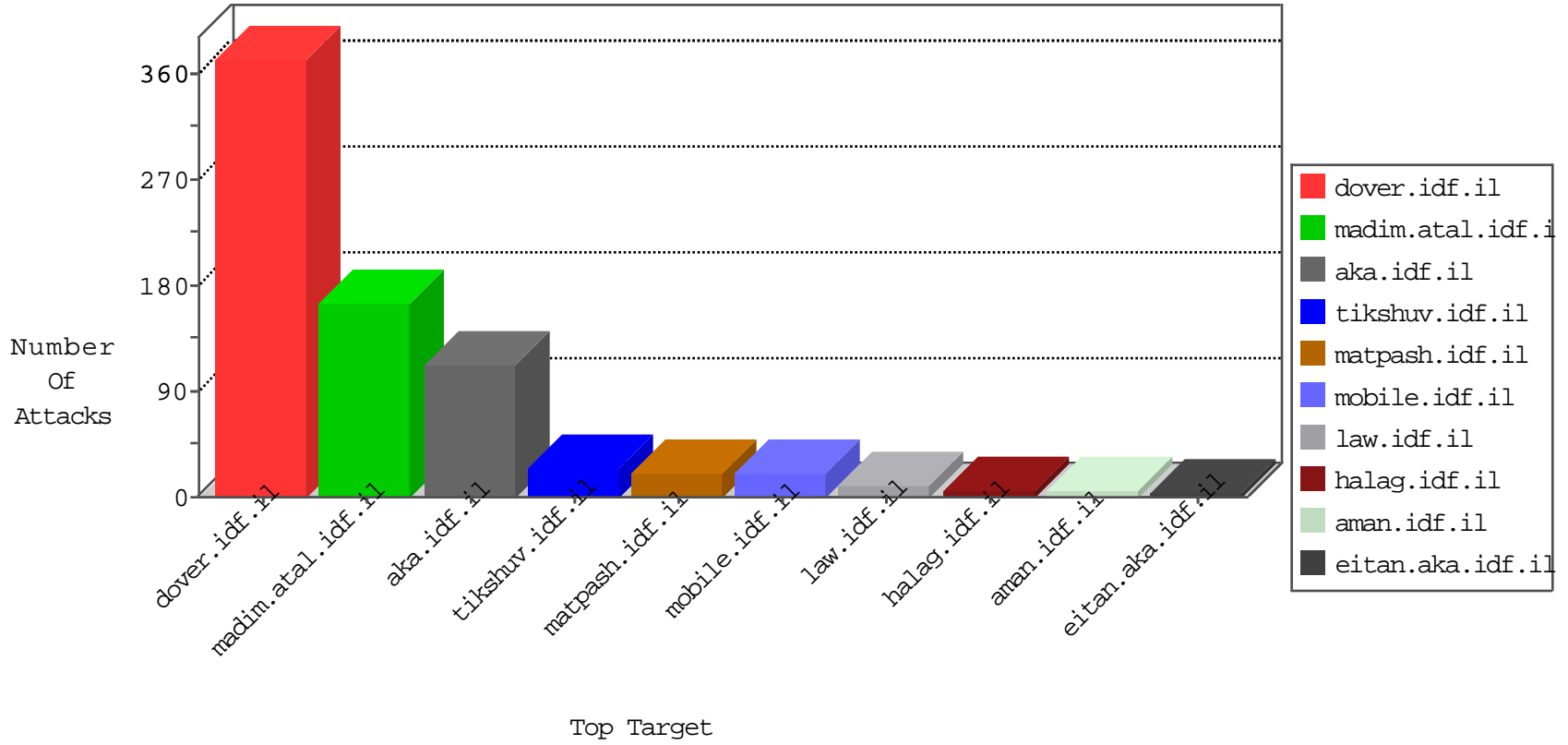


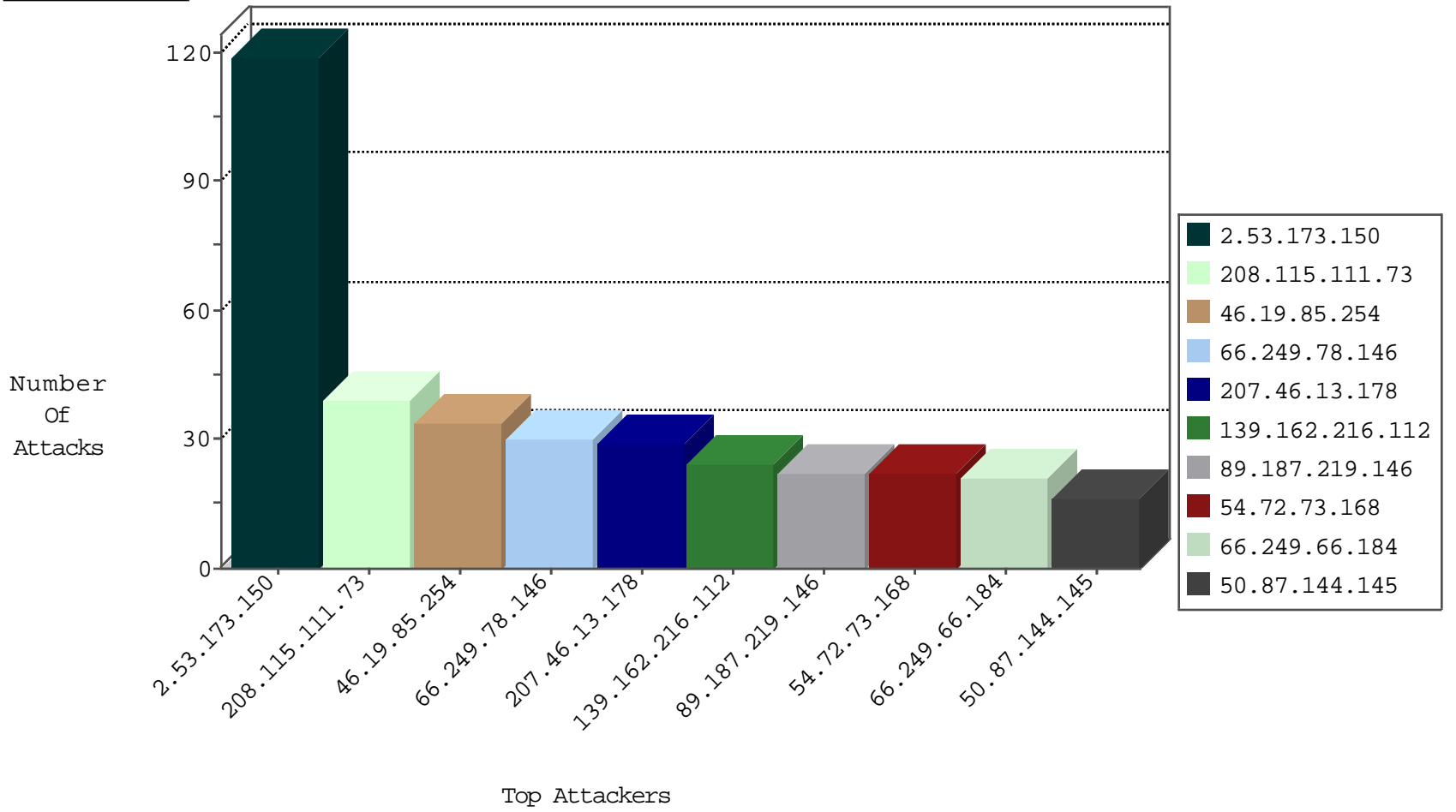
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	1
71.6.167.142	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1

05-01-2016-06:04:08 to 05-01-2016-07:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

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
208.100.26.228	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
203.86.29.220	147.237.77.212	China	e.dover.idf.il	ET SCAN NMAP -f -sS	1
130.211.77.81	147.237.76.30	United States	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
113.240.250.154	147.237.76.148	China	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
104.197.72.206	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
79.177.128.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
203.86.29.220	147.237.77.212	China	e.dover.idf.il	ET SCAN NMAP -sS window 2048	1
113.240.250.154	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
106.186.113.132	147.237.77.176	Japan	matpash.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
80.82.78.38	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
66.249.66.184	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
89.187.219.146	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
68.180.231.43	United States	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
198.58.103.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.92	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
190.75.122.26	Venezuela	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
2.53.149.36	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
37.46.39.103	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.177.89.141	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
130.203.136.75	United States	147.237.77.74	law.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	7
108.253.77.26	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.22.130.125	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.246.139.152	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
207.241.226.94	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.53.149.36	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
97.32.192.201	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
66.249.64.41	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
97.32.192.201	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
106.186.113.132	Japan	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
217.132.239.180	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.64.244	United States	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.245	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
108.46.100.66	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
95.215.62.89	Spain	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.255.215.87	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.34.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.64.98	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.130.189.99	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.249.64.181	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
185.32.179.163	Israel	147.237.77.243	mobile.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
