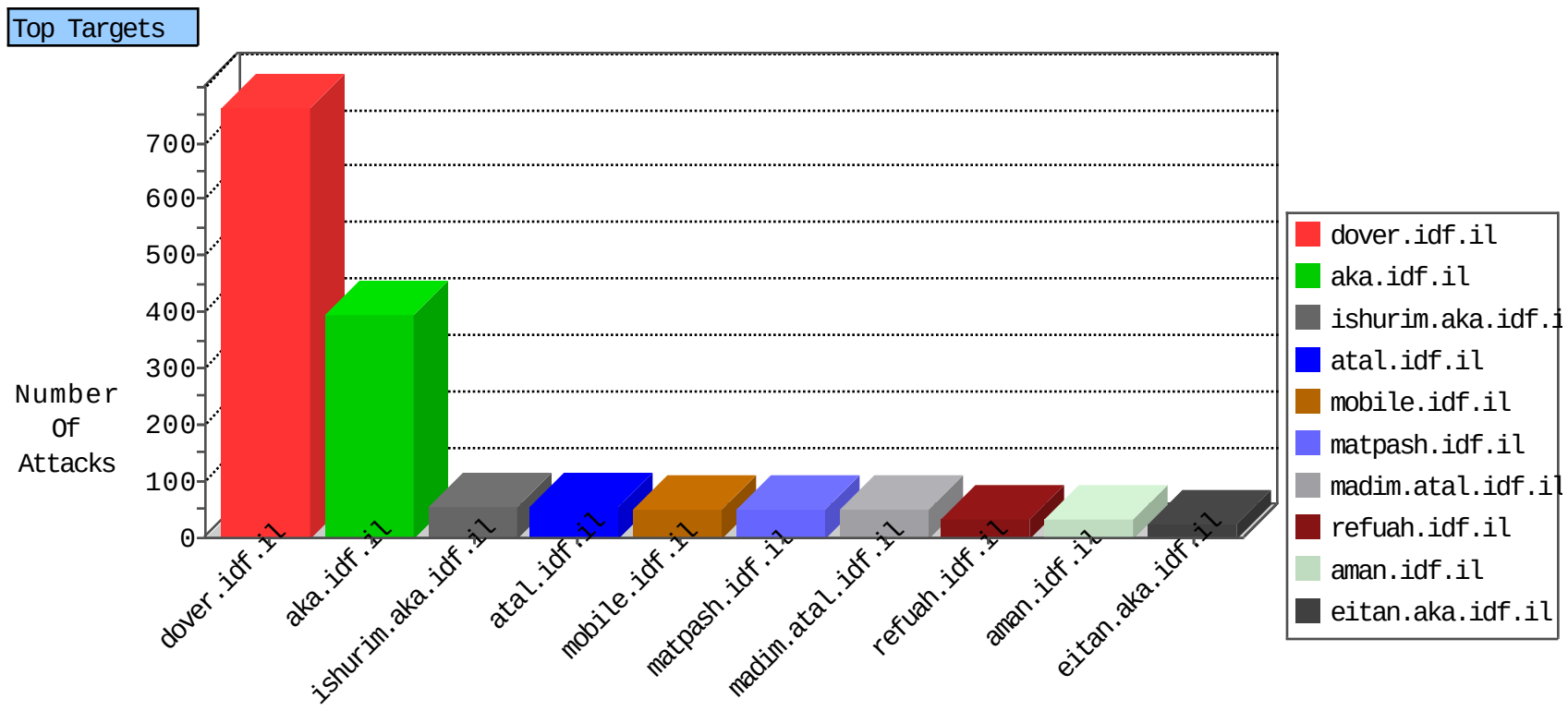
04-25-2016-13:04:08 to 04-25-2016-14:04:08

