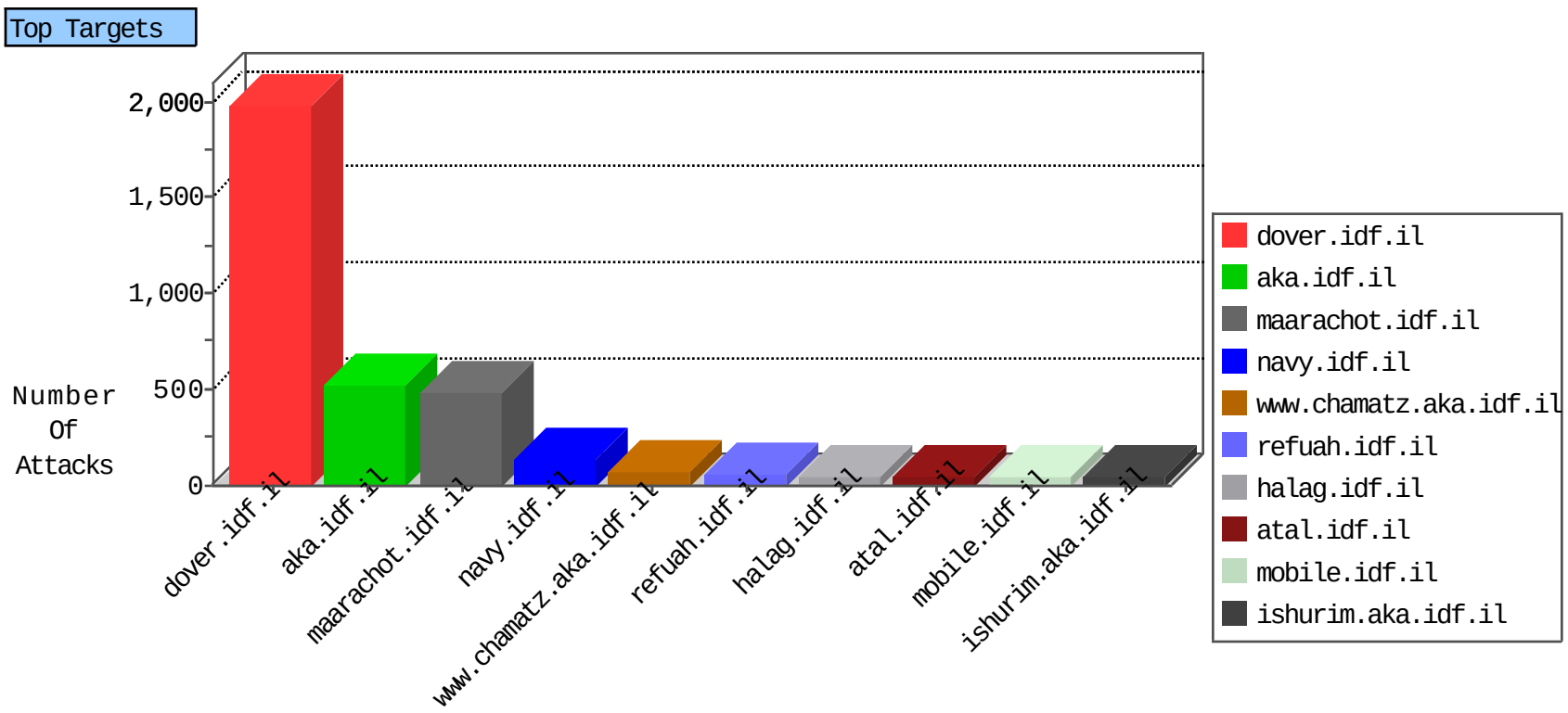
10-29-2015-01:04:07 to 10-29-2015-02:04:07

