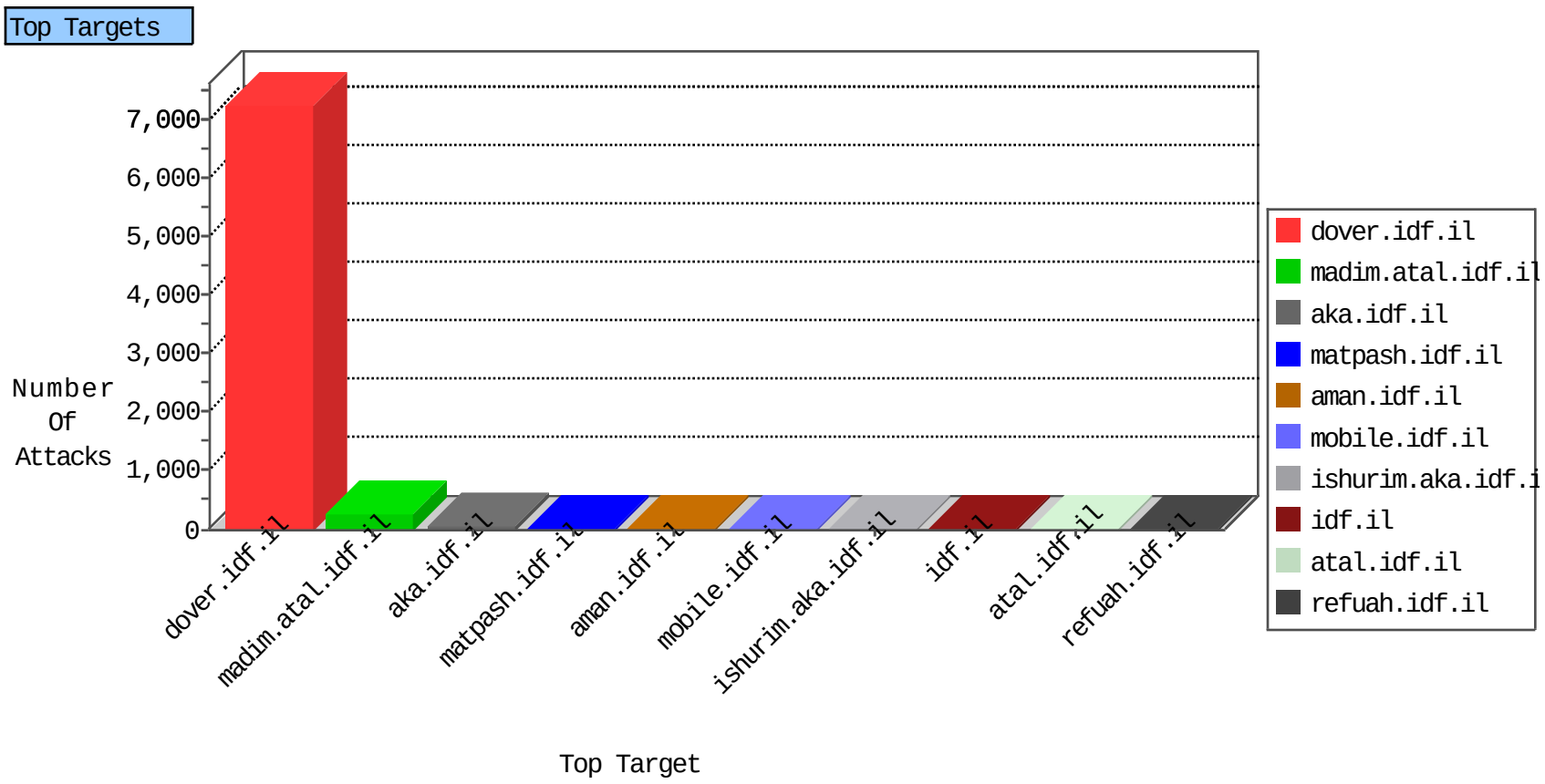
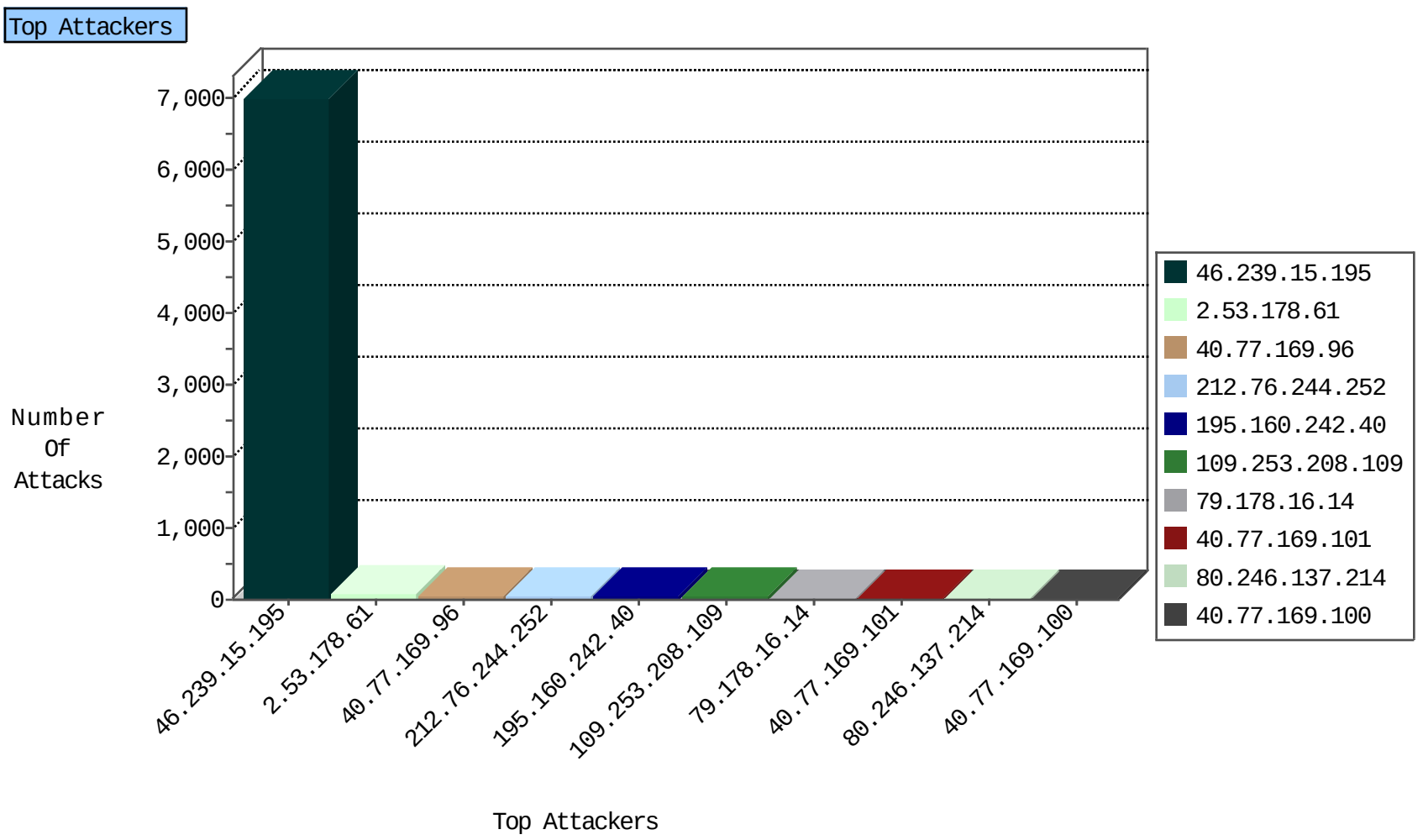
08-28-2016-08:04:10 to 08-28-2016-09:04:10

