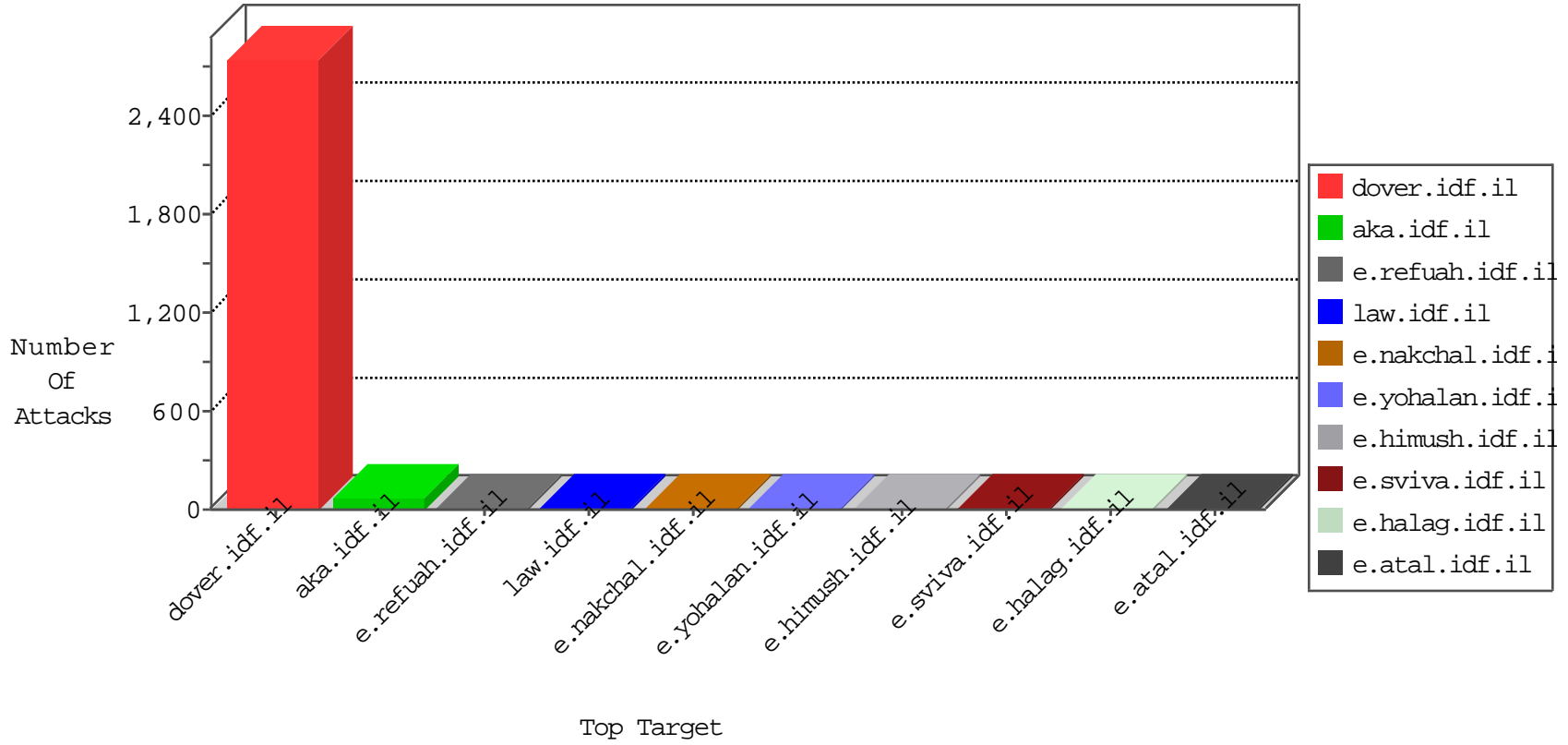
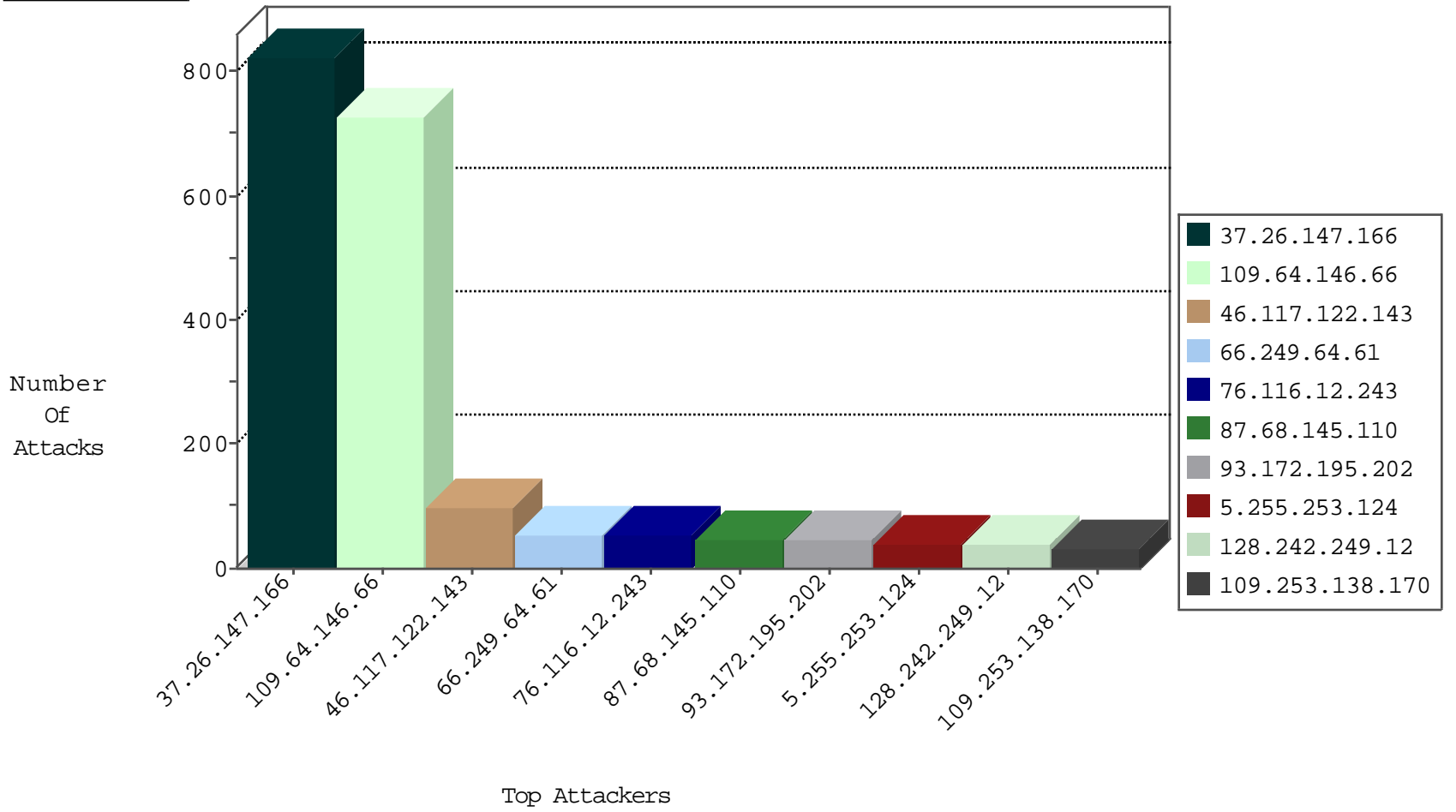


Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.67.40	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	77
43.255.190.60	Japan	147.237.76.147	chimuch.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
76.22.14.237	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
66.249.67.24	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1
76.22.14.237	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
192.3.194.138	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
69.171.112.117	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	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	34
85.65.59.115	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
85.25.103.50	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.202	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1

## Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.67.24	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.73	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.26	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
113.59.33.61	China	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
111.13.30.109	China	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
69.12.92.137	United States	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
59.41.39.125	China	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.190.60	Japan	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
113.59.33.61	China	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 4096	1
113.59.33.61	China	147.237.77.205	prisha.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.64	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.190.60	Japan	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
43.255.190.60	Japan	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
37.26.147.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	816
109.64.146.66	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	726
46.117.122.143	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	96
66.249.64.61	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	54
76.116.12.243	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	53
93.172.195.202	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	46
87.68.145.110	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	46
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
109.253.138.170	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
176.12.147.136	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
108.59.253.71	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
84.228.190.34	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
109.253.157.228	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
109.253.135.28	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
136.243.36.88	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
79.179.160.222	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
37.8.63.152	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
77.125.134.92	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
31.186.228.32	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
207.46.13.61	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
31.186.228.62	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
31.186.228.28	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
176.12.146.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
75.126.221.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
31.186.228.67	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
31.186.228.95	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
31.186.228.25	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
31.186.228.90	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
134.191.232.68	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
