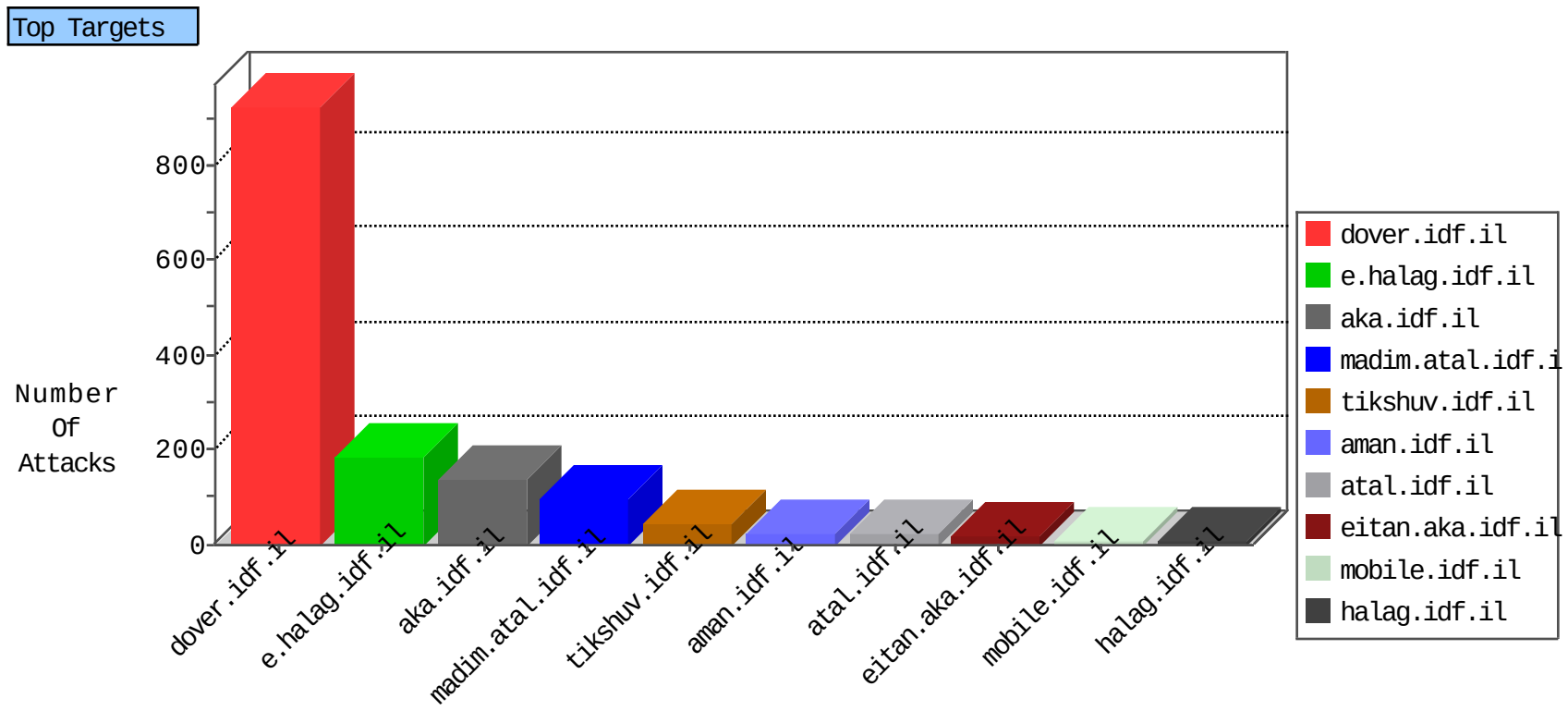
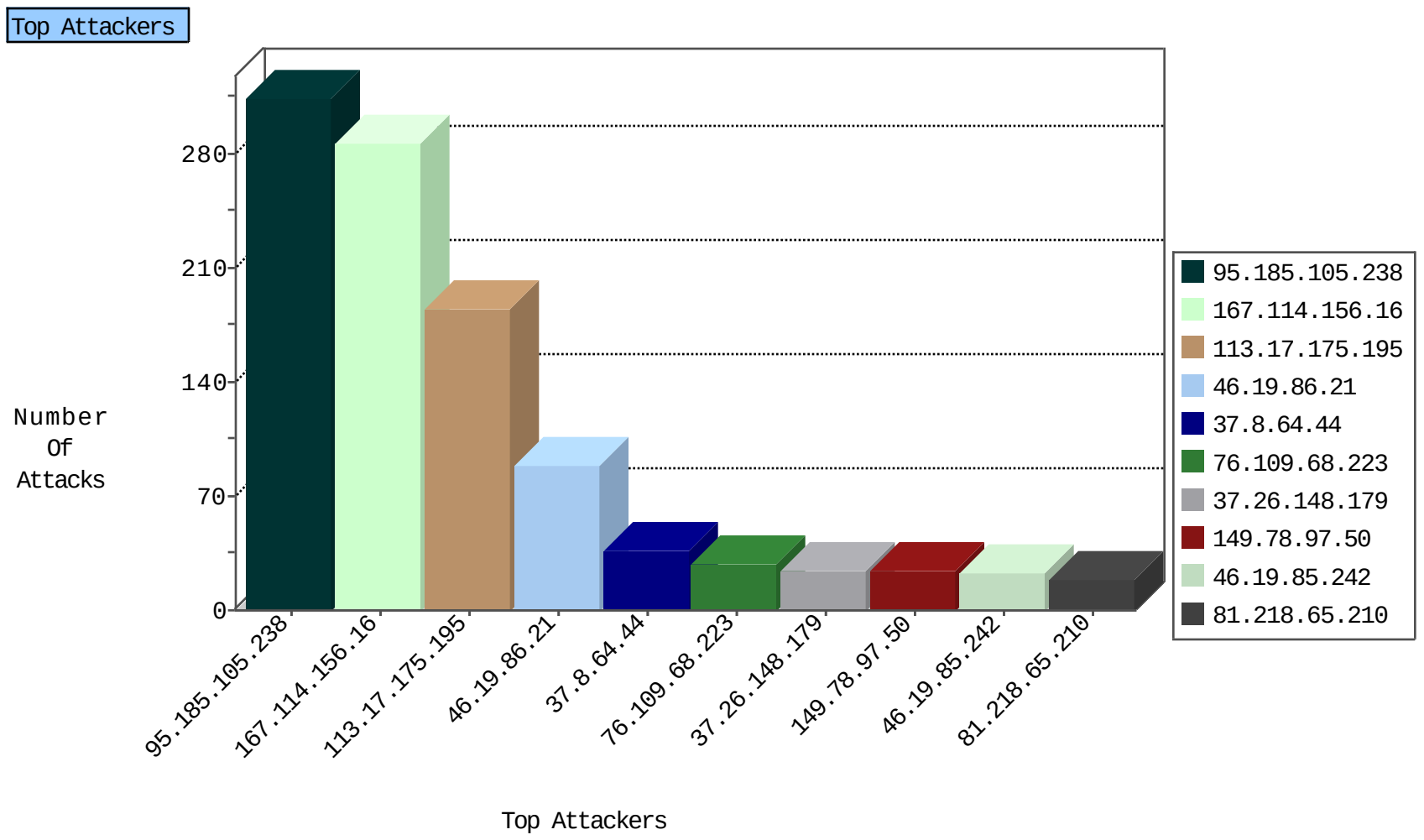
04-24-2016-23:04:06 to 04-25-2016-00:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-24-2016-23:04:06 to 04-25-2016-00:04:06

