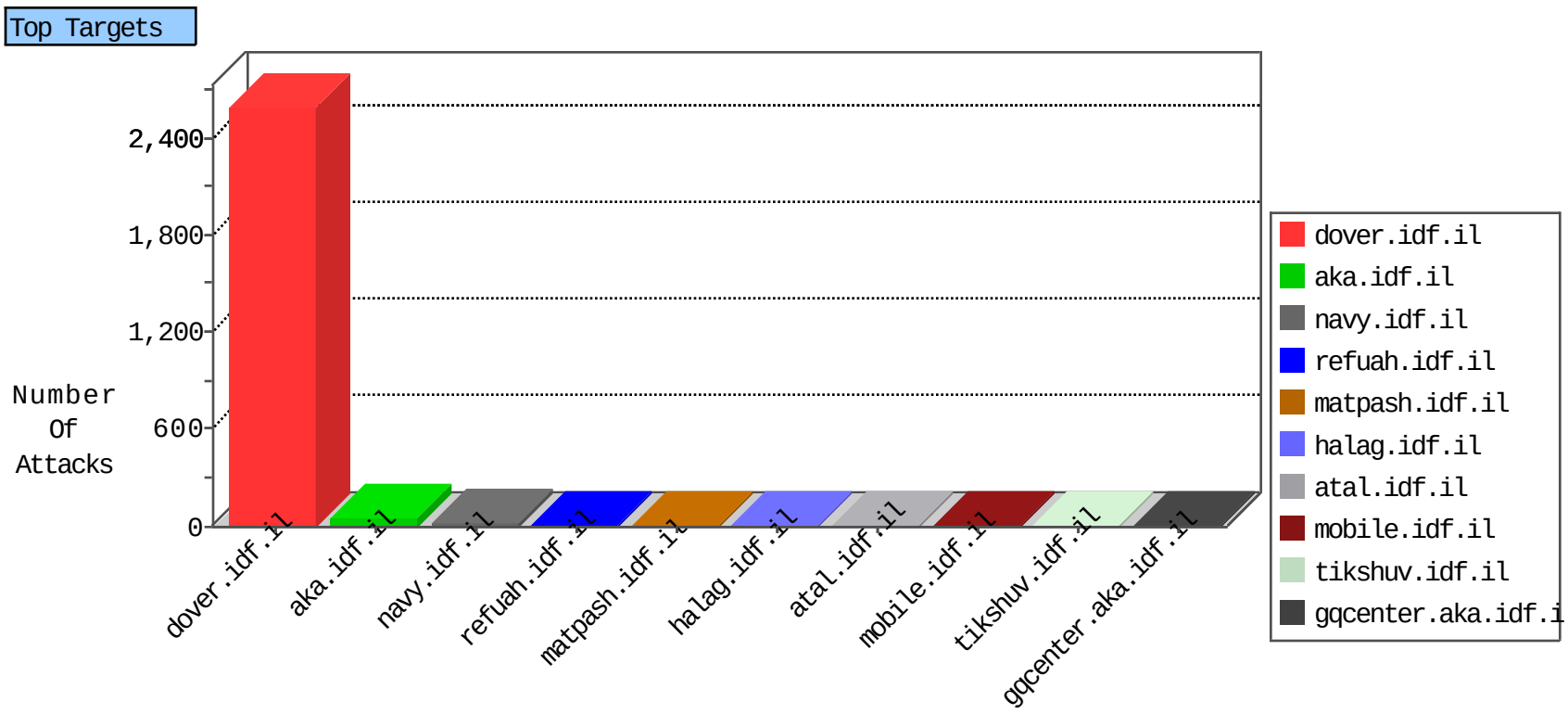
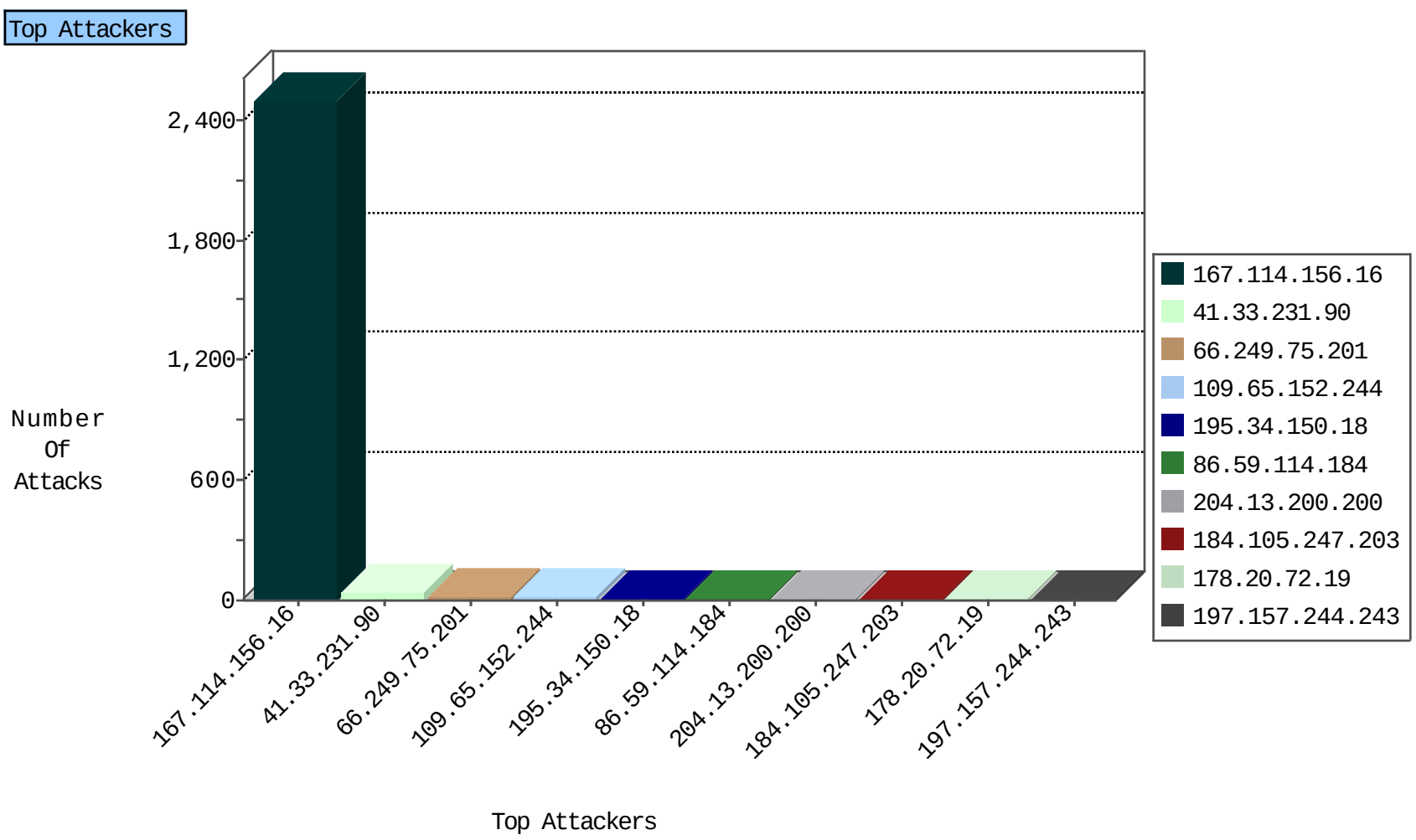
12-22-2015-06:04:07 to 12-22-2015-07:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-22-2015-06:04:07 to 12-22-2015-07:04:07

