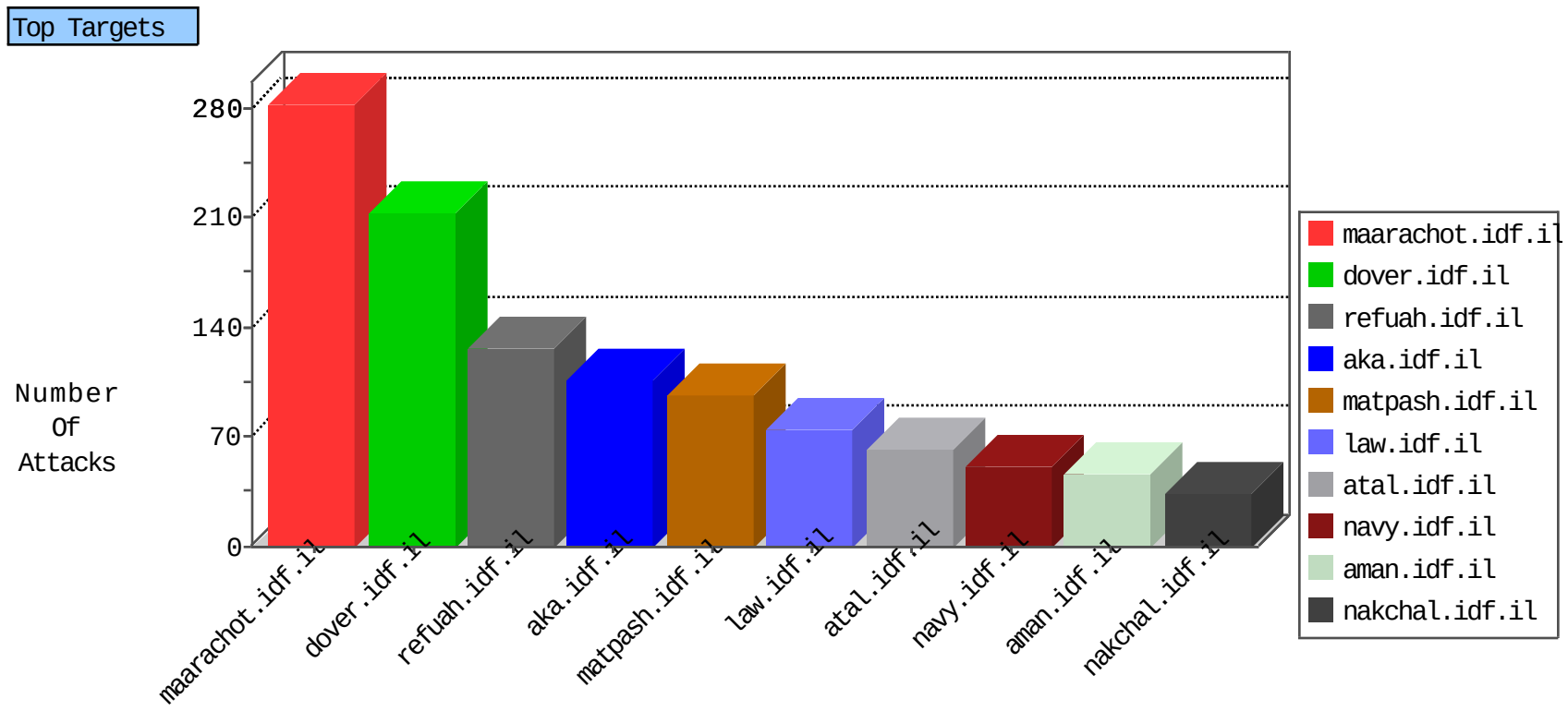
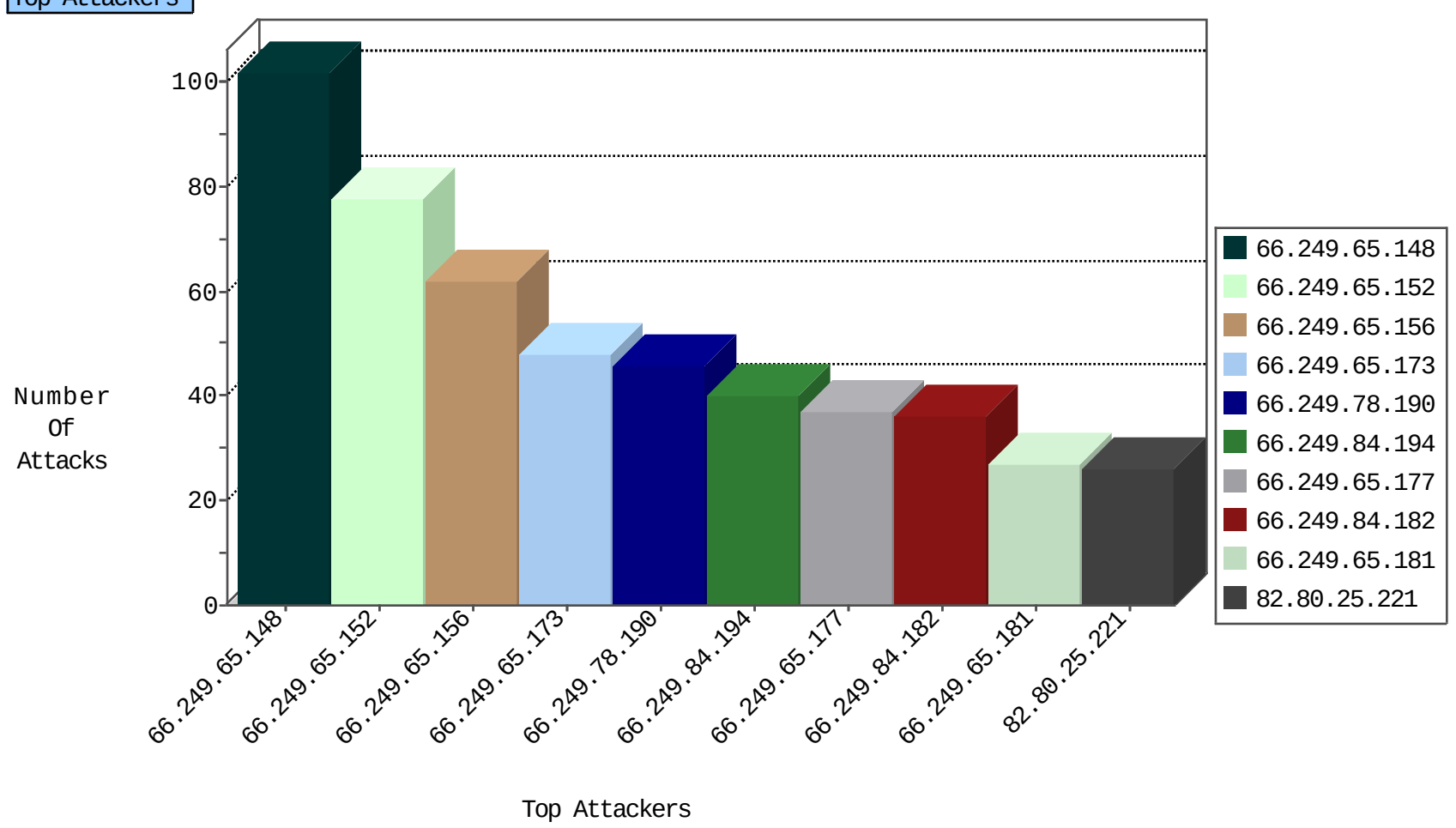
04-05-2015-03:03:02 to 04-05-2015-04:03:02