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-28-2016-08:04:10 to 08-28-2016-09:04:10

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.76.70	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
46.239.15.195	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	2
58.218.204.245	China	147.237.76.199	e.nakchal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
212.25.74.130	Israel	147.237.72.166	aka.idf.il	Black List	drop	1
82.80.78.2	Israel	147.237.77.216	dover.idf.il	Black List	drop	1
52.204.200.107	United States	147.237.76.44	e.refuah.idf.il	Black List	drop	1
104.238.184.170	United Kingdom	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1

08-28-2016-08:04:10 to 08-28-2016-09:04:10

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.197.177.26	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
138.201.127.112	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

08-28-2016-08:04:10 to 08-28-2016-09:04:10

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.227.67.172	147.237.77.121	Sweden	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
191.96.249.232	147.237.0.33	Chile	idf.il	ET SCAN NMAP -sS window 1024	1
2.53.13.136	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
190.252.56.113	147.237.0.35	Colombia	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
163.172.220.43	147.237.0.17	United Kingdom	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.76.196	United Kingdom	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
120.236.19.10	147.237.0.19	China	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
94.102.48.195	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.34.223	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.246.136.100	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
222.186.34.223	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.218.204.245	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
212.143.240.190	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.210.186.246	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
191.96.249.189	147.237.77.212	Chile	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.169.150	147.237.76.197	United Kingdom	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
120.236.19.10	147.237.0.19	China	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
94.102.48.195	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 1024	1
92.29.70.104	147.237.77.205	United Kingdom	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.34.223	147.237.0.200	China	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.179.187.120	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.69.133.223	147.237.72.166	Russian Federation	aka.idf.il	portscan: TCP Distributed Portscan	1

08-28-2016-08:04:10 to 08-28-2016-09:04:10

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.239.15.195	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6992
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
212.76.244.252	Belgium	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	17
40.77.169.100	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	17
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	13
40.77.169.101	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	11
199.203.179.99	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	10
40.77.169.97	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
40.77.169.102	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
77.75.77.17	Czech Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
203.133.171.21	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
40.77.169.99	United States	147.237.72.156	aman.idf.il	drop	SAM rule	drop	6
40.77.169.100	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	5
212.29.203.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
40.77.169.98	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	5
40.77.169.102	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
40.77.169.101	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
40.77.169.100	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	2
176.13.248.245	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	2
31.13.100.119	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
93.158.152.52	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
213.8.115.122	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	2
40.77.169.100	United States	147.237.77.216	dover.idf.il	drop		drop	2
93.173.235.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.147	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
216.72.40.185	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	2
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
31.13.109.118	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.212.11	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
176.13.239.157	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.128.94	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
62.0.204.129	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.223.126	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
212.235.33.100	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.134.181	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.160	United States	147.237.0.33	idf.il	drop		drop	1
46.19.85.153	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.105.247.236	United States	147.237.0.33	idf.il	drop		drop	1
31.13.103.100	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.137.137	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.161	United States	147.237.0.33	idf.il	drop		drop	1
40.77.169.100	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
192.168.173.102		147.237.77.216	dover.idf.il	drop		drop	1
31.13.103.107	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

08-28-2016-08:04:10 to 08-28-2016-09:04:10

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.178.61	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	84
109.253.208.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	32
79.178.16.14	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
80.246.137.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	28
109.253.215.154	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
2.53.180.51	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	13
109.253.229.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
2.53.162.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
2.53.172.170	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
46.19.86.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
85.65.127.79	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.65.127.79	Block	5
108.171.128.172	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/navmenu/	Block	4
108.171.128.172	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	4
109.253.159.2	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
37.26.147.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.140.58	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.53.11.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.235.82	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.216.75	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.10	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.53.23.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.240.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.27	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.253.206.78	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.5.72	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
37.60.40.116	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mains/sachar	Block	2
80.246.136.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
212.179.21.194	Israel	147.237.0.19	madim.atal.idf.i	Multiple Unauthorized URL Access from 212.179.21.194	Block	2
37.26.147.148	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
62.219.138.136	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
79.181.175.184	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
192.118.48.248	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
46.19.86.12	Israel	147.237.72.166	aka.idf.il	Unknown Parameter doc in www.aka.idf.il/main/giyus/general.aspx	None	1
2.53.0.63	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
212.199.84.131	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
68.180.230.171	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx	Block	1
66.102.9.118	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/drushim/	Block	1
46.19.85.103	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
109.66.161.98	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
80.246.130.18	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
194.242.168.227	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/sitemap.aspx	Block	1
85.65.127.79	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
2.53.0.63	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 2.53.0.63	Block	1
212.199.84.131	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/wp-login.php	Block	1
77.125.10.42	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1247-he/atal.aspx	Block	1
66.249.64.105	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/m/main/giyus/general.aspx	Block	1
176.13.233.88	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.230	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1

08-28-2016-08:04:10 to 08-28-2016-09:04:10