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
188.51.103.77	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.173.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	119
46.19.85.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
66.102.7.226	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
185.32.179.85	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
66.102.7.240	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
27.22.21.158	China	147.237.72.166	aka.idf.il	PHP Attempt	Block	3
80.246.136.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.22.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.102.7.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
27.22.21.158	China	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 27.22.21.158	Block	2
85.130.189.99	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	2
176.13.18.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
213.57.48.76	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1250-he/atal.aspx	Block	1
157.55.39.229	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/links/links.aspx	Block	1
82.102.136.65	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
51.255.65.19	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1514-en/dover.aspx.	Block	1
138.134.192.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
75.97.217.22	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
157.55.39.251	United States	147.237.72.166	aka.idf.il	Unknown Parameter 136cd360 in www.aka.idf.il/main/home/default.aspx	None	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
51.255.65.37	France	147.237.72.166	aka.idf.il	Unknown Parameter amp;pageNum in www.aka.idf.il/iturin/asp/displayallsoldiers.asp	None	1
194.28.112.51	Netherlands	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/hnap1/	Block	1
151.80.31.178	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/signals/atar/	Block	1
77.237.138.202	Czech Republic	147.237.77.176	matpash.idf.il	Unauthorized URL Access to /	Block	1
66.249.64.41	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/homepage/asp	Block	1
170.130.62.5	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/patzar	Block	1
27.22.21.158	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
106.186.113.132	Japan	147.237.77.176	matpash.idf.il	Multiple Untraceable SSL Sessions from 106.186.113.132 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9694-he/refuah.aspx	Block	1
51.255.65.64	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list3.htm	Block	1
207.46.13.178	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
151.80.31.183	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
66.249.64.80	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
46.19.85.226	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
106.186.113.132	Japan	147.237.77.176	matpash.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
157.55.39.106	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-19142-en/dover...the	Block	1
27.22.21.158	China	147.237.72.166	aka.idf.il	Admin Blocking	Block	1
80.246.139.152	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
131.253.25.211	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1