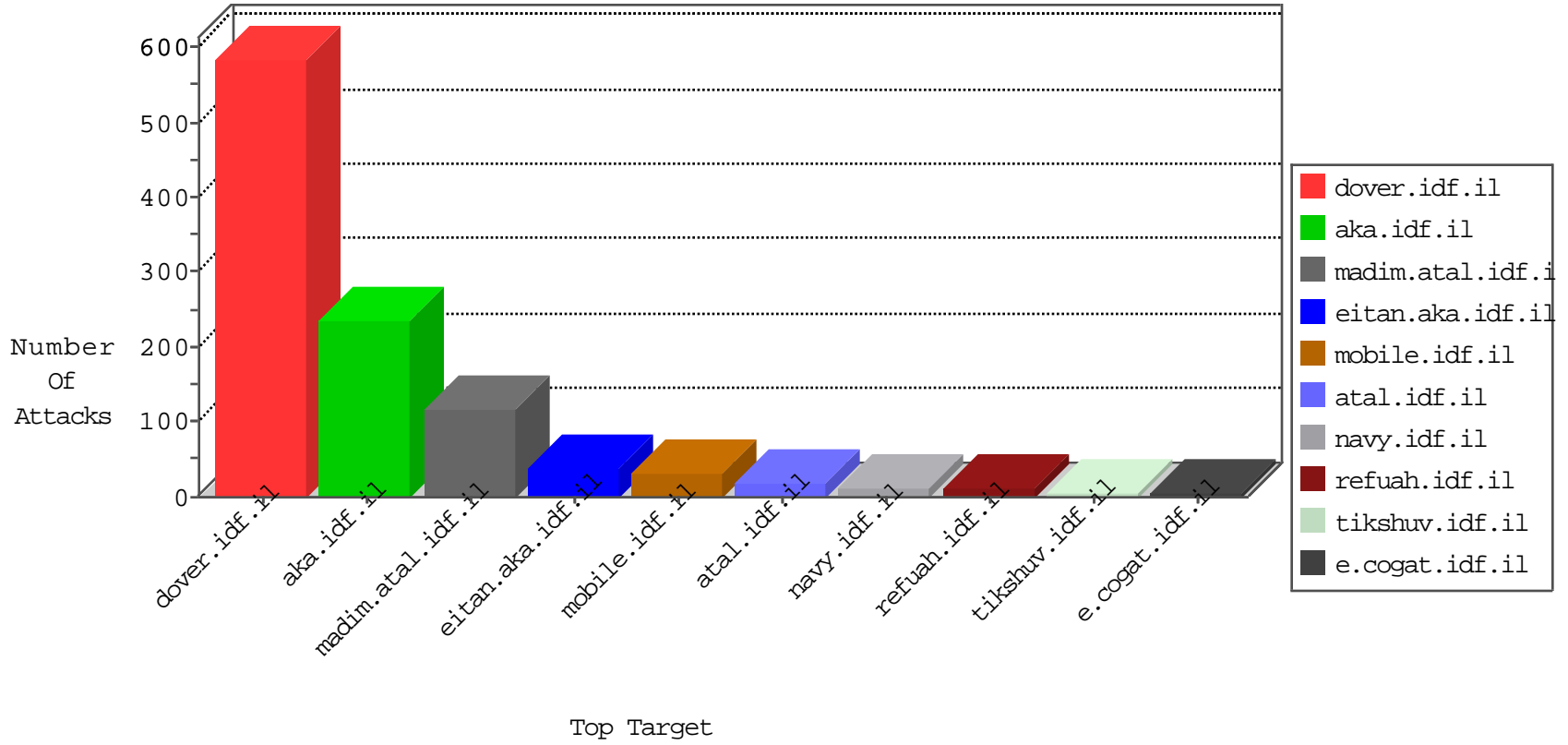


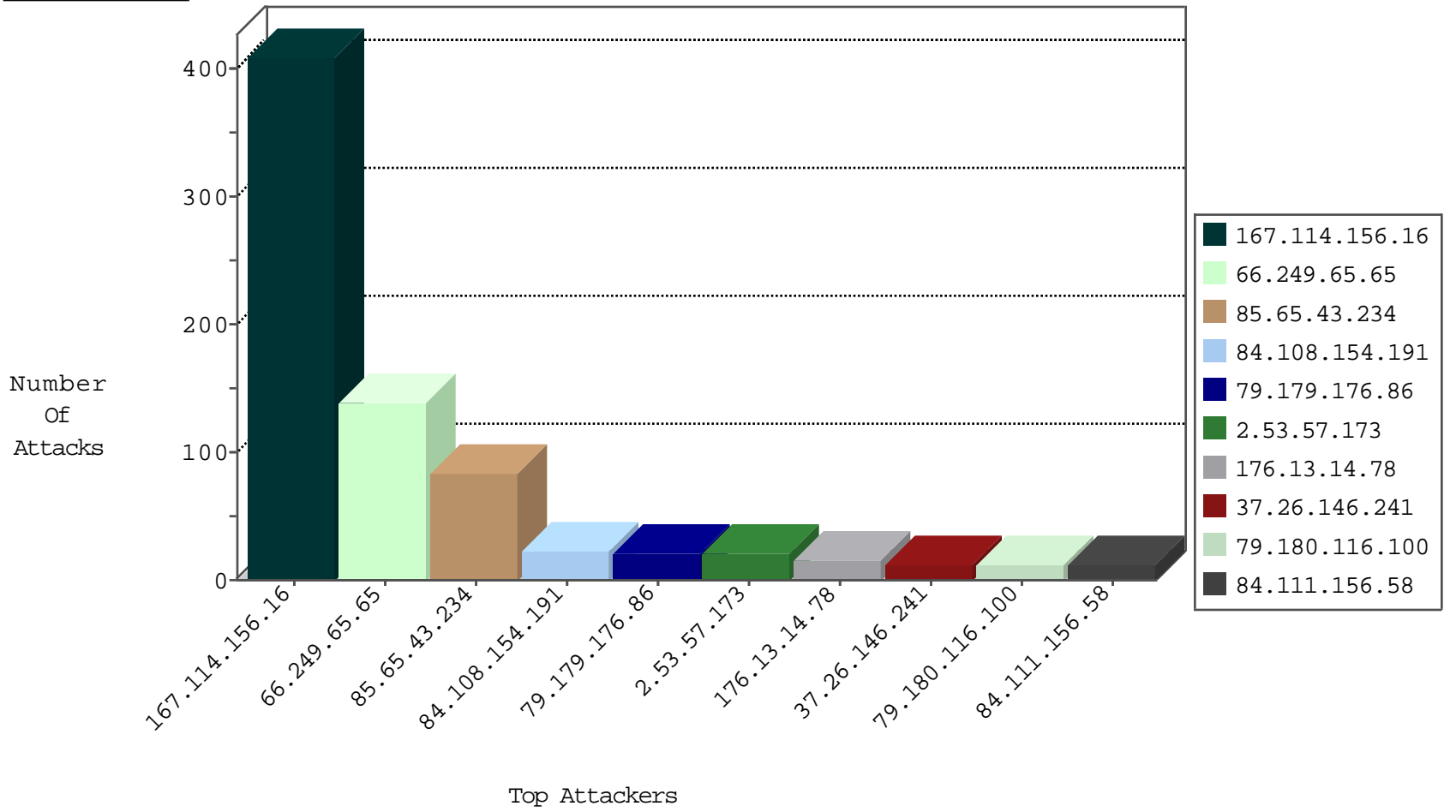
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	17199
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1540
94.159.132.102	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	210
87.70.40.16	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	204
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
107.150.46.37	United States	147.237.76.42	refuah.idf.il	block-sp-trafl	forward	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
69.197.185.18	United States	147.237.0.34	tikshuv.idf.il	block-sp-trafl	forward	1
94.102.52.10	Netherlands	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
69.197.185.22	United States	147.237.77.176	matpash.idf.il	block-sp-trafl	drop	1

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
176.13.14.78	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
188.214.249.145	147.237.77.216	Romania	dover.idf.il	Xenu Link Sleuth User Agent	2
82.117.208.243	147.237.72.14		dover.idf.il(olc	ET SCAN NMAP -sS window 1024	1
61.240.144.67	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
45.62.254.174	147.237.76.198	Canada	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
188.14.242.67	147.237.77.121	Italy	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
95.86.101.21	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
80.246.130.163	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.124	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.39.222.253	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
188.14.242.67	147.237.77.121	Italy	e.navy.idf.il	ET SCAN NMAP -sS window 4096	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.65.65	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	135
84.108.154.191	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
79.179.176.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
79.180.116.100	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.146.241	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.151.209.182	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
80.178.157.116	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.85.34	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.14.78	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
209.190.204.29	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
198.58.103.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.53.57.173	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.55.148.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.111.156.58	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.78.5	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.117.61.244	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
84.111.156.58	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.70.93.28	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.14.78	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
85.250.243.165	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.249.79.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.46.39.208	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
87.70.93.28	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
149.88.150.78	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.26.146.255	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
188.120.154.3	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.53.15.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.86.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	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