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	13075
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	6179
95.185.105.238	Saudi Arabia	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Product	dest-reset	231
113.17.175.195	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	184
85.65.60.227	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	101
81.218.65.210	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	12
95.185.105.238	Saudi Arabia	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	7
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
107.150.32.61	United States	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
80.82.78.38	Netherlands	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
74.91.17.179	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
61.182.170.38	China	147.237.76.197	e.himush.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
37.97.185.129	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
46.174.52.5	Russian Federation	147.237.76.199	e.nakchal.idf.il	L4 Source or Dest Port Zero	drop	1
149.78.126.217	United States	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1
46.174.52.5	Russian Federation	147.237.0.35	akaws.idf.il	L4 Source or Dest Port Zero	drop	1
107.150.32.62	United States	147.237.77.234	halag.idf.il	block-sp-traf1	drop	1
46.174.52.5	Russian Federation	147.237.77.178	e.matpash.idf.il	L4 Source or Dest Port Zero	drop	1
37.97.185.129	Netherlands	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
74.91.17.181	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	drop	1
46.174.52.5	Russian Federation	147.237.72.156	aman.idf.il	L4 Source or Dest Port Zero	drop	1
107.150.46.38	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	drop	1
46.174.52.5	Russian Federation	147.237.77.243	mobile.idf.il	L4 Source or Dest Port Zero	drop	1
37.97.185.129	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
80.82.78.38	Netherlands	147.237.0.34	tikshuv.idf.il	block-sp-traf1	drop	1
46.174.52.5	Russian Federation	147.237.72.167	ishurim.aka.idf.il	L4 Source or Dest Port Zero	drop	1
84.111.42.162	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1

