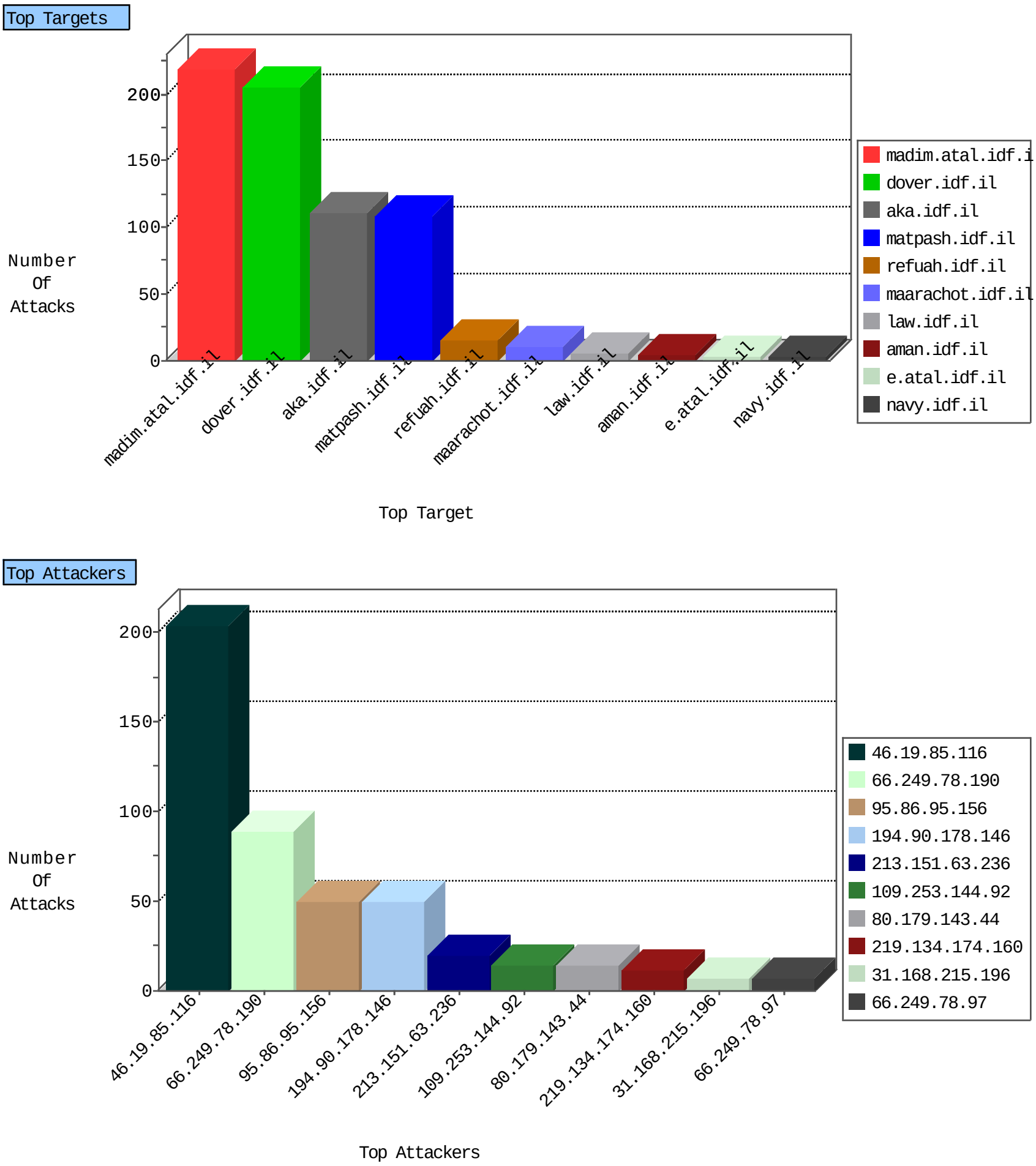
04-26-2015-16:03:07 to 04-26-2015-17:03:07

