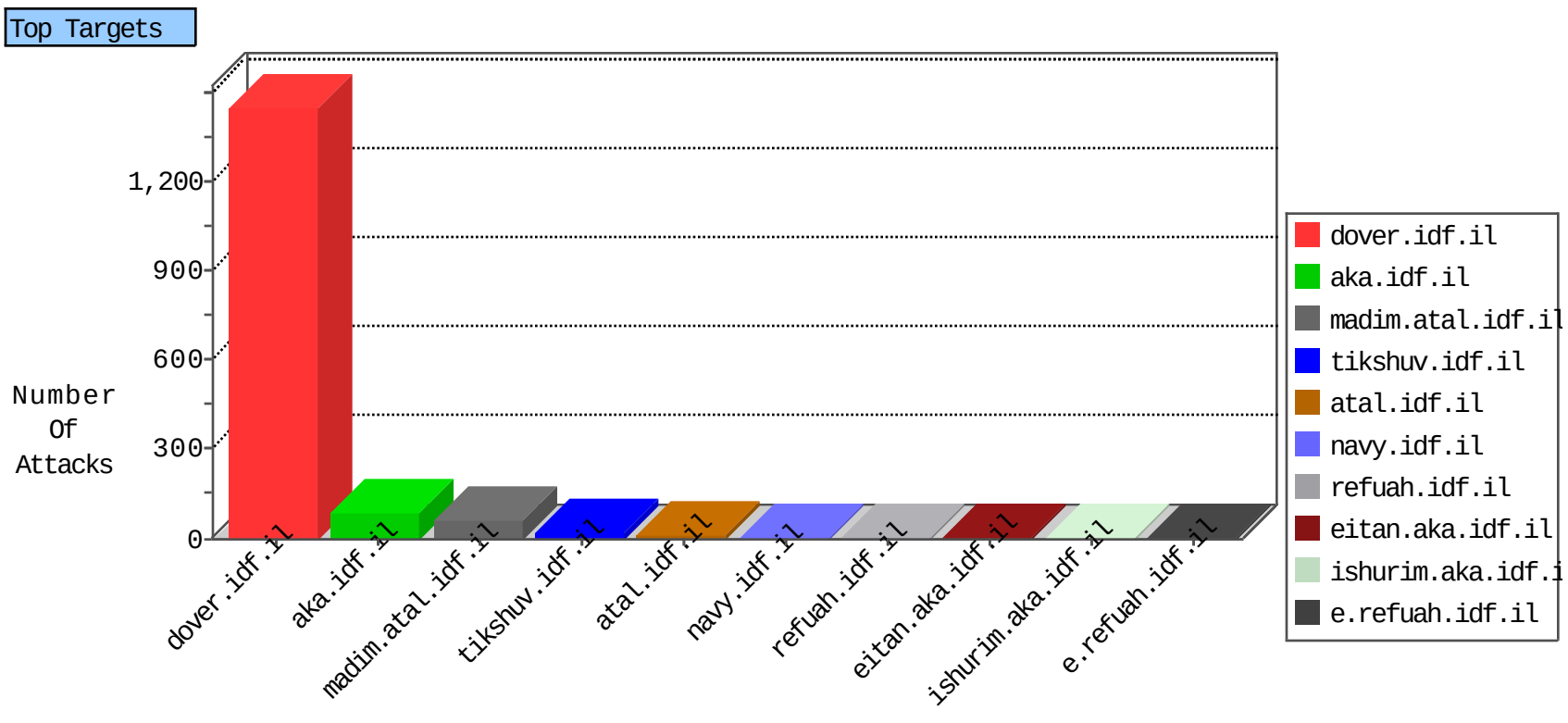
04-15-2016-01:07:38 to 04-15-2016-02:07:38

