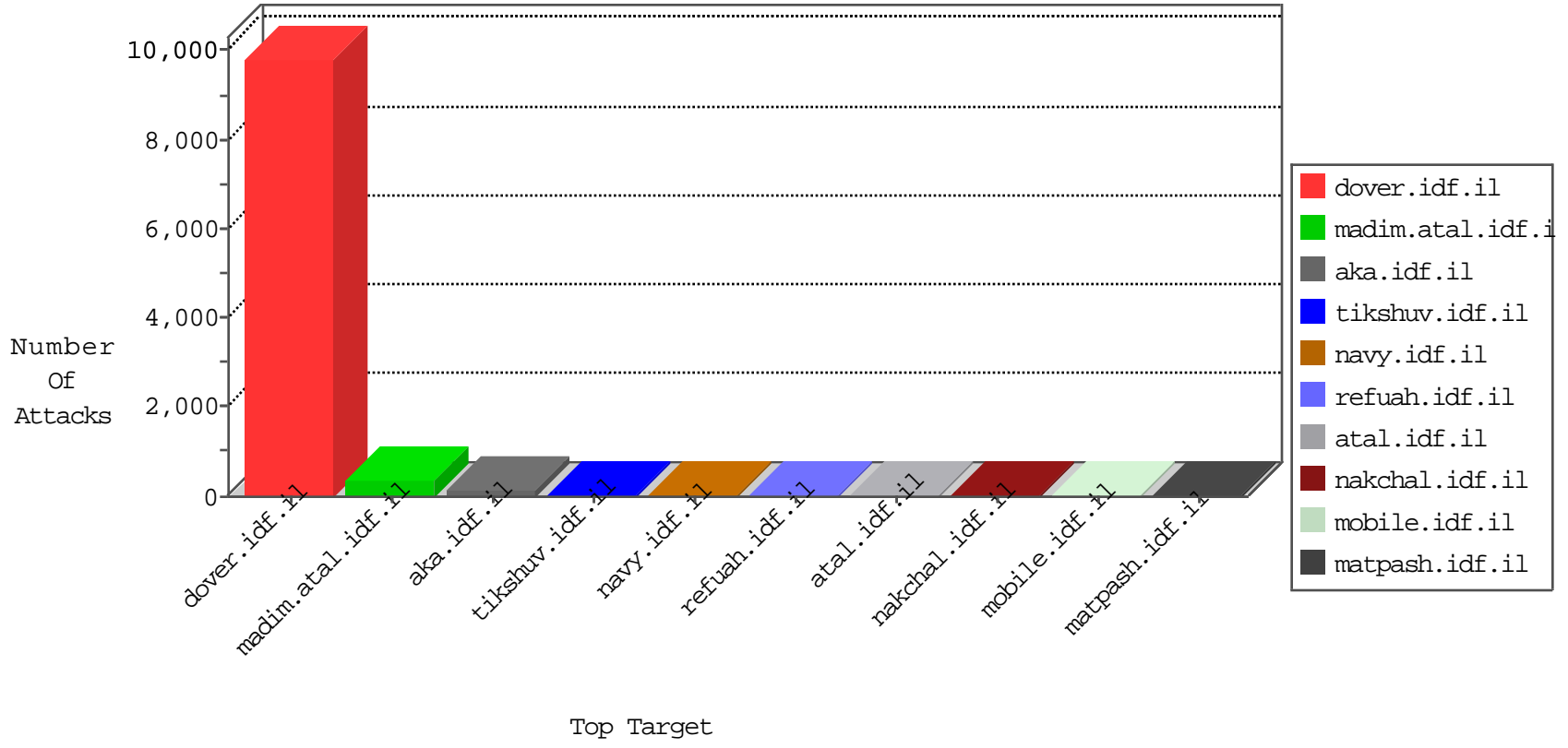


