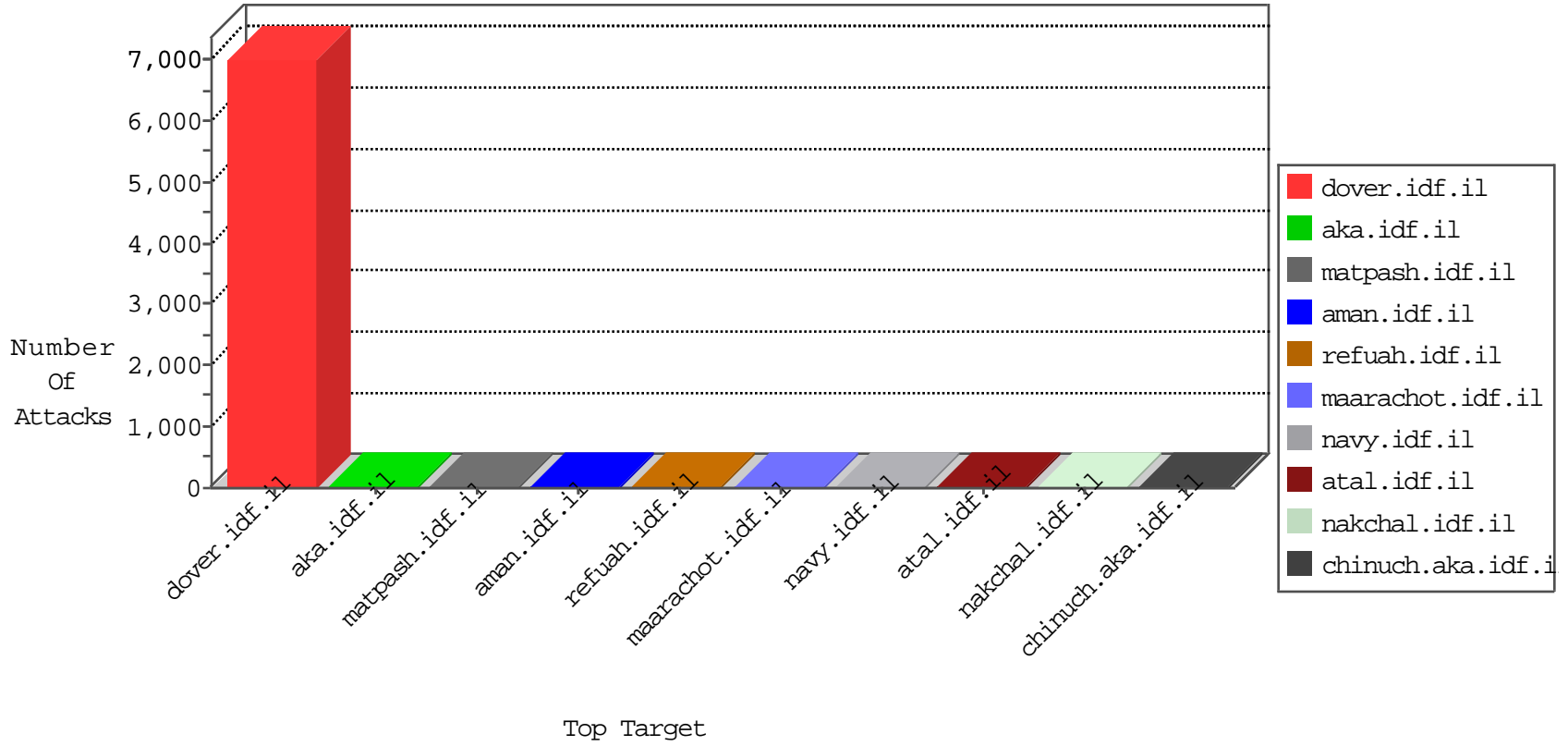
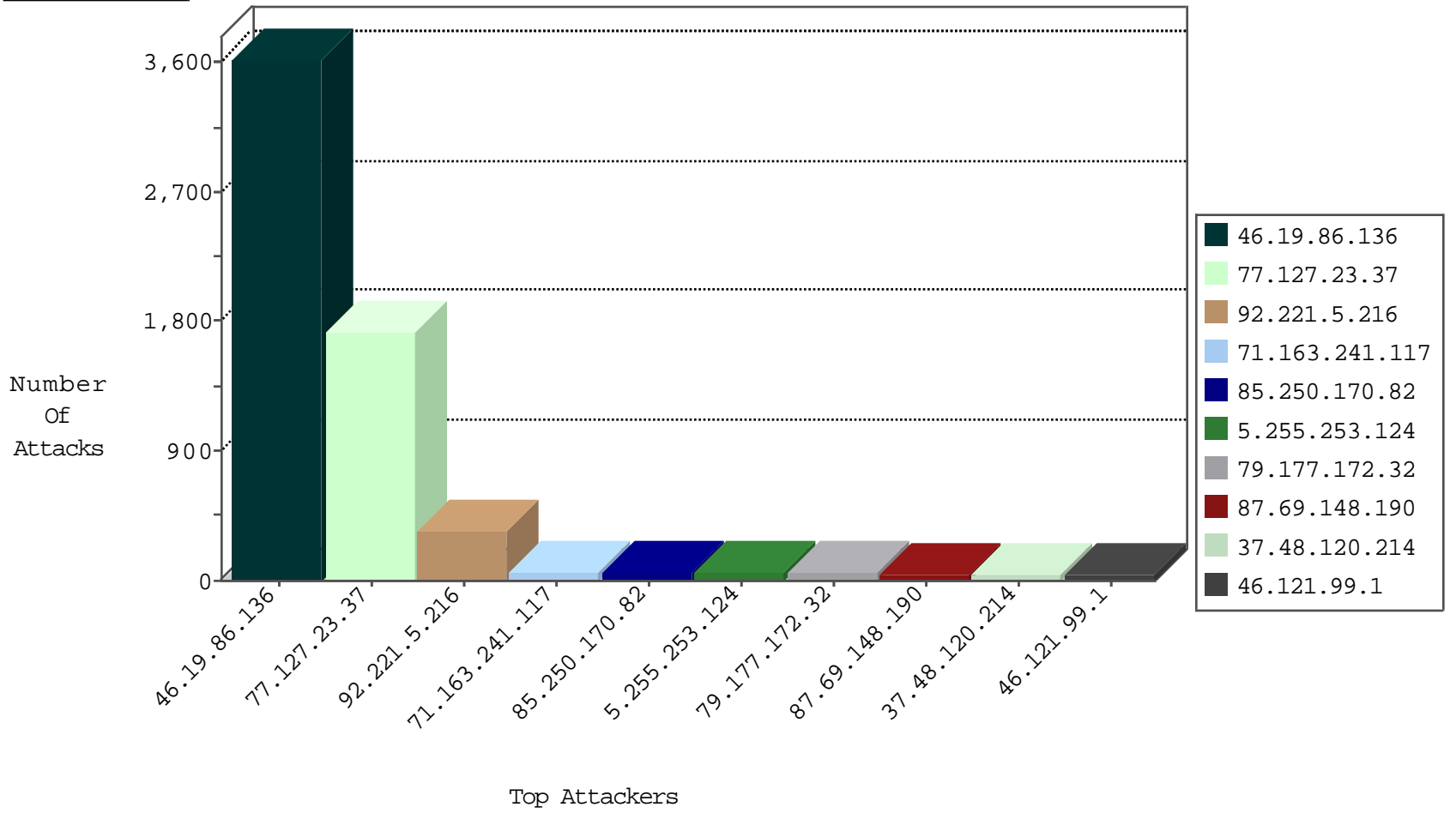


Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.67.32	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	2641
66.249.67.24	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	200
93.173.233.64	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	112
37.187.180.168	France	147.237.77.205	prisha.idf.il	JLM_Purple_Con_Limit_Http	drop	1
212.7.209.11	Netherlands	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
37.187.180.168	France	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
124.232.142.220	China	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
124.232.142.220	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
192.3.194.138	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
90.61.124.227	France	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	22
112.111.174.43	China	147.237.72.166	aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
85.25.103.50	Germany	147.237.0.17	m.ny-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	2
71.6.165.200	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	2
188.138.9.50	Germany	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	2
66.240.192.138	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.17	m.ny-kosher-kravi.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
85.25.103.50	Germany	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.33	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
66.240.192.138	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.34	yohalan.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
85.25.103.50	Germany	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.34	yohalan.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	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.50	e.tikshuv.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
188.138.9.50	Germany	147.237.77.178	e.matpash.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
71.6.165.200	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.86	navy.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
93.120.27.62	Romania	147.237.76.147	chinuch.aka.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

## 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	22
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.78.190	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	4
128.30.52.73	United States	147.237.77.233	atal.idf.il	Tehila - Perl LWP with fake user agent	2
218.3.243.223	China	147.237.76.30	hinush.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
212.7.209.11	Netherlands	147.237.0.34	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
122.228.207.77	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
212.7.209.11	Netherlands	147.237.0.17	m.ny-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.65	China	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
123.138.215.145	China	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
122.228.207.77	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
218.3.243.223	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.76.148	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
218.3.243.223	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
212.7.209.11	Netherlands	147.237.0.35	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
122.228.207.77	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
212.7.209.11	Netherlands	147.237.0.19	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.65	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