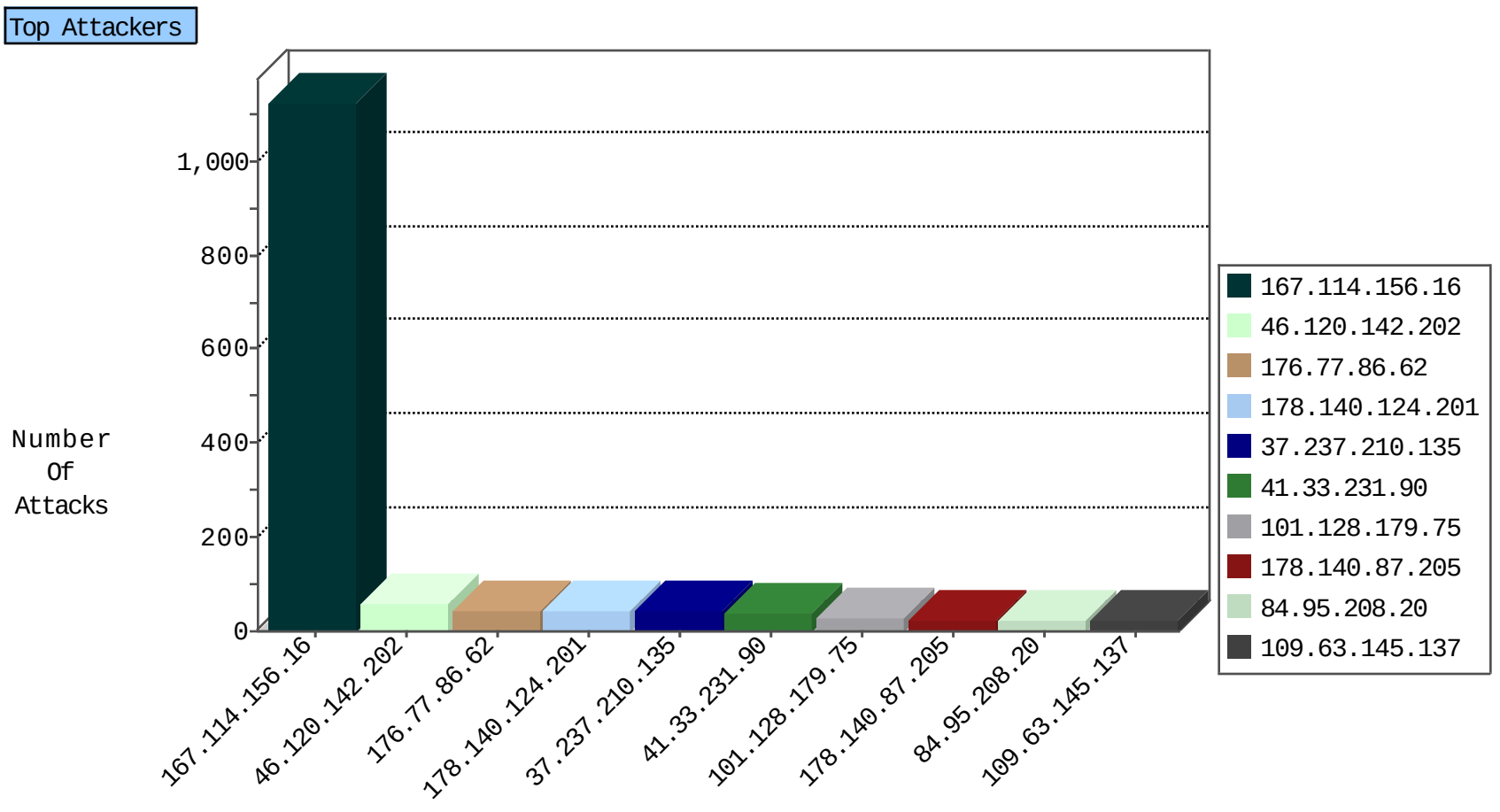
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

04-15-2016-01:07:38 to 04-15-2016-02:07:38

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	Block_Ip_Web_In	drop	1127
203.189.74.44	Sri Lanka	147.237.77.176	matpash.idf.il	L4 Source or Dest Port Zero	drop	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
89.248.160.138	Netherlands	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1

04-15-2016-01:07:38 to 04-15-2016-02:07:38

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.102.153.58	United Kingdom	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
91.121.211.59	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
40.77.167.85	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
65.55.210.108	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.162	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-15-2016-01:07:38 to 04-15-2016-02:07:38