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	DOS-Tool-SwitchbladG	dest-reset	3483
204.42.253.130	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	2
112.6.209.207	China	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
112.6.209.207	China	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
198.20.69.98	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1

12-22-2015-06:04:07 to 12-22-2015-07:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
27.5.160.123	India	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	2

12-22-2015-06:04:07 to 12-22-2015-07:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
86.59.114.184	147.237.77.176	Austria	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
197.157.244.243	147.237.76.31	Somalia	nakchal.idf.il	ET SCAN Potential SSH Scan	1
196.12.190.13	147.237.8.45	Puerto Rico	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
178.20.72.19	147.237.0.17	Italy	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
166.63.122.229	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
78.193.2.8	147.237.72.217	France	e.idf.il	ET SCAN NMAP -sS window 1024	1
202.95.141.114	147.237.76.42	Indonesia	refuah.idf.il	ET SCAN NMAP -sS window 2048	1
202.95.141.114	147.237.76.42	Indonesia	refuah.idf.il	ET SCAN NMAP -f -sS	1
197.157.244.243	147.237.77.233	Somalia	atal.idf.il	ET SCAN Potential SSH Scan	1
197.157.244.243	147.237.0.34	Somalia	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
196.12.190.13	147.237.8.45	Puerto Rico	e.eitan.idf.il	ET SCAN NMAP -sS window 3072	1
180.97.106.162	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
166.63.122.229	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 4096	1
5.39.222.253	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
202.95.141.114	147.237.76.42	Indonesia	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
197.157.244.243	147.237.77.243	Somalia	mobile.idf.il	ET SCAN Potential SSH Scan	1

12-22-2015-06:04:07 to 12-22-2015-07:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
66.249.75.201	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
109.65.152.244	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.65.152.244	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
101.177.16.132	Australia	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.86.33	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.176.204.58	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.176.212.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.126.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
91.200.12.143	Ukraine	147.237.77.233	atal.idf.il	drop	SAM rule	drop	2
66.249.66.39	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
91.200.12.143	Ukraine	147.237.76.30	himush.idf.il	drop	SAM rule	drop	2
66.249.75.209	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
201.51.45.85	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.246	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
149.78.145.250	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.6	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.80	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.95	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
2.52.157.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
85.64.166.191	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.115	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.121.96.199	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.3.146.249	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
42.62.74.77	China	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	1
178.20.72.19	Italy	147.237.0.33	idf.il	drop		drop	1
216.218.206.88	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.99	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.203	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.22.134.81	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
137.116.71.170	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
85.64.185.72	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
218.22.211.69	China	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
178.20.72.19	Italy	147.237.0.35	akaws.idf.il	drop		drop	1
104.37.3.69	United States	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
216.218.206.88	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.203	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
46.19.86.120	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
5.102.254.121	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
137.116.71.170	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
85.64.185.72	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
196.219.224.69	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
178.20.72.19	Italy	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
107.150.61.10	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
216.218.206.107	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.229	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

12-22-2015-06:04:07 to 12-22-2015-07:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
86.59.114.184	Austria	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
176.13.8.167	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.151.145	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.65.152.244	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
86.59.114.184	Austria	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 86.59.114.184	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
207.46.13.151	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/iturim/asp/displayallsoliders.asp	Block	1
157.55.39.13	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/faq.aspx	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
77.247.181.165	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.255.215.87	Block	1
46.19.86.99	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
109.67.18.141	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
86.59.114.184	Austria	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	1
157.55.39.51	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.51	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
80.74.100.131	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.114.91.233	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.204	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
141.212.122.129	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to /x	Block	1
87.68.64.116	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
157.55.39.51	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bundles/bootstrap	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
84.110.37.147	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
141.212.122.129	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to /x	Block	1
104.37.3.69	United States	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8906-he/refuah.aspx	Block	1
176.12.151.175	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
155.94.222.12	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
104.37.3.69	United States	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
69.58.178.56	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1

12-22-2015-06:04:07 to 12-22-2015-07:04:07