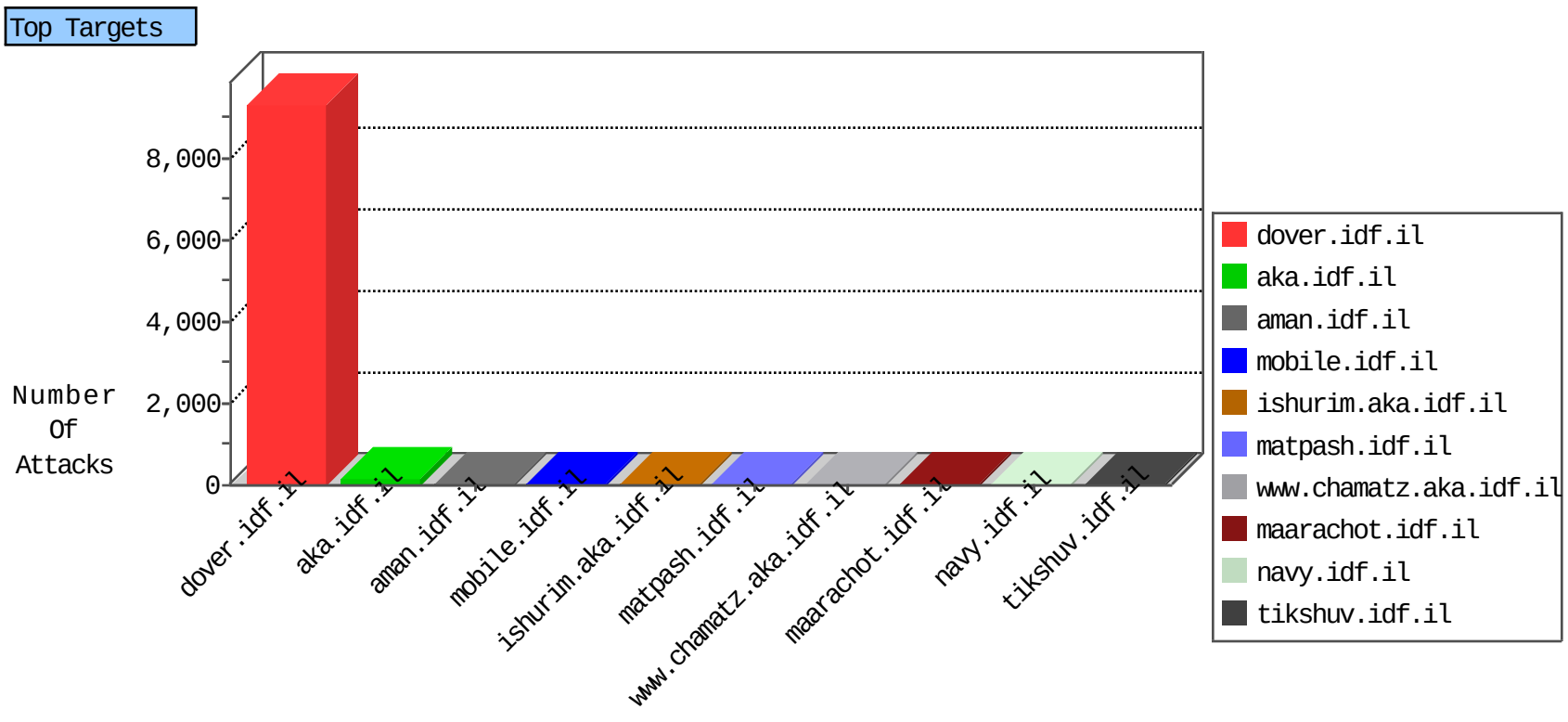
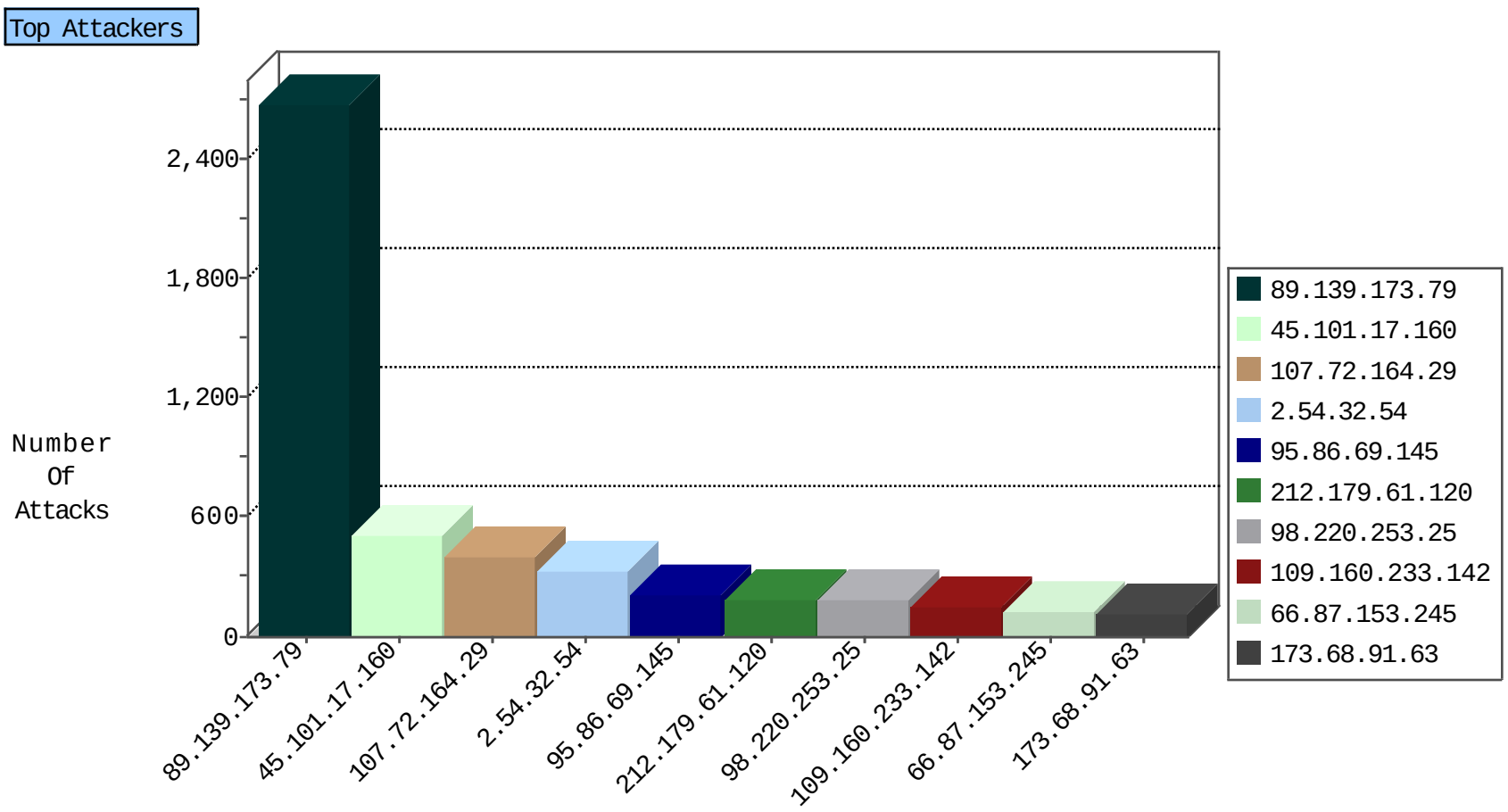
04-19-2015-23:03:03 to 04-20-2015-00:03:03

