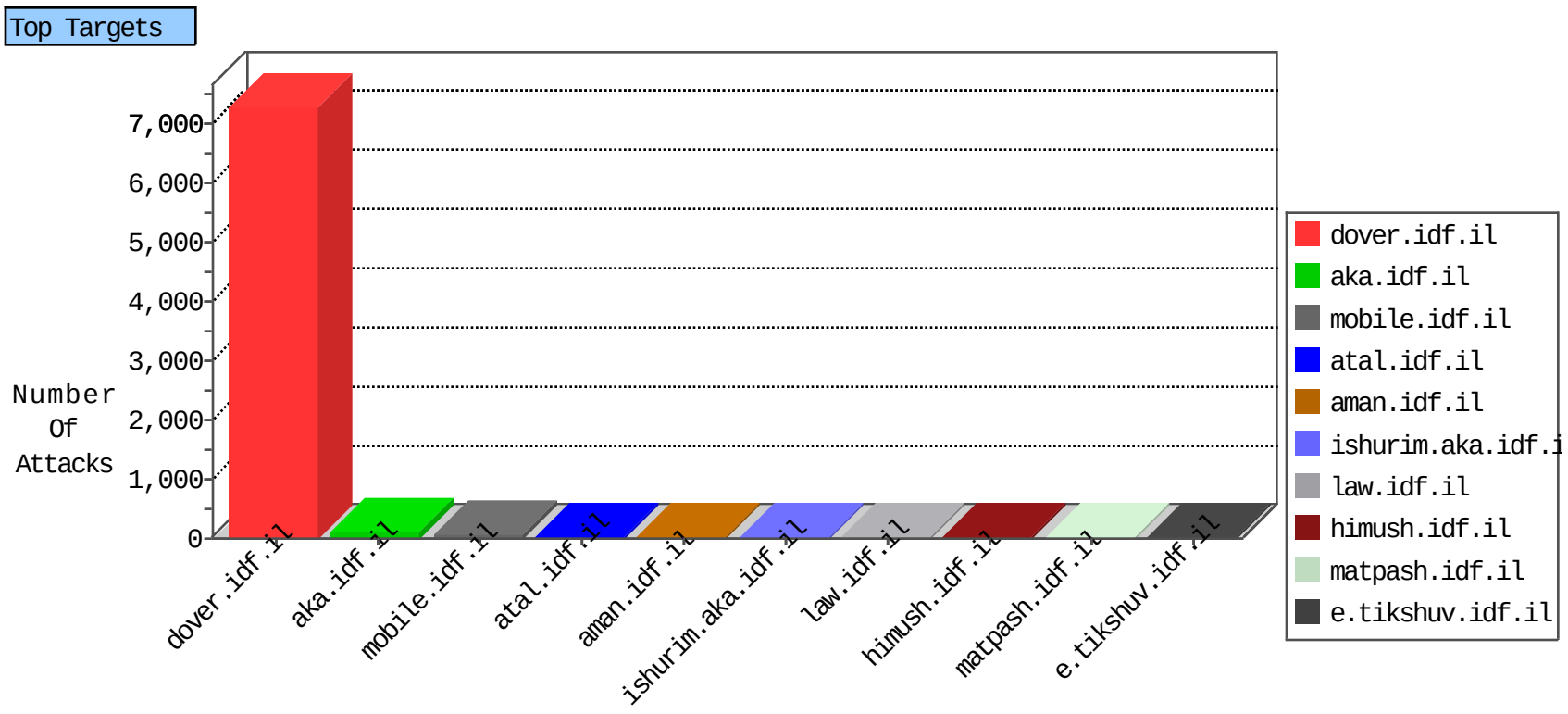
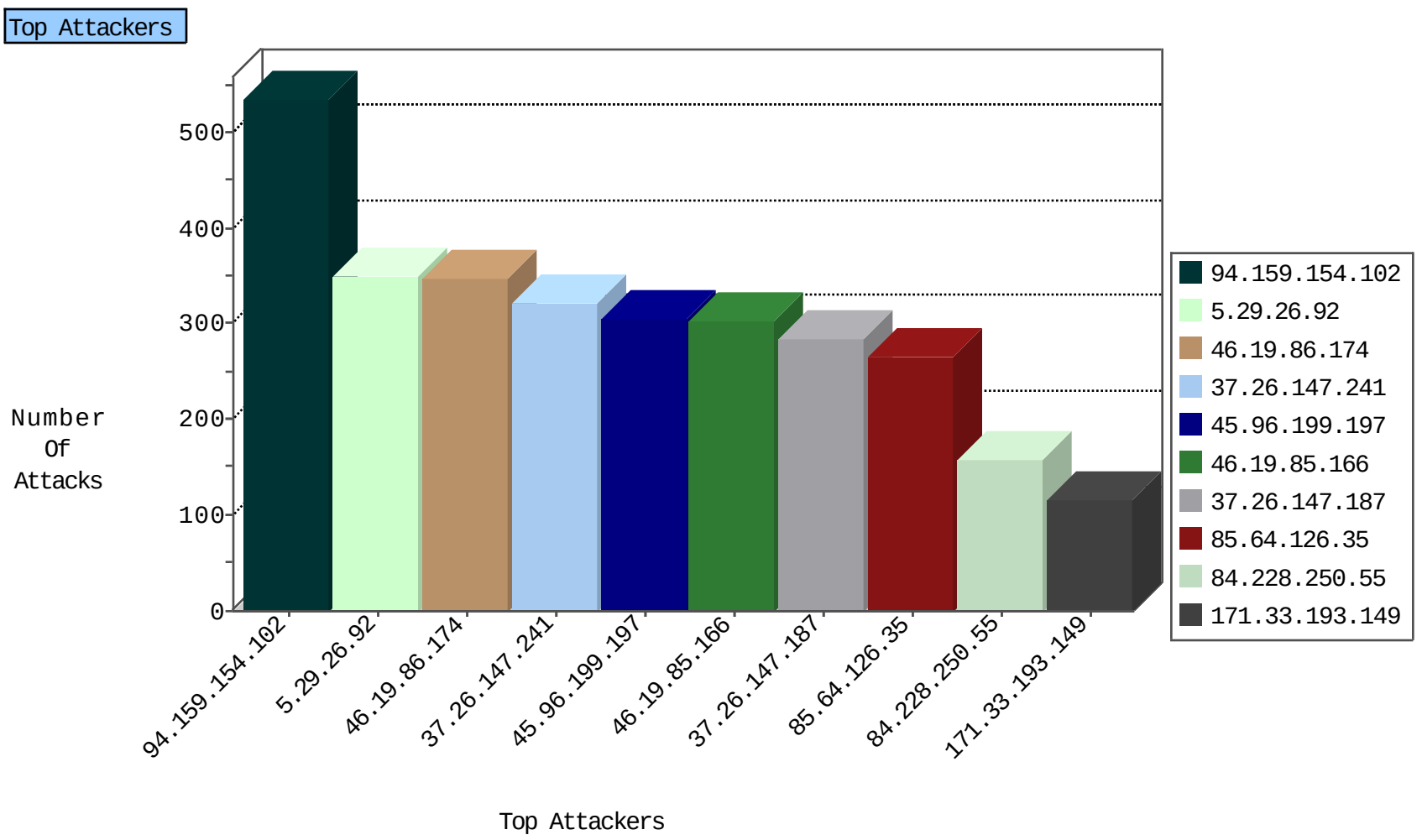
04-17-2015-17:03:07 to 04-17-2015-18:03:07

