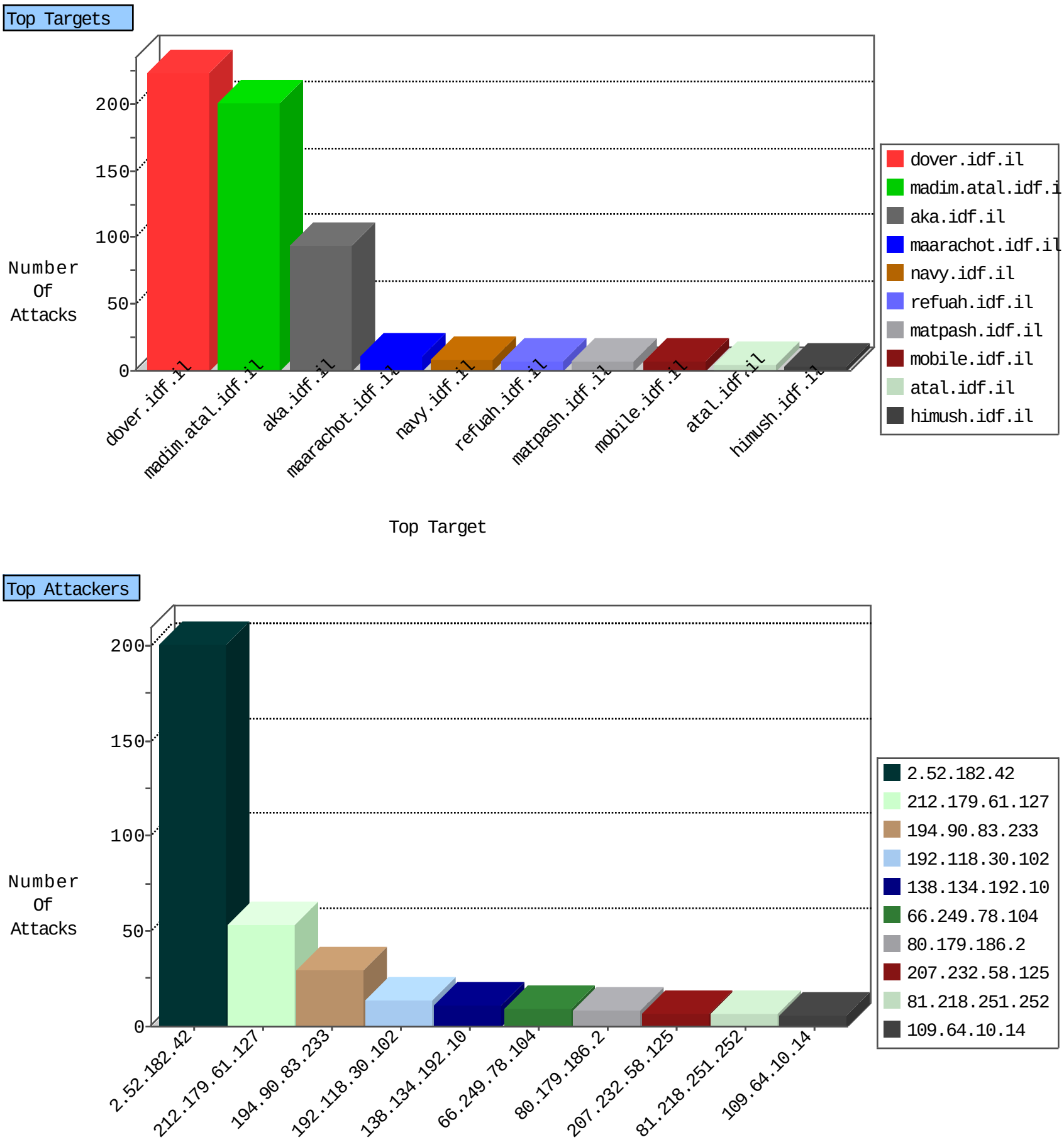
04-26-2015-09:03:09 to 04-26-2015-10:03:09

