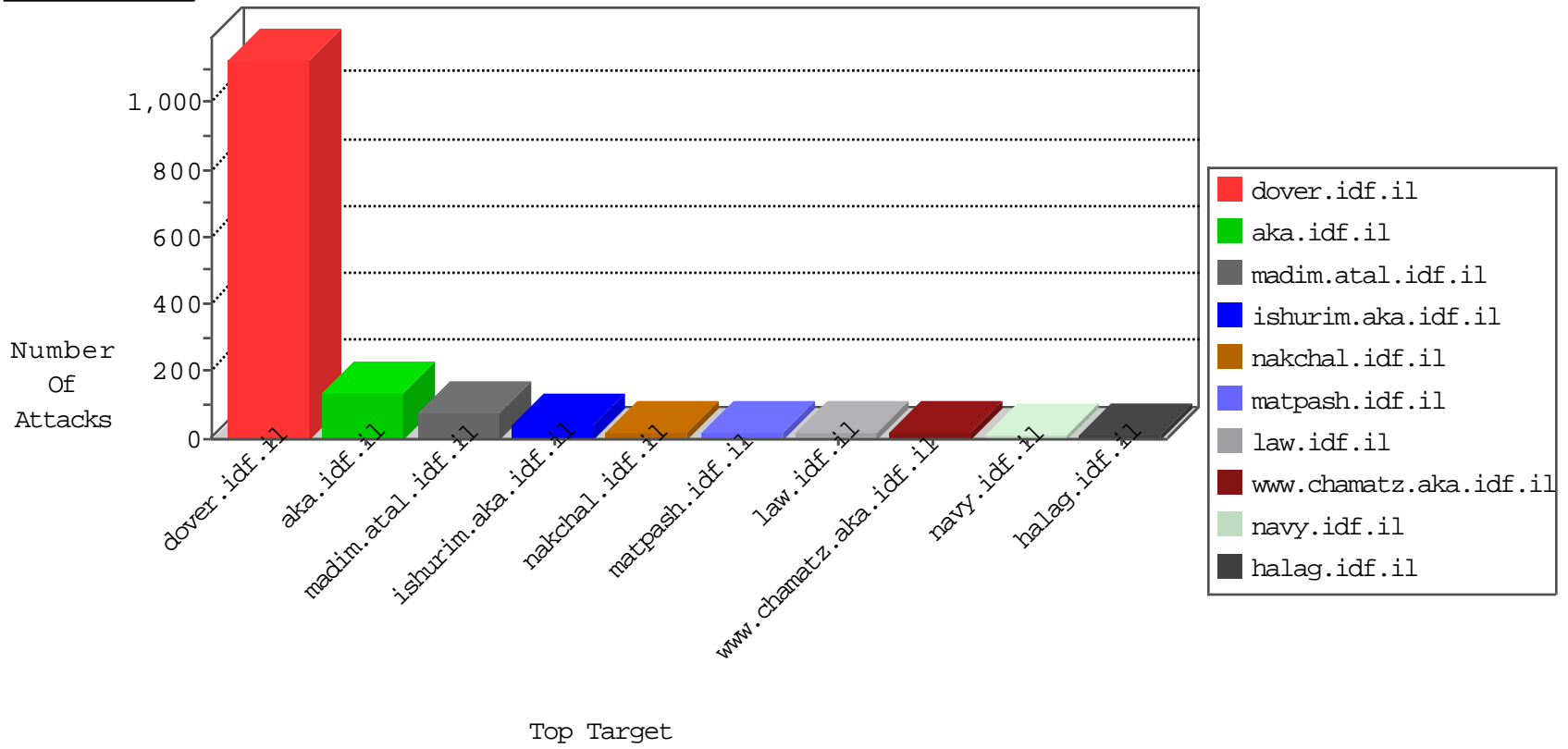
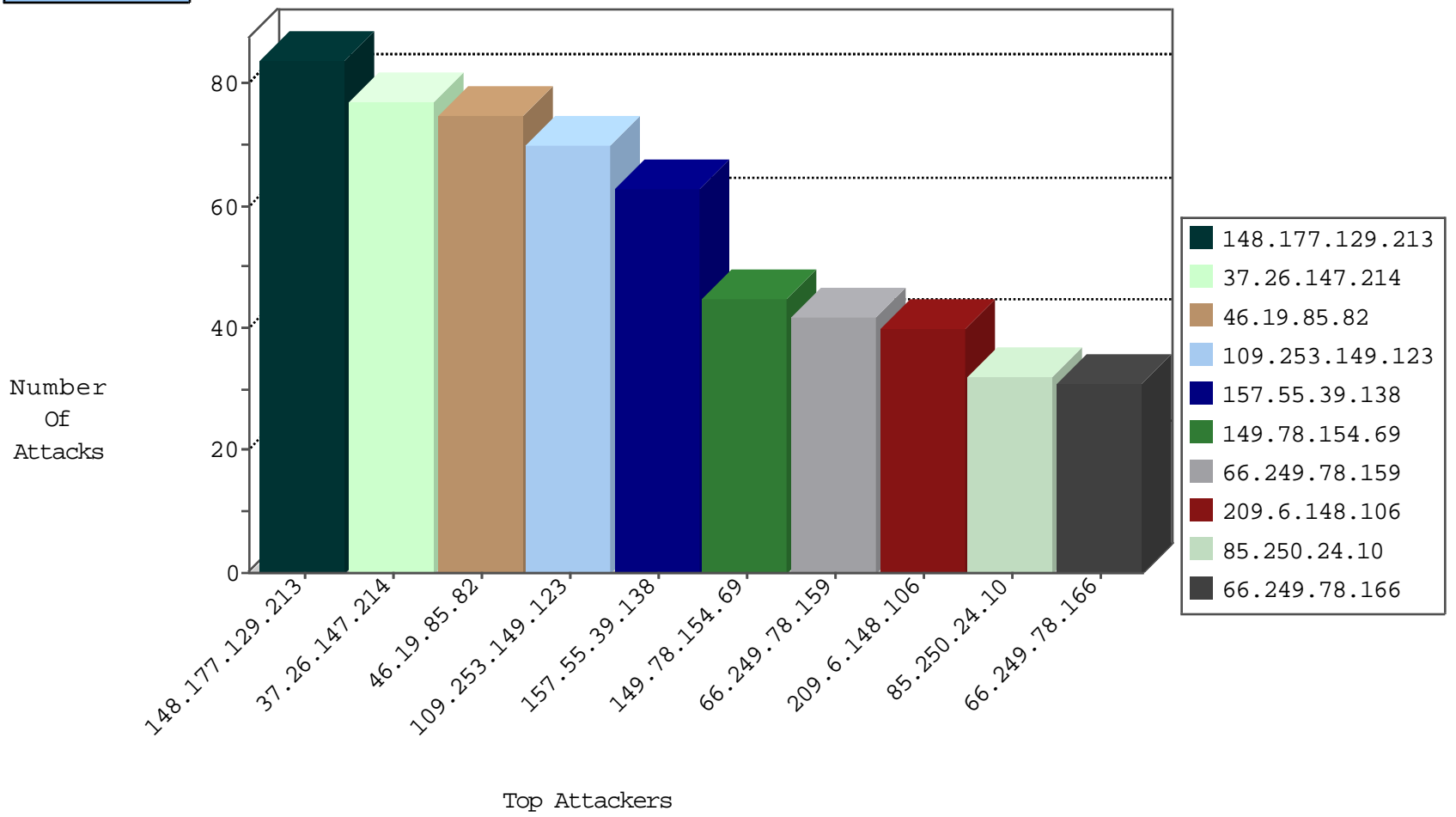


Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3485
192.168.14.12		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15
46.120.44.25	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	13
2.52.55.198	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
46.120.44.25	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
79.177.132.219	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
176.12.137.208	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
2.52.152.101	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
153.191.51.38	Japan	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	2
118.5.131.219	Japan	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
71.6.135.131	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.85.210	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
109.253.88.176	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.232	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.116.202.157	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
98.246.110.40	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.120.184.63	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
93.120.27.62	Romania	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
177.36.204.12	Brazil	147.237.72.167	ishurim.aka.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
85.25.103.50	Germany	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.198	e.ychalan.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
66.240.192.138	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
178.175.128.50	Moldova, Republic of	147.237.76.202	e.halag.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	147.237.8.46	e.chinuch.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	5
66.249.78.96	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.34	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
80.246.133.14	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.75.13	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	2
190.75.239.240	Venezuela	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
190.75.239.240	Venezuela	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
183.136.216.3	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
41.159.136.195	Gabon	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
84.108.102.33	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
41.159.136.195	Gabon	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
79.183.51.181	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
218.77.79.43	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
190.75.239.240	Venezuela	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
190.75.239.240	Venezuela	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
190.75.239.240	Venezuela	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
190.75.239.240	Venezuela	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.238	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.132.118	Russian Federation	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
41.159.136.195	Gabon	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
2.52.152.101	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
72.209.236.114	United States	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
190.75.239.240	Venezuela	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