IDF Under Attack
04-17-2015-17:03:07

Top Targets



Top Attackers



04-17-2015-17:03:07 to 04-17-2015-18:03:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
91.240.80.30	Lebanon	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
50.207.82.46	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
79.177.205.154	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
192.168.14.32		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
204.184.37.4	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
124.232.142.220	China	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

04-17-2015-17:03:07 to 04-17-2015-18:03:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	10
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	10
149.78.135.192	United States	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
198.20.69.98	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	2
71.6.167.142	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	2
188.138.9.50	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.121	e.navy.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
66.240.192.138	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.234	halag.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
66.240.236.119	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.50	e.tikshuv.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
71.6.135.131	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
93.115.87.78	Anonymous Proxy	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
2.54.178.41	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	147.237.72.166	aka.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
71.6.135.131	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.234	halag.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
71.6.165.200	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
167.57.50.117		147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
71.6.135.131	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1

04-17-2015-17:03:07 to 04-17-2015-18:03:07

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	6
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	3
66.249.65.12	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
122.228.207.76	China	147.237.76.198	e.yohalan.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	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
113.21.226.56	New Zealand	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.74	United States	147.237.76.86	navy.idf.il	ET DROP Dshield Block Listed Source	1
128.199.207.123	Singapore	147.237.72.166	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
61.160.223.70	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.77.226	www.chamatz.aka.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
122.228.207.76	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
61.160.223.70	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
128.199.165.82	Singapore	147.237.72.166	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
122.228.207.76	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1

