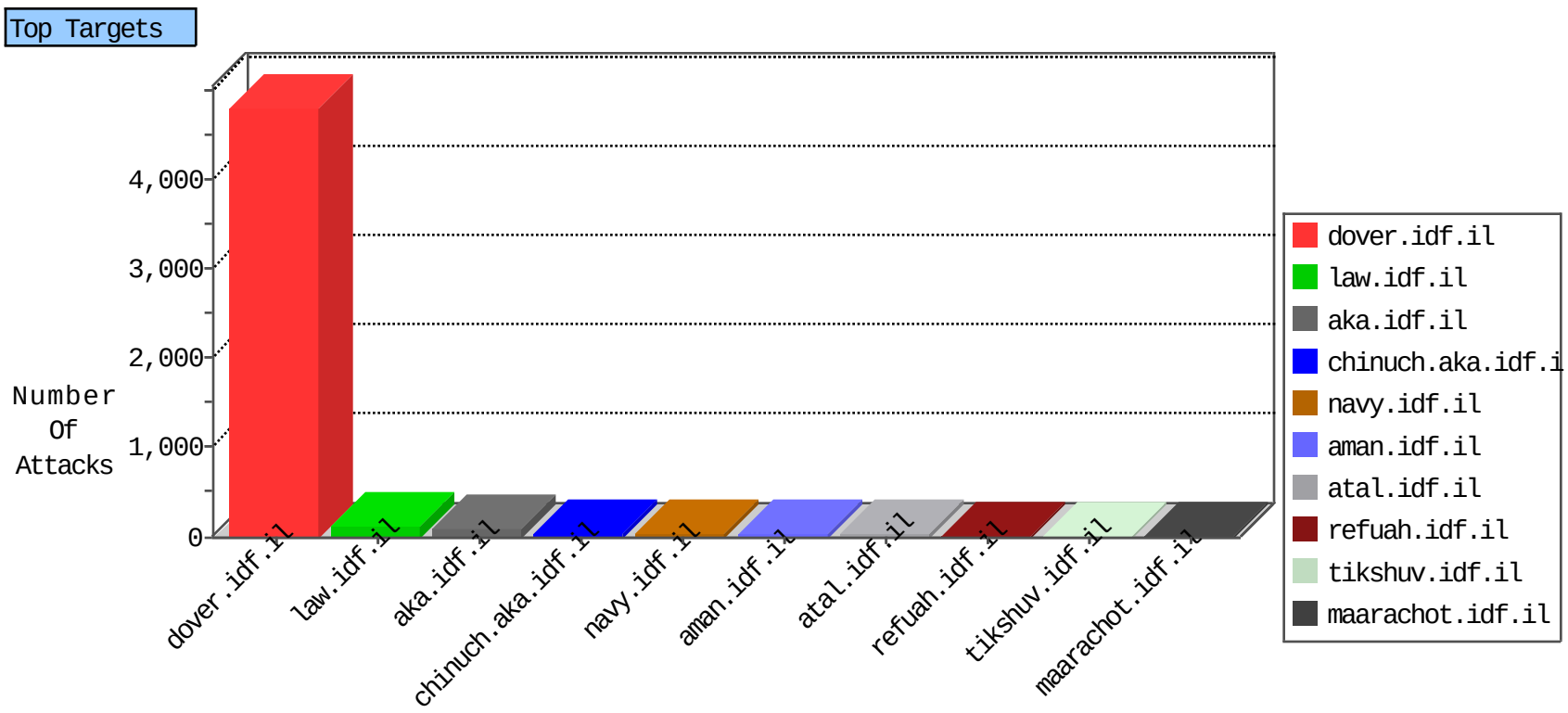
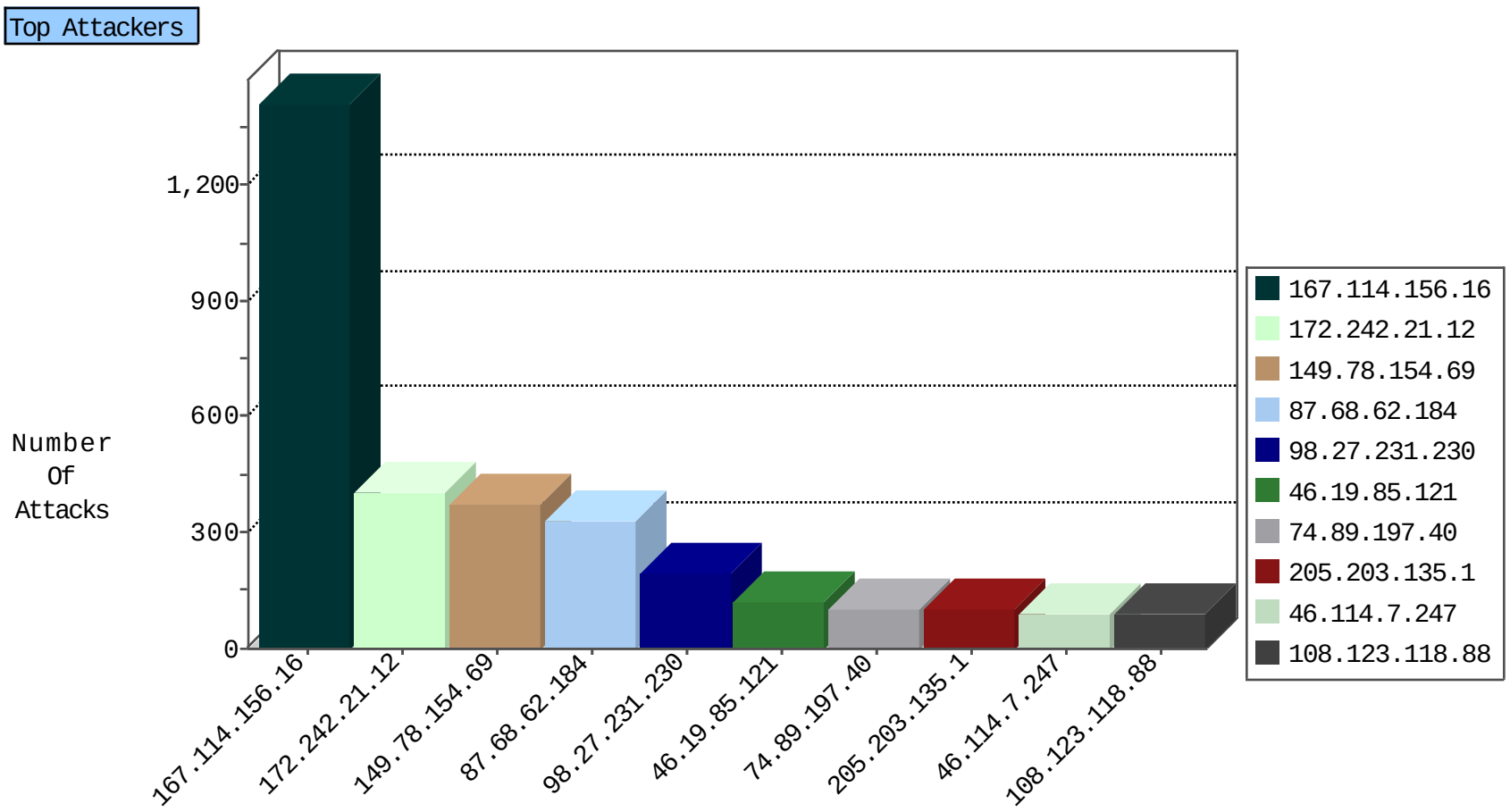
11-02-2015-03:04:07 to 11-02-2015-04:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-02-2015-03:04:07 to 11-02-2015-04:04:07

