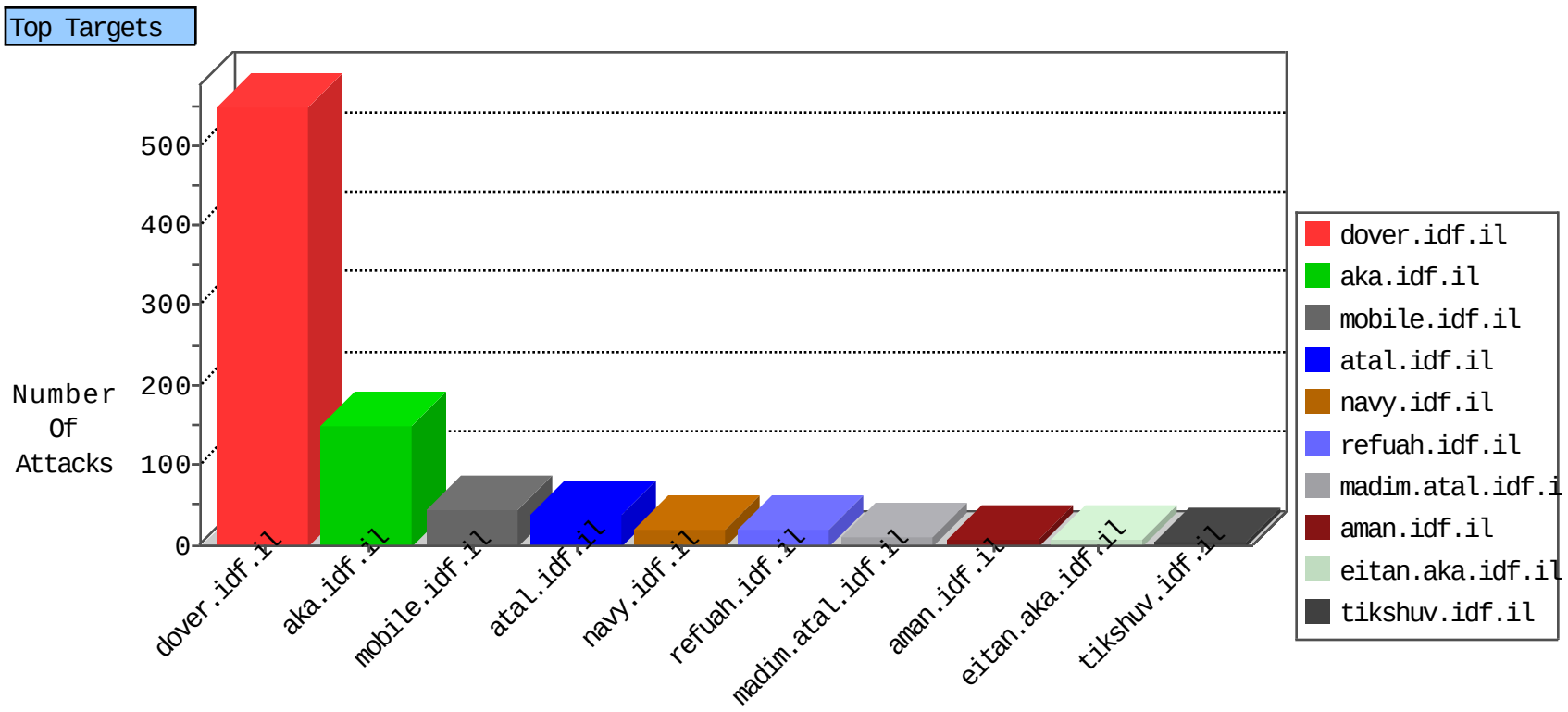
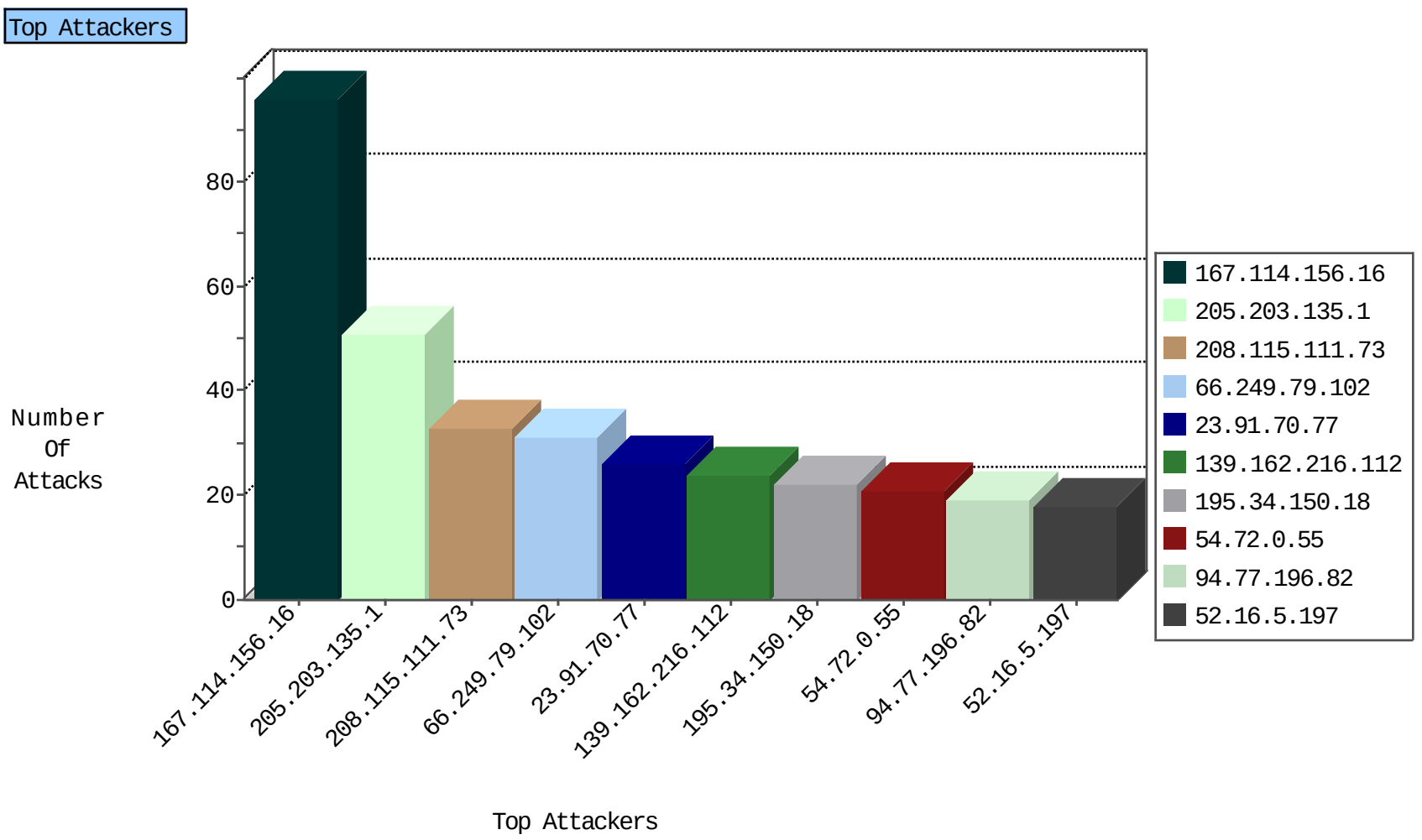
04-30-2016-10:04:01 to 04-30-2016-11:04:01

