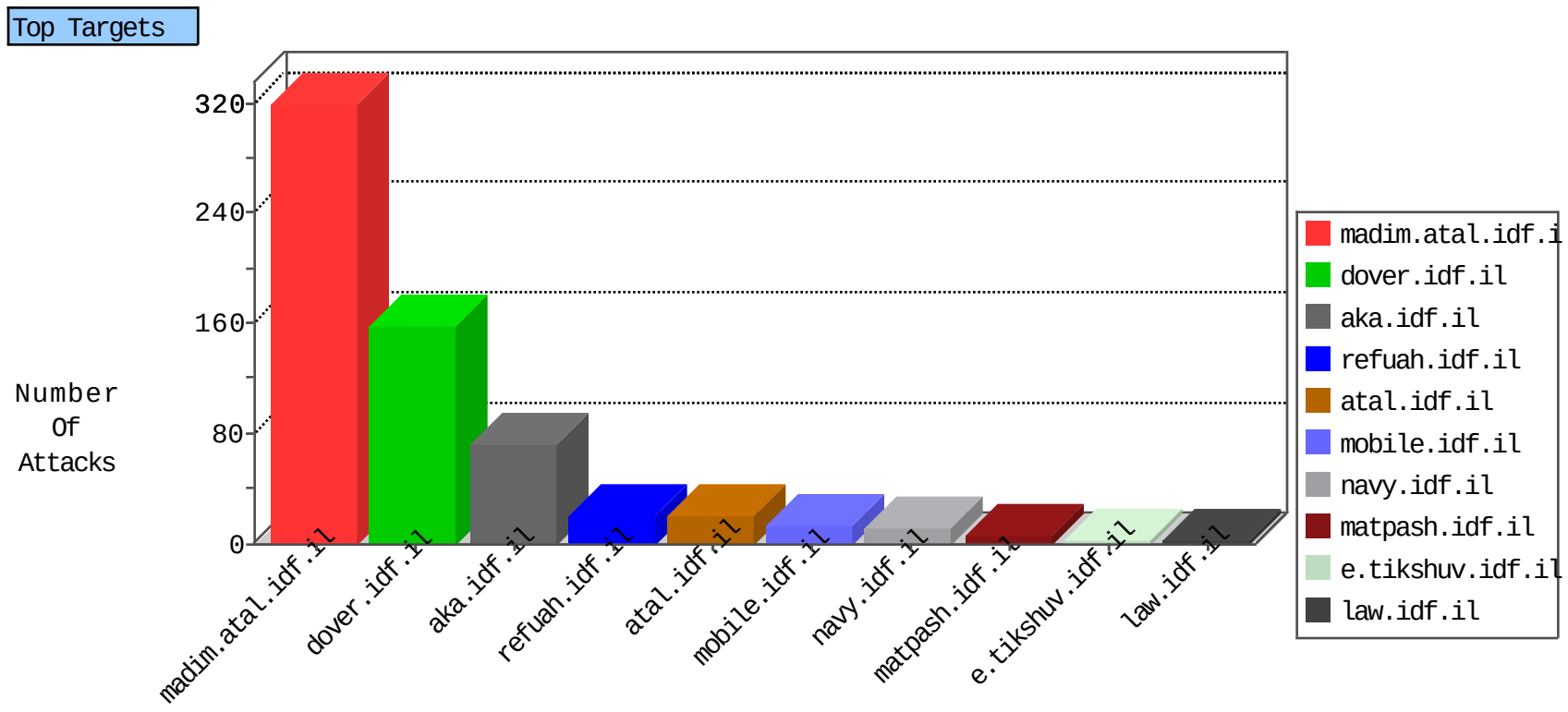
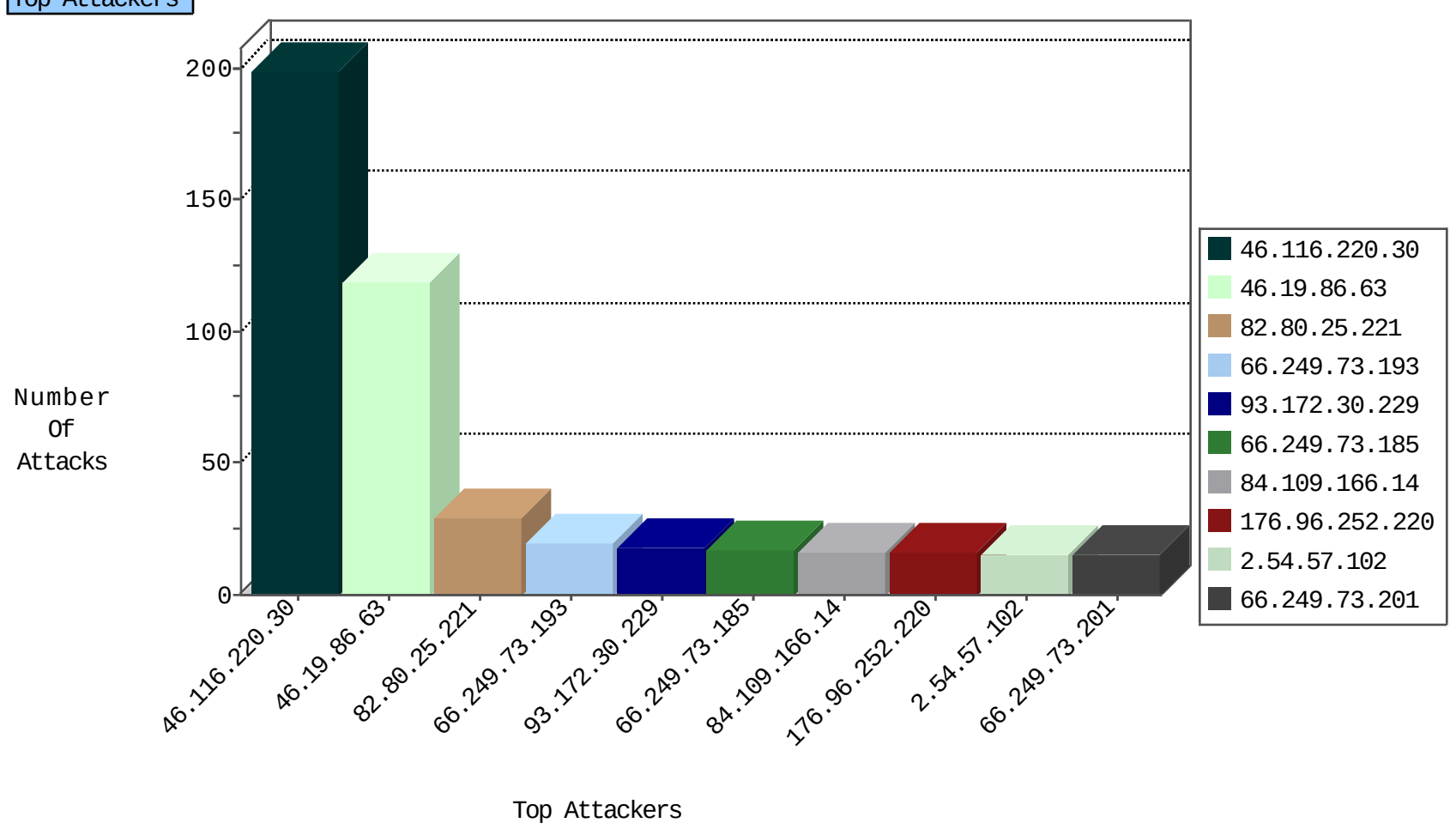
03-28-2015-13:03:00 to 03-28-2015-14:03:00