04-24-2016-23:04:06 to 04-25-2016-00:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-24-2016-23:04:06 to 04-25-2016-00:04:06

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

04-24-2016-23:04:06 to 04-25-2016-00:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
95.185.105.238	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
37.8.64.44	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
76.109.68.223	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
149.78.97.50	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
40.77.167.59	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
146.148.67.248	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
151.24.159.54	Italy	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
79.181.137.213	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
105.112.32.48	Nigeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
177.92.51.109	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.26.148.179	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	8
149.78.97.50	United States	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
84.108.10.192	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.226.45.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.26	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.93.180	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.130.218	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
84.108.10.192	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
31.210.186.140	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.44.58.174	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
207.46.13.173	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.189	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.148.179	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
93.172.194.189	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.121.116.245	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.26.148.179	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.95.57.206	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
31.210.186.118	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.242	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
46.19.85.242	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
65.55.210.103	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.26.148.179	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
188.161.91.37	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.242	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
37.26.148.179	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
188.225.132.124	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.13.3.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.136.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.168	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.93.245	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.160.181.0	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.84.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-24-2016-23:04:06 to 04-25-2016-00:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	84
46.19.86.21	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	3
5.29.82.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
147.75.208.226	Switzerland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.26.149.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.232	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	2
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/eitan/listpage/	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
176.13.3.37	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
109.64.22.76	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
2.53.16.61	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
79.177.116.106	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
213.57.129.54	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	1
149.78.23.191	United States	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
85.65.31.90	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.79.142	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/edim/yoman/yoman.asp	Block	1
66.249.64.151	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8929-he/refuah.aspx	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19108-he/kkkkkkk=8afde7b5kkkkkkk_8afde7b5	Block	1
109.67.177.122	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.67.177.122	Block	1
5.29.20.21	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$cb14640971 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
79.177.116.106	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
66.249.66.50	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
149.78.97.50	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
89.205.28.238	Macedonia, the Former Yugoslav Republic of	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
66.249.64.182	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
199.30.24.102	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.67.177.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/5/71725.pdf'	Block	1
80.82.78.38	Netherlands	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.baidu.com/cache/global/img/gs.gif	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/eitan/listpage/	Block	1
46.120.52.252	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl41 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
157.55.39.27	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
89.205.28.238	Macedonia, the Former Yugoslav Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
68.180.230.184	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20624-he/dover.aspx	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17474-en/dover.aspxhttp:/	Block	1
84.95.57.206	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/images/1.he/infocenteritem/	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/edim/yoman/yoman.asp	Block	1
46.120.131.6	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
157.55.39.96	United States	147.237.77.233	atal.idf.il	Abnormally Long Request URL	Block	1
95.86.66.60	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
74.91.17.179	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.xy966.com/	Block	1
213.57.129.54	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	1
149.78.23.191	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 149.78.23.191	Block	1
85.64.21.70	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1

04-24-2016-23:04:06 to 04-25-2016-00:04:06