IDF Under Attack
04-26-2015-16:03:07



04-26-2015-16:03:07 to 04-26-2015-17:03:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.187	China	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2152
66.249.78.97	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1984
138.134.102.15	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1983
5.29.89.59	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	978
149.88.91.94	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	973
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	40
213.8.96.180	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	12
81.218.131.214	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
66.249.78.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
168.63.139.43	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
87.68.53.54	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
24.90.111.185	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
212.199.52.66	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
79.180.219.95	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.19.85.29	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

04-26-2015-16:03:07 to 04-26-2015-17:03:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.240.236.119	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
46.116.211.238	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1

04-26-2015-16:03:07 to 04-26-2015-17:03:07

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.78.190	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	89
66.249.78.11	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	3
222.186.34.23	China	147.237.77.216	dover.idf.il	SERVER-APACHE Apache Tomcat Web Application Manager access	2
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
193.43.244.102	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.23.89	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
178.33.132.22	France	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
149.78.137.56	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
94.159.193.36	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.65	China	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.4	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
222.186.21.68	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
36.72.228.72	Indonesia	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 2048	1
193.104.115.2	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
5.196.147.122	Germany	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
192.116.108.151	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.182.73	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
176.12.151.86	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.186.124	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
84.228.113.154	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.64	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.34.23	China	147.237.77.216	dover.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	1
36.72.228.72	Indonesia	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 3072	1
36.72.228.72	Indonesia	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -f -sS	1

04-26-2015-16:03:07 to 04-26-2015-17:03:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
95.86.95.156	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
194.90.178.146	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
213.151.63.236	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
212.45.46.36	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
31.168.215.196	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	6
46.19.86.76	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
46.19.86.114	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	alert	3
2.52.148.161	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
207.241.237.166	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.52.148.161	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	2
212.76.127.44	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
109.67.97.6	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
192.116.98.164	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
81.218.145.177	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
212.179.46.21	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
54.224.21.23	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
82.166.181.57	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
162.243.2.119	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
60.225.211.88	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.19.86.121	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
188.165.15.13	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
66.249.67.58	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
5.29.194.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
54.84.198.40	United States	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
212.76.127.111	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
109.253.135.0	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
54.173.176.222	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
2.52.148.161	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
109.253.137.195	Israel	147.237.77.243	mobile.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
46.19.85.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	204
109.253.144.92	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	14
80.179.143.44	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	11
219.134.174.160	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 219.134.174.160	Block	10
84.229.45.69	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
46.19.85.211	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
178.137.85.64	Ukraine	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il//901-11442-en/	Block	3
212.150.155.130	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
46.121.233.12	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
109.67.3.9	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	3
46.119.113.155	Ukraine	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il//901-11442-en/	Block	3
149.78.194.187	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
109.67.135.244	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
213.57.182.163	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
82.80.26.10	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.182.127.174	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
37.26.147.229	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
77.126.212.188	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
89.139.176.236	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
134.83.1.241	United Kingdom	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
2.54.22.220	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.183.19.35	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	2
2.54.35.47	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
94.159.158.154	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
31.168.215.196	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//webresource.axd	Block	1
79.183.21.146	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	1
109.67.118.116	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19149-he/dover	Block	1
46.120.6.133	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
213.57.72.74	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
87.236.105.61	Germany	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
81.218.179.41	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233//1134-he/atal.aspx	Block	1
37.142.156.172	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.177.180.3	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
2.54.52.88	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.158.108	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	1
95.179.91.22	Russian Federation	147.237.77.176	matpash.idf.il	Admin Blocking	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19478-he/idfgdover.aspx	Block	1
212.143.118.8	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.86.228	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
31.210.183.11	Israel	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
157.55.39.3	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.120.23.33	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
89.138.212.200	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
46.19.85.110	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
185.32.179.4	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.128.30	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
132.72.134.143	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1

04-26-2015-16:03:07 to 04-26-2015-17:03:07