31.186.228.61	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
31.186.228.27	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
31.186.228.23	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
31.186.228.24	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
31.186.228.65	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
5.29.123.58	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
31.186.228.89	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
31.186.228.63	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
31.186.228.170	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
31.186.228.87	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
109.253.157.40	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	3
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	3
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
77.127.183.192	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	2
66.249.64.63	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.63	Block	1
188.165.15.117	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19265-he/dover.aspx	Block	1
31.193.51.59	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
82.221.105.7	Iceland	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
66.249.78.87	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
66.199.231.242	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.52	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/alnajah/alnajah.stm	Block	1
158.222.10.42		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/grapheat.stm	Block	1
69.30.240.46	United States	147.237.76.31	nakchal.idf.il	Illegal HTTP Version	Block	1
66.249.64.63	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/rights/asp/faq.asp	None	1
195.159.233.44	Norway	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 195.159.233.44 (Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE))	None	1
46.8.161.47	Russian Federation	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.198.170.220	Ukraine	147.237.77.216	dover.idf.il	Unknown HTTP Request Method COOK in URL www.idf.il/1283-16223-en/dover.aspx	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/webresource.axd	Block	1
66.249.64.24	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/scriptresource.axd	Block	1
217.69.136.205	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/newsflash/newsflash.aspx/	Block	1
158.222.10.50		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/english/news/grapheat.stm	Block	1
66.249.65.178	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
195.159.233.44	Norway	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 195.159.233.44 (Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE))	None	1
54.83.158.198	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
114.112.91.97	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/english/news/grapheat.stm	Block	1
66.249.64.59	Israel	147.237.72.166	aka.idf.il	Unknown Parameter newsItem in www.aka.idf.il/megurim/news/	None	1
158.222.14.21		147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
66.249.73.211	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
195.159.233.44	Norway	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE)	None	1
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 54.245.64.111	Block	1
145.255.163.42	Kazakstan	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
188.165.15.78	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2003/march/21.stm	Block	1
79.179.30.239	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	1
66.249.78.74	Israel	147.237.76.30	himush.idf.il	Unknown Parameter pageNum in chimush.atal.idf.il/938-he/himush.aspx	None	1
64.19.78.240	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
199.30.25.244	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
157.55.39.129	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1