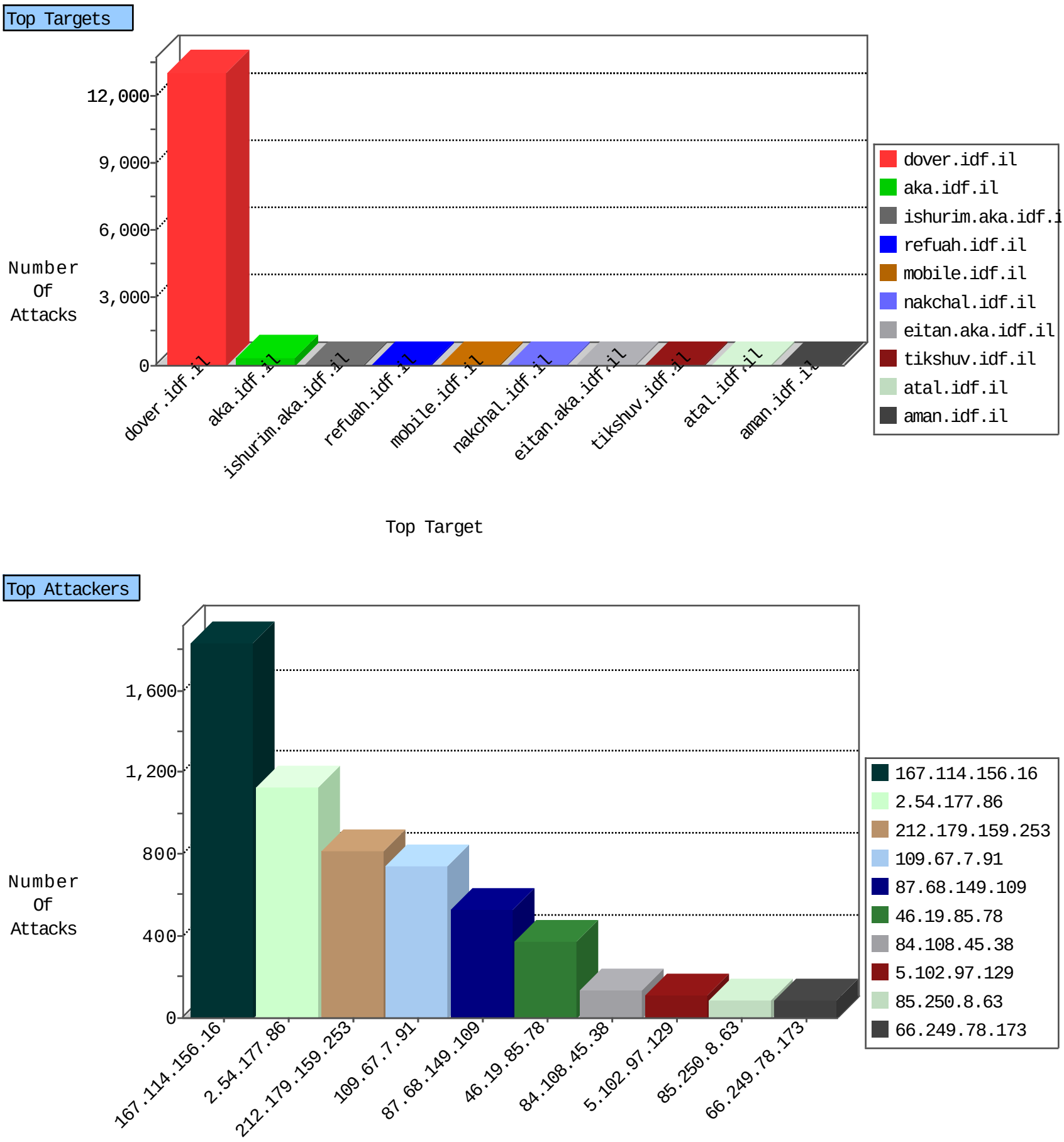
11-03-2015-12:04:03 to 11-03-2015-13:04:03

IDF Under Attack
Daily Report



11-03-2015-12:04:03 to 11-03-2015-13:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.27	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3490
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2736
176.13.1.164	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2506
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	848
77.125.131.72	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	54
109.64.205.231	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	36
89.139.43.181	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	33
84.228.62.44	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
192.114.23.210	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	28
46.19.85.162	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
185.32.179.27	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
79.180.14.109	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	23
46.19.85.62	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	22
82.80.147.76	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	21
109.67.167.225	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
212.143.122.11	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
195.244.23.42	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
46.19.85.180	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
176.12.145.62	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
82.80.196.44	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
2.54.182.152	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
176.12.145.13	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
46.19.86.199	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
185.32.179.253	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
80.149.240.82	Germany	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
185.120.126.11		147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
31.154.3.17	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
79.182.129.248	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
176.13.5.121	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
176.12.149.241	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
89.108.144.114	Lebanon	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
37.26.148.235	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
176.12.146.32	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
101.181.130.74	Australia	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
192.116.90.248	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
176.12.142.31	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
138.134.102.15	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
109.67.103.122	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
92.63.159.229	Austria	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
84.108.87.125	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
2.54.170.160	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
93.172.98.62	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.128.85	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.13.15.142	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.52.31.166	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
193.106.54.33	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
93.173.239.195	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.4.234	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
88.150.161.75	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5