IDF Under Attack
03-28-2015-13:03:00

Top Targets



Top Attackers



03-28-2015-13:03:00 to 03-28-2015-14:03:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count

03-28-2015-13:03:00 to 03-28-2015-14:03:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
188.161.8.224	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
37.205.9.131	Slovakia	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
109.65.176.253	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
37.205.9.131	Slovakia	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
109.160.239.165	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.19.85.0	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
77.127.132.2	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
87.69.246.162	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

03-28-2015-13:03:00 to 03-28-2015-14:03:00

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	29
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
176.96.252.220	Russian Federation	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.141	Japan	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
176.96.252.220	Russian Federation	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.141	Japan	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
176.96.252.220	Russian Federation	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.141	Japan	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
176.96.252.220	Russian Federation	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.141	Japan	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
115.231.218.147	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
27.50.132.61	China	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 3072	1
176.96.252.220	Russian Federation	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
115.231.218.147	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
176.96.252.220	Russian Federation	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
176.96.252.220	Russian Federation	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.141	Japan	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
176.96.252.220	Russian Federation	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.141	Japan	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
176.96.252.220	Russian Federation	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.141	Japan	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
176.96.252.220	Russian Federation	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.141	Japan	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
176.96.252.220	Russian Federation	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.141	Japan	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
211.138.34.58	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
176.96.252.220	Russian Federation	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.141	Japan	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
176.96.252.220	Russian Federation	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
115.231.218.147	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
27.50.132.61	China	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
176.96.252.220	Russian Federation	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
115.231.218.147	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
176.96.252.220	Russian Federation	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
176.96.252.220	Russian Federation	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.141	Japan	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1

