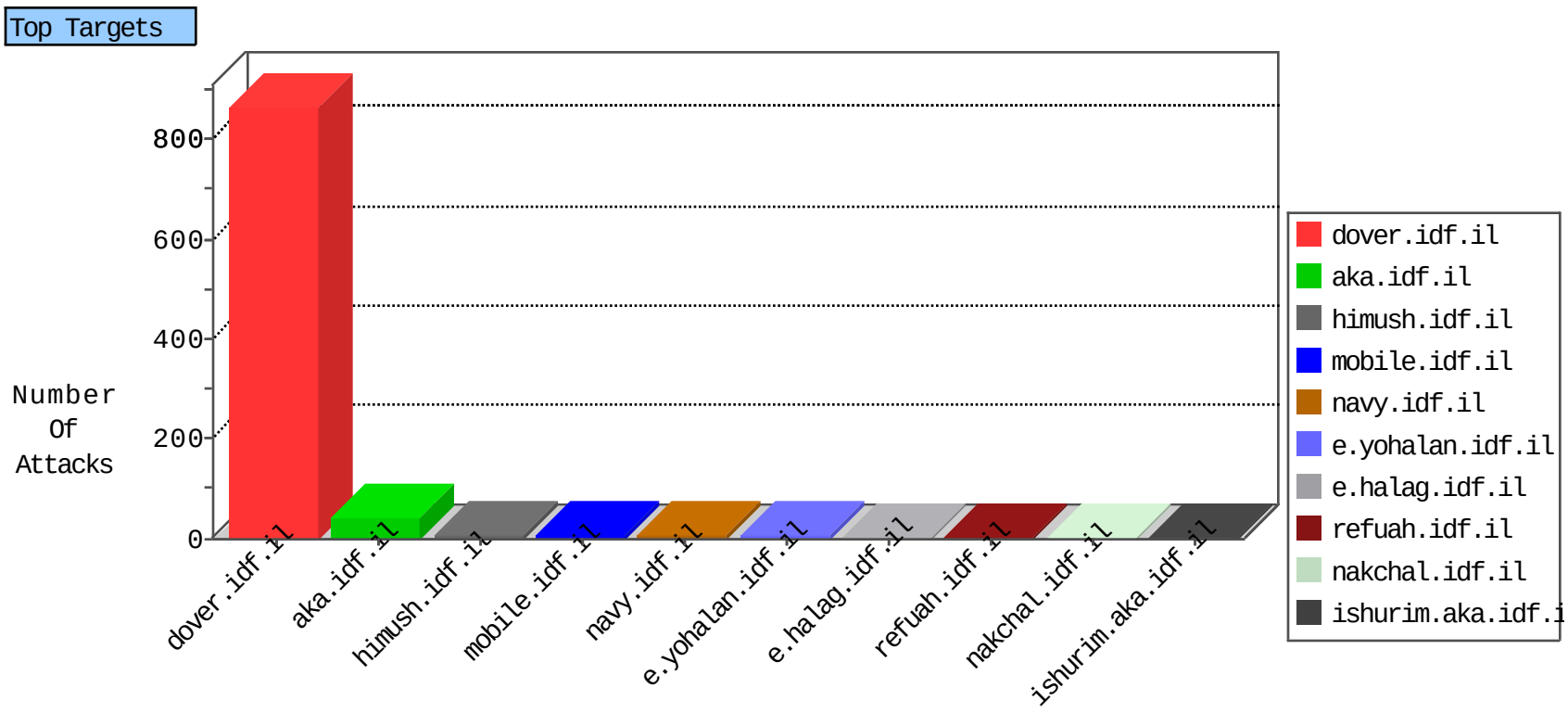
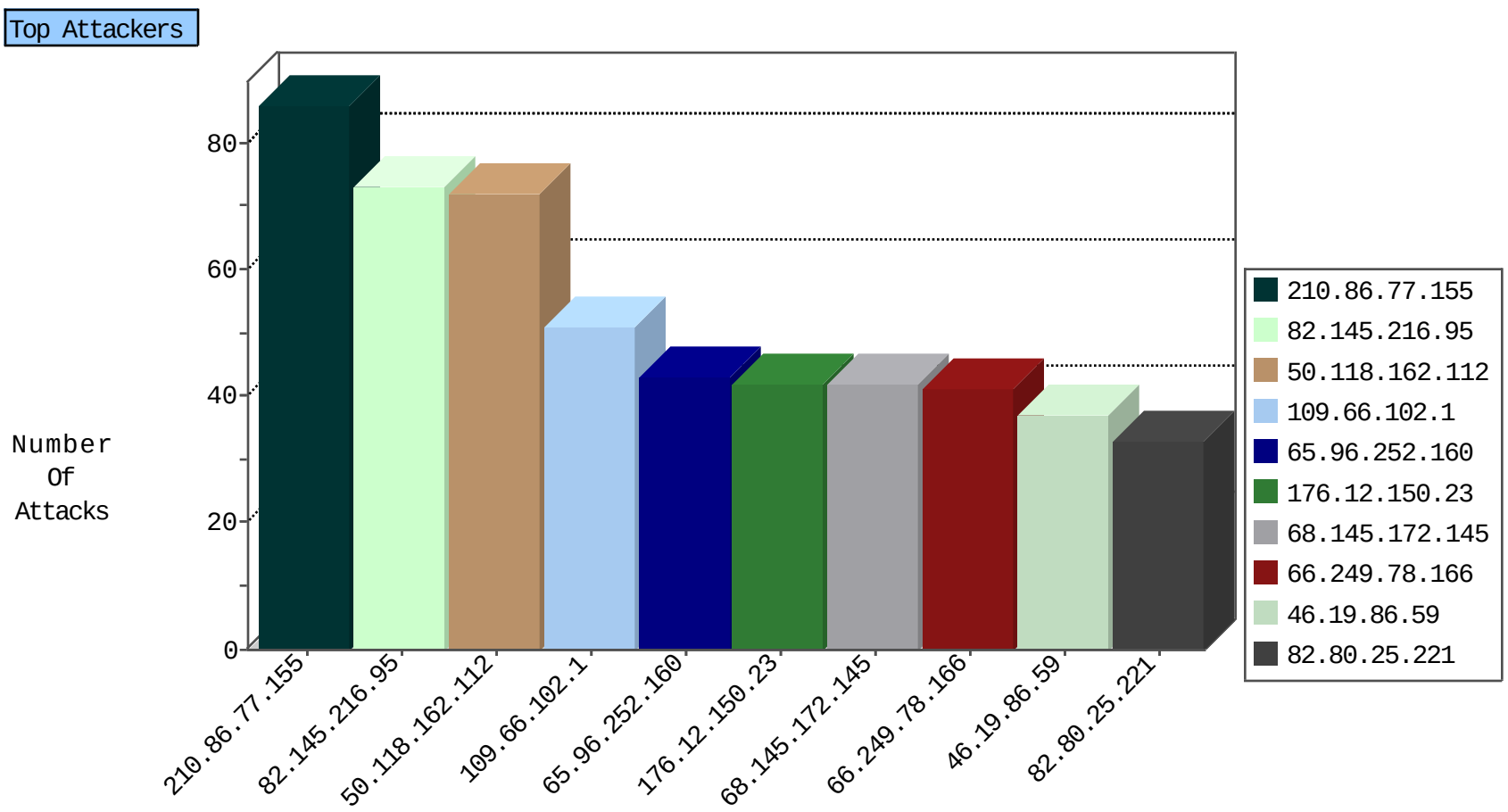
04-17-2015-04:03:02 to 04-17-2015-05:03:02