IDF Under Attack
04-19-2015-23:03:03





04-19-2015-23:03:03 to 04-20-2015-00:03:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
109.186.56.204	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	311
84.228.138.29	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	151
84.108.237.43	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	61
66.249.78.159	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33
5.29.120.22	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15
5.22.130.60	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
84.110.49.53	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
85.130.139.64	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
46.210.113.179	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
204.8.154.50	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
71.6.167.142	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
204.8.154.50	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
98.220.253.25	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
2.52.32.38	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

04-19-2015-23:03:03 to 04-20-2015-00:03:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
149.88.108.175	United States	147.237.77.216	dover.idf.il	1633: HTTP: WebDAV Protocol PROPFIND Method	Block	5
71.6.167.142	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	2
41.252.193.62	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
198.20.69.98	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
85.65.140.254	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.53	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	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	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
94.159.213.41	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
84.108.62.201	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.17	m.my-kosher-kravi.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
71.6.165.200	United States	147.237.0.15	kosher-kravi.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
85.25.103.50	Germany	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.212	e.dover.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	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1

04-19-2015-23:03:03 to 04-20-2015-00:03:03

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	21
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
37.162.110.165	France	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.204	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.50	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.64	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
222.69.94.13	China	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 2048	1
101.226.2.99	China	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
88.249.106.23	Turkey	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
77.127.125.68	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.127	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
61.240.144.65	China	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
222.69.94.13	China	147.237.77.176	matpash.idf.il	ET SCAN NMAP -f -sS	1
124.234.13.254	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
101.226.2.99	China	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1

04-19-2015-23:03:03 to 04-20-2015-00:03:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
89.139.173.79	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2677
45.101.17.160		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	507
107.72.164.29	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	395
2.54.32.54	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	321
95.86.69.145	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	206
212.179.61.120	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	184
98.220.253.25	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	180
109.160.233.142	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	148
66.87.153.245	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	128
173.68.91.63	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	115
93.173.19.67	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	110
162.243.222.48	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	92
46.19.85.199	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	91
46.19.86.180	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	84
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	68
77.101.125.202	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	61
41.252.193.62	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	59
109.64.164.85	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	54
85.65.128.197	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	51
46.120.101.205	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
109.253.135.8	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	46
109.253.157.154	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
85.64.70.26	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
109.253.140.167	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
109.253.157.231	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
109.253.138.236	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
109.253.141.127	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
79.176.201.179	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
80.230.95.56	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
109.253.143.238	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
109.253.138.220	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
66.249.81.218	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
5.102.254.165	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
46.19.86.236	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
149.254.58.140	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
192.118.73.46	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
46.117.158.219	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
207.46.13.35	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
109.253.146.242	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
207.46.13.52	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
109.253.147.97	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
176.12.138.118	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
109.253.146.102	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
213.57.58.109	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
94.249.79.241	Jordan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
149.78.229.149	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	39
95.86.127.69	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	14
149.88.108.175	United States	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	4
87.69.241.92	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 87.69.241.92	Block	4
46.19.86.11	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	3
195.242.218.133	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-11442-en/	Block	3
87.69.241.92	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt.aspx	Block	2
79.182.102.221	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	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
66.249.78.127	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 66.249.78.127	Block	2
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	2
66.249.78.134	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 66.249.78.134	Block	2
180.76.4.146	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
68.180.228.57	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il//modiin/default.aspx	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-13967-he/dover.aspx	Block	1
109.253.141.96	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
54.159.218.151	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.49	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/iturim/asp/list.asp	Block	1
66.249.78.134	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/shared/usercontrols/headerupper/	Block	1
109.65.134.250	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.65.161	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
46.19.85.96	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.65.171.187	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
188.165.15.181	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9059-he/refuah.aspx	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/smalim/html/1.asp	Block	1
66.249.78.120	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/modules/forums.frm/frmprintmessage.aspx	Block	1
140.32.16.3	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/yohalan/main/main	Block	1
93.172.161.161	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
58.22.150.79	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/info.asp/trackback/	Block	1
80.246.140.206	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forgotpassword.aspx	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
109.67.16.220	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/giyus/terms.aspx	None	1
66.249.65.178	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
85.65.201.14	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
93.172.163.139	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.64.20	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/scriptresource.axd	Block	1
83.130.115.211	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
157.55.39.208	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/homefront/faq/5.stm	Block	1
66.249.67.49	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
109.160.183.101	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
46.116.148.204	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
87.69.233.240	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.207.237.131	France	147.237.72.166	aka.idf.il	Abnormally Long Request URL	Block	1
213.57.182.91	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/userdetails/updateuserdetails.aspxhttps:/www.aka.idf.il/main/giyus/userdetails/updateuserdetails.aspx	Block	1
66.249.78.127	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/modules/forums.frm/frmuserdetails.aspx	Block	1
66.249.64.63	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.26.147.217	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
84.109.165.222	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1