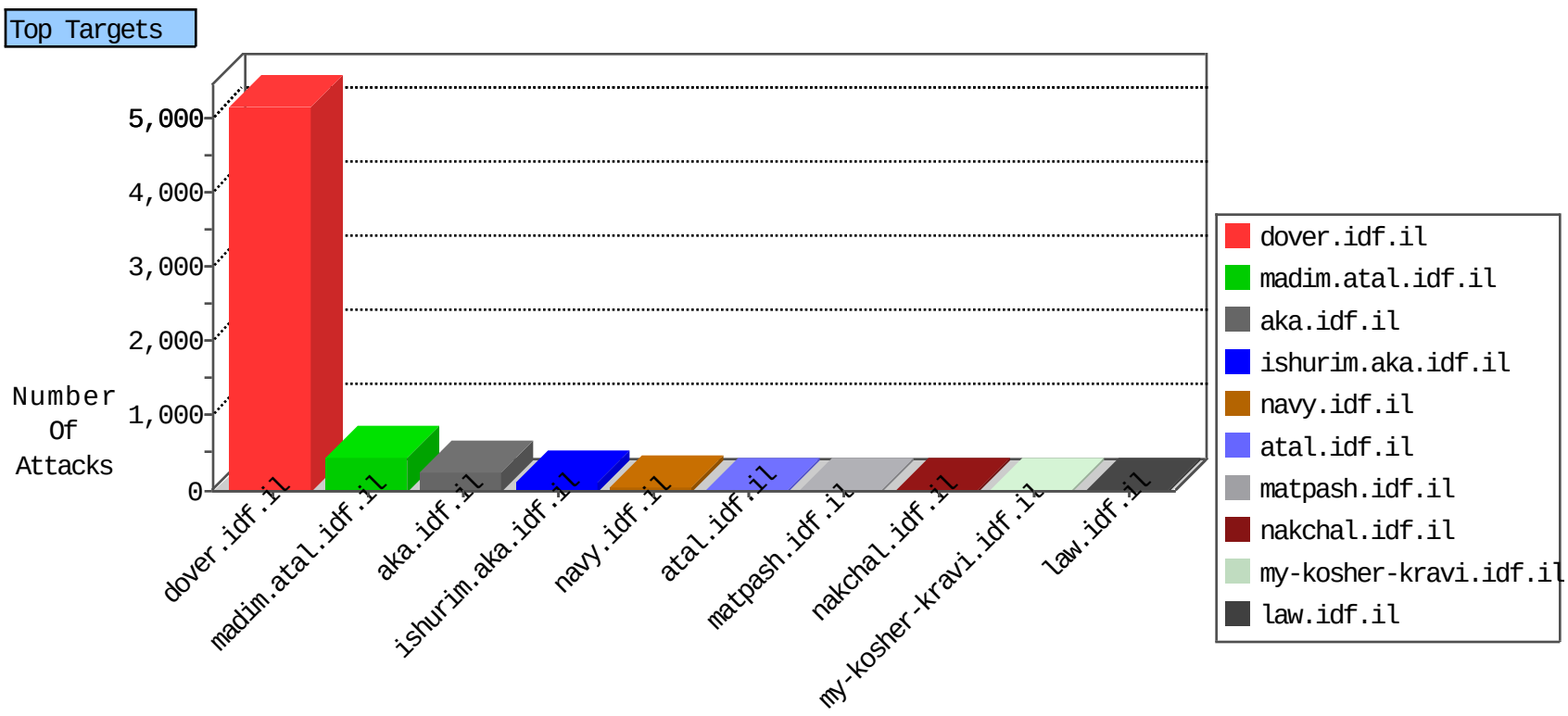
10-21-2015-07:04:04 to 10-21-2015-08:04:04

