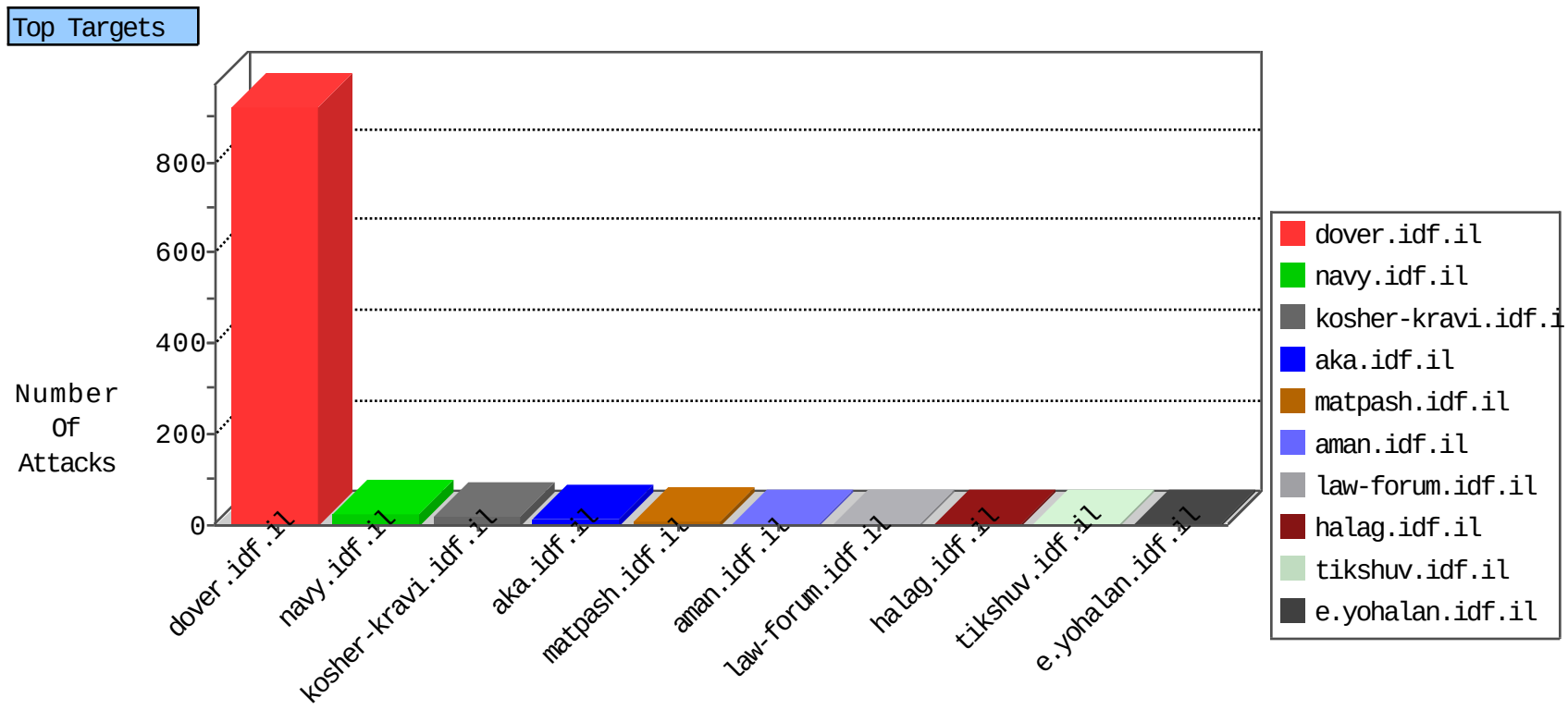
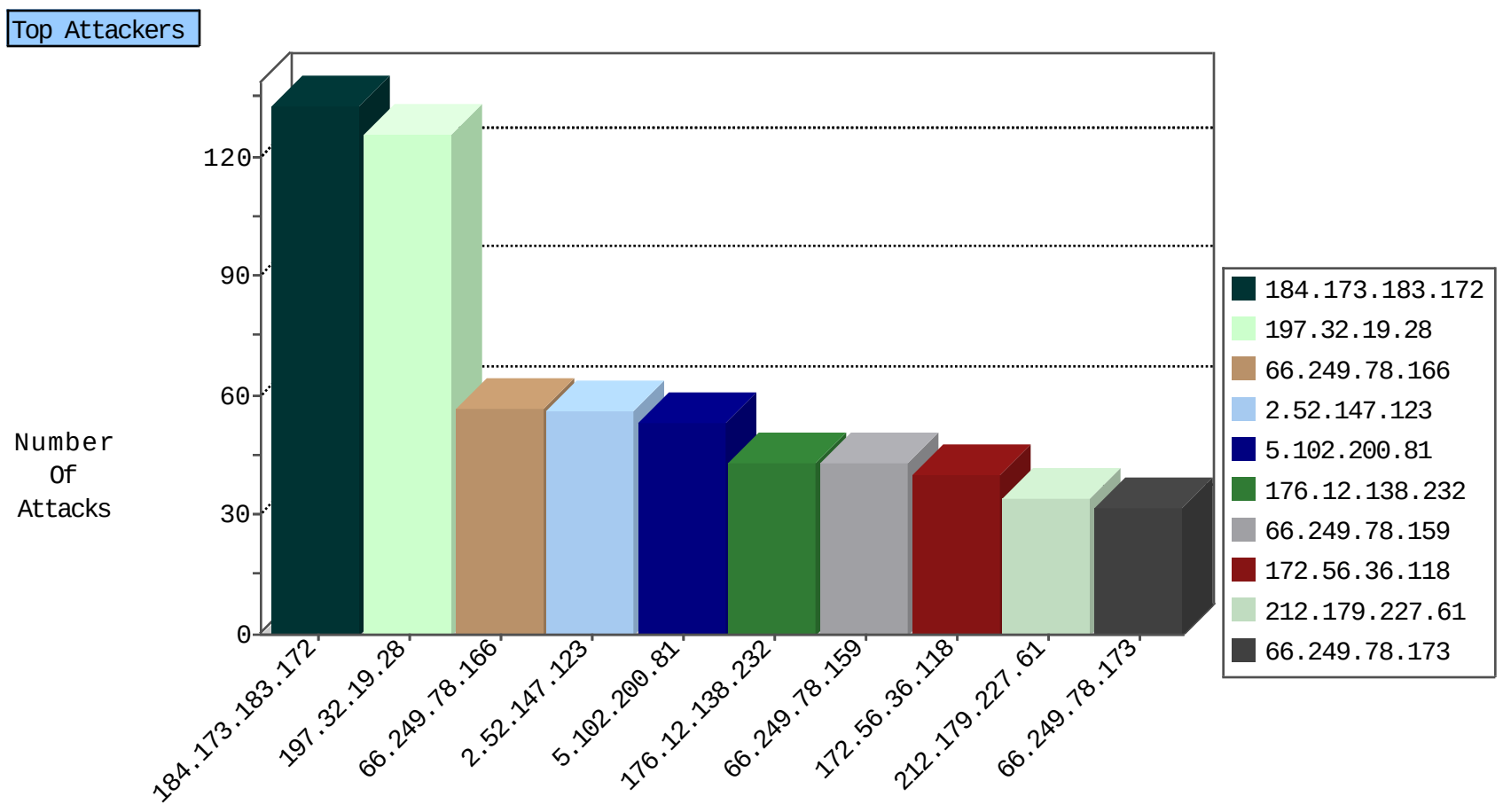
05-09-2015-02:03:01 to 05-09-2015-03:03:01