123.138.215.145	China	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
37.220.34.55	Netherlands	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
123.138.215.145	China	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -f -sS	1
122.228.207.77	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
218.3.243.223	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
46.19.86.136	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3624
77.127.23.37	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1732
92.221.5.216	Norway	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	349
71.163.241.117	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	62
85.250.170.82	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	59
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	59
79.177.172.32	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	49
87.69.148.190	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
46.121.99.1	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
79.183.171.112	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
79.176.114.69	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
109.65.49.93	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
176.12.145.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
94.230.80.207	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
136.243.36.88	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
87.68.36.8	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
176.12.149.96	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
5.29.107.185	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
176.12.147.252	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
160.39.123.123	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
176.12.138.11	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
66.249.64.72	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
92.243.181.74	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
93.173.131.39	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
109.253.146.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
54.72.73.168	United States	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	12
75.126.221.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
152.231.31.34		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
212.179.21.195	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
87.69.86.244	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
79.178.102.229	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
66.249.64.74	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
37.26.147.177	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
90.61.124.227	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
217.21.7.197	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
66.249.64.76	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
37.8.63.152	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
87.69.44.115	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
79.182.149.121	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
46.19.86.15	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
176.12.151.134	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
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	4
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
198.46.81.7	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
89.106.244.18	Belgium	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
