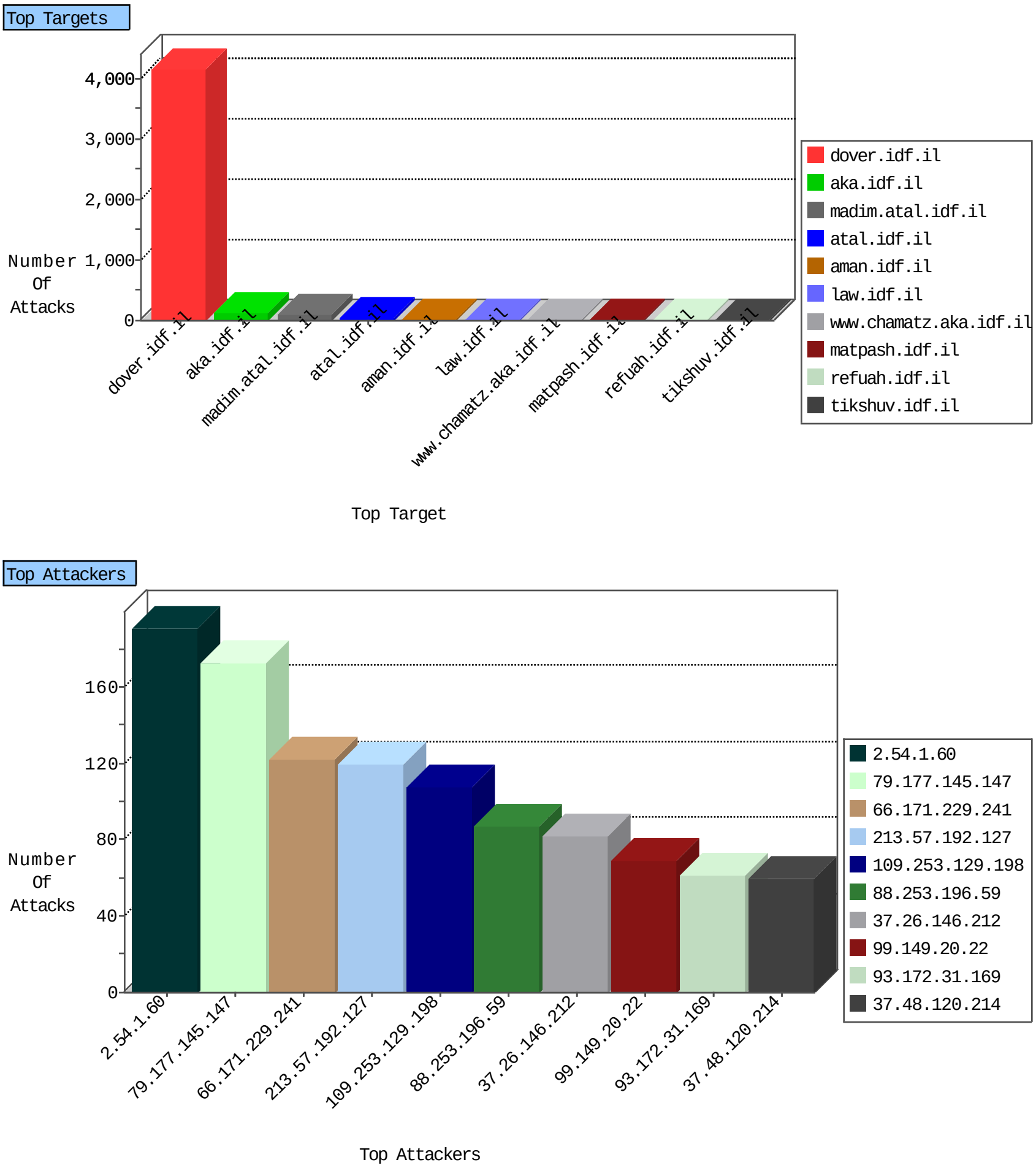
04-18-2015-15:03:01 to 04-18-2015-16:03:01

IDF Under Attack
04-18-2015-15:03:01



04-18-2015-15:03:01 to 04-18-2015-16:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
87.68.151.205	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	145
2.52.141.193	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
79.183.62.253	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	2
107.154.64.10	United States	147.237.0.35	akaws.idf.il	L4 Source or Dest Port Zero	drop	1
124.232.142.220	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
79.183.62.253	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
124.232.142.220	China	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
124.232.142.220	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1

