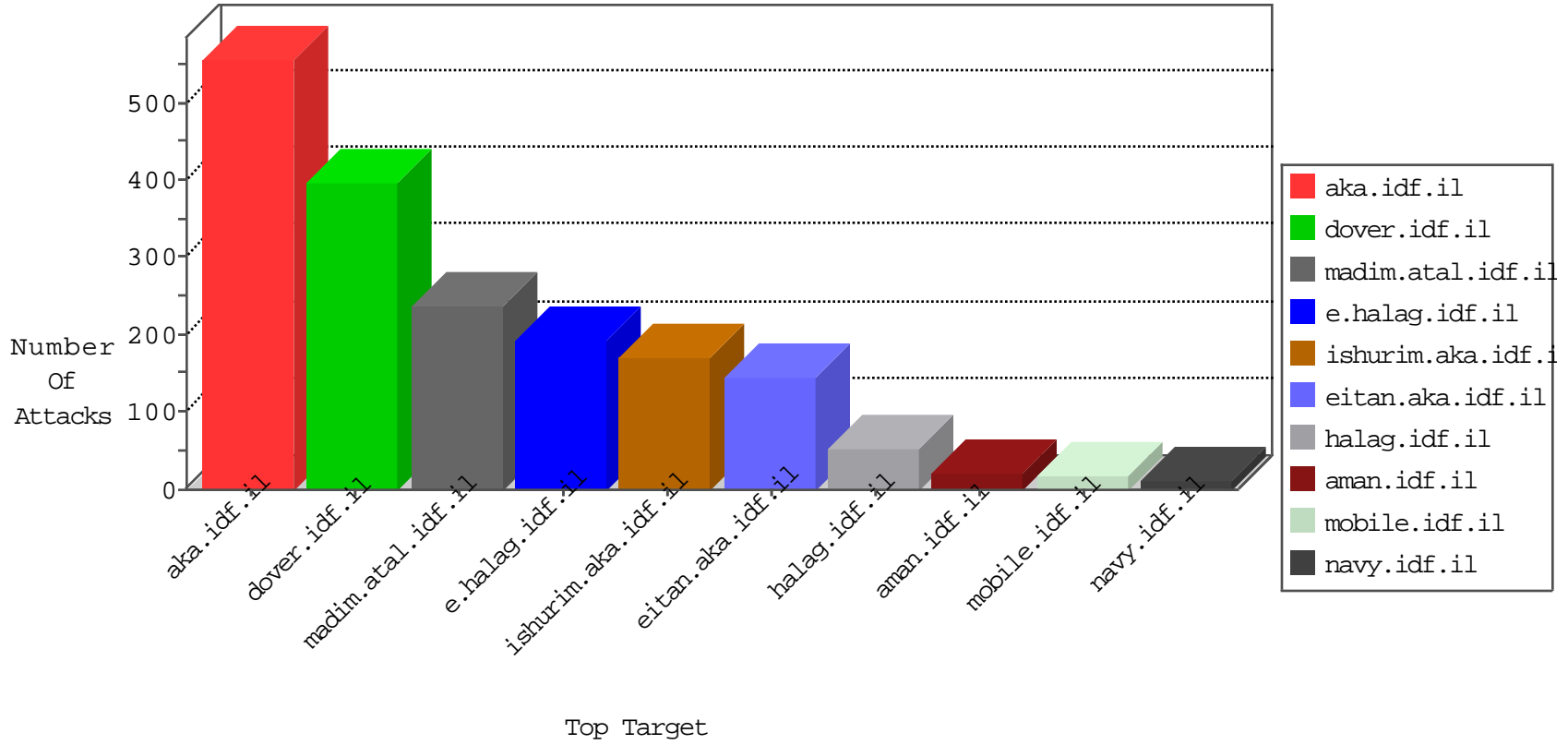


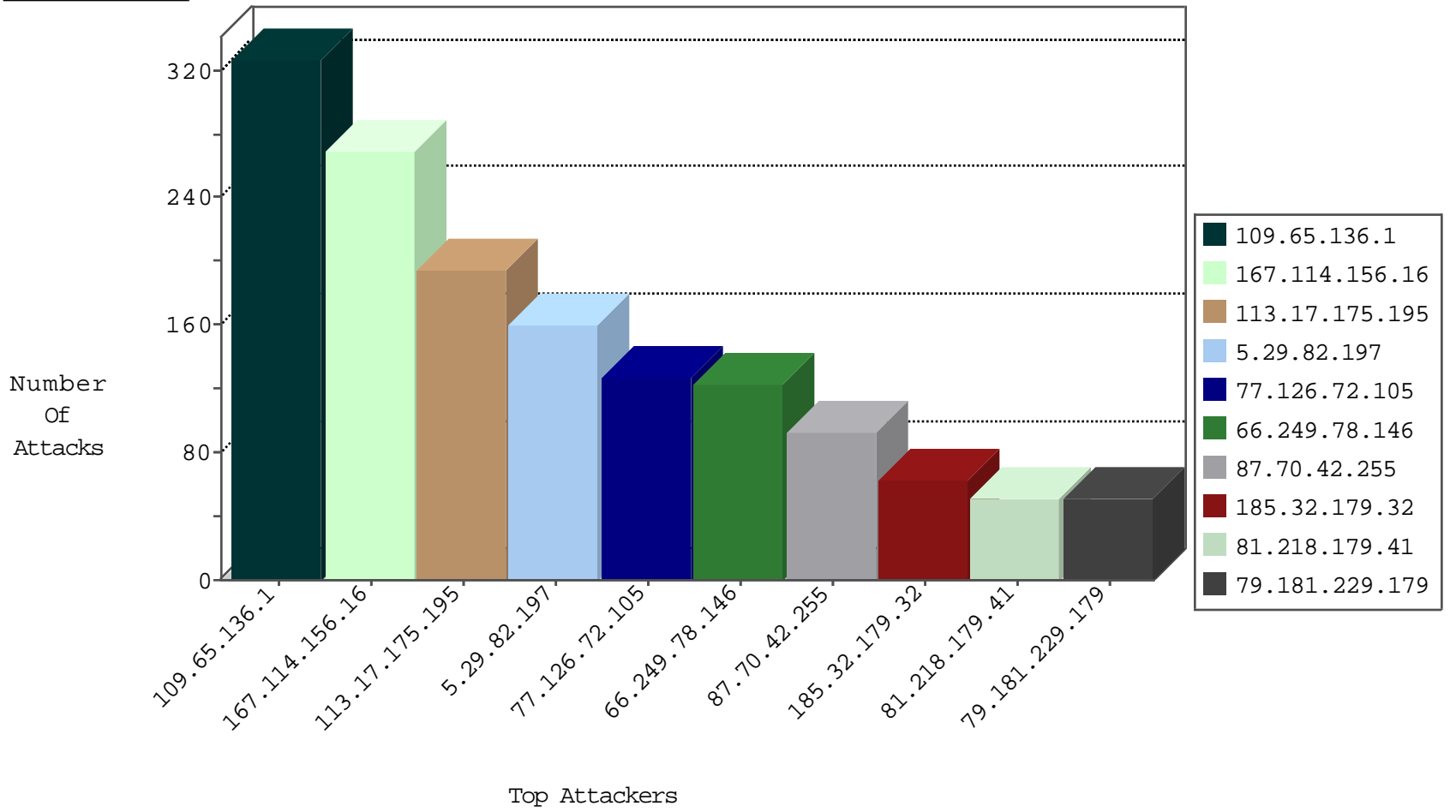
# IDF Under Attack Daily Report



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	15383
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	598
113.17.175.195	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	192
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
81.218.65.210	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
79.178.112.168	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
107.150.32.60	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
107.150.46.38	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
74.91.18.44	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
69.30.198.147	United States	147.237.72.156	aman.idf.il	block-sp-traf1	drop	1
74.91.17.181	United States	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
94.102.52.10	Netherlands	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	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

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.65.136.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	327
77.126.72.105	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	127
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	120
87.70.42.255	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	87
79.181.229.179	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
81.218.179.41	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	50
79.183.255.165	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
77.126.82.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.63.143.28	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
87.70.42.255	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
89.139.141.5	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
172.56.28.189	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
5.102.254.118	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
188.138.9.41	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.206	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.29.82.197	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.117.128.146	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.148.249	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
5.29.82.197	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.148.249	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.29.82.197	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
40.77.167.59	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.148.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.148.249	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
109.64.189.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.249	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	3
109.64.235.60	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.183.64.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.200.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.206	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.249	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
5.22.129.85	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
188.120.148.138	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.160.207.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.224.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.12.145	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.4.150	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
