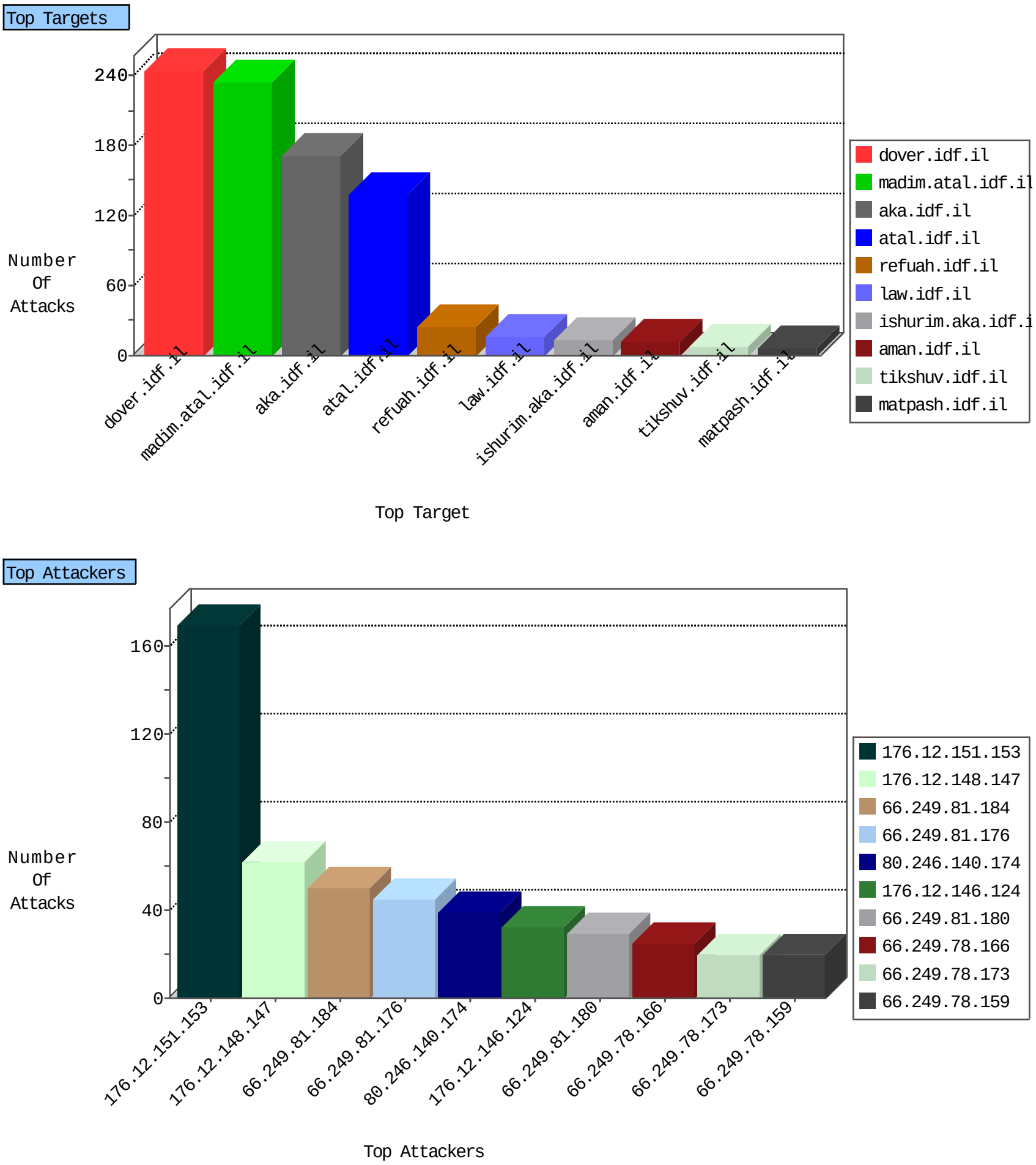
03-29-2015-11:03:08 to 03-29-2015-12:03:08

IDF Under Attack
03-29-2015-11:03:08



03-29-2015-11:03:08 to 03-29-2015-12:03:08

Top Attackers In DDoS-Defence

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

03-29-2015-11:03:08 to 03-29-2015-12:03:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
62.219.65.115	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
46.19.85.227	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.65.216.32	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.19.85.118	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
79.182.187.217	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
93.120.27.62	Romania	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
80.246.136.176	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
192.117.103.139	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
81.88.48.97	Italy	147.237.76.31	nakchal.idf.il	EgovRep_B-N_70-99	Block	1
31.168.205.159	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
79.178.190.199	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
84.111.112.108	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.19.85.85	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
79.180.160.42	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