IDF Under Attack
04-17-2015-04:03:02

Top Targets



Top Attackers



04-17-2015-04:03:02 to 04-17-2015-05:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
58.176.120.254	Hong Kong	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	3
109.66.102.1	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
204.42.253.2	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	2
222.186.21.202	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
204.42.253.2	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	2
80.82.70.198	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
180.4.238.144	Japan	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
80.82.70.198	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
107.154.64.10	United States	147.237.76.197	e.himush.idf.il	L4 Source or Dest Port Zero	drop	1

04-17-2015-04:03:02 to 04-17-2015-05:03:02

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	25
109.66.102.1	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
85.25.103.50	Germany	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	2
66.240.236.119	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.226	www.chamatz.aka.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
71.6.165.200	United States	147.237.76.202	e.halag.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
198.20.69.98	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.35	akaws.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
71.6.165.200	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.147	chinuch.aka.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
188.138.9.50	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.200	eitan.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
71.6.165.200	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1

04-17-2015-04:03:02 to 04-17-2015-05:03:02

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	33
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
221.235.188.212	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
101.226.2.99	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 2048	1
221.235.188.212	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
93.190.92.127	Germany	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1
221.235.188.212	China	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
117.135.163.104	China	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 3072	1
61.160.224.128	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
101.226.2.99	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
221.235.188.212	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
101.226.2.99	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -f -sS	1
221.235.188.212	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
111.203.22.56	China	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 3072	1

