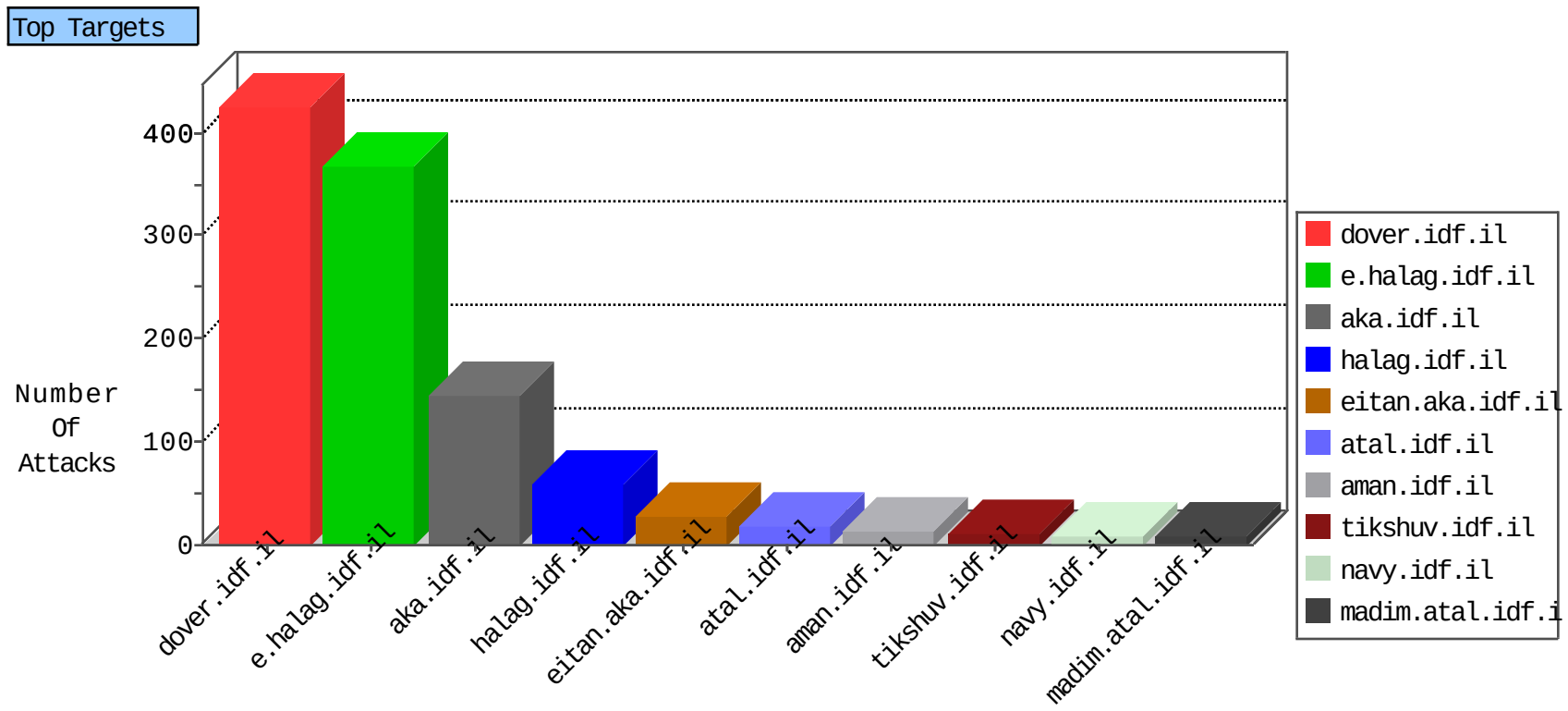
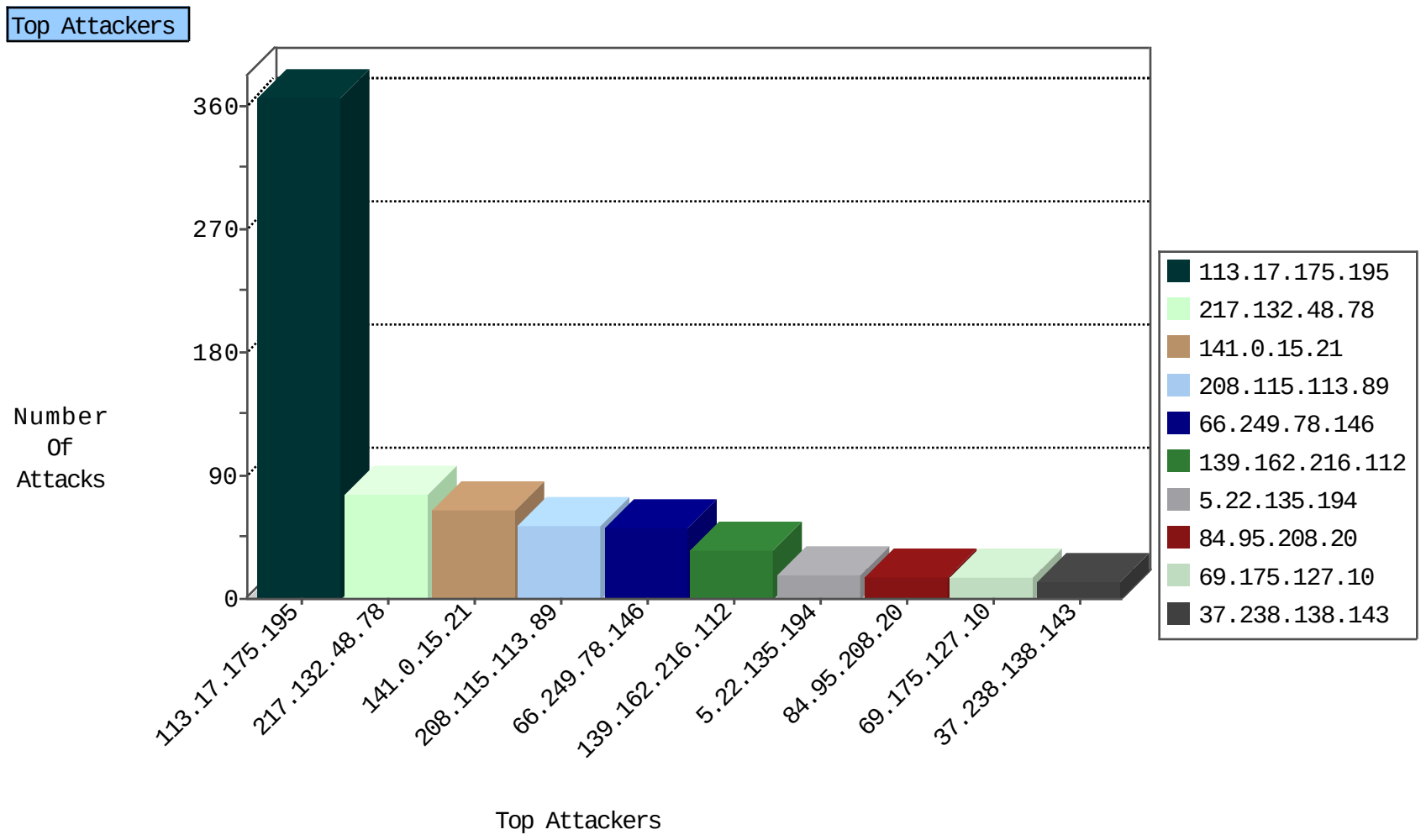
04-25-2016-01:04:19 to 04-25-2016-02:04:19