03-29-2015-11:03:08 to 03-29-2015-12:03:08

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
84.108.212.193	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
37.142.234.70	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
109.253.131.29	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
93.172.180.39	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
218.200.188.213	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
218.200.188.213	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
217.194.204.41	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
61.160.224.130	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
195.34.150.18	Austria	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
193.107.17.72	Russian Federation	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.131.98	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
103.238.214.79		147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
90.15.80.37	France	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.93.90	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
218.200.188.213	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
67.194.229.137	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
218.200.188.213	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
212.179.46.16	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
58.20.54.249	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1
193.107.17.72	Russian Federation	147.237.72.217	e.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

03-29-2015-11:03:08 to 03-29-2015-12:03:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.81.184	United States	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	50
66.249.81.176	United States	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	45
176.12.146.124	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
66.249.81.180	United States	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	29
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
80.246.140.174	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	13
80.246.140.174	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	13
80.246.140.174	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	13
176.12.143.120	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
212.235.13.12	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
180.253.15.3	Indonesia	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	8
176.12.139.107	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
46.19.86.214	Israel	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	7
46.19.85.85	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
81.218.77.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
213.57.88.197	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	5
195.200.205.225	Israel	147.237.72.167	ishurim.aka.idf.i	First packet isn't SYN	drop	drop	5
212.117.152.82	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	5
46.19.85.94	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
46.19.85.100	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
31.168.193.13	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	4
176.12.145.37	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
46.19.85.74	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	4
176.12.146.205	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
46.19.85.11	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	alert	3
46.116.104.182	Israel	147.237.72.156	aman.idf.il	First packet isn't SYN	drop	drop	3
46.19.85.193	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
37.26.146.207	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
46.19.85.11	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
89.138.52.30	Israel	147.237.77.216	dover.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	3
81.218.77.163	Israel	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	3
80.179.114.19	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
109.65.153.76	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	3
80.246.133.166	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
5.102.254.116	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
207.241.229.212	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
2.54.139.146	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.19.86.185	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
185.32.178.153	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	2
46.19.85.74	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	alert	2
89.138.52.30	Israel	147.237.77.216	dover.idf.il	SYN retransmit with different window scale	Bad TCP sequence	alert	2
207.241.237.105	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
46.19.85.124	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid ACK number	Bad TCP sequence	monitor	2
66.249.75.66	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
195.200.205.225	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
185.32.178.153	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
176.12.137.236	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
176.12.151.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	170
176.12.148.147	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.148.147	Block	62
17.142.151.243	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.151.243	Block	9
95.86.122.220	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	6
109.64.7.53	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	4
17.142.151.243	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
46.19.85.55	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	3
95.86.75.152	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
109.253.130.233	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
157.55.39.42	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.42	Block	2
207.46.13.16	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.16	Block	2
176.12.139.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	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
2.52.141.46	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.78.159	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
46.19.85.26	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
37.26.147.160	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
5.29.245.105	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
199.203.215.1	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
89.138.52.30	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 89.138.52.30	Block	1
46.210.151.236	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
37.140.141.39	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/signals/signals.stm	Block	1
176.12.138.251	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.246.130.39	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.173	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	1
109.253.147.98	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.117	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
180.76.4.232	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
84.108.159.7	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.143.100	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.237.154.221	Czech Republic	147.237.77.233	atal.idf.il	Unauthorized URL Access to /	Block	1
109.253.134.119	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.104	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 54.245.64.111	Block	1
176.12.149.196	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
89.138.52.30	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	1
37.140.188.29	Russian Federation	147.237.76.30	himush.idf.il	Unknown Parameter SortDir in www.chimush.atal.idf.il/994-he/himush.aspx	None	1
80.246.140.162	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.78.173	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/jenin/site/english/main	Block	1
149.78.149.184	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
66.249.78.2	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/×©×§×• ×¤×™×™×ª 15	Block	1
185.32.178.144	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.66.152.67	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
84.111.112.108	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
46.19.85.160	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gtytt	Block	1
176.12.144.121	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2003/june/23.stm	Block	1
79.178.190.199	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
109.253.139.215	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.111	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1

03-29-2015-11:03:08 to 03-29-2015-12:03:08