11-03-2015-12:04:03 to 11-03-2015-13:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
10.0.0.24		147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
82.80.51.175	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
79.183.198.161	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
109.67.103.122	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
94.126.81.100	Sweden	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
101.181.130.74	Australia	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
204.15.96.67	United States	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

11-03-2015-12:04:03 to 11-03-2015-13:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	2
66.249.67.34	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
46.253.81.99	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.65	147.237.77.216	Israel	dover.idf.il	ET SCAN NMAP -sA (2)	1
188.138.9.51	147.237.0.16	Germany	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.157.48	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
180.169.20.145	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
180.169.20.145	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
91.135.170.240	147.237.76.39	Austria	mobile.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
67.214.204.126	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
62.219.165.105	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.121.80.100	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
185.32.179.201	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
180.169.20.145	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
180.169.20.145	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
91.135.170.240	147.237.76.39	Austria	mobile.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
91.135.170.240	147.237.76.39	Austria	mobile.meitav.idf.il	ET SCAN NMAP -f -sS	1

11-03-2015-12:04:03 to 11-03-2015-13:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.177.86	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1125
212.179.159.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	813
109.67.7.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	742
87.68.149.109	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	530
46.19.85.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	370
84.108.45.38	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	134
5.102.97.129	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	108
184.105.255.230	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	74
188.161.67.201	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	73
84.109.37.80	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
46.19.85.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
138.134.102.15	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
37.26.147.235	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
37.26.147.219	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
66.249.78.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
46.120.24.108	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
41.218.185.71	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
37.26.146.214	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
66.249.78.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
46.19.86.145	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
46.185.150.37	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
52.3.130.218	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
85.250.8.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
2.52.2.84	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
185.4.252.172	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
79.183.14.73	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
46.19.85.35	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
99.225.77.233	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
2.54.143.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
89.108.144.114	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
85.250.8.63	Israel	147.237.76.42	refuah.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	40
185.6.59.238	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
176.12.144.156	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
77.125.131.72	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
176.12.138.33	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
176.13.1.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
195.212.29.181	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
101.181.130.74	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
31.168.17.161	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
46.19.85.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
46.121.158.3	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
109.67.103.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
5.29.6.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.120.69.107	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 46.120.69.107	Block	7
188.161.67.201	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	3
79.180.208.184	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	2
80.246.136.100	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.85.61	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Open Mode	None	2
2.54.21.134	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.67.103.122	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
79.176.42.202	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
31.154.159.101	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
195.160.240.11	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res ources/images/innerpage/goback.gif	Block	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
141.212.122.160	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
95.86.111.147	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.86.111.147	Block	1
54.66.198.160	Australia	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/wp-login.php	Block	1
46.19.85.205	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
208.115.113.89	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/67906.pdf	Block	1
2.54.147.209	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	1
66.249.64.113	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
109.67.103.122	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/	Block	1
46.116.206.225	Israel	147.237.72.166	aka.idf.il	Unknown Parameter _ in www.aka.idf.il/main/giyus/	None	1
85.65.233.241	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
37.26.148.164	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
203.133.168.79	Korea, Republic of	147.237.76.147	chinuch.aka.idf.i	Unknown Parameter l in www.chinuch.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	None	1
2.52.26.78	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
167.114.211.10	Canada	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wordpress/wp-admin/	Block	1
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
95.86.111.147	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-13807-he/dover.aspx&sa=u&ved=0cdyqqoubahukewj 1n8m0i_tiahwjcrqkhwqia3o&sig2=tepj0gd5fix-7smhzyoisa&usg=afqjcnf _yysnn5nenyeifqzj5giiszwr1a	Block	1
54.172.55.174	United States	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
46.19.86.196	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.25.112.2	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/960.css	Block	1
82.102.170.194	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.102.97.129	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuh g	Block	1
193.201.224.32	Ukraine	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-ar/cogat.aspx	Block	1
66.249.64.118	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/163-he/patzar.aspx	Block	1
109.226.22.161	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.130.226.205	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	1
80.74.126.8	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.26.148.164	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
207.46.13.98	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/smalim.aspx	None	1
2.52.155.20	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/0/kkkkkkk=6feac0adkkkkkkk_6feac0ad	Block	1
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
109.67.21.97	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
54.172.55.174	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/wp-login.php	Block	1
46.116.80.231	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
212.235.20.193	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4616.jpg	Block	1

11-03-2015-12:04:03 to 11-03-2015-13:04:03