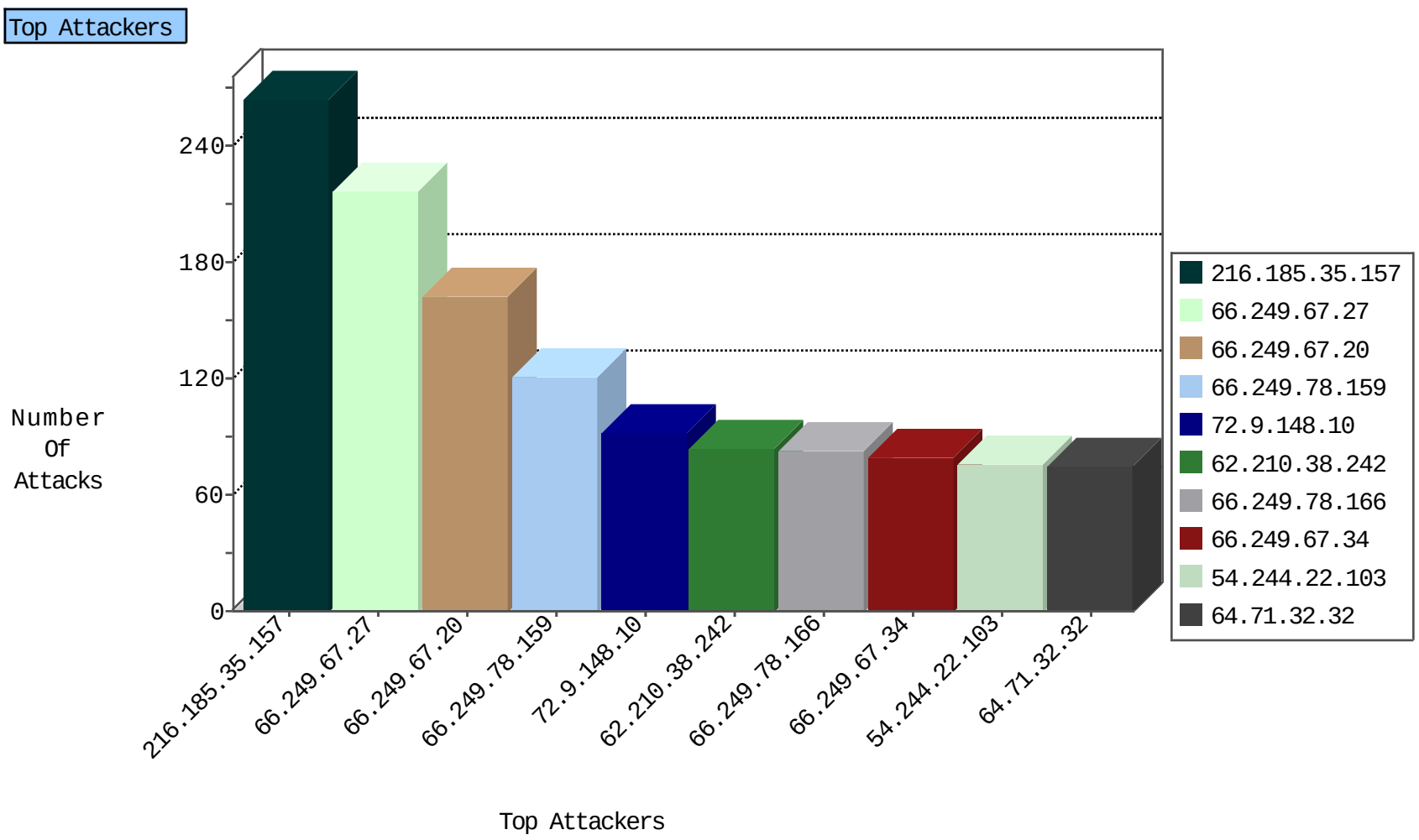
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-29-2015-01:04:07 to 10-29-2015-02:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.20	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	19177
66.249.67.27	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	19146
66.249.69.85	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	13939
66.249.67.34	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	8689
37.26.148.143	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7170
66.249.67.79	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1451
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1270
66.249.67.122	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	572
66.249.67.73	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	374
66.249.67.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	265
66.249.75.114	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	111
66.249.69.77	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	76
37.157.220.77	Armenia	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
37.26.147.248	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	19
2.52.154.126	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15
90.141.219.156	Sweden	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
46.19.86.107	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
79.182.29.98	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
94.208.139.70	Netherlands	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
66.249.78.159	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
111.91.235.228	Vietnam	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	2
80.179.91.149	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
66.249.75.60	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	2
79.177.160.110	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
66.249.67.18	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	2
5.108.144.151	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.19.85.210	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
177.188.180.249	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
89.248.172.98	Netherlands	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
99.13.200.94	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
89.248.172.98	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
69.248.86.176	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.166.188.68	Netherlands	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
176.13.5.69	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
89.248.172.98	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
79.177.160.110	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

