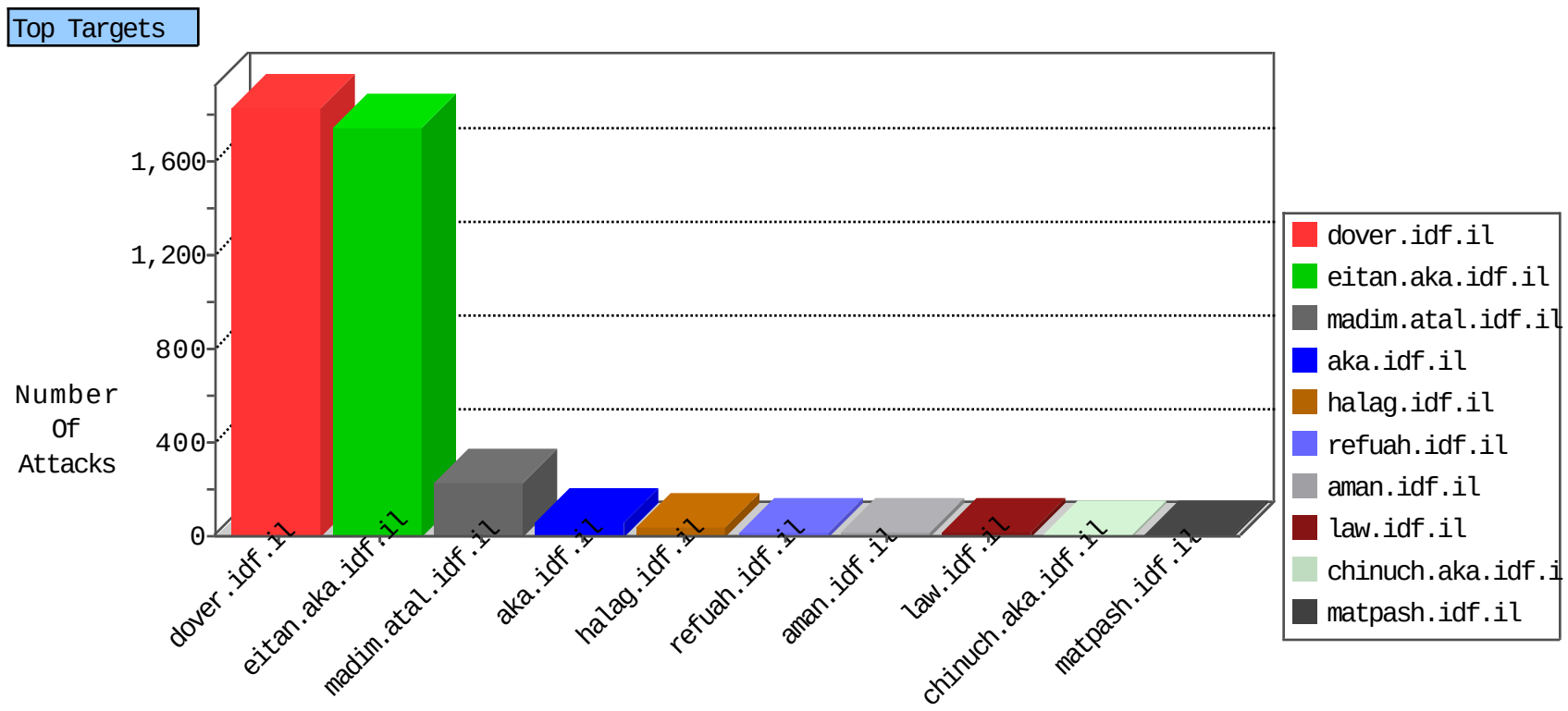
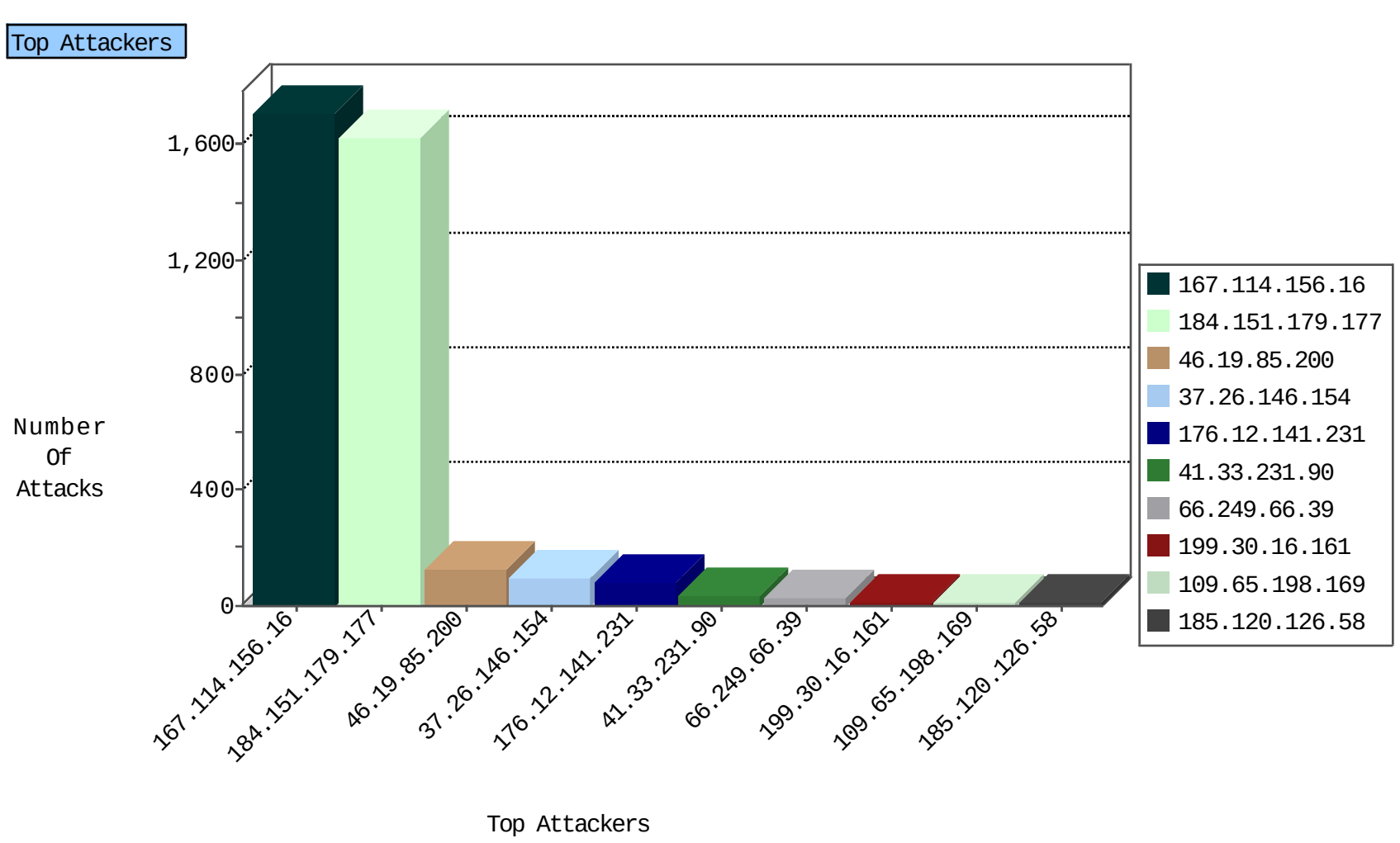
12-06-2015-06:04:00 to 12-06-2015-07:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-06-2015-06:04:00 to 12-06-2015-07:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3485
66.249.66.61	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3379
115.239.228.8	China	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Http	drop	2
185.106.94.126		147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

