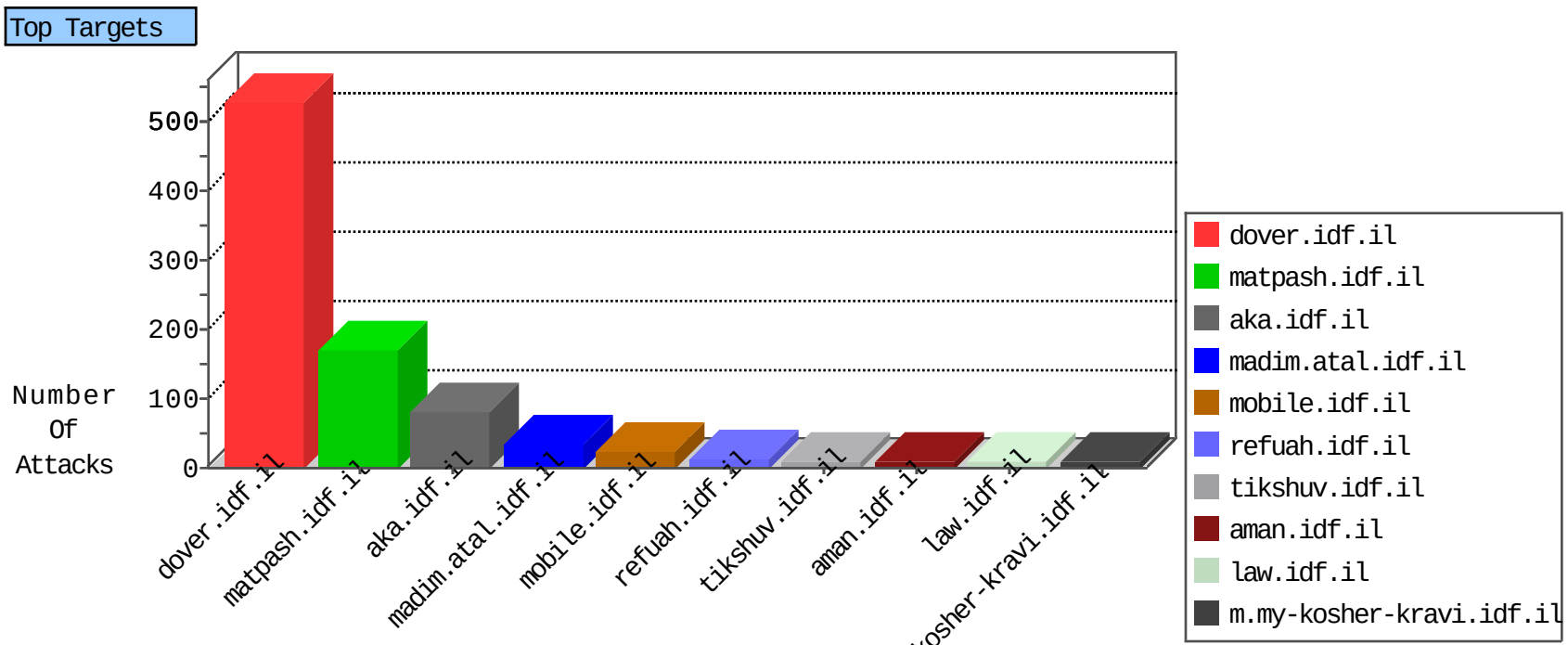
05-09-2015-15:03:05 to 05-09-2015-16:03:05