IDF Under Attack
05-09-2015-02:03:01

Top Targets



Top Attackers



05-09-2015-02:03:01 to 05-09-2015-03:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.100	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	118
220.181.108.109	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	82
190.93.209.229	Argentina	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
146.185.239.100	Russian Federation	147.237.77.176	matpash.idf.il	block-sp-traf1	drop	1

05-09-2015-02:03:01 to 05-09-2015-03:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	133
71.6.167.142	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	2
71.6.165.200	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	2
188.138.9.50	Germany	147.237.76.177	ncore.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	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
46.116.210.130	Israel	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	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
2.52.149.98	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1

05-09-2015-02:03:01 to 05-09-2015-03:03:01

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	5
213.57.109.176	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
183.136.216.3	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
89.147.87.20	Hungary	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
121.127.241.167	Hong Kong	147.237.77.19	law-forum.idf.il	SERVER-WEBAPP JBoss web console access attempt	1
61.240.144.66	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
89.147.87.20	Hungary	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
89.147.87.20	Hungary	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
89.147.87.20	Hungary	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
89.147.87.20	Hungary	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
89.147.87.20	Hungary	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
89.147.87.20	Hungary	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
89.147.87.20	Hungary	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
183.136.216.3	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
121.127.241.167	Hong Kong	147.237.77.19	law-forum.idf.il	GPL WEB_SERVER WEB-MISC JBoss web-console access	1
61.240.144.64	China	147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
89.147.87.20	Hungary	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
12.139.34.20	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 4096	1
89.147.87.20	Hungary	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
89.147.87.20	Hungary	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
89.147.87.20	Hungary	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
89.147.87.20	Hungary	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
89.147.87.20	Hungary	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1

05-09-2015-02:03:01 to 05-09-2015-03:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
197.32.19.28	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	126
2.52.147.123	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	56
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	54
5.102.200.81	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	53
176.12.138.232	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
172.56.36.118	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
212.179.227.61	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
86.24.66.239	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
134.134.139.74	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
134.134.139.77	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
68.180.228.224	United States	147.237.0.15	kosher-kravi.idf.i	SAM rule	drop	drop	18
93.233.110.83	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
138.210.34.20	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
70.199.65.56	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
107.77.90.113	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
75.118.97.205	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
134.134.137.75	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
134.134.139.77	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
66.249.64.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
66.249.64.178	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
12.41.136.2	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
157.55.39.136	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
96.127.65.79	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
2.54.1.13	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
68.196.254.209	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
77.127.73.198	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
157.55.39.162	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
65.19.138.33	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.73.223	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
37.140.141.39	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
188.165.15.99	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.191	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
134.134.139.70	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
68.180.229.51	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.19.86.216	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
213.57.161.45	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
134.134.137.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
162.243.225.144	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
134.134.139.76	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
64.121.96.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
134.134.137.75	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2

05-09-2015-02:03:01 to 05-09-2015-03:03:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
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	20
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	5
157.55.39.66	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.66	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
207.46.13.26	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.26	Block	2
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.253	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/m/	Block	1
66.249.65.181	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1250-he/atal.aspx	Block	1
180.76.6.147	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/info.asp	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.stm	Block	1
207.46.13.26	United States	147.237.72.166	aka.idf.il	Unknown Parameter pageNum in aka.idf.il/patzar/klali/default.asp	None	1
58.162.228.12	Australia	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
157.55.39.144	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
66.249.67.91	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71868-he/maarachot.aspx	Block	1
188.165.15.117	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kamlar/news/www.israelbar.org.il	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
207.46.13.99	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 207.46.13.99	Block	1
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/armored/hativa7/structure.stm	Block	1
157.55.39.162	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
121.127.241.167	Hong Kong	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/web-console/serverinfo.jsp	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1065-he/dover.aspx	Block	1
192.171.235.196	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english.	Block	1
207.46.13.99	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/about/pages/aboutus.aspx	Block	1
66.249.64.245	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18858-he/dover.aspx	Block	1
157.55.39.191	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_text.asp	Block	1
121.127.241.167	Hong Kong	147.237.77.19	law-forum.idf.il	WEB MISC Unauthorized File Access	None	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19748-he/idfgdover.aspx	Block	1
46.19.123.125	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
157.55.39.136	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
213.57.161.45	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.64.253	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/	Block	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/shalishut/site/faq.aspx	None	1
58.162.228.12	Australia	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1

05-09-2015-02:03:01 to 05-09-2015-03:03:01