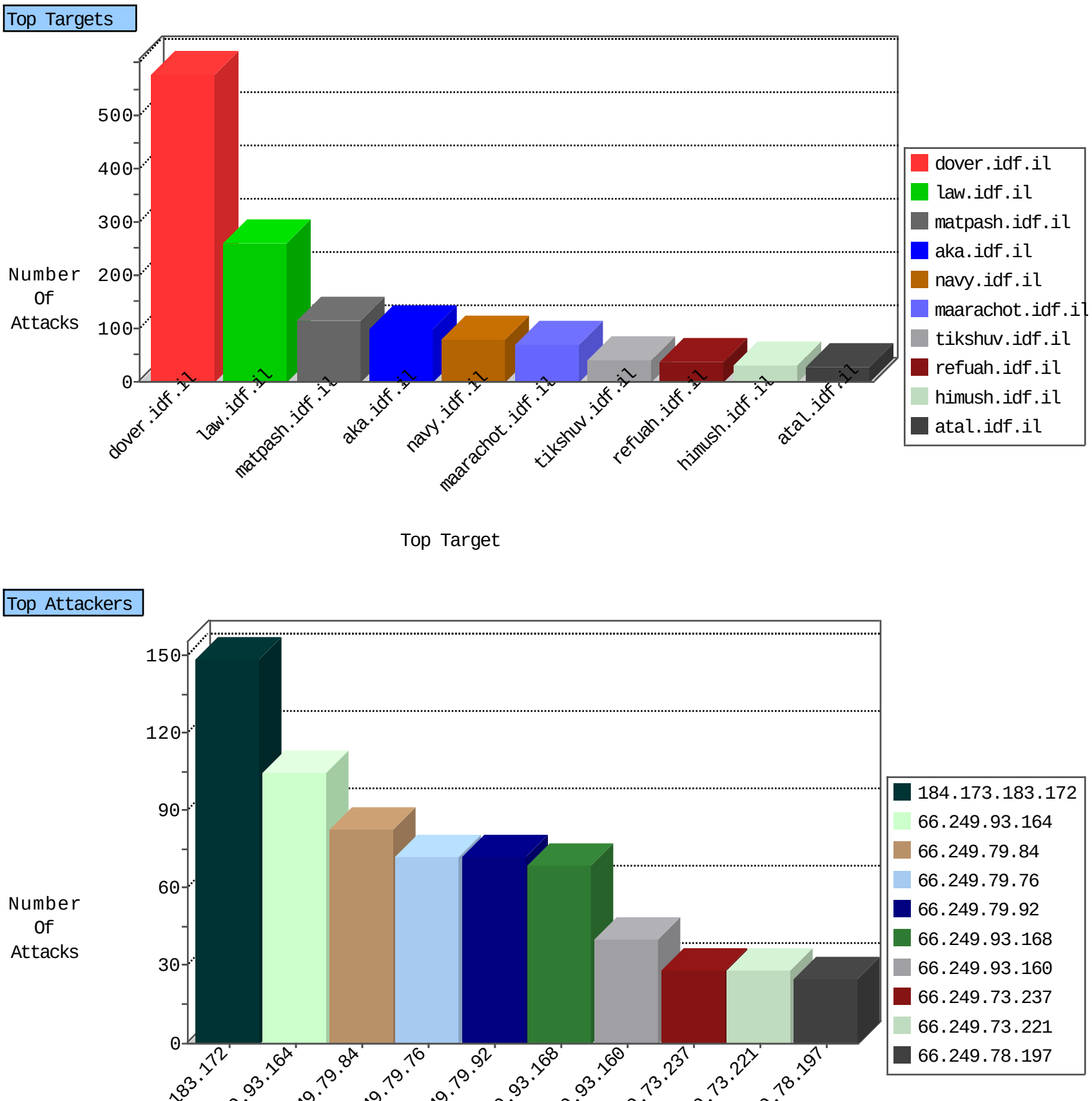
04-03-2015-03:03:07 to 04-03-2015-04:03:07

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

Top Targets



Top Attackers

04-03-2015-03:03:07 to 04-03-2015-04:03:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	102
66.249.79.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	82
66.249.79.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	72
66.249.79.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	70
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	69
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	40
66.249.73.221	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	28
66.249.73.237	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	28
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	25
66.249.93.175	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	23
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	22
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	22
66.249.73.229	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	21
66.249.81.215	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	20
66.249.79.151	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	20
66.249.79.108	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	19
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	19
66.249.64.23	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	17
66.249.69.34	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	14
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	14
66.249.64.10	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	13
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	13
66.249.93.171	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	13
66.249.69.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	13
66.249.79.159	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	12
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	12
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	12
66.249.75.13	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.69.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.81.212	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	12
66.249.75.117	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	11
66.249.91.196	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	10
66.249.79.116	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	10
66.249.64.19	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	10
66.249.81.218	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	9
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	8
66.249.75.5	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.64.151	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	8
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	8
66.249.80.102	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	7
66.249.79.143	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	7
66.249.75.64	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	7
66.249.64.14	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	6
66.249.84.144	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	6
66.249.64.55	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	6
66.249.84.182	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	5
66.249.64.6	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	5
66.249.93.179	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	5