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	3089
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2304
66.249.67.20	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	559
66.249.67.34	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	348
66.249.75.76	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	183
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	115
98.27.231.230	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	14
73.26.166.207	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	4
200.158.178.16	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
185.115.124.16		147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
222.186.56.42	China	147.237.0.33	idf.il	Frk_Under_Attack_Con_Tcp	drop	1
108.123.118.88	United States	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1
177.157.174.214	Brazil	147.237.0.34	tikshuv.idf.il	ID-OpenSSL-Heartbeat-ex1	dest-reset	1
141.212.122.166	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

11-02-2015-03:04:07 to 11-02-2015-04:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-02-2015-03:04:07 to 11-02-2015-04:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.67.34	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	12
41.33.231.90	147.237.77.216	Egypt	dover.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
66.249.75.76	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
115.182.17.13	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -sS window 2048	1
5.8.66.101	147.237.76.44	Russian Federation	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
115.182.17.13	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -f -sS	1
5.8.66.101	147.237.76.38	Russian Federation	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
5.8.66.101	147.237.76.30	Russian Federation	himush.idf.il	ET SCAN Potential SSH Scan	1
31.184.242.17	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
180.210.201.106	147.237.76.147	Singapore	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
5.8.66.101	147.237.77.243	Russian Federation	mobile.idf.il	ET SCAN Potential SSH Scan	1
180.210.201.106	147.237.0.35	Singapore	akaws.idf.il	ET SCAN Potential SSH Scan	1
5.8.66.101	147.237.77.205	Russian Federation	prisha.idf.il	ET SCAN Potential SSH Scan	1
173.13.131.125	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
5.8.66.101	147.237.76.202	Russian Federation	e.halag.idf.il	ET SCAN Potential SSH Scan	1
124.167.165.149	147.237.8.27	China	e.madim.atal.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.8.66.101	147.237.76.197	Russian Federation	e.himush.idf.il	ET SCAN Potential SSH Scan	1
115.182.17.13	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
5.8.66.101	147.237.76.86	Russian Federation	navy.idf.il	ET SCAN Potential SSH Scan	1
115.182.17.13	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
5.8.66.101	147.237.76.42	Russian Federation	refuah.idf.il	ET SCAN Potential SSH Scan	1
5.8.66.101	147.237.76.31	Russian Federation	nakchal.idf.il	ET SCAN Potential SSH Scan	1
5.8.66.101	147.237.8.50	Russian Federation	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
180.210.201.106	147.237.76.200	Singapore	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
14.141.156.27	147.237.8.28	India	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 4096	1
180.210.201.106	147.237.0.200	Singapore	m4u.idf.il	ET SCAN Potential SSH Scan	1
5.8.66.101	147.237.77.216	Russian Federation	dover.idf.il	ET SCAN Potential SSH Scan	1
180.210.201.106	147.237.0.19	Singapore	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
5.8.66.101	147.237.77.179	Russian Federation	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
128.65.123.74	147.237.0.15	Italy	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
5.8.66.101	147.237.76.200	Russian Federation	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
115.182.17.13	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -sS window 4096	1
5.8.66.101	147.237.76.196	Russian Federation	e.sviva.idf.il	ET SCAN Potential SSH Scan	1

11-02-2015-03:04:07 to 11-02-2015-04:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
172.242.21.12	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	406
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	372
87.68.62.184	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	330
98.27.231.230	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	182
205.203.135.1	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	102
74.89.197.40	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	102
46.114.7.247	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	88
108.123.118.88	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	86
86.97.89.24	United Arab Emirates	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	63
189.120.135.195	Brazil	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	63
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	58
212.199.182.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	57
17.142.152.111	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	52
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	50
67.7.198.58	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	49
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	48
77.126.98.214	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	48
94.242.206.244	Luxembourg	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	43
95.219.113.53	Romania	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
82.80.25.221	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
17.142.152.85	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
197.162.24.131	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
50.141.111.79	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
17.142.152.72	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
17.142.152.68	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
93.172.51.255	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
66.249.78.166	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
73.209.254.56	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
67.247.3.70	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
17.142.145.3	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
151.80.31.112	Italy	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
64.233.173.46	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
64.233.173.41	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
198.58.102.158	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
17.142.152.89	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
75.32.236.68	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
108.59.253.71	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
41.239.12.61	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
107.6.122.130	Singapore	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
192.117.12.65	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
66.249.78.166	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
207.46.13.137	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
107.77.72.116	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
76.69.122.52	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10

11-02-2015-03:04:07 to 11-02-2015-04:04:07

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	30
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
46.19.85.121	Israel	147.237.77.74	law.idf.il	Illegal HTTP Version	Block	15
157.55.39.14	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	15
66.249.78.66	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	15
46.19.85.121	Israel	147.237.77.74	law.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.121	Block	15
82.118.237.100	Bulgaria	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/	Block	15
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	15
46.19.85.121	Israel	147.237.77.74	law.idf.il	Malformed URL _pk_ses.115.5e0a=*	Block	15
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/sendtofriend/kkkkkkk=f1d1ae64kkkkkkk_f1d1ae64	Block	15
66.249.78.247	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	15
46.19.85.121	Israel	147.237.77.74	law.idf.il	Unknown HTTP Request Method k_id.115.5e0a=feb2f92dc78ce9b0.1446429307.1.1446429307.1446429307.; in URL _pk_ses.115.5e0a=*	Block	15
94.242.206.244	Luxembourg	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	15
66.249.69.89	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1398-he/atal.aspx	Block	15
46.19.85.121	Israel	147.237.77.74	law.idf.il	Multiple Abnormally Long Request from 46.19.85.121	Block	15
181.47.141.182	Argentina	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 181.47.141.182	Block	15
68.180.228.59	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/589-he/patzar.aspx=	Block	15
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/main/rabanut/general.aspx	Block	15
155.41.66.16	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	15
66.249.78.4	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	15
181.47.141.182	Argentina	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/spanish	Block	15
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
46.19.85.121	Israel	147.237.77.74	law.idf.il	Abnormally Long Request method	Block	15
155.41.66.16	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	15
66.249.78.52	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	15
46.19.85.121	Israel	147.237.77.74	law.idf.il	Multiple Malformed URL from 46.19.85.121	Block	15
207.46.13.76	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/links.aspx	Block	15
82.118.237.100	Bulgaria	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	15
46.19.85.121	Israel	147.237.77.74	law.idf.il	Multiple Illegal HTTP Version from 46.19.85.121	Block	14

11-02-2015-03:04:07 to 11-02-2015-04:04:07