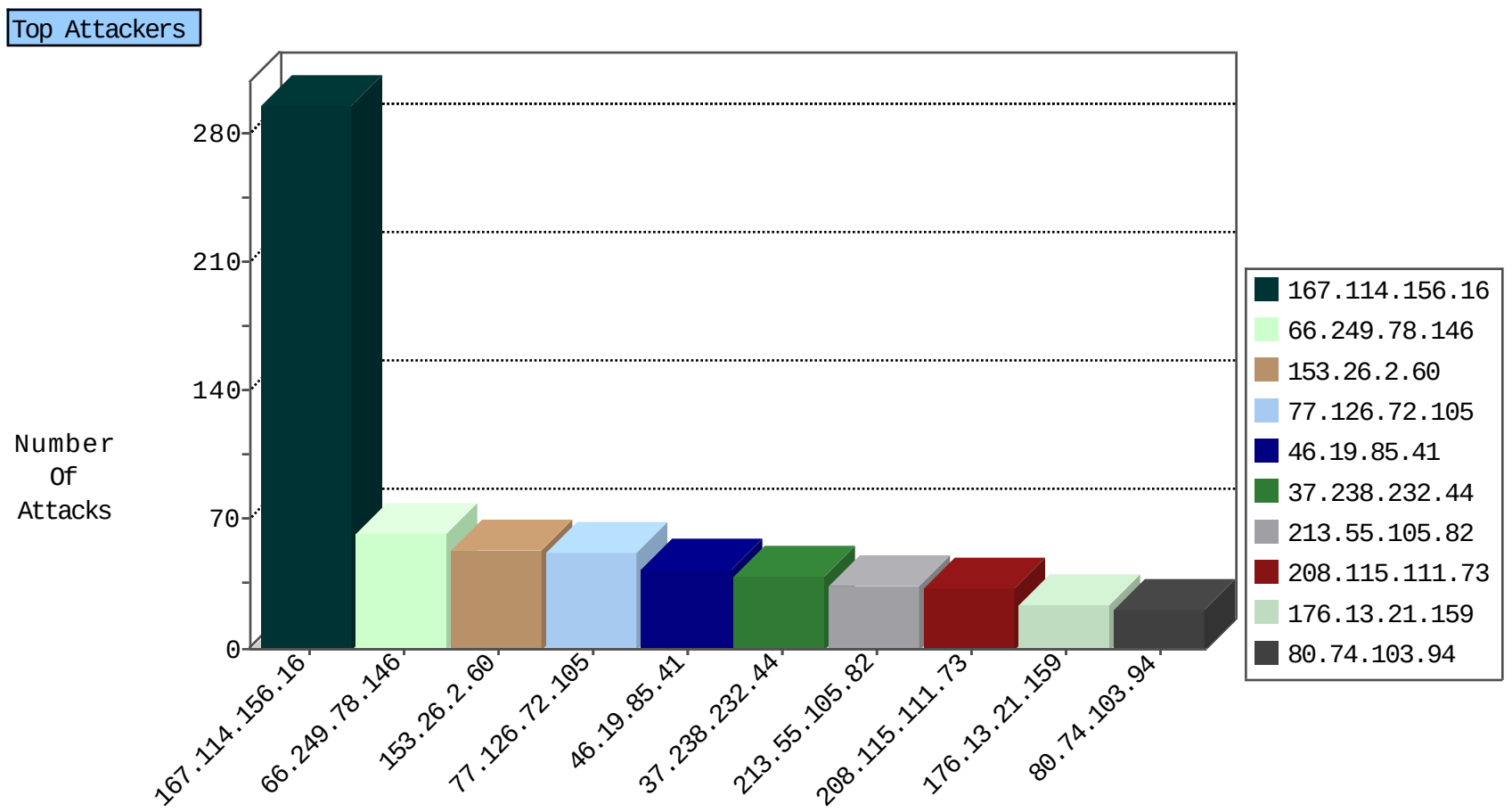
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

04-25-2016-13:04:08 to 04-25-2016-14:04:08

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	12882
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	4900
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	139
81.218.65.210	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	9
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
31.168.233.62	Israel	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
94.102.52.10	Netherlands	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
45.63.20.231	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1