IDF Under Attack
Daily Report

Top Targets



Top Attackers



04-30-2016-10:04:01 to 04-30-2016-11:04:01

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	HTTP-POST-Segmented-DoS	dest-reset	3683
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3536
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1158
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	4
60.191.74.83	China	147.237.0.16	my-kosher-kravi.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
198.20.70.114	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.132	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
71.6.165.200	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.132	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
198.20.69.74	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.132	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1

04-30-2016-10:04:01 to 04-30-2016-11:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
23.91.70.77	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
23.91.70.77	United States	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
23.91.70.77	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
70.68.224.173	Canada	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3

04-30-2016-10:04:01 to 04-30-2016-11:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
23.91.70.77	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	14
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
70.68.224.173	147.237.77.74	Canada	law.idf.il	SQL Injection - Select From	2
203.86.29.220	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
66.240.213.93	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
185.110.132.55	147.237.76.197	Ukraine	e.himush.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.55	147.237.76.39	Ukraine	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
112.169.100.157	147.237.76.202	Korea, Republic of	e.halag.idf.il	ET SCAN Potential SSH Scan	1
112.169.100.157	147.237.0.19	Korea, Republic of	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
107.158.255.194	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -f -sS	1
107.158.255.194	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 2048	1
203.86.29.220	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
85.214.134.155	147.237.76.202	Germany	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
203.86.29.220	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
66.240.213.93	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
185.110.132.55	147.237.76.200	Ukraine	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.55	147.237.76.86	Ukraine	navy.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.55	147.237.0.16	Ukraine	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
112.169.100.157	147.237.76.148	Korea, Republic of	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
107.158.255.194	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 2048	1
107.158.255.194	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 3072	1
107.158.255.194	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -f -sS	1

04-30-2016-10:04:01 to 04-30-2016-11:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
66.249.79.102	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
198.58.102.95	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.179.22.150	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.64.3	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
91.121.165.101	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
91.155.235.138	Finland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.60.25.157	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
95.170.192.221	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.151	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
87.69.122.69	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
162.243.104.237	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
114.253.32.35	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.64.124	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.229.173.67	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.64.28.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.29.197.253	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
41.218.23.111	Sudan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.3.147.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.71.22.123	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.221.249	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
93.157.82.162	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
46.19.85.191	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
31.13.162.132	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
82.26.91.180	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.53.145.149	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
66.249.66.177	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
199.30.25.60	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.64.75	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.184	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.33	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
31.210.186.128	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-30-2016-10:04:01 to 04-30-2016-11:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
217.132.96.204	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 217.132.96.204	Block	11
2.53.18.167	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
109.253.208.38	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	4
109.65.207.214	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 109.65.207.214	Block	3
109.65.207.214	Israel	147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	3
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.177	Block	3
79.179.22.150	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.253.221.249	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.151	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.151	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.55.38.216	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/milluim/index	Block	2
66.249.66.5	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/150302011yezu.aspx	Block	1
46.19.85.55	Israel	147.237.77.216	dover.idf.il	Malformed URL _pk_id.20.8afc=f7b484780610c6ce.1454268433.4.1462002032.1462002032.;	Block	1
216.218.206.66	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
93.157.82.162	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
46.119.127.129	Ukraine	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
178.153.66.31	Qatar	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
17.142.156.109	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.55	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method F%22%5D; in URL _pk_id.20.8afc=f7b484780610c6ce.1454268433.4.1462002032.1462002032.	Block	1
216.218.206.67	United States	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to 147.237.0.19/	Block	1
157.55.12.80	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
94.230.86.243	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
46.119.127.129	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.119.127.129	Block	1
178.153.66.31	Qatar	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
17.142.156.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
109.67.134.50	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
157.55.39.52	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 157.55.39.52	Block	1
103.255.4.35	Pakistan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
46.120.211.11	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
46.19.85.55	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1
185.3.144.33	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
109.253.134.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
68.180.229.215	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakhal.idf.il/1108-he/nakhal.aspx	Block	1
217.132.96.204	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
157.55.39.52	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/navmenu/mazi.idf.il	Block	1
109.64.28.40	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
61.115.87.240	Japan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
46.19.85.55	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version _pk_ses.20.8afc=*	Block	1
212.150.221.248	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
46.119.127.129	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
157.55.39.53	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1

04-30-2016-10:04:01 to 04-30-2016-11:04:01