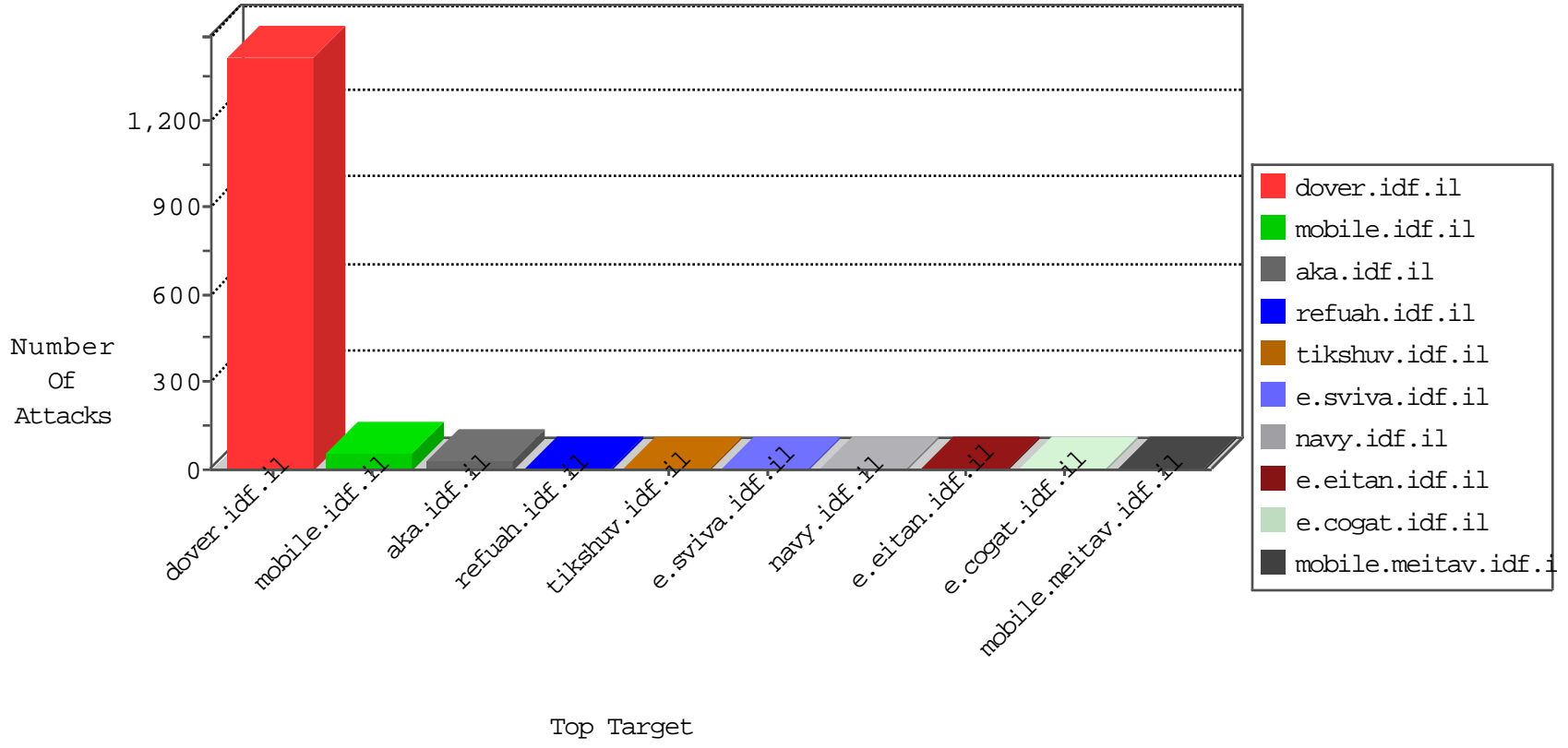
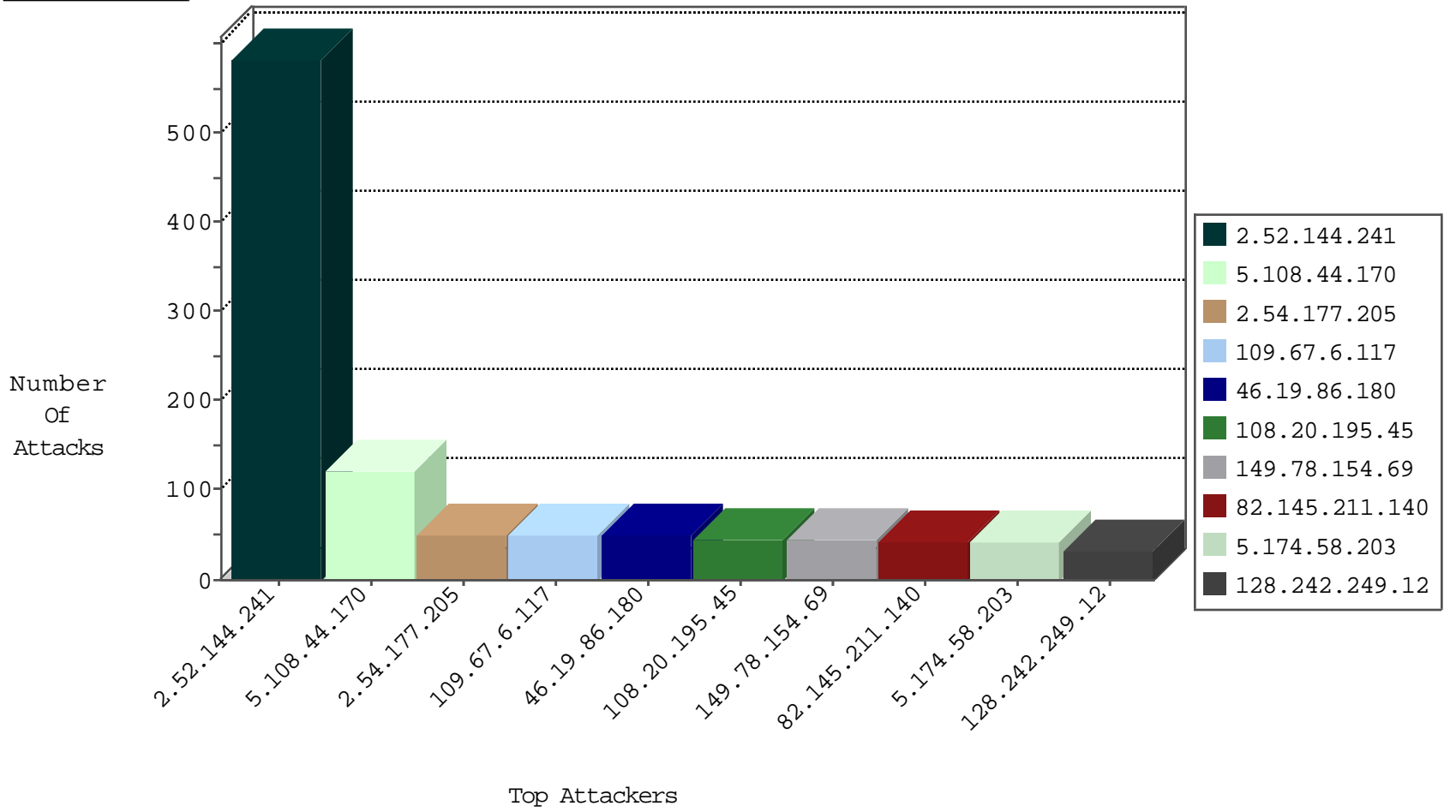




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
46.19.86.180	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	134
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
123.52.105.88	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
192.3.207.66	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	30
203.237.127.232	Korea, Republic of	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
188.138.9.50	Germany	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
220.181.125.15	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
71.6.165.200	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
31.223.176.34	Palestinian Territory, Occupied	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
37.130.227.133	United Kingdom	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
88.249.106.23	Turkey	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
188.138.9.51	Germany	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
77.104.110.104	Iran, Islamic Republic of	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 2048	1
128.136.227.196	United States	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.66	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.130		147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.65	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.93.50	Netherlands	147.237.76.202	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.174.93.50	Netherlands	147.237.76.196	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.174.93.50	Netherlands	147.237.76.86	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.77.79.43	China	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.50	Netherlands	147.237.76.30	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.77.79.43	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.50	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
188.138.9.51	Germany	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
77.104.110.104	Iran, Islamic Republic of	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
128.136.227.196	United States	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
77.104.110.104	Iran, Islamic Republic of	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -f -sS	1
114.112.90.54	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.93.50	Netherlands	147.237.77.61	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.174.93.50	Netherlands	147.237.76.201	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.174.93.50	Netherlands	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.174.93.50	Netherlands	147.237.76.44	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.77.79.43	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.50	Netherlands	147.237.0.19	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
2.52.144.241	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	537
5.108.44.170	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	121
2.54.177.205	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	51
109.67.6.117	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	49
108.20.195.45	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	46
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	44
82.145.211.140	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
46.19.86.180	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
5.174.58.203	Poland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