04-17-2015-17:03:07 to 04-17-2015-18:03:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
94.159.154.102	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	536
5.29.26.92	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	350
46.19.86.174	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	348
37.26.147.241	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	323
45.96.199.197		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	305
46.19.85.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	303
37.26.147.187	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	284
85.64.126.35	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	266
84.228.250.55	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	159
171.33.193.149	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	116
200.70.47.146	Argentina	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	99
84.111.7.209	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	82
103.242.190.242	India	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	76
204.184.37.4	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	70
46.19.85.26	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	68
79.178.167.209	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	67
101.170.85.77	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	65
149.78.208.132	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	62
79.182.123.28	Israel	147.237.77.243	mobile.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	60
85.250.192.105	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	59
77.126.22.187	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	56
96.242.131.75	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	52
46.19.86.198	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	51
85.250.55.98	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
87.69.59.252	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	49
212.76.106.191	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	49
46.19.86.96	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
2.54.178.235	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	46
84.228.158.236	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	44
66.249.93.160	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
109.67.109.67	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
68.177.122.37	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
178.221.59.60		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
176.12.149.204	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
95.86.105.38	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
46.120.64.113	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
46.120.160.217	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
66.249.93.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
109.253.146.112	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
109.253.145.44	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
85.65.48.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
207.38.173.98	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
46.116.149.165	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
84.228.114.105	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
207.46.13.77	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
176.12.136.107	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.64.186.173	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	5
2.54.141.22	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	4
157.55.39.130	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	3
85.130.255.53	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	3
207.46.13.104	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
89.80.33.85	France	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	2
149.78.235.116	United States	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
79.181.195.104	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
66.249.73.219	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	2
109.66.58.199	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/kapatz/undefined	Block	2
5.29.26.144	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
95.86.125.168	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//https:/www.idf.il/	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
66.249.73.203	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
46.121.115.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
80.230.93.132	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	1
70.167.8.42	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluimtemplates/inner.asp	Block	1
5.29.153.5	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
94.159.175.255	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.133	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/templates/oprolescategory/oprolescategory.in.aspx	Block	1
87.69.101.143	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
46.19.85.2	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
79.180.21.188	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/sitemap/sitemap.aspx	Block	1
66.249.73.211	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
89.139.57.195	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.95.57.145	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
46.147.176.30	Russian Federation	147.237.77.74	law.idf.il	Unknown HTTP Request Method COOK in URL www.law.idf.il/14-en/patzar.aspx	Block	1
24.15.69.250	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
94.159.175.255	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method Â¦tl00_ctl00_ScriptManager1_HiddenField=&__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=5cgLVfqdOscdJazANXkxdebd%2FSp6QQqPHJz4ZxlIC9jbFr2by6KVx1d0L1jnrHy8W4RXVqyqXgAQ0%2FQKQWcm7W6vL1FxD0Nlj%2Bd3ewQ0JHnz8uCRo5TP3ciIaeygZhpu77UtQ7pm0THKCKnJ0uFXAN4cyFYoqds8P69vwsN6GOnLoODC&ctl00%24ctl00%24txtSearch=&ctl00%24ctl00%24rbSearchSites=rbAllSites&ctl00%24ctl00%24cphMain%24TochenPlaceHolder%24txtPassword=srudcv76%3F&ctl00%24ctl00%24cphMain%24TochenPlaceHolder%24txtRepeatPassword=srud	Block	1
87.69.101.143	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/kapatz/citizencontact.aspx	None	1
66.249.67.32	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/m/	Block	1
46.19.85.7	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.20.151	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
109.65.17.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
66.249.78.215	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.kosher-kravi.idf.il/mobile/	Block	1
93.172.75.237	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
84.109.208.242	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/info.asp?moduleid=2&catid=22703&docid=22716	Block	1
79.178.4.235	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gius	Block	1
31.13.110.122	Ireland	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	1
157.55.39.179	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
94.159.175.255	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method Â¦tl00_ctl00_ScriptManager1_HiddenField=&__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=5cgLVfqdOscdJazANXkxdebd%2FSp6QQqPHJz4ZxlIC9jbFr2by6KVx1d0L1jnrHy8W4RXVqyqXgAQ0%2FQKQWcm7W6vL1FxD0Nlj%2Bd3ewQ0JHnz8uCRo5TP3ciIaeygZhpu77UtQ7pm0THKCKnJ0uFXAN4cyFYoqds8P69vwsN6GOnLoODC&ctl00%24ctl00%24txtSearch=&ctl00%24ctl00%24rbSearchSites=rbAllSites&ctl00%24ctl00%24cphMain%24TochenPlaceHolder%24txtPassword=srudcv76%3F&ctl00%24ctl00%24cphMain%24TochenPlaceHolder%24txtRepeatPassword=srudcv76%3F&ct	Block	1
87.69.210.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
66.249.67.42	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/mobile/	Block	1