148.177.129.213	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	84
37.26.147.214	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	77
46.19.85.82	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	72
157.55.39.138	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	58
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	44
209.6.148.106	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
85.250.24.10	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
107.188.21.130		147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	27
80.179.47.82	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
109.253.135.56	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
81.218.13.225	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
212.179.46.20	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
5.28.146.106	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
37.26.148.191	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
81.218.40.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
46.19.86.180	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
2.52.152.101	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
46.19.86.22	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
109.253.135.190	Israel	147.237.76.31	nakchal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	12
80.179.9.7	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
71.170.41.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
79.176.106.135	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
46.19.85.238	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
109.253.149.123	Israel	147.237.0.19	madim.atal.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
82.102.169.113	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
46.19.86.84	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	7
2.52.55.198	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
174.106.72.40	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
188.120.148.221	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
50.87.144.145	United States	147.237.77.216	dover.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
66.249.64.76	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.19.85.163	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	6
46.19.85.163	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
46.120.184.63	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
46.19.85.210	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
109.253.136.113	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
50.106.13.80	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
37.26.148.214	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
108.26.191.232	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
178.93.173.199	Ukraine	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.253.149.123	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.149.123	Block	61
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	21
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	9
178.137.19.143	Ukraine	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/templates/getfile/	Block	6
157.55.39.146	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 157.55.39.146	Block	6
157.55.39.33	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 157.55.39.33	Block	5
157.55.39.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom Temporary	Block	4
93.172.179.18	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 93.172.179.18	Block	4