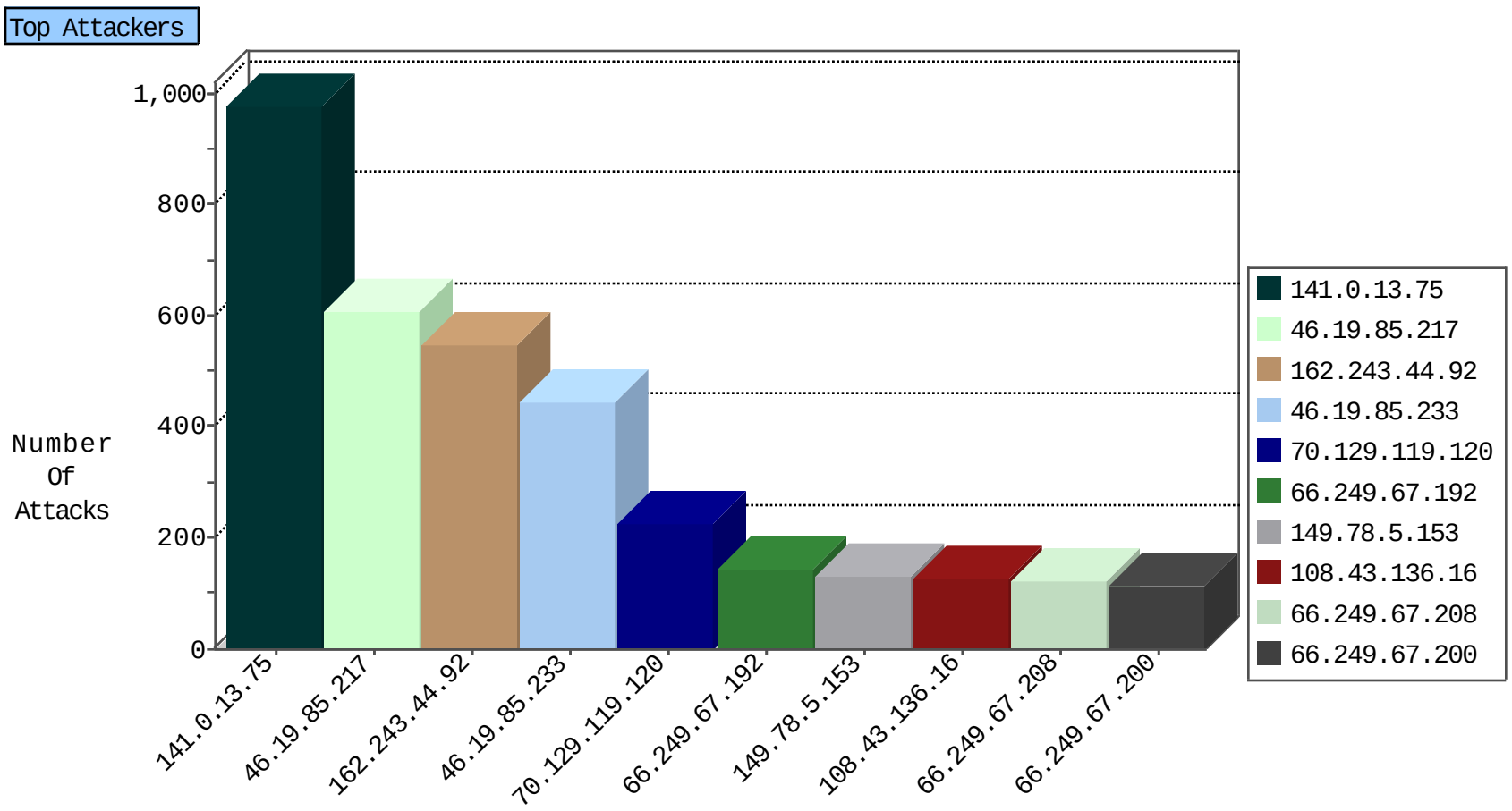
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-21-2015-07:04:04 to 10-21-2015-08:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.59	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	195
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	83
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	69
46.19.85.4	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	57
87.69.2.206	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
46.19.85.120	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
176.13.18.103	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
185.32.179.193	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
46.19.86.209	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
203.116.59.35	Singapore	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
5.22.130.28	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
176.12.140.152	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
46.19.86.209	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
195.160.240.11	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
109.64.166.3	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.86.79	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.86.157	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
80.230.16.3	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.86.200	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.12.141.153	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
192.118.11.120	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.13.6.131	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
142.160.216.26	Canada	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
108.43.136.16	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.116.217.136	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
24.94.54.23	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
81.218.48.37	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
93.174.93.146	Netherlands	147.237.8.50	e.tikshuv.idf.il	Invalid TCP Flags	drop	1
46.19.86.209	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
89.248.172.98	Netherlands	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