108.91.85.17	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
2.52.144.241	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	18
2.52.144.241	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	18
80.62.117.147	Denmark	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
87.68.214.191	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
66.249.81.215	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
5.174.58.203	Poland	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	15
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
46.19.86.109	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
45.217.180.148		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
86.84.62.57	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
176.12.142.254	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
73.149.108.198	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
2.52.144.241	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	9
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
149.78.16.107	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
84.111.189.198	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
66.249.81.218	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
185.19.221.90	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
5.29.43.4	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
79.182.60.3	Israel	147.237.0.34	tikshuv.idf.il	First packet isn't SYN	drop	drop	6
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
174.236.195.237	United States	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	5
174.236.195.237	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	5
174.236.195.237	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
46.244.68.249	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
2.54.151.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.19.86.83	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
31.13.97.112	Ireland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
37.26.147.160	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
93.173.28.247	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
31.13.97.115	Ireland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
96.21.121.34	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
157.55.39.191	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
79.180.195.130	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
128.242.249.12	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
95.86.66.52	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	6
198.204.249.34	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/default.aspx	Block	3
178.255.215.87	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.255.215.87	Block	1
213.57.215.137	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18670-en/kkkkkkkk=c37066e4kkkkkkkk_c37066e4	Block	1
2.52.144.241	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
122.59.2.124	New Zealand	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/matah	Block	1
188.165.15.85	France	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1
46.19.85.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
197.27.107.1	Tunisia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/idf-admin	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
157.55.39.162	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.229.51	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0202-5.stm	Block	1