IDF Under Attack
04-05-2015-03:03:02

Top Targets



Top Attackers



04-05-2015-03:03:02 to 04-05-2015-04:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.65.148	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	102
66.249.65.152	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	78
66.249.65.156	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	62
66.249.65.173	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	48
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	46
66.249.84.194	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	40
66.249.65.177	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	37
66.249.84.182	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	36
66.249.65.181	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	27
66.249.84.188	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	26
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	25
66.249.78.144	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	25
66.249.78.82	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	24
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	23
66.249.78.9	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	22
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	21
66.249.65.187	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	20
66.249.78.153	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	18
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	18
66.249.79.63	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	17
66.249.79.42	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	15
66.249.78.89	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	15
66.249.78.254	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	15
66.249.78.130	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	14
66.249.79.34	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	12
66.249.78.37	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	12
66.249.78.146	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.79.71	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	11
66.249.79.26	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	11
66.249.79.55	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	11
66.249.69.91	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	10
66.249.75.23	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	10
66.249.78.96	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	10
66.249.78.29	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	10
66.249.78.148	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	10
66.249.79.132	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	9
66.249.79.124	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	8
66.249.78.160	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.67.66	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	7
66.249.78.134	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	7
66.249.78.228	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	7
66.249.79.140	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	7
66.249.65.195	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	7
66.249.78.120	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	7
66.249.81.144	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	6
66.249.69.99	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	6
66.249.78.2	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.78.140	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	6
66.249.73.136	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	6
66.249.78.15	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	5