04-03-2015-03:03:07 to 04-03-2015-04:03:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	149
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	24
72.245.29.209	United States	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
192.139.153.25	Canada	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
119.124.107.36	China	147.237.72.166	aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
79.177.27.166	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
2.54.144.39	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
45.96.146.109		147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
185.19.221.8	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.76.39	mobile.meitav.idf.i	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1

04-03-2015-03:03:07 to 04-03-2015-04:03:07

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
43.255.191.170	Japan	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
188.138.9.51	Germany	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.170	Japan	147.237.76.39	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
183.136.216.7	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.170	Japan	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
85.194.93.41	Saudi Arabia	147.237.76.196	e.sviva.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
69.12.92.160	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.170	Japan	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
188.138.9.51	Germany	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.170	Japan	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
188.138.9.51	Germany	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.170	Japan	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
183.136.216.7	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
75.104.70.37	United States	147.237.77.216	dover.idf.il	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	1
69.12.92.160	United States	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.170	Japan	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1

04-03-2015-03:03:07 to 04-03-2015-04:03:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
75.104.70.37	United States	147.237.77.216	dover.idf.il		drop	drop	11
81.144.138.34	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
82.80.25.221	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	8
75.104.70.37	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	7
197.38.165.110	Egypt	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
119.124.107.36	China	147.237.72.166	aka.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	4
197.38.139.188	Egypt	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
59.127.37.14	Taiwan	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	3
196.205.116.158	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
178.137.186.251	Ukraine	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
188.138.1.218	Germany	147.237.8.24	e.lifestyle.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
89.138.242.130	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
64.125.239.45	United States	147.237.76.44	e.refuah.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
216.218.206.87	United States	147.237.77.178	e.matpash.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
146.185.239.104	Russian Federation	147.237.0.35	akaws.idf.il		drop	drop	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	1
89.216.115.8		147.237.77.216	dover.idf.il	SAM rule	drop	drop	1
64.125.239.48	United States	147.237.0.33	idf.il		drop	drop	1
146.185.239.104	Russian Federation	147.237.77.61	e.cogat.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
64.125.239.29	United States	147.237.76.148	gqcenter.aka.idf.i		drop	drop	1
64.125.239.49	United States	147.237.77.212	e.dover.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
176.12.144.249	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	1
64.125.239.34	United States	147.237.77.227	e.hamaz.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
141.105.70.64	Russian Federation	147.237.77.216	dover.idf.il	header rejection pattern found in request	Header Rejection	monitor	1
64.125.239.50	United States	147.237.0.35	akaws.idf.il		drop	drop	1
64.125.239.35	United States	147.237.0.200	m4u.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
141.212.121.153	United States	147.237.76.202	e.halag.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
70.39.186.222	Satellite Provide	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1

04-03-2015-03:03:07 to 04-03-2015-04:03:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
81.144.138.34	United Kingdom	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.144.138.34	Block	3
188.165.15.198	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.198	Block	3
81.144.138.34	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	3
75.104.70.37	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 75.104.70.37	Block	2
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	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
141.105.70.64	Russian Federation	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
69.163.152.120	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
109.186.173.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
37.16.72.139	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19667-he/idfgdover.aspx)	Block	1
218.28.24.238	China	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
70.54.123.21	Canada	147.237.72.166	aka.idf.il	Unknown Parameter __EVENTTARGET in aka.idf.il/main/sachar/	None	1
188.165.15.238	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8868-he/refuah.aspx	Block	1
119.124.107.36	China	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 119.124.107.36	Block	1
75.104.70.37	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/clientscripts/{0}	Block	1
59.127.37.14	Taiwan	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
219.94.128.197	Japan	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
157.55.39.153	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1113-2.stm" target="_blank	Block	1
85.64.81.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
70.54.123.21	Canada	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in aka.idf.il/main/sachar/home.aspx	None	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
119.124.107.36	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1.asp	Block	1
75.104.70.37	United States	147.237.77.216	dover.idf.il	XSS - Basic 3	Block	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
219.166.63.51	Japan	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on refua.atal.idf.il//wp-admin/	Block	1
178.137.186.251	Ukraine	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
89.31.140.21	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
70.167.8.42	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/portalmiluimtemplates/inner.asp	Block	1
207.46.13.5	United States	147.237.72.166	aka.idf.il	Unknown Parameter 9ff3fe30 in www.aka.idf.il/main/home/default.aspx	None	1
141.105.70.64	Russian Federation	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
77.127.29.89	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/payslips.aspx	None	1
180.76.4.47	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
109.65.19.135	Israel	147.237.72.166	aka.idf.il	Unknown Parameter q in www.aka.idf.il/main/giyus/login.aspx	None	1
213.251.182.10	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	1

04-03-2015-03:03:07 to 04-03-2015-04:03:07