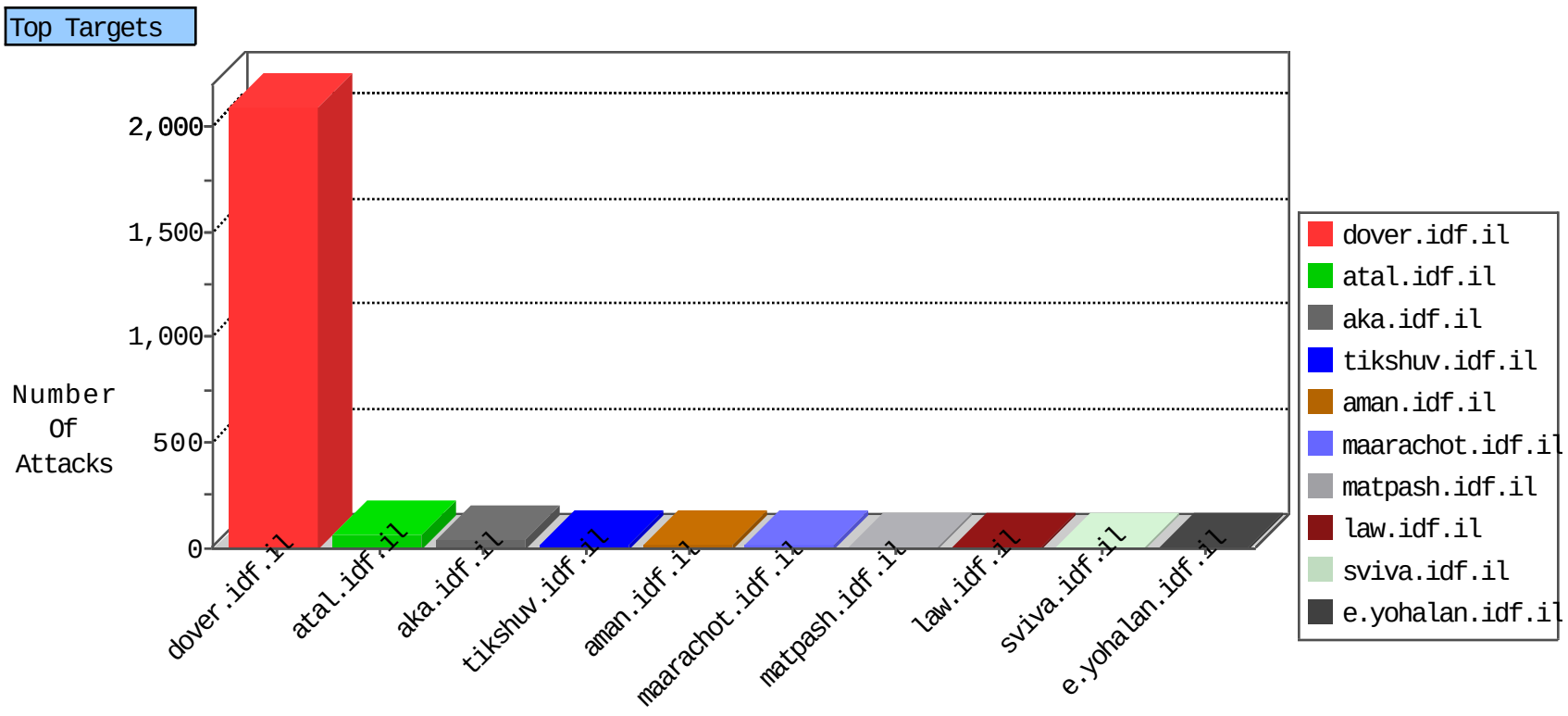
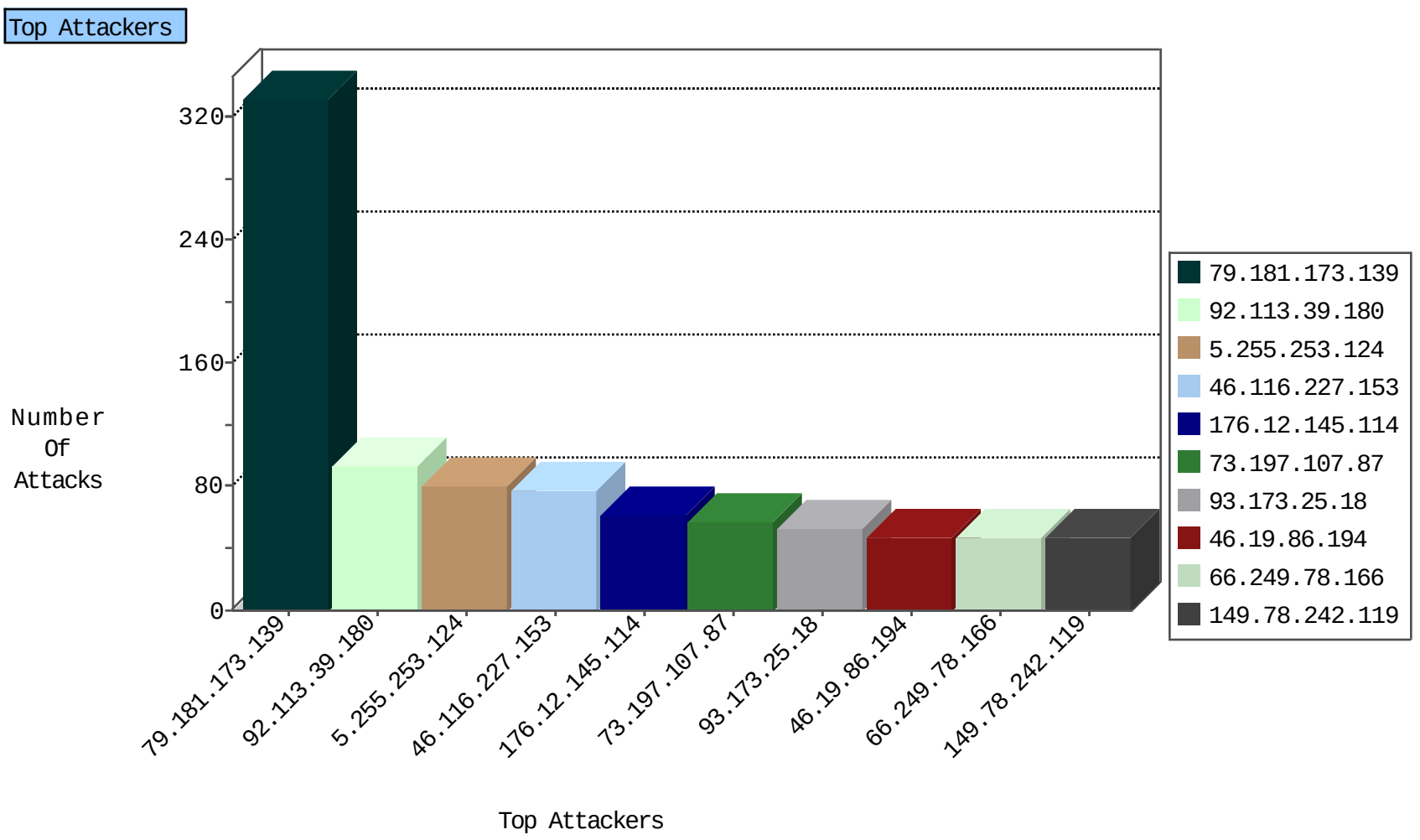
05-08-2015-22:03:03 to 05-08-2015-23:03:03