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
94.102.153.58	147.237.72.166	United Kingdom	aka.idf.il	SQL Injection - Select From	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
180.97.81.71	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
66.37.80.113	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
198.20.69.98	147.237.77.170	United States	maarachot.idf.il	ET DROP Dshield Block Listed Source	1
188.14.242.67	147.237.77.234	Italy	halag.idf.il	ET SCAN NMAP -sS window 3072	1
106.186.113.132	147.237.76.42	Japan	refuah.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
88.204.187.90	147.237.72.167	Kazakstan	ishurim.aka.idf.il	ET SCAN NMAP -sS window 3072	1

04-15-2016-01:07:38 to 04-15-2016-02:07:38

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.77.86.62	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
178.140.124.201	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
101.128.179.75	Japan	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	27
109.63.145.137	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
178.140.87.205	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
37.237.210.135	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	20
37.237.210.135	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
93.81.122.89	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
109.253.198.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
123.126.113.101	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
141.0.13.245	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
190.210.137.105	Argentina	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
87.69.230.170	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
217.70.44.165	Sweden	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
199.30.24.229	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
94.73.150.148	Turkey	147.237.77.233	atal.idf.il	drop	SAM rule	drop	4
41.185.31.40	South Africa	147.237.77.233	atal.idf.il	drop	SAM rule	drop	4
2.55.132.80	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.212.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
38.111.147.86	United States	147.237.77.216	dover.idf.il	drop		drop	2
84.110.37.248	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
128.232.110.29	United Kingdom	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
84.110.37.248	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
128.232.110.29	United Kingdom	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
93.33.107.182	Italy	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
84.95.208.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
128.232.110.29	United Kingdom	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
106.186.113.132	Japan	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
159.226.95.66	China	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.130	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.115	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
190.234.106.105	Peru	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
93.33.107.182	Italy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.215	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.122	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.175	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	illegal header format detected: Illegal start line in request	monitor	1
106.186.113.132	Japan	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
89.248.167.131	Netherlands	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.120.142.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
197.165.138.165	Egypt	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.165.138.165	Block	3
37.238.188.41	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
149.78.192.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
130.185.155.10	Sweden	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
87.69.206.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
197.165.138.165	Egypt	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	1
84.94.176.72	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method æ,MXþú	Block	1
130.185.155.10	Sweden	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-8520-he/dover.aspx	Block	1
87.69.206.51	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	1
84.94.176.72	Israel	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
157.55.39.217	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
106.186.113.132	Japan	147.237.76.42	refuah.idf.il	Multiple Untraceable SSL Sessions from 106.186.113.132 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
46.19.85.175	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
87.69.206.51	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 87.69.206.51	Block	1
84.94.176.72	Israel	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 5	Block	1
131.253.25.142	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.230.184	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1486-he/atal.aspx	Block	1
23.235.227.106	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ID in www.idf.il/1294-ar/dover.aspx	Block	1
87.69.206.51	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
84.94.176.72	Israel	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	1
173.252.79.116	United States	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1294-ar/dover.aspx parameter ID	Block	1
106.186.113.132	Japan	147.237.76.42	refuah.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.19.85.175	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method xocpms in URL	Block	1
87.69.206.51	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
197.165.138.165	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/uhljlj	Block	1
84.94.176.72	Israel	147.237.72.166	aka.idf.il	Malformed URL	Block	1
69.121.60.58	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
37.237.210.135	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
87.69.206.51	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 87.69.206.51	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/div.item	Block	1
84.94.176.72	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name	Block	1
173.252.90.106	United States	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1294-ar/dover.aspx parameter ID	Block	1
130.185.155.10	Sweden	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 130.185.155.10	Block	1
87.69.206.51	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
199.30.24.240	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.94.176.72	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method æ,MXþú	Block	1
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	1
157.55.39.98	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/portalmiluim/templates/www.behazdaa.org	Block	1
87.69.206.51	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
87.69.206.51	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
174.129.228.67	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
84.94.176.72	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
66.249.64.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
87.69.206.51	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
212.179.21.194	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/sip_storage/files/3/1773.jpg	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1

04-15-2016-01:07:38 to 04-15-2016-02:07:38