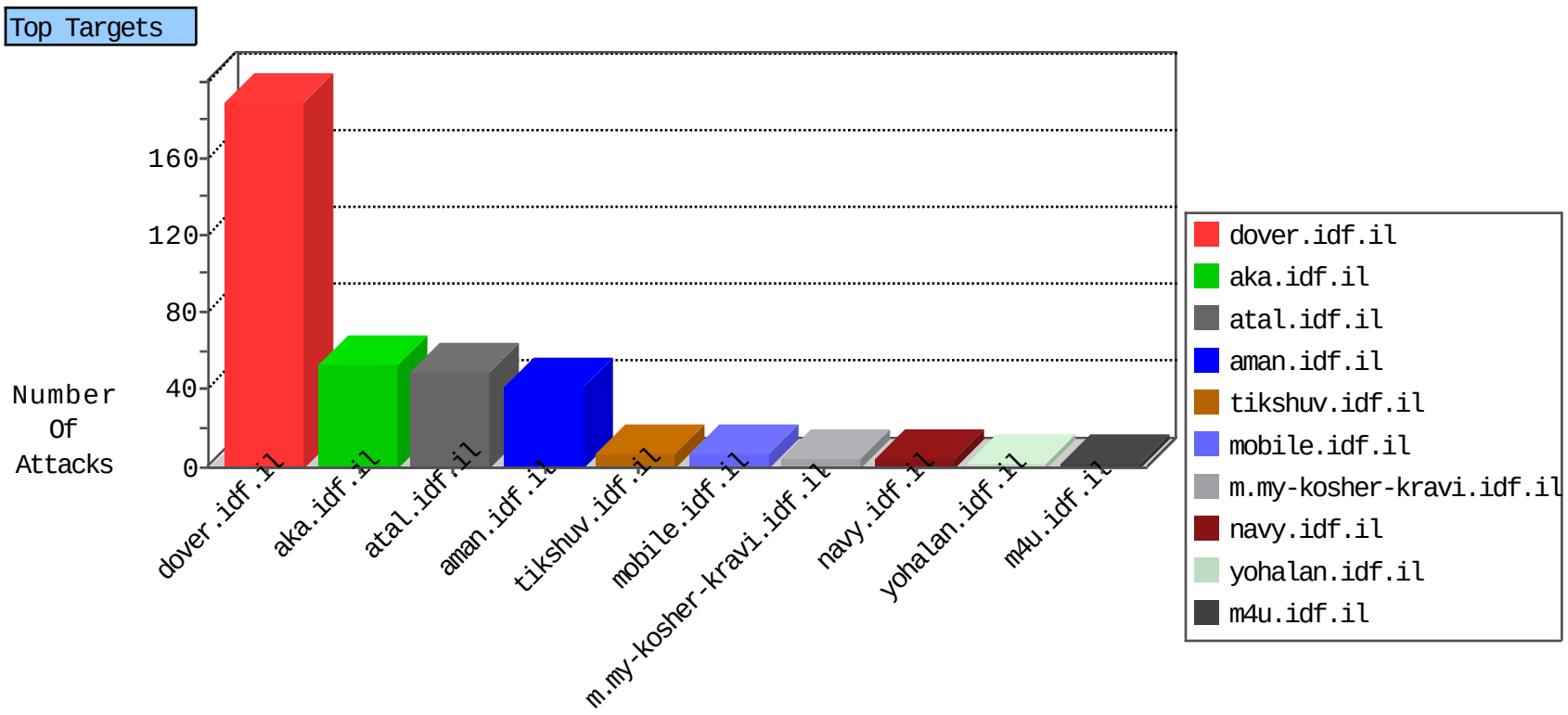
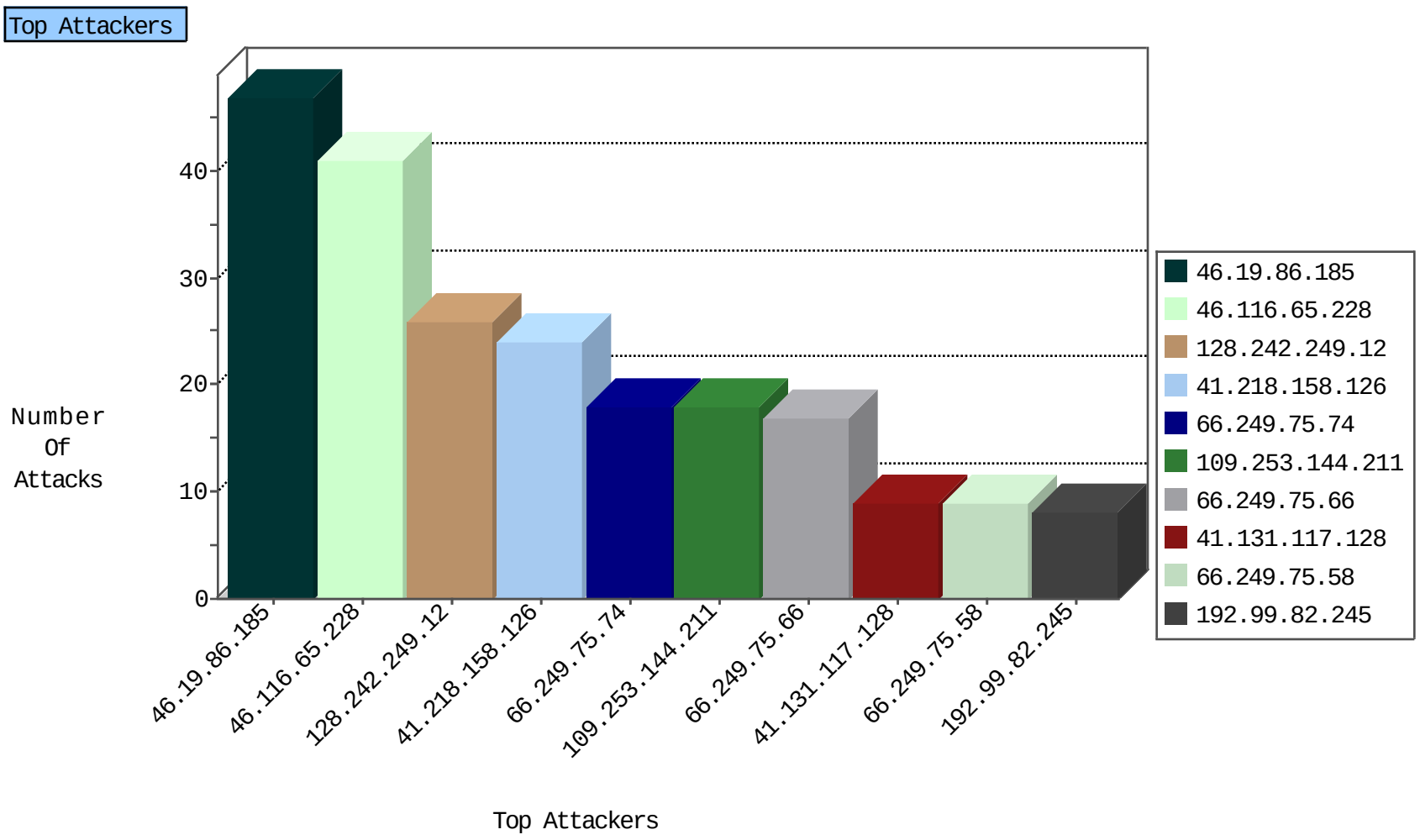
04-02-2015-00:03:10 to 04-02-2015-01:03:10