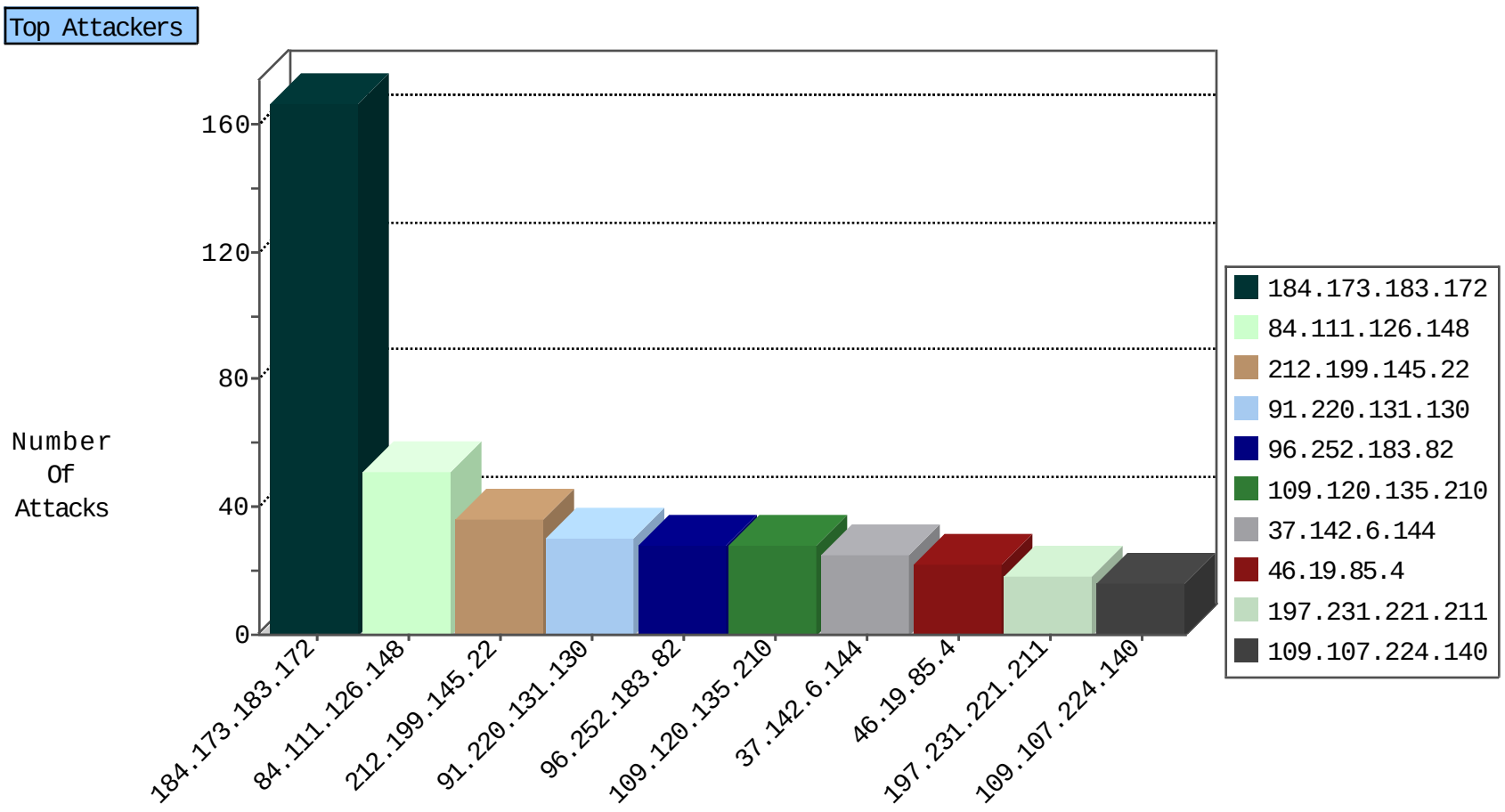
IDF Under Attack
05-09-2015-15:03:05

Top Targets



Top Target

Top Attackers



Top Attackers

05-09-2015-15:03:05 to 05-09-2015-16:03:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.88	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	586
84.111.126.148	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	205
66.249.67.126	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	153
84.108.96.57	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	64
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	8
188.120.148.194	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
77.126.117.24	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
94.159.187.130	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
134.147.203.115	Germany	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1

05-09-2015-15:03:05 to 05-09-2015-16:03:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	167
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	5
91.220.131.130	Russian Federation	147.237.0.19	madim.atal.idf.il	DVRep_P-N_40-59	Permit	4
91.220.131.130	Russian Federation	147.237.0.15	kosher-kravi.idf.il	DVRep_P-N_40-59	Permit	4
91.220.131.130	Russian Federation	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	4
91.220.131.130	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	DVRep_P-N_40-59	Permit	4
91.220.131.130	Russian Federation	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_P-N_40-59	Permit	4
91.220.131.130	Russian Federation	147.237.0.33	idf.il	DVRep_P-N_40-59	Permit	2
66.240.192.138	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	2
91.220.131.130	Russian Federation	147.237.0.35	akaws.idf.il	DVRep_P-N_40-59	Permit	2
91.220.131.130	Russian Federation	147.237.0.200	m4u.idf.il	DVRep_P-N_40-59	Permit	2
198.20.69.98	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.130	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
80.246.136.209	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
5.29.125.250	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1

