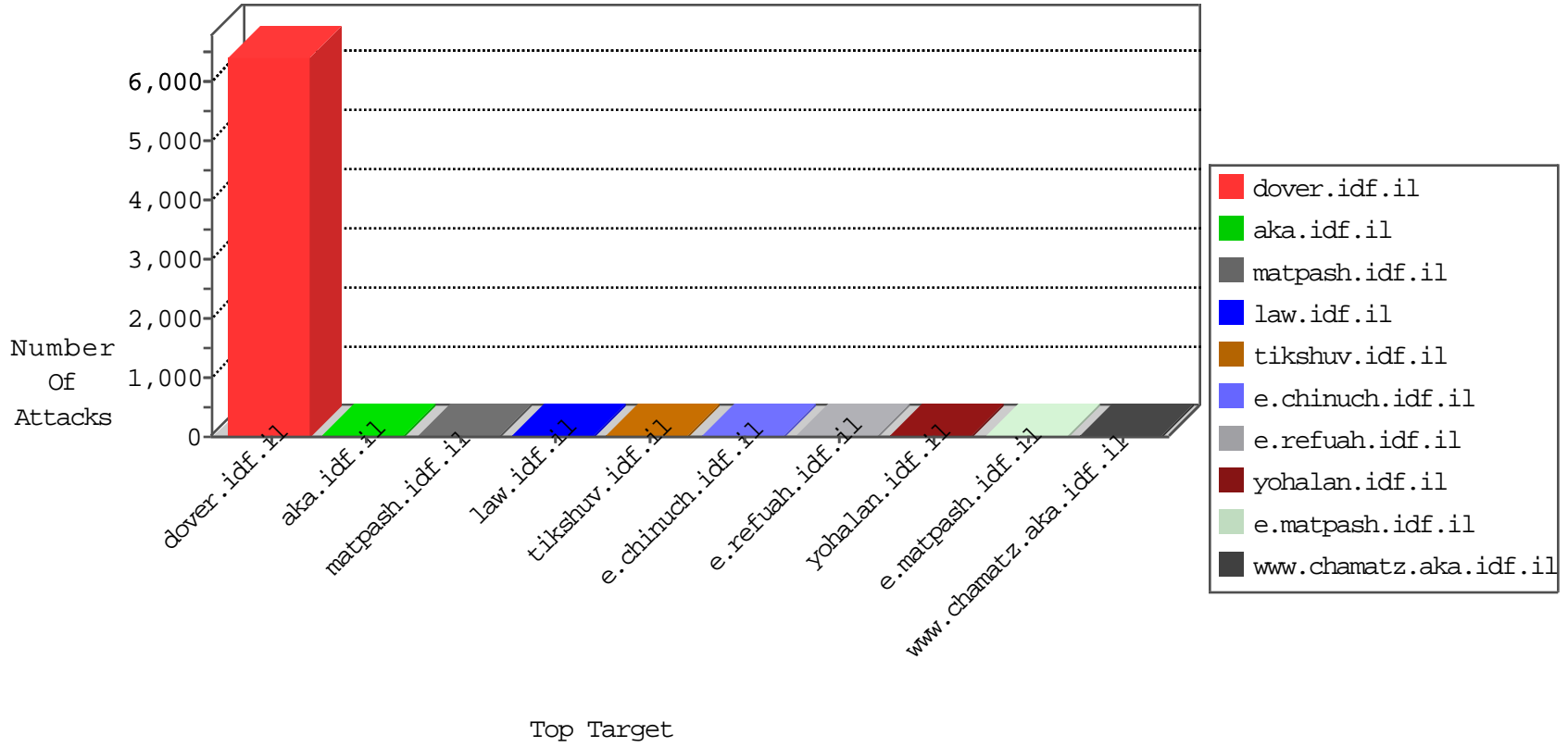
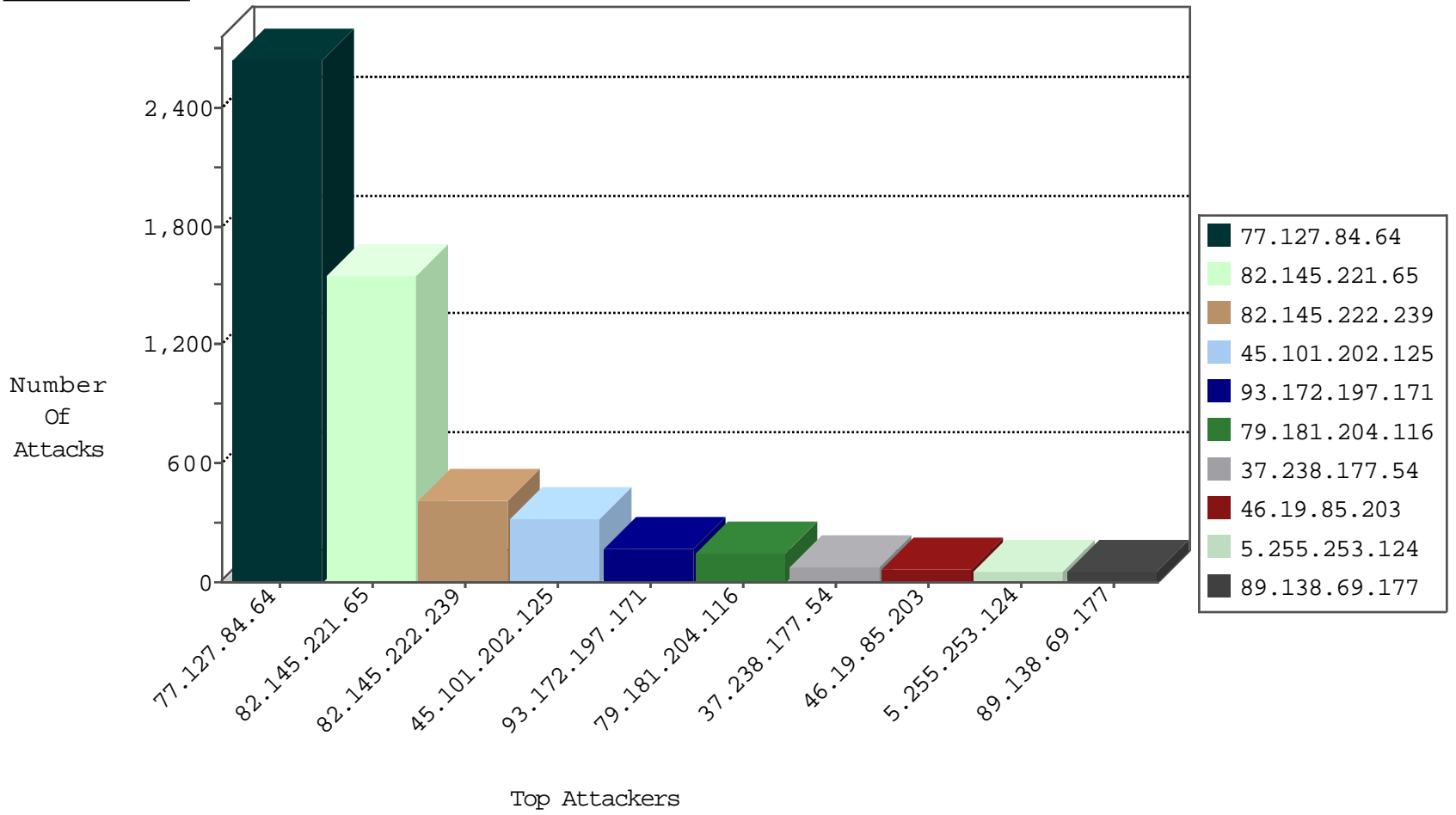




Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
68.9.98.110	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	11
202.55.87.83	Singapore	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	2

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
71.6.167.142	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	2
66.240.236.119	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	2
198.20.69.98	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.19	law-forum.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
188.138.9.50	Germany	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.8.46	e.chinuch.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
71.6.135.131	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.14	e.orchot.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	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.200	eitan.aka.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	147.237.0.19	madim.atal.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
84.108.76.174	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.76.202	e.halag.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	26
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
84.108.76.174	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
66.249.73.211	United States	147.237.77.74	law.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
66.249.78.197	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.40	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
111.203.22.57	China	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
93.90.240.18	Russian Federation	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
93.90.240.18	Russian Federation	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
93.90.240.18	Russian Federation	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.90.240.18	Russian Federation	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.0.35	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.90.240.18	Russian Federation	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
202.160.175.231	India	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
81.200.91.2	Russian Federation	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
175.98.165.170	Taiwan	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
93.90.240.18	Russian Federation	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
93.90.240.18	Russian Federation	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
93.90.240.18	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.90.240.18	Russian Federation	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.0.200	mAu.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.90.240.18	Russian Federation	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
202.160.175.231	India	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 3072	1
37.220.34.55	Netherlands	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
81.200.91.2	Russian Federation	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