IDF Under Attack
04-02-2015-00:03:10

Top Targets



Top Attackers



04-02-2015-00:03:10 to 04-02-2015-01:03:10

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
46.116.65.228	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	605
192.3.203.226	United States	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
46.28.204.46	Switzerland	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1

04-02-2015-00:03:10 to 04-02-2015-01:03:10

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	26
192.99.82.245	Canada	147.237.72.166	aka.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	4
85.25.103.50	Germany	147.237.76.148	gqcenter.aka.idf.i	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.15	kosher-kravi.idf.i	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
37.26.146.254	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
176.40.153.87	Turkey	147.237.76.86	navy.idf.il	C1000101: HTTP Hacked in the URL	Block	1
71.6.167.142	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1

04-02-2015-00:03:10 to 04-02-2015-01:03:10

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
192.99.82.245	Canada	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	4
2.54.29.112	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.19.86.94	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
188.138.9.51	Germany	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
222.69.94.13	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 3072	1
117.135.163.104	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
117.135.163.104	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -f -sS	1
221.235.188.212	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
70.138.98.152	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
221.235.188.212	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	1
212.231.9.86	Spain	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
212.231.9.86	Spain	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
212.231.9.86	Spain	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
128.61.240.66	United States	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
222.69.94.13	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
117.135.163.104	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
221.235.188.212	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
212.231.9.86	Spain	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
212.231.9.86	Spain	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1

04-02-2015-00:03:10 to 04-02-2015-01:03:10

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
41.218.158.126	Egypt	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	21
46.19.86.185	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	18
109.253.144.211	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
66.249.75.66	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
66.249.75.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
46.19.86.185	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	alert	13
41.131.117.128	Egypt	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
46.19.86.185	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	8
82.80.25.221	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	8
66.249.75.58	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
46.19.86.185	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	7
109.253.129.15	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
207.46.13.16	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
176.12.136.209	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
176.12.141.197	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
109.253.139.158	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid ACK number	Bad TCP sequence	alert	4
41.218.158.126	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
80.246.130.116	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
37.26.147.230	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
37.26.147.230	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
109.253.131.175	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
109.253.131.175	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
80.246.130.116	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
176.12.150.96	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
46.19.85.203	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
188.138.1.218	Germany	147.237.8.28	e.mobile-ks.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
109.253.144.121	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
81.218.226.75	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
141.212.122.193	United States	147.237.0.200	m4u.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.19.85.236	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
196.206.193.173	Morocco	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
81.218.226.75	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.86.191	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
79.177.80.35	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
37.46.39.25	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.178	United States	147.237.8.14	e.orchot.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.19.86.230	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.85.106	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
5.22.130.244	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
213.151.172.135	France	147.237.77.216	dover.idf.il	header rejection pattern found in request	Header Rejection	monitor	1
141.212.122.182	United States	147.237.76.202	e.halag.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
84.108.101.165	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.85.107	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
31.210.186.132	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
41.196.79.106	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
141.212.122.186	United States	147.237.0.33	idf.il		drop	drop	1
91.224.132.118	Russian Federation	147.237.77.121	e.navy.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.86.204	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	5
93.172.163.96	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	4
116.53.130.245	China	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 116.53.130.245	Block	4
149.78.11.207	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
116.53.130.245	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	3
79.181.66.174	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
54.215.43.237	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 54.215.43.237	Block	2
157.55.39.137	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/rabanut/webresource.axd	Block	2
203.133.169.157	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0115-2.stm	Block	1
66.249.75.13	United States	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/chinuch/klali/	None	1
176.12.136.234	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.135.137	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
66.249.75.117	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/bamachane/	Block	1
176.12.151.2	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.246.138.120	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il//categorytemplates/listchildsubcategories/1423	Block	1
207.46.13.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.112	Block	1
66.249.75.58	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.58	Block	1
176.12.137.248	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.142.34	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
54.177.31.205	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/news/main.stm	Block	1
199.203.240.93	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
149.78.11.207	Israel	147.237.72.166	aka.idf.il	Unknown Parameter q in www.aka.idf.il/main/giyus/login.aspx	None	1
212.199.57.203	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	1
66.249.75.66	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ zahal	Block	1
2.54.142.215	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
176.12.139.92	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
116.53.130.245	China	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
199.203.240.93	Israel	147.237.72.166	aka.idf.il	Unknown Parameter wb48617274 in www.aka.idf.il/main/rabanut/scriptresource.axd	None	1
95.86.64.250	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
213.151.172.135	France	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
66.249.75.74	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.74	Block	1
2.54.149.151	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/tfasim.aspx	None	1
176.12.141.197	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.127.135.11	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
203.133.169.157	Korea, Republic of	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 203.133.169.157	Block	1
54.215.43.237	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1
176.12.136.76	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.132.136	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
213.151.172.135	France	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
66.249.75.74	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arafat/english/index2.stm	Block	1
46.19.86.185	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
176.12.146.212	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1