IDF Under Attack
04-26-2015-09:03:09



04-26-2015-09:03:09 to 04-26-2015-10:03:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
37.236.37.110	Iraq	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	982
66.249.78.104	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	550
46.19.85.13	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	344
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	105
216.185.38.91	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	64
194.90.83.233	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
80.179.186.2	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12
194.90.83.233	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10
79.181.116.41	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
37.26.147.157	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
109.226.33.18	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
80.179.186.2	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
10.0.0.28		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
134.147.203.115	Germany	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	2
212.143.137.173	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
79.182.214.12	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
79.178.233.60	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
46.117.100.163	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
79.179.134.32	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
176.228.130.26	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
81.218.40.194	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
71.6.135.131	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
89.139.163.220	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
54.72.73.168	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
37.26.147.139	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
204.42.253.2	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
147.236.33.45	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
81.218.152.21	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
23.95.82.226	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
99.97.23.9	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1
207.46.13.95	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
172.245.109.82	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
85.250.120.40	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
217.55.244.222	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.117.152.129	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
31.168.87.11	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
212.68.153.241	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
87.68.231.67	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
221.250.60.92	Japan	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
54.72.0.55	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
37.26.147.139	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
198.48.92.104	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

04-26-2015-09:03:09 to 04-26-2015-10:03:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.85.128	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
71.6.135.131	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
2.54.175.248	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.131	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
212.143.136.123	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-26-2015-09:03:09 to 04-26-2015-10:03:09

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
109.253.131.176	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.152.21	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.204	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	1
66.249.78.82	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	1
58.20.54.249	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
5.255.85.232	Netherlands	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
202.71.25.29	India	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
149.78.254.209	United States	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
84.229.28.109	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.137.175	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
58.97.2.66	Thailand	147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 3072	1
218.77.79.43	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.225	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
218.77.79.43	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
2.54.41.43	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
218.77.79.43	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1

04-26-2015-09:03:09 to 04-26-2015-10:03:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.61.127	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
194.90.83.233	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
81.218.251.252	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
84.228.16.124	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
79.178.11.149	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
2.54.143.188	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
85.65.164.102	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
79.176.0.204	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
37.26.147.245	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
84.229.28.109	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
213.57.190.109	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
147.236.238.10	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
80.179.194.168	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
77.125.121.143	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
50.118.188.18	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
207.46.13.95	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
220.255.1.38	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
212.179.8.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
109.253.138.94	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
79.176.221.175	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
220.255.1.67	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
185.32.178.22	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	1
64.12.253.130	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
109.253.138.242	Israel	147.237.77.243	mobile.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.86.139	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
220.255.1.173	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
192.117.158.88	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
66.249.93.164	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
5.102.204.134	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.19.86.242	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
87.68.214.121	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
216.185.38.91	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
149.78.19.13	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
89.157.44.124	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
31.168.128.18	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
185.32.178.22	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.52.182.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	201
207.232.58.125	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
138.134.192.10	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 138.134.192.10	Block	6
138.134.192.10	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
109.64.10.14	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 109.64.10.14	Block	5
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	4
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	4
212.68.153.188	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
195.95.183.205	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
62.90.35.34	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	3
84.229.31.49	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
85.64.74.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
213.8.96.230	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
192.114.86.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	2
50.118.188.18	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
147.236.238.70	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
109.65.221.226	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
212.179.61.127	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
2.52.174.93	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
188.165.15.13	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.13	Block	1
66.249.81.202	Israel	147.237.76.30	himush.idf.il	Suspicious Response Code	Block	1
109.253.128.178	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
66.249.78.89	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/935	Block	1
46.19.86.57	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
213.57.226.203	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	1
31.168.68.51	Israel	147.237.72.166	aka.idf.il	Unknown Parameter q861 in www.aka.idf.il/main/giyus/login.aspx	None	1
79.180.164.166	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//894-he/refuah.aspx	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/announcements/2004/february/08.stm	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Abnormally Long Request URL	Block	1
91.199.69.254	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
62.90.91.177	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catI in www.aka.idf.il/sites/klali/default.asp	None	1
80.246.133.255	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
37.140.141.27	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/hinuch	Block	1
212.179.61.127	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
192.114.86.2	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.114.86.2	Block	1
66.249.81.205	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.104	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/mobile/	Block	1
46.120.126.46	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
79.181.131.238	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
31.168.120.255	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.1	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.1	Block	1
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.197	Block	1
157.55.39.115	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
62.90.194.27	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
82.80.168.23	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.142.56.39	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
5.28.155.34	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
69.30.240.46	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal HTTP Version	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/ramon.stm	Block	1

04-26-2015-09:03:09 to 04-26-2015-10:03:09