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-25-2016-01:04:19 to 04-25-2016-02:04:19

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	TCP handshake violation, first packet not syn	drop	2741
113.17.175.195	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	367
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	3
173.208.197.252	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
74.91.23.109	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
74.91.23.110	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
69.197.185.21	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
5.196.72.168	France	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
74.91.23.106	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	drop	1
69.30.198.146	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	drop	1
141.212.122.214	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
69.197.185.20	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	1
107.150.46.34	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
74.91.23.110	United States	147.237.77.205	prisha.idf.il	block-sp-traf1	drop	1

04-25-2016-01:04:19 to 04-25-2016-02:04:19

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-25-2016-01:04:19 to 04-25-2016-02:04:19

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.i	Tehila - Perl LWP with fake user agent	4
62.98.90.59	147.237.77.216	Italy	dover.idf.i	Xenu Link Sleuth User Agent	2
66.249.78.158	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1

04-25-2016-01:04:19 to 04-25-2016-02:04:19

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.0.15.21	Norway	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
217.132.48.78	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	58
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
5.22.135.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
217.132.48.78	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
69.175.127.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
37.238.138.143	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
77.124.31.167	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.99.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
177.146.132.18	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
185.6.18.208	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
157.55.39.26	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
108.91.41.234	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
40.77.167.59	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
77.126.82.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
68.180.231.43	United States	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
66.249.78.199	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.200.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
141.0.15.21	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
217.132.143.71	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	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
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
104.131.147.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.63.143.28	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
207.46.13.173	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
199.30.16.188	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.206	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	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
204.237.2.151	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.181.206.109	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.46.13.41	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.93.249	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.27.105.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.42.255	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.229.179	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
108.228.12.143	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	9
46.19.85.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.183.112.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
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
72.88.207.79	United States	147.237.76.42	refuah.idf.il	Abnormally Long Request method	Block	1
37.238.138.143	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
136.243.11.18	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
78.0.235.197	Croatia	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8944-he/refuah.aspx	Block	1
207.46.13.173	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy.	Block	1
62.98.90.59	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
93.103.13.172	Slovenia	147.237.77.74	law.idf.il	PHP Attempt	Block	1
72.88.207.79	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Method	Block	1
66.249.66.44	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/edim/yoman/enlarge.asp	Block	1
151.236.172.63	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
38.111.147.84	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
79.180.140.39	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 79.180.140.39 (Open Mode)	None	1
68.180.230.108	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1073-he/nakhal.aspx	Block	1
213.8.204.64	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/site/templates/controller.asp	Block	1
66.220.145.245	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr	Block	1
93.103.13.172	Slovenia	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/wp-login.php	Block	1
72.88.207.79	United States	147.237.76.42	refuah.idf.il	NULL Character in Method	Block	1
66.249.78.158	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
173.208.197.252	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.xy966.com/	Block	1
41.143.42.108	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/'	Block	1
79.180.140.39	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
69.197.185.20	United States	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on www.fc376.com/	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
217.132.48.78	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
107.150.46.34	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to www.fc376.com/	Block	1
74.91.23.109	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.178tx.com/	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/listpage/	Block	1
185.92.72.32	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
70.72.202.44	Canada	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/edim/yoman/yoman.asp	Block	1
37.8.23.18	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
131.253.25.170	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
74.91.23.110	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.178tx.com/	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
198.58.103.158	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
62.98.90.59	Italy	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 62.98.90.59	Block	1

04-25-2016-01:04:19 to 04-25-2016-02:04:19