81.200.91.2	Russian Federation	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -f -sS	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
77.127.84.64	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2645
82.145.221.65	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1553
82.145.222.239	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	410
45.101.202.125		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	325
93.172.197.171	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	174
79.181.204.116	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	147
37.238.177.54	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	79
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	57
89.138.69.177	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	52
98.225.206.60	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	49
46.19.85.203	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
176.12.140.168	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
62.219.153.146	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
197.33.100.96	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
109.253.142.138	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
199.30.24.141	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
109.253.142.74	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
60.241.205.139	Australia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
2.52.10.17	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
112.198.30.3	Philippines	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.253.143.181	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
68.77.56.105	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
68.9.98.110	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
66.249.81.215	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
66.249.81.215	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
66.249.78.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
66.249.64.74	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
66.249.78.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
74.71.251.87	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
66.249.78.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
80.246.130.195	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
124.107.104.10	Philippines	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
77.126.221.242	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
5.102.214.172	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
46.19.85.203	Israel	147.237.77.216	dover.idf.i	Invalid sequence number	Bad TCP sequence	monitor	8
119.122.240.76	China	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	8
119.122.240.76	China	147.237.77.216	dover.idf.i	Unexpected post SYN packet - RST or SYN expected	drop	drop	8
46.19.85.203	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	8
119.122.240.76	China	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	alert	8
66.249.80.67	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
109.253.149.46	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
46.116.184.66	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