93.172.179.18	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	4
46.120.184.63	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	3
207.46.13.104	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 207.46.13.104	Block	3
37.26.148.174	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom Temporary	Block	2
46.229.164.99	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatatz	Block	2
109.186.173.252	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom Temporary	Block	2
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.72	Block	2
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1451-he/dover.aspx	Block	1
157.55.39.205	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2003/march/24.stm	Block	1
149.88.127.124	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom Temporary	Block	1
66.249.67.22	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//938-he/hamaz.aspx	Block	1
46.229.164.114	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatatz	Block	1
109.64.32.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
31.168.173.121	Israel	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
188.165.15.236	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1133-he/atal.aspx	Block	1
66.249.75.34	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx	Block	1
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/1226.stm	Block	1
207.46.13.133	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/	Block	1
172.245.118.217	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/rk=0/rs=ccbipmdtcblxvp5ea_n4gz9.pia-	Block	1
66.249.78.125	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/69-he/patzar.aspx	Block	1
157.55.39.24	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/994-7798-he/nakhal.aspx	Block	1
66.249.67.41	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
109.65.12.168	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
197.2.244.114	Tunisia	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
66.249.79.6	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//938-he/hamaz.aspx	Block	1
66.249.75.117	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom Temporary	Block	1
157.55.39.138	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.138	Block	1
113.163.45.52	Vietnam	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
66.249.64.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-13878-he/dover.aspx	Block	1
212.179.46.23	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
66.249.67.120	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1206-he/refuah.aspx	Block	1
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
37.204.143.49	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/pazan/oded.stm	Block	1
207.46.13.100	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/109335.pdf* »Âç×"×ÿÂ¿Â½Â»×"×ÿÂ¿Â½Â»-×"×ÿÂ¿Â½Â»×"×ÿÂ¿Â½Â»×"×ÿÂ¿Â½Â»×"×ÿÂ¿Â½Â»	Block	1
85.65.49.173	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom Temporary	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20399-he/dover.aspx	Block	1
125.209.235.186	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/info02.stm	Block	1
66.249.67.6	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//938-he/hamaz.aspx	Block	1
94.153.9.66	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/	Block	1
46.229.164.99	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ishurim/exampcert	Block	1