173.205.127.243	United States	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	2
151.236.44.13	United Kingdom	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
74.117.156.246	United States	147.237.76.42	refuah.idf.il	PHP Attempt	Block	2
50.193.224.117	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
183.54.48.73	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 183.54.48.73	Block	2
79.179.30.239	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/milum/templates/http://www.aka.idf.il/sip_storage/files/6/66556.pdf	Block	2
69.16.243.169	United States	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
50.193.224.117	United States	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	2
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1020-2.stm	Block	1
184.105.247.196	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.73.219	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
66.249.64.68	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/pratim/pirteychayal/	Block	1
136.243.36.88	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19405-he/dover.aspx)	Block	1
5.28.169.235	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/1156-he/â€?â€?internet explorer	Block	1
173.205.127.243	United States	147.237.76.42	refuah.idf.il	Distributed Admin Blocking	Block	1
66.249.67.120	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1321-he/refuah.aspx	Block	1
52.4.217.116	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/reserve/	Block	1
188.165.15.43	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9059-he/refuah.aspx	Block	1
66.249.73.229	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
66.249.64.83	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/mobile/	Block	1
151.236.44.13	United Kingdom	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
50.193.224.117	United States	147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	1
74.117.156.246	United States	147.237.76.42	refuah.idf.il	Admin Blocking	Block	1
207.46.13.1	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19020-he/dov...	Block	1
66.249.67.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8728-he/refuah.aspx	Block	1
89.204.74.178	Russian Federation	147.237.77.176	matpash.idf.il	Distributed Unknown HTTP Request Method	Block	1
66.249.64.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
68.180.228.251	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
192.116.94.12	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19396-he/idfgdover.aspx	Block	1
66.249.64.88	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	1
207.46.13.104	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	1
66.249.73.166	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/m/	Block	1
112.111.174.43	China	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 112.111.174.43	Block	1
66.249.64.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
69.16.243.169	United States	147.237.72.166	aka.idf.il	Admin Blocking	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
195.211.188.16	Ukraine	147.237.77.176	matpash.idf.il	Distributed Unknown HTTP Request Method	Block	1
66.249.65.13	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
157.55.39.5	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/console/core/doc_mgr/general.aspx	Block	1
50.193.224.117	United States	147.237.77.170	maarachot.idf.il	Distributed Admin Blocking	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	1
212.76.7.234	Kazakstan	147.237.77.176	matpash.idf.il	Distributed Unknown HTTP Request Method	Block	1