87.70.12.145	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
207.46.13.41	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.29.82.197	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
173.252.90.233	United States	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
5.29.82.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	145
185.32.179.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
46.19.85.232	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	11
46.116.63.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
37.238.140.77	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	5
79.180.152.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.40.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.69.168.165	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	2
178.62.4.206	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	2
46.19.86.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.179	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	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
107.150.46.38	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.fc376.com/	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
150.70.188.165	Japan	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
87.69.168.165	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 87.69.168.165	Block	1
66.249.64.167	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter &SortDir in www.eitan.aka.idf.il/938-he/eitan.aspx	None	1
46.19.85.179	Israel	147.237.77.216	dover.idf.il	Malformed URL he-us,en-us;q=0.8	Block	1
130.185.155.82	Sweden	147.237.76.147	chinuch.aka.idf.il	PHP Attempt	Block	1
66.249.79.254	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/eitan/tmuna/default.asp	Block	1
46.116.200.15	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
31.13.110.111	Ireland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
150.70.188.171	Japan	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.64.219	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/news/pages/pascha.aspx	Block	1
207.46.13.173	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.179	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method -Language: in URL he-us,en-us	Block	1
130.185.155.82	Sweden	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/wp-login.php	Block	1
51.255.65.3	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/military-police	Block	1
176.52.56.16	Russian Federation	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/controls/login.aspx'	Block	1
87.69.168.165	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/1/	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1129-he/dover.aspx	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/daily	Block	1
81.218.179.41	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
58.250.93.83	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/usercontrols/headerupper/	Block	1
37.239.135.128	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
107.150.32.60	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to www.fc376.com/	Block	1
66.249.73.206	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/mobile/	Block	1
2.53.40.30	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
141.212.122.129	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to /x	Block	1
87.69.129.22	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
65.55.210.210	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1