04-05-2015-03:03:02 to 04-05-2015-04:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
198.20.69.98	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	1
198.20.69.98	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.234	halag.idf.il	DVRep_P-N_40-59	Permit	1
85.25.43.94	Germany	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
89.139.182.210	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.19	madim.atal.idf.il	DVRep_P-N_40-59	Permit	1

04-05-2015-03:03:02 to 04-05-2015-04:03:02

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
61.240.144.64	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.213	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
140.113.110.21	Taiwan	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
41.140.40.209	Morocco	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 4096	1
221.235.188.213	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
140.113.110.21	Taiwan	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
27.50.132.60	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
221.235.188.213	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
140.113.110.21	Taiwan	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.213	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
140.113.110.21	Taiwan	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
207.241.229.213	United States	147.237.72.166	aka.idf.il	WEB-CGI redirect access	1
118.186.216.62	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
188.138.9.51	Germany	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
99.244.135.30	Canada	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 4096	1
140.113.110.21	Taiwan	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
140.113.110.21	Taiwan	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.213	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
140.113.110.21	Taiwan	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.213	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
140.113.110.21	Taiwan	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
41.140.40.209	Morocco	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
140.113.110.21	Taiwan	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
41.140.40.209	Morocco	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.213	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
140.113.110.21	Taiwan	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.213	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
140.113.110.21	Taiwan	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.213	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
118.186.216.62	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.130		147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 3072	1
140.113.110.21	Taiwan	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
69.12.92.160	United States	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
140.113.110.21	Taiwan	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.213	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
140.113.110.21	Taiwan	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1

04-05-2015-03:03:02 to 04-05-2015-04:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	26
220.255.1.151	Singapore	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
8.37.228.77	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	2
94.230.86.138	Israel	147.237.77.243	mobile.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
8.37.227.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1
61.135.190.72	China	147.237.0.34	tikshuv.idf.il	SAM rule	drop	drop	1
141.212.122.91	United States	147.237.76.148	gqcenter.aka.idf.i		drop	drop	1
70.39.186.218	Satellite Provider	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
141.212.122.97	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
8.37.228.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1
70.39.186.222	Satellite Provider	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	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
46.19.86.41	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
8.37.227.70	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1
216.218.206.86	United States	147.237.76.200	eitan.aka.idf.il		drop	drop	1
49.151.61.85	Philippines	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	1

04-05-2015-03:03:02 to 04-05-2015-04:03:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.67.157.176	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/6_s3_	Block	1
188.165.15.198	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.198	Block	1
70.167.8.42	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/yohalanfaq/faq.asp	Block	1
207.46.13.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19667-he/idfgdover.aspx)	Block	1
157.55.39.12	United States	147.237.76.42	refuah.idf.i	Unauthorized URL Access to 147.237.76.42/templates/sendtofriend/sendtofriend.aspx	Block	1
5.29.202.22	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	1
188.165.15.198	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/idf_in_pictures/2001/march/20.stm	Block	1
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	1
216.218.206.68	United States	147.237.77.243	mobile.idf.i	Unauthorized URL Access to 147.237.77.243/	Block	1
157.55.39.17	United States	147.237.76.42	refuah.idf.i	Unauthorized URL Access to 147.237.76.42/scriptresource.axd	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	1
190.105.222.168	Argentina	147.237.77.216	dover.idf.il	Unknown HTTP Request Method COOK in URL www.idf.il/1116-en/dover.aspx	Block	1
91.143.235.243	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
220.181.108.185	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.26.148.132	Israel	147.237.76.42	refuah.idf.i	Distributed Unauthorized URL Access on 147.237.76.42//webresource.axd	Block	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
109.67.157.176	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 109.67.157.176	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/military-police	Block	1
52.4.217.116	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0119-3.stm	Block	1
207.46.13.72	United States	147.237.76.42	refuah.idf.i	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1

04-05-2015-03:03:02 to 04-05-2015-04:03:02