82.117.130.181	Czech Republic	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
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
5.35.253.155	Germany	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	2
198.154.240.106	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
210.211.118.119	Vietnam	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	2
157.55.39.130	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ishurim/man	Block	1
5.29.81.231	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
82.117.130.181	Czech Republic	147.237.72.166	aka.idf.il	Admin Blocking	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
46.19.123.125	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
197.33.100.96	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
119.122.240.76	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/usercontrols/headerupper/	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kamlar/klali/mull	Block	1
66.249.65.14	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/894-he	Block	1
209.105.181.239	United States	147.237.77.176	matpash.idf.il	eMail Hoarding	Block	1
180.76.5.194	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
5.35.253.155	Germany	147.237.77.74	law.idf.il	Distributed Admin Blocking	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0202-6.stm	Block	1
66.249.64.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
198.154.240.106	United States	147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	1
155.94.131.205		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/english/news/grapheat.stm	Block	1
210.211.118.119	Vietnam	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
66.249.78.87	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
180.76.6.45	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/901-11435-he/cogat.aspx	Block	1
95.132.40.13	Ukraine	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.66	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx	Block	1
155.94.254.143		147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
77.75.79.32	Czech Republic	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.78.94	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
188.165.15.43	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9840-he/refuah.aspx	Block	1
37.115.187.54	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
104.222.192.251		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/iaf/iaf4.stm	Block	1
66.249.64.68	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx	Block	1
207.46.13.104	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
81.218.158.127	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	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
188.165.15.78	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1004-3.stm	Block	1
37.140.141.39	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/band	Block	1
109.253.137.243	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
66.249.64.86	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
209.105.181.239	United States	147.237.77.176	matpash.idf.il	E-mail collector robots 14	Block	1