03-28-2015-13:03:00 to 03-28-2015-14:03:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
93.172.30.229	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
66.249.73.185	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
66.249.73.193	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
109.65.176.253	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
66.249.73.201	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
84.109.166.14	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	10
2.54.57.102	Israel	147.237.76.42	refuah.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
207.46.13.112	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
46.19.86.149	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	monitor	8
46.19.85.0	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	7
84.109.166.14	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	alert	6
93.19.144.15	France	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	6
157.55.39.153	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
37.46.39.185	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
176.12.145.231	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
77.126.82.229	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
46.19.85.240	Israel	147.237.77.243	mobile.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
94.230.86.147	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
46.19.85.187	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
149.78.232.246	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	3
2.54.39.211	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
2.54.39.211	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
38.111.147.86	United States	147.237.76.42	refuah.idf.il		drop	drop	2
94.230.86.233	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
212.253.107.198	Turkey	147.237.77.74	law.idf.il	SAM rule	drop	drop	2
46.19.85.194	Israel	147.237.77.243	mobile.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
2.54.39.211	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	2
212.253.107.198	Turkey	147.237.77.176	matpash.idf.il	SAM rule	drop	drop	2
213.57.101.245	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.6	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
46.117.97.244	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
188.165.15.196	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.19.85.173	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.199	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
141.212.122.83	United States	147.237.77.227	e.hamaz.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
216.218.206.83	United States	147.237.76.202	e.halag.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.19.86.63	Israel	147.237.0.19	madim.atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.179	United States	147.237.76.147	chinuch.aka.idf.il		drop	drop	1
141.212.122.203	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
141.212.122.88	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.19.86.115	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.180	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
141.212.122.203	United States	147.237.76.34	yohalan.idf.il		drop	drop	1
141.212.122.91	United States	147.237.76.148	gqcenter.aka.idf.il		drop	drop	1
87.69.225.61	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
184.105.139.67	United States	147.237.0.16	my-kosher-kravi.idf.il	SAM rule	drop	drop	1
141.212.122.184	United States	147.237.0.200	m4u.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.19.85.240	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.93	United States	147.237.8.14	e.orchot.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.19.86.229	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.116.220.30	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.116.220.30	Block	198
46.19.86.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	118
207.46.13.16	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.16	Block	5
66.249.73.193	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.193	Block	4
94.180.61.227	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 94.180.61.227	Block	4
5.22.129.237	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
2.54.57.102	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 2.54.57.102	Block	4
77.125.151.180	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/	Block	3
66.249.73.201	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.201	Block	3
176.12.149.178	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
46.43.68.138	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	3
188.165.15.176	France	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 188.165.15.176	Block	2
2.54.57.102	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	2
217.132.91.202	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	2
2.54.189.51	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	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
66.249.73.185	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/briefing040102.stm	Block	1
207.46.13.114	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-14363-he/dover.aspx	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
37.140.141.27	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/info.asp?moduleid=5&catid=22707&docid=72354	Block	1
87.69.172.162	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
77.125.151.180	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 77.125.151.180	Block	1
149.78.196.205	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/894-he/miluim.aspx	Block	1
79.183.108.51	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
176.12.148.51	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.142.184.202	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
93.172.7.213	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
188.165.15.196	France	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
50.16.112.199	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 50.16.112.199	Block	1
157.55.39.6	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0122-1.stm	Block	1
79.183.175.159	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/default.×ž×™×œ×•×?×™×?	Block	1
217.132.101.40	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
77.127.19.80	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
50.16.112.199	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp	Block	1
207.46.13.2	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
157.55.39.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/roshhamas.stm	Block	1
84.228.175.45	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	1
180.76.4.24	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
94.180.61.227	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/article.in.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
79.179.120.65	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 79.179.120.65	Block	1
66.249.69.28	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//	Block	1
37.26.147.225	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/kamlar/styles/import/bottomnavigation.asp	Block	1
84.229.134.5	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
188.165.15.121	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1232-he/atal.aspx	Block	1
46.116.220.30	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
109.66.6.199	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl01 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
79.179.120.65	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1