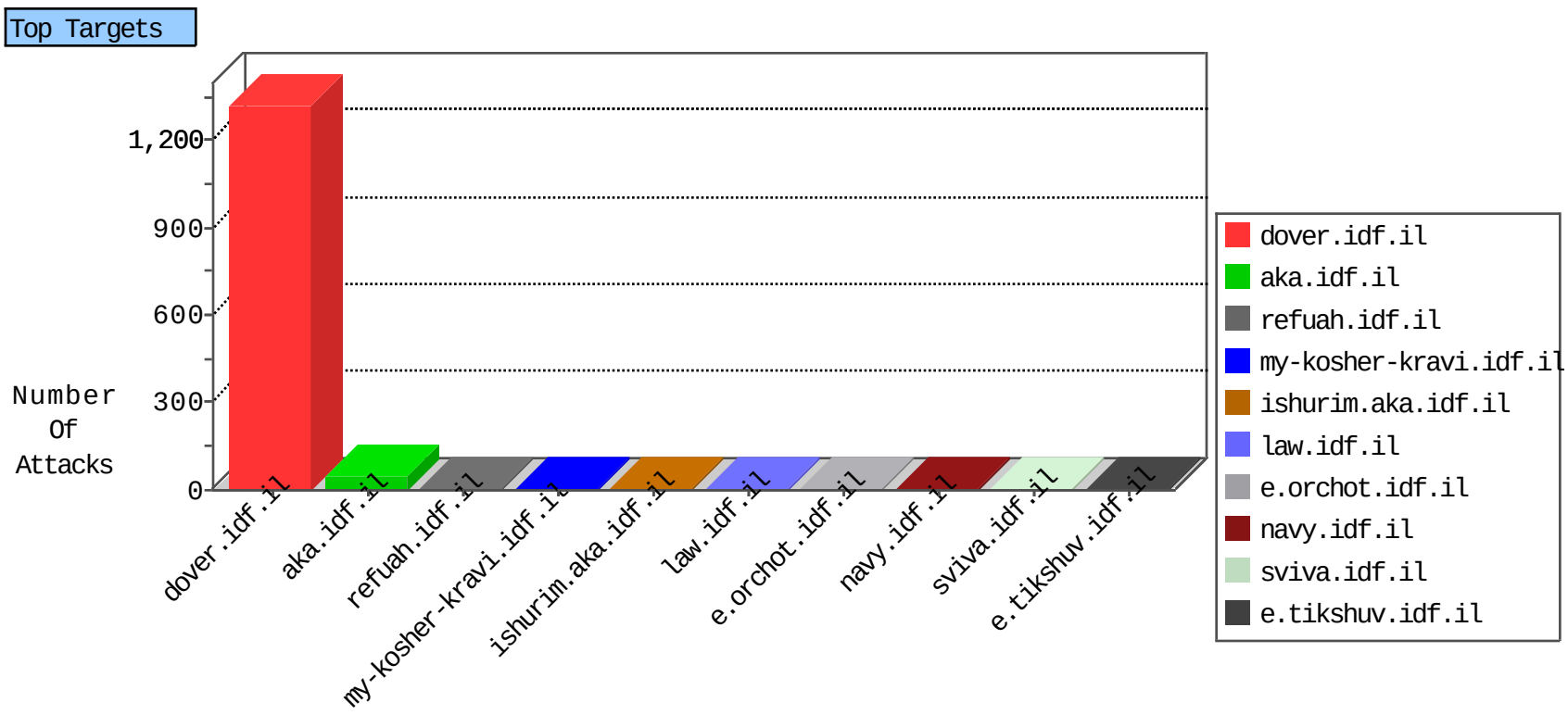
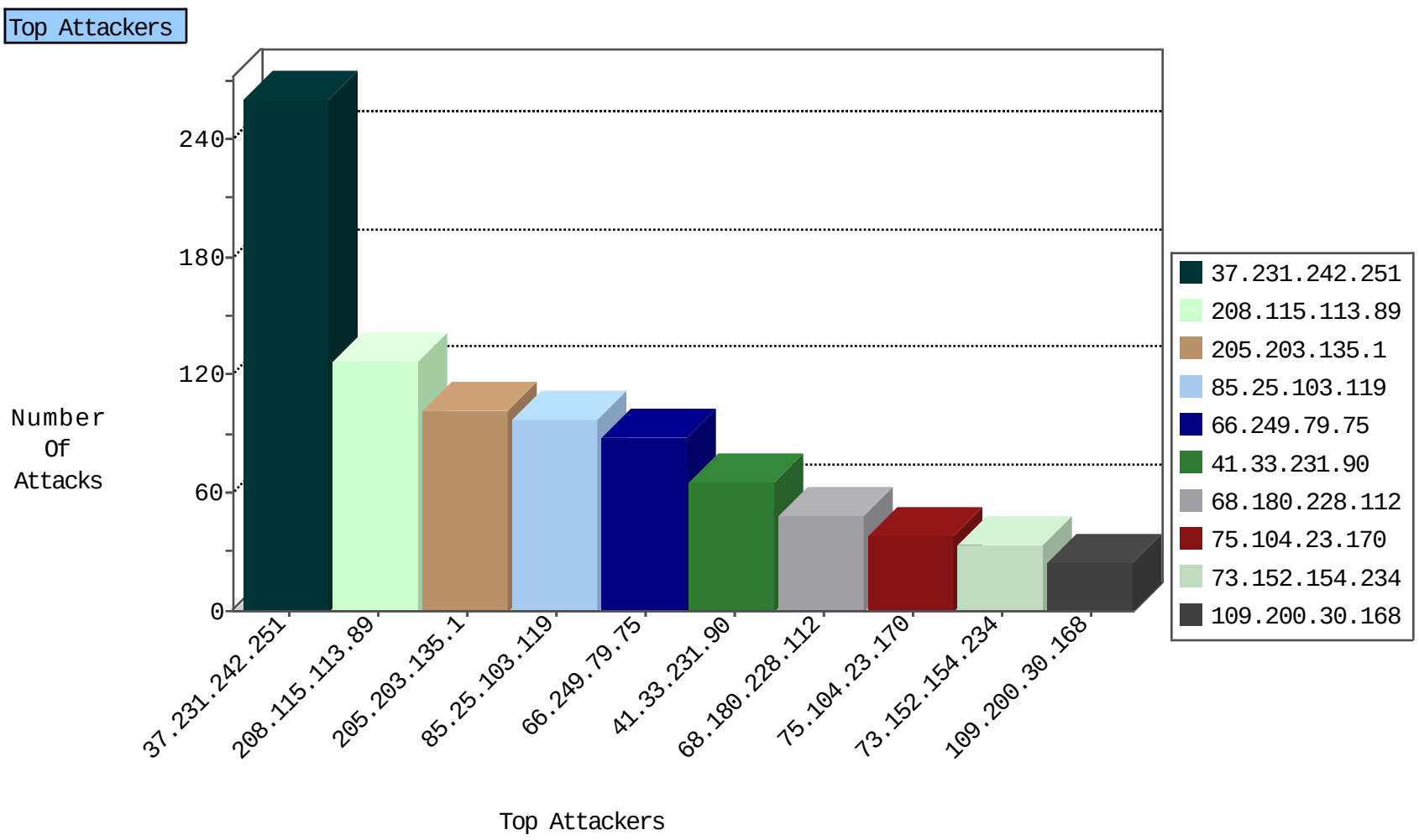
11-24-2015-03:04:09 to 11-24-2015-04:04:09