10-29-2015-01:04:07 to 10-29-2015-02:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-29-2015-01:04:07 to 10-29-2015-02:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.69.69	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.73	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
111.43.131.162	147.237.8.50	China	e.tikshuv.idf.i	ET SCAN Potential SSH Scan	1
114.218.240.2	147.237.76.31	China	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

10-29-2015-01:04:07 to 10-29-2015-02:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
216.185.35.157	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	264
62.210.38.242	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
99.13.200.94	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
176.13.10.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
92.40.249.104	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
46.19.85.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
153.107.97.167	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
216.189.187.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
5.108.144.151	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
69.248.86.176	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
37.142.136.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	35
37.142.253.217	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	35
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
37.26.147.248	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
46.19.86.195	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
66.102.8.238	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
140.241.253.162	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
109.64.152.57	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
2.52.154.126	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
37.26.148.143	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	26
37.26.146.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
54.244.22.103	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
212.179.220.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.102.8.243	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.249.69.16	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
93.173.1.92	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
66.249.69.8	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
80.178.207.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.181.6.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.13.208	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.69.128	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.180.142.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
62.219.136.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
177.188.180.249	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.86.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.84.165	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9

10-29-2015-01:04:07 to 10-29-2015-02:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
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	90
64.71.32.32	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 64.71.32.32	Block	60
66.249.64.159	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.159	Block	45
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	45
2.54.17.128	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	30
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.6	Block	30
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	30
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	30
66.249.69.81	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1437-he/atal.aspx	Block	15
176.228.175.19	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	15
54.90.156.165	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 54.90.156.165	Block	15
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-16189-en/dover.aspx-title=idf	Block	15
66.249.75.16	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/5/size100x0/3365.jpg	Block	15
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1146-he/chinuch.aspx	Block	15
77.237.138.202	Czech Republic	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /	Block	15
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-9728-he/dover.aspx	Block	15
66.249.69.97	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-8517-he/atal.aspx	Block	15
180.76.15.153	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/headerupper/	Block	15
66.249.64.233	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/894-he	Block	15
54.90.156.165	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	15
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
66.249.75.94	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 66.249.75.94	Block	15
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	15
109.64.31.231	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	15
64.71.32.32	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/test/wp-admin/	Block	15
5.29.78.243	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$cb13801263 in www.aka.idf.il/main/sachar/payslips.aspx	None	15
66.249.69.107	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	15
188.40.11.194	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 188.40.11.194	Block	15
54.145.196.149	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	15
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/historyfs.html	Block	15
66.249.75.94	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/1132-8613-he/navy.aspx.aspx	Block	15
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	15
140.241.253.162	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4616.jpg	Block	15
66.249.64.153	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.153	Block	15
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	15
5.102.254.227	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/kesher	Block	15
66.249.69.123	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/1115-he/nakhal.aspx	Block	15
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1153-he/chinuch.aspx	Block	15
188.165.15.162	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8802-he/refuah.aspx	Block	15
66.249.75.114	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	15
66.249.67.251	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
141.212.122.128	United States	147.237.77.19	law-forum.idf.il	Malformed URL proxytest.zmap.io:80	Block	15
66.249.64.153	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/1086-en/hamaz.aspx	Block	15
54.82.33.159	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	15
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/images/shared/home.png	Block	15
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.13	Block	15
64.71.32.23	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	15
77.237.138.51	Czech Republic	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /	Block	15
66.249.75.120	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.75.120	Block	15

10-29-2015-01:04:07 to 10-29-2015-02:04:07