12-06-2015-06:04:00 to 12-06-2015-07:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
188.165.15.60	France	147.237.77.74	law.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.202	France	147.237.72.156	aman.idf.il	C228: HTTP: AhrefBot crawler	Block	1

12-06-2015-06:04:00 to 12-06-2015-07:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.66.75	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.61	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
104.192.0.226	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
104.192.0.226	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
78.193.2.8	147.237.77.74	France	law.idf.il	ET SCAN NMAP -sS window 1024	1
185.107.212.159	147.237.77.216		dover.idf.il	ET SCAN Potential SSH Scan	1
125.65.165.215	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
125.65.165.215	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
104.219.238.10	147.237.77.178		e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
104.219.238.10	147.237.76.148		gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
104.219.238.10	147.237.76.86		navy.idf.il	ET SCAN NMAP -sS window 1024	1
104.192.0.226	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.174.89.82	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
78.193.2.8	147.237.77.61	France	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
125.65.165.215	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
125.65.165.215	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
104.219.238.10	147.237.77.216		dover.idf.il	ET SCAN Potential SSH Scan	1
104.219.238.10	147.237.77.170		maarachot.idf.il	ET SCAN Potential SSH Scan	1
104.219.238.10	147.237.76.147		chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1

12-06-2015-06:04:00 to 12-06-2015-07:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
184.151.179.177	Canada	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1458
37.26.146.154	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	96
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
66.249.66.39	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
199.30.16.161	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
109.65.198.169	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.183.205.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.176	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
109.64.213.176	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
109.64.213.176	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
199.30.24.17	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
91.231.192.149	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
149.78.19.112	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.126.58		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
66.249.74.6	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.178.164.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.126.58		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.11.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
79.176.28.39	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
37.26.148.151	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	2
87.69.132.200	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
37.26.149.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
91.231.192.149	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.75.38	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
87.69.132.200	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.179.213.124	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	2
93.173.134.205	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
66.249.78.170	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
62.219.187.7	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
89.139.173.158	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
66.249.66.45	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
93.173.134.205	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
176.13.11.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
66.249.78.184	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
212.199.141.138	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
185.120.126.58		147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
37.26.146.154	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
61.135.190.72	China	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
46.19.86.208	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.91	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.26.149.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
74.82.47.11	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.95	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
66.87.116.227	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

12-06-2015-06:04:00 to 12-06-2015-07:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
184.151.179.177	Canada	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 184.151.179.177	Block	171
46.19.85.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	111
176.12.141.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
46.19.85.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	19
46.19.85.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
66.249.66.32	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
2.52.2.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.34.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
176.12.141.231	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.141.231	Block	2
45.55.53.138		147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 45.55.53.138	Block	2
79.176.172.249	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 79.176.172.249	None	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	2
176.13.4.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
2.54.38.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
62.219.187.7	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.249.147.28	Italy	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
78.46.4.61	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
195.154.227.118	France	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 195.154.227.118	Block	1
66.249.73.242	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
66.249.66.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1065-he/dover.aspx	Block	1
89.138.178.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
74.208.205.43	United States	147.237.77.74	law.idf.il	E-mail collector robots 14	Block	1
184.168.152.148	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
66.249.66.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/main/giyus/general.aspx	Block	1
123.152.196.35	China	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
64.19.78.242	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/	Block	1
37.26.148.151	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
79.176.172.249	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding n.	None	1
198.20.69.74	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/m/	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/chinuch/search/searchresults.asp	None	1
92.53.113.89	Russian Federation	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
74.208.205.43	United States	147.237.77.74	law.idf.il	eMail Hoarding	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
184.168.200.76	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
66.249.66.78	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/giyus/general.aspx	Block	1
128.70.122.5	Russian Federation	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/9/	Block	1
66.249.64.181	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/8/638.pdf	Block	1
202.188.32.46	Malaysia	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.66.72	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/coordinationgaza/govermment/pages/coordinatortransport.aspx	Block	1
98.139.204.36	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
46.19.86.179	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/894-he/atal.aspx	Block	1
74.208.205.43	United States	147.237.77.176	matpash.idf.il	E-mail collector robots 14	Block	1
190.104.117.168	Guatemala	147.237.77.216	dover.idf.il	Distributed eMail Hoarding	Block	1
66.249.66.81	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/×©×§×•×¤×™×ª 2	Block	1
141.8.142.16	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
66.249.65.18	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1

12-06-2015-06:04:00 to 12-06-2015-07:04:00