IDF Under Attack Daily Report





11-24-2015-03:04:09 to 11-24-2015-04:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.15	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	155
60.174.198.81	China	147.237.76.202	e.halag.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
115.239.228.8	China	147.237.0.16	my-kosher-kravi.idf.il	Frk_Under_Attack_Con_Http	drop	2
66.249.79.75	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
104.192.0.226	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
185.106.94.28		147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
115.239.228.8	China	147.237.0.16	my-kosher-kravi.idf.il	Frk_Purple_Con_Limit_Http	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1

11-24-2015-03:04:09 to 11-24-2015-04:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
210.209.85.92	Hong Kong	147.237.77.216	dover.idf.il	0854: HTTP: upload* Access	Block	3
151.80.31.139	Italy	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.127	France	147.237.77.170	maarachot.idf.il	C228: HTTP: AhrefBot crawler	Block	1
192.166.218.214	Poland	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1

11-24-2015-03:04:09 to 11-24-2015-04:04:09

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	2
66.249.79.84	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.89	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
213.168.248.217	147.237.8.50	Ireland	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
173.14.248.34	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
139.217.27.17	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
46.228.207.18	147.237.77.234	Germany	halag.idf.il	ET SCAN NMAP -sS window 1024	1
212.7.199.208	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.14.248.34	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 4096	1
139.217.27.17	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
103.35.151.192	147.237.76.38		e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.149.17	147.237.8.14	Israel	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
31.6.71.154	147.237.77.205	Poland	prisha.idf.il	ET SCAN NMAP -sS window 1024	1

11-24-2015-03:04:09 to 11-24-2015-04:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.231.242.251	Kuwait	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	261
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	127
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
85.25.103.119	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	96
66.249.79.75	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
75.104.23.170	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
73.152.154.234	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
109.200.30.168	United Kingdom	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
208.54.37.172	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
204.12.251.37	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
107.167.117.26	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	19
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
66.249.79.75	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
50.116.30.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.73.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
207.46.13.17	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	9
77.250.201.52	Netherlands	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
40.77.167.0	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
199.17.232.4	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
95.108.158.152	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
65.19.138.33	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
207.46.13.87	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
68.50.95.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
76.108.162.135	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
207.46.13.17	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
65.55.210.26	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.79.79	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.37.59	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
95.108.158.171	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
73.141.237.42	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.54.170.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.140.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
173.34.186.54	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.255.253.150	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
107.178.194.79	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
60.240.131.164	Australia	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	5
41.220.69.208	Nigeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
98.211.192.152	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
100.38.194.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.79.75	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
2.54.166.63	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.79.77	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
77.250.201.52	Netherlands	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.66.109	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
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
206.196.184.20	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
157.55.39.123	United States	147.237.72.166	aka.idf.il	Unknown Parameter KEY in aka.idf.il/ishurim/cityofficers/	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/yoav.stm/	Block	1
46.166.190.147	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
220.181.108.161	China	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
176.10.99.204	Switzerland	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
31.193.51.80	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.57	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/â€Ž	Block	1
157.55.39.124	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8903-he/refuah.aspx	Block	1
66.249.66.99	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
184.105.247.195	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	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
66.249.79.79	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
41.220.69.208	Nigeria	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
207.46.13.87	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.210	United States	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/sites/skira/default.asp	None	1
199.59.148.210	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/6/size220x0/4636.jpg	Block	1
109.64.125.147	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.79.123	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1598-14847-he/dover.aspx	Block	1
46.19.86.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.244	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/general.aspx	Block	1
80.246.136.3	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
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	1
141.212.122.96	United States	147.237.77.235	sviva.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
46.166.170.3	Lithuania	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
171.25.193.235	Sweden	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1