IDF Under Attack
05-08-2015-22:03:03

Top Targets



Top Attackers



05-08-2015-22:03:03 to 05-08-2015-23:03:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.105	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	1376
66.249.67.126	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	356
220.181.108.157	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	178
84.228.83.136	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	134
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
27.141.42.102	Japan	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	2
182.168.160.204	Japan	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
124.232.142.220	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

05-08-2015-22:03:03 to 05-08-2015-23:03:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
71.6.135.131	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	2
188.138.9.50	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	2
71.6.167.142	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	2
71.6.167.142	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.61	e.cogat.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	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
85.250.82.4	Israel	147.237.77.170	maarachot.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
105.155.68.246	Morocco	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
173.199.65.4	Canada	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1

05-08-2015-22:03:03 to 05-08-2015-23:03:03

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
66.249.65.9	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	4
109.253.143.83	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
88.198.5.141	Germany	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
77.127.47.121	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.65.148.234	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
88.198.5.141	Germany	147.237.77.216	dover.idf.il	SERVER-WEBAPP Mambo upload.php access	2
66.249.67.152	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
181.111.241.43	Argentina	147.237.76.202	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
60.18.162.244	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
181.111.241.43	Argentina	147.237.76.42	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
181.111.241.43	Argentina	147.237.0.34	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.77.79.43	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
178.19.107.114	Poland	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
218.24.113.2	China	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 4096	1
198.154.60.27	United States	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
181.111.241.43	Argentina	147.237.77.179	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
181.111.241.43	Argentina	147.237.77.170	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
60.18.162.244	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
181.111.241.43	Argentina	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
60.18.162.244	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -f -sS	1
181.111.241.43	Argentina	147.237.76.31	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
178.19.107.114	Poland	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
144.0.0.60	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
218.24.113.2	China	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
195.178.167.163	Sweden	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
181.111.241.43	Argentina	147.237.77.235	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
181.111.241.43	Argentina	147.237.77.176	matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.67	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1

05-08-2015-22:03:03 to 05-08-2015-23:03:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
79.181.173.139	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	332
92.113.39.180	Ukraine	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	93
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	80
73.197.107.87	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	57
176.12.145.114	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	56
46.116.227.153	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	56
93.173.25.18	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	53
149.78.242.119	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
46.19.86.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
108.59.253.71	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	46
77.125.4.10	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
80.179.188.98	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
77.126.69.92	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
173.68.91.63	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
84.94.43.63	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
66.249.81.215	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
191.189.153.245	Brazil	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
109.65.33.187	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
46.116.131.7	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
46.116.227.153	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
52.16.5.197	United States	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
179.213.125.249	Brazil	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
197.231.221.211	Liberia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
80.189.1.175	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
167.115.115.2	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
84.110.210.65	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
176.106.42.148	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
79.177.139.79	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
109.67.55.102	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
46.98.11.155	Ukraine	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
79.182.12.253	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
172.56.17.72	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
46.116.120.16	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
2.54.132.215	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
109.65.148.234	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
46.19.86.158	Israel	147.237.77.216	dover.idf.i	Invalid sequence number	Bad TCP sequence	monitor	11
46.19.86.158	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	alert	11
46.19.86.158	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	11
66.249.64.168	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
66.249.78.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
216.113.160.72	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
66.249.64.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
66.249.64.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	10
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	6
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	5
85.250.200.15	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
87.68.149.84	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
50.243.68.162	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 50.243.68.162	Block	2
50.243.68.162	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	2
167.115.115.2	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en	Block	2
31.13.161.111	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
66.249.67.190	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/993/patzar.aspx	Block	1
109.253.137.110	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.94.49.39	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
2.54.132.215	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip.storage/files/4/	Block	1
66.249.64.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/scriptresource.axd	Block	1
38.98.125.162	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
87.69.121.17	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.67.218	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1196-he/refuah.aspx	Block	1
109.253.149.81	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233//1134-he/atal.aspx	Block	1
85.64.34.2	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.168.211	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.153	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.153	Block	1
66.249.64.245	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1065-en/dover.aspx	Block	1
46.116.227.153	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
89.138.6.242	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.stm	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
66.249.78.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/	Block	1
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.173	Block	1
85.65.157.45	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/russian/0306-2.stm	Block	1
66.249.78.153	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/portalmi	Block	1
66.249.67.92	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/163-6313-he/patzar.aspx	Block	1
46.121.108.84	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
105.155.68.246	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/	Block	1
2.52.147.94	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19538-he/dover.aspx	Block	1
180.76.5.166	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0608-2.stm	Block	1
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.178	Block	1
27.45.249.163	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/news/news.in.aspx	Block	1
66.249.67.105	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/templates/getfile/getfile.aspx	Block	1
46.121.108.84	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
109.186.117.192	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
68.180.229.51	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.229.51	Block	1
2.54.30.11	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18489-he/dover.aspx	Block	1
199.180.114.153	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17436-en/dover.aspx/trackback/	Block	1
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/panmaz/index.stm	Block	1

05-08-2015-22:03:03 to 05-08-2015-23:03:03