10-21-2015-07:04:04 to 10-21-2015-08:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-21-2015-07:04:04 to 10-21-2015-08:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.186.91.47	147.237.77.216	Finland	dover.idf.il	ET SCAN Potential SSH Scan	1
89.248.172.201	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.186.91.47	147.237.77.205	Finland	prisha.idf.il	ET SCAN Potential SSH Scan	1
89.248.172.201	147.237.77.74	Netherlands	law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.186.91.47	147.237.77.176	Finland	matpash.idf.il	ET SCAN Potential SSH Scan	1
89.248.172.201	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.151.52.8	147.237.77.74	Ukraine	law.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.172.201	147.237.72.217	Netherlands	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
202.106.211.99	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
89.248.172.201	147.237.72.166	Netherlands	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
202.106.211.99	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
89.248.172.201	147.237.0.33	Netherlands	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
195.68.62.253	147.237.0.17	United Kingdom	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
80.186.91.47	147.237.77.235	Finland	sviva.idf.il	ET SCAN Potential SSH Scan	1
123.151.149.222	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
80.186.91.47	147.237.77.226	Finland	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
89.248.172.201	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.186.91.47	147.237.77.212	Finland	e.dover.idf.il	ET SCAN Potential SSH Scan	1
89.248.172.201	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.186.91.47	147.237.77.178	Finland	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
89.248.172.201	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.186.91.47	147.237.77.170	Finland	maarachot.idf.il	ET SCAN Potential SSH Scan	1
89.248.172.201	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
45.33.70.65	147.237.76.200		eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
89.248.172.201	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
202.106.211.99	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
89.248.172.201	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
202.106.211.99	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
80.186.91.47	147.237.77.243	Finland	mobile.idf.il	ET SCAN Potential SSH Scan	1
177.225.54.120	147.237.76.148	Mexico	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
80.186.91.47	147.237.77.233	Finland	atal.idf.il	ET SCAN Potential SSH Scan	1
89.248.172.201	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

10-21-2015-07:04:04 to 10-21-2015-08:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.0.13.75	Norway	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	879
46.19.85.217	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	608
162.243.44.92	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	519
70.129.119.120	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	226
149.78.5.153	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	131
108.43.136.16	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	123
46.19.86.30	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	107
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	100
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	57
79.181.97.22	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	52
142.160.216.26	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
54.187.55.213	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	46
176.13.18.103	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	45
176.13.9.6	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
185.32.179.193	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
80.230.39.74	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
109.67.62.16	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
203.116.59.35	Singapore	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
46.116.217.136	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
37.60.42.208	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
46.19.86.235	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	32
37.142.221.155	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	31
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
217.23.45.213	Jordan	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	29
93.172.184.58	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
46.19.86.79	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
166.137.126.111	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
195.160.240.11	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	SAM rule	drop	23
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
212.179.90.106	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
212.235.98.139	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
176.106.227.231	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
66.249.67.192	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
46.19.86.138	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
66.249.67.192	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
87.69.2.206	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
212.199.182.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
66.249.67.208	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
66.249.67.200	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
85.65.133.30	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
66.249.67.208	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
37.142.219.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
46.19.86.209	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
109.65.15.218	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13

10-21-2015-07:04:04 to 10-21-2015-08:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.233	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.233	Block	442
66.249.67.200	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.200	Block	65
66.249.67.192	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.192	Block	65
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	52
66.249.67.208	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.208	Block	52
66.249.67.192	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	39
66.249.67.208	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	39
162.243.44.92	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 162.243.44.92	Block	26
166.137.126.111	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.idf.il/1038-en/dover.aspx	Block	13
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	13
66.249.64.239	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	13
199.16.156.126	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 199.16.156.126	Block	13
2.54.171.57	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	13
176.12.141.1	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/mobile/templates/basket/basket.aspx	Block	13
66.249.81.133	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/1746-he/lifestyle.aspx	Block	13
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/4/size220x0/17374.jpg	Block	13
80.246.136.153	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	13
5.175.13.138	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/qiyus/qeneral/default.a	Block	13
176.106.227.231	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/igf	Block	13
66.249.93.154	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyu	Block	13
207.46.13.141	United States	147.237.72.166	aka.idf.il	Unknown Parameter 136cd360 in www.aka.idf.il/main/home/default.aspx	None	13
84.110.144.251	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	13
182.118.54.73	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/webresource.axd%3fd	Block	13
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	13
216.218.206.68	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	13
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	13
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 54.245.64.111	Block	13
183.136.142.96	China	147.237.76.31	nakchal.idf.il	URL is Above Root Directory nakhal.idf.il/../shared/clientscripts/jquery.plugins/jquery.equalheights.js	Block	13
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/an	Block	13
66.249.67.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	13
66.249.67.200	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10

10-21-2015-07:04:04 to 10-21-2015-08:04:04