04-25-2016-13:04:08 to 04-25-2016-14:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-25-2016-13:04:08 to 04-25-2016-14:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
209.66.70.253	147.237.77.176	United States	matpash.idf.il	Tehila - Perl LWP with fake user agent	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
106.184.2.29	147.237.76.177	Japan	ncore.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
84.95.83.134	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
58.218.204.211	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
187.241.168.143	147.237.77.235	Mexico	sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
179.26.48.223	147.237.0.35	Uruguay	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
173.193.130.54	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 3072	1
84.200.15.174	147.237.77.212	Germany	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
80.178.157.53	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.240	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.24	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
187.241.168.143	147.237.77.176	Mexico	matpash.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
173.193.130.54	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 4096	1

04-25-2016-13:04:08 to 04-25-2016-14:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
153.26.2.60	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
77.126.72.105	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	52
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
176.13.21.159	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
37.238.232.44	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
80.74.103.94	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
213.55.105.82	Ethiopia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
188.209.52.109	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
5.22.129.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
213.162.68.60	Austria	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	18
79.178.187.185	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.208.141	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.22.135.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.41	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.41	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
37.238.232.44	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
23.27.244.239	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.253.142.159	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.177.43.199	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
212.143.122.8	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
213.55.105.82	Ethiopia	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
109.159.60.134	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.55.55.90	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.41	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.140.163	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.235.22.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
70.39.186.218	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	6
157.55.39.148	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.68.2.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.93.184	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.210.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.41	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
188.120.148.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.153	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.43	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.22	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.23.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.238.232.44	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	6
46.19.85.43	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.57.36.22	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.22	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
8.37.227.70	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	5

04-25-2016-13:04:08 to 04-25-2016-14:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.138.191.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
2.53.35.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
188.120.154.88	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 188.120.154.88	Block	10
81.218.162.192	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/article/mobile	Block	5
46.116.24.31	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	5
81.218.162.192	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.162.192	Block	4
213.55.105.82	Ethiopia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.55.105.82	Block	3
46.19.86.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.57.251.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.121.65.228	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/pniot.aspx'	Block	2
109.253.208.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.64.117.166	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	2
176.13.23.14	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
213.55.105.82	Ethiopia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	2
131.253.25.204	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
84.94.191.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
207.46.13.173	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.64.117.166	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 85.64.117.166	Block	1
213.8.204.28	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
46.19.85.252	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Method	Block	1
2.53.34.174	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
89.138.68.219	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl13 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
68.180.229.24	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/shared/usercontrols/headerupper/	Block	1
46.19.85.178	Israel	147.237.76.86	navy.idf.il	Abnormally Long Request method	Block	1
79.177.43.199	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$38 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
188.215.123.176	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
74.82.47.2	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
109.253.208.141	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.178	Israel	147.237.76.86	navy.idf.il	Illegal HTTP Version _pk_id.27.434e=74099cf88afc7c3d.1461579752.1.1461579752.1461579752.; _pk_ses.27.434e=*	Block	1
85.64.117.166	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/5/	Block	1
79.179.62.155	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
176.120.63.141	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1044-he/ishurim.aspx	Block	1
105.104.22.62	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.238.232.44	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
81.218.162.192	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/departmentslobby/mobile	Block	1
199.47.81.11	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1503-	Block	1
74.82.47.3	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
46.19.85.178	Israel	147.237.76.86	navy.idf.il	Malformed URL _pk_ref.27.434e=["","",1461579752,"https://www.google.co.il/"];	Block	1
88.198.230.79	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 88.198.230.79	Block	1
79.182.18.143	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
66.249.64.145	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8802-he/refuah.aspx	Block	1
184.105.139.70	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
109.67.113.220	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$22 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
40.77.167.96	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
74.208.180.106	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/c149292faedbbc35e337409e93583191	Block	1
46.19.85.178	Israel	147.237.76.86	navy.idf.il	Unknown HTTP Request Method vs=571defe4f709493e000; in URL	Block	1
149.88.69.147	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$60 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
2.53.26.132	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1

04-25-2016-13:04:08 to 04-25-2016-14:04:08