05-09-2015-15:03:05 to 05-09-2015-16:03:05

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
109.253.144.133	Israel	147.237.72.166	aka.idf.il	INDICATOR-SCAN myscan	2
77.126.117.24	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
149.78.235.82	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.253.144.133	Israel	147.237.72.166	aka.idf.il	GPL SCAN myscan	2
187.35.70.102	Brazil	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
61.160.224.130	China	147.237.77.205	prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
187.35.70.102	Brazil	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
61.160.224.130	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
176.12.139.104	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.160.224.130	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
144.0.0.60	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
144.0.0.60	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
121.88.5.177	Korea, Republic of	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
211.149.240.162	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
188.138.9.51	Germany	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
187.35.70.102	Brazil	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
61.160.224.130	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
178.19.107.114	Poland	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.130	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
5.29.41.221	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
144.0.0.60	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
144.0.0.60	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
115.249.128.114	India	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1

05-09-2015-15:03:05 to 05-09-2015-16:03:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.199.145.22	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
96.252.183.82	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
46.19.85.4	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
84.111.126.148	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	21
109.107.224.140	Jordan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
77.126.247.130	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	15
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
66.249.83.194	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
37.46.39.29	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	10
220.255.1.168	Singapore	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
46.117.137.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
79.183.120.57	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
62.210.162.148	France	147.237.76.42	refuah.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	8
185.14.29.221	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
87.69.1.98	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
84.111.126.148	Israel	147.237.77.216	dover.idf.il		Bad TCP sequence	monitor	7
203.127.96.245	Singapore	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
68.180.229.51	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
109.186.10.22	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
109.67.100.204	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
220.255.1.103	Singapore	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
149.78.29.98	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
212.199.107.106	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
220.255.1.150	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
46.19.85.69	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
176.228.61.187	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
37.142.6.239	Israel	147.237.0.19	madim.atal.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
78.12.163.147	Italy	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
96.44.71.57	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
79.176.23.11	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
5.29.41.221	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.121.40.183	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
84.111.126.148	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	3
149.78.234.74	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
46.19.85.130	Israel	147.237.76.31	nakchal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
197.160.233.14	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
128.242.249.12	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
62.128.48.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
183.89.231.180	Thailand	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	3
46.120.244.160	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
93.125.87.185	Belarus	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
37.142.6.144	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.142.6.144	Block	25
2.54.53.174	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	8
178.137.19.143	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/	Block	6
77.125.143.245	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
79.181.133.245	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.181.133.245	Block	4
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
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
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.181.39.107	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	1
149.78.29.98	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
52.6.246.135	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.26.234.154	Russian Federation	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
203.133.170.144	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/hebrew/ns-news.stm	Block	1
77.125.96.163	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding c7KmD[:!YRKV1RqhUD$n$aozQ%YyVZ5R]HweeNyGGCv[d0VJ{K*E14e8@*]R;u_Afkm in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
66.249.67.206	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//	Block	1
157.55.39.162	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
93.125.87.185	Belarus	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
37.142.6.226	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
176.12.150.128	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
149.78.29.98	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
62.210.162.148	France	147.237.76.42	refuah.idf.il	Admin Blocking	Block	1
85.64.175.240	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
77.125.96.163	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 77.125.96.163	None	1
66.249.67.218	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1442-he/refuah.aspx	Block	1
157.55.39.162	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sachar/forms/downloadform.asp	Block	1
109.65.191.17	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.218.254.108	Germany	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/test/wp-admin/	Block	1
79.181.133.245	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	1
65.99.237.150	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-admin/	Block	1
149.88.13.246	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.65.111.199	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
207.46.13.26	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/yohalan/main/main.asp?catid=59118	Block	1
66.249.78.80	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//938-he/hamaz.aspx	Block	1
157.55.39.162	United States	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/shalishut/site/faq.aspx	None	1
118.97.76.41	Indonesia	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.85.101	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//navy/	Block	1
84.108.36.121	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
183.89.231.180	Thailand	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1125-2.stm	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.250.46.103	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
79.176.23.180	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/giyus/terms.aspx	None	1
157.55.39.191	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/console/core/doc_mgr/mce_src=	Block	1
66.249.78.87	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
149.78.20.188	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.117.16.124	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1

05-09-2015-15:03:05 to 05-09-2015-16:03:05