04-18-2015-15:03:01 to 04-18-2015-16:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	23
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	5
109.186.132.136	Israel	147.237.77.234	halag.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.120	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
198.20.69.98	United States	147.237.72.217	e.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
85.25.103.50	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.34	yohalan.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
85.25.103.50	Germany	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.61	e.cogat.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	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
79.178.198.34	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
198.20.69.98	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
85.65.12.204	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	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
89.139.169.215	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1

04-18-2015-15:03:01 to 04-18-2015-16:03:01

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	10
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
31.168.81.129	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.190	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.73.211	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
46.121.134.85	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.173	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.89	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
130.211.138.52		147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
95.226.30.92	Italy	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
89.139.169.215	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.67	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
130.211.138.52		147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
95.226.30.92	Italy	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
95.226.30.92	Italy	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.64	China	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1

04-18-2015-15:03:01 to 04-18-2015-16:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
2.54.1.60	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	191
79.177.145.147	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	173
66.171.229.241	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	122
213.57.192.127	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	120
88.253.196.59	Turkey	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	87
37.26.146.212	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	82
99.149.20.22	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	63
93.172.31.169	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	61
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	60
46.120.67.182	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	57
46.19.85.16	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	54
82.205.66.168	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	48
2.54.130.236	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
109.253.133.226	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	45
109.253.145.180	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	44
176.12.143.255	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
68.66.102.219	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
176.12.147.220	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
93.172.78.21	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
79.182.155.99	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
109.253.131.14	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
94.159.211.20	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
109.253.130.140	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
46.120.86.39	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
213.57.145.187	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
109.253.156.131	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
37.26.147.152	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
46.19.86.199	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
62.219.111.97	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
79.180.197.89	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
80.178.67.228	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	26
87.68.21.64	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
79.182.56.87	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
207.46.13.1	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
87.162.160.155	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
85.250.22.4	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
31.168.81.129	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
77.127.72.207	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
46.19.86.55	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
46.116.94.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
89.139.160.123	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
93.172.77.65	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
31.51.200.8	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
82.80.25.221	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
109.65.5.49	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
176.12.151.94	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.253.129.198	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.129.198	Block	107
216.69.245.101	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	4
176.12.137.77	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	4
176.12.144.15	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	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
83.169.34.93	Germany	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
91.146.108.170	United Kingdom	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
157.55.39.5	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.5	Block	2
176.12.140.209	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	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
46.4.13.87	Germany	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
93.173.133.83	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/logi×§×™×• ×¡×§ ×ž×™×“×¢ ×?×™×©×™n.aspx	Block	2
62.219.78.146	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
157.55.39.178	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.178	Block	2
78.46.203.72	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
37.122.208.145	United Kingdom	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
216.69.245.101	United States	147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	2
108.167.132.74	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
31.186.228.30	United Kingdom	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
180.76.4.171	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
157.55.39.130	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.130	Block	1
109.253.144.248	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
66.249.65.13	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
37.140.141.27	Russian Federation	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.181.176.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/sachar/faq.aspx	None	1
66.249.78.87	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
62.210.114.129	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/8/3198.pdf/trackback/	Block	1
109.186.132.136	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
84.108.65.245	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
31.186.228.93	United Kingdom	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
192.99.39.235	Canada	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/doctor	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.178	Block	1
149.78.6.119	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.65.178	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
46.4.13.87	Germany	147.237.77.74	law.idf.il	Distributed Admin Blocking	Block	1
220.181.132.217	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/894-he/cogat.aspx	Block	1
93.173.63.64	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.178.67.228	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1400-he/atal.aspx	Block	1
157.55.39.5	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/1133-ar/hamaz.aspx	Block	1
62.219.78.146	Israel	147.237.77.74	law.idf.il	Distributed Admin Blocking	Block	1
109.253.129.198	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
84.108.130.24	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
31.186.228.95	United Kingdom	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
194.44.30.18	Ukraine	147.237.77.176	matpash.idf.il	Unknown HTTP Request Method COOK in URL www.cogat.idf.il/894-en/matpash.aspx	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/bamachane	Block	1
149.78.149.184	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
66.249.73.211	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1

04-18-2015-15:03:01 to 04-18-2015-16:03:01