109.66.13.99	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.124.43.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.86.190	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.73.251	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.253.143.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.22.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.124	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
66.249.78.230	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.184	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.171.123	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
128.242.249.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

05-04-2016-00:04:02 to 05-04-2016-01:04:02

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.53.165.163	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.65.43.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
2.53.57.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
2.53.158.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
149.78.58.145	United States	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.55.147.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.81.15.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.108.97.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
31.13.98.113	Ireland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
149.50.84.56	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
77.237.138.202	Czech Republic	147.237.77.235	sviva.idf.il	Unauthorized Method HEAD for /	Block	1
66.249.65.18	Israel	147.237.72.166	aka.idf.il	Unknown Parameter tm in www.aka.idf.il/main/giyus/	None	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2378.jpg	Block	1
37.26.147.251	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.180.178.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
66.249.65.65	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.65.65	Block	1
89.139.20.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
66.249.78.252	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/apple-app-site-association	Block	1
46.19.85.34	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
151.80.31.153	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8905-he/refuah.aspx	Block	1
66.249.65.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/main/smalim/smalim.aspx	Block	1
2.55.177.129	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
93.201.117.36	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
69.171.228.117	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.86.135	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	1
188.241.241.254	Romania	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.65.65	Israel	147.237.72.166	aka.idf.il	Unknown Parameter Do in www.aka.idf.il/giyus/general/default.asp	None	1
104.172.208.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
70.197.140.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.117.139.227	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
188.241.241.254	Romania	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
84.111.226.232	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/oprolescategor/mobile	Block	1
66.249.73.161	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
31.13.98.117	Ireland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1