04-17-2015-04:03:02 to 04-17-2015-05:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
210.86.77.155	New Zealand	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	86
82.145.216.95	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	73
50.118.162.112	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	72
68.145.172.145	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
176.12.150.23	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
65.96.252.160	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
46.19.86.59	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
109.66.102.1	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
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
181.47.37.49	Argentina	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
79.183.5.45	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
99.160.2.170	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
66.249.67.5	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
176.12.146.105	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
46.19.85.152	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	9
54.246.252.171	Ireland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
66.249.64.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
69.144.212.63	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
66.249.64.72	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.19.86.254	Israel	147.237.76.30	himush.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
176.12.144.20	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
79.109.63.120	Spain	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
220.255.1.85	Singapore	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
184.166.117.119	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
181.66.157.178	Peru	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
65.55.217.218	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
180.249.170.117	Indonesia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
68.180.228.117	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
157.55.39.33	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
79.181.134.142	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	3
207.46.13.77	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
183.91.86.31	Indonesia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
109.66.102.1	Israel	147.237.77.216	dover.idf.il	Unexpected post SYN packet - RST or SYN expected	drop	drop	3
128.242.249.11	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
109.66.102.1	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
84.228.169.6	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
50.43.26.55	United States	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
99.238.150.210	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
207.46.13.1	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
66.249.64.76	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
37.26.146.140	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
218.213.29.101	Hong Kong	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
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	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
109.66.102.1	Israel	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 109.66.102.1	Block	1
31.193.141.19	United Kingdom	147.237.76.42	refuah.idf.il	Multiple signatures from 31.193.141.19	Block	1
66.249.79.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-he/refuah.aspx	Block	1
207.46.13.104	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/tizmoret/klali/default.asp	None	1
66.249.78.6	Israel	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on 147.237.76.86//scriptresource.axd	Block	1
184.105.247.196	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
66.249.67.5	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/info.asp?moduleid=2&catid=22703&docid=22716	Block	1
75.139.228.201	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/navy/navy12.stm	Block	1
66.249.67.157	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.31	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-18984-he	Block	1
148.251.41.235	Germany	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
31.193.141.19	United Kingdom	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
66.249.79.143	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
66.249.78.13	Israel	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on 147.237.76.86//webresource.axd	Block	1
66.249.67.5	Israel	147.237.72.166	aka.idf.il	Unknown Parameter newsItem in www.aka.idf.il/megurim/news/	None	1
188.165.15.78	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19667-he/idfgdover.aspx)	Block	1
77.125.143.74	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/iturim/iturim.aspx	None	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	1
66.249.67.157	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.157	Block	1
207.46.13.77	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.77	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/chamatz/home/d...sp	Block	1
37.115.187.54	Ukraine	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
66.249.78.20	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/webresource.axd	Block	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
192.0.101.59	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/0/size220x0/8280.jpg&zoom=2	Block	1
93.190.92.127	Germany	147.237.77.216	dover.idf.il	Multiple signatures from 93.190.92.127	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/media.stm	Block	1
207.46.13.77	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-15554-he/dover.aspx-title=	Block	1
66.249.67.157	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/5/×©×§×• ×¤×™×ª 3	Block	1
157.55.39.33	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-17899-he/dover.aspx×³Â¦×³Ö³Æ'Ö¶â€™Ö³â€šÖ²Â¯Ö³Æ'×'â,¬ÂšÖ³â€šÖ²Â¿Ö³Æ'×'â,¬ÂšÖ³â€šÖ²Â½×³Ö³Æ'Ö¶â€™Ö³â€šÖ²Â¯Ö³Æ'×'â,¬ÂšÖ³â€šÖ²Â¿Ö³Æ'×'â,¬ÂšÖ³â€šÖ²Â½×³Ö³Æ'Ö¶â€™Ö³â€šÖ²Â¯Ö³Æ'×'â,¬ÂšÖ³â€šÖ²Â¿Ö³Æ'×'â,¬ÂšÖ³â€šÖ²Â½×³Â?:	Block	1
66.249.64.16	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/scriptresource.axd	Block	1
66.249.78.120	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/modules/forums.frm/frmsendmessage.aspx	Block	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kenesatuda	Block	1
207.46.13.1	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.1	Block	1
93.190.92.127	Germany	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
207.46.13.104	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.73.211	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
158.222.14.24		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//english/news/grapheat.stm	Block	1
66.249.67.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
74.82.47.2	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.67.45	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.1	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-12847-he/dover.aspx×³Â¡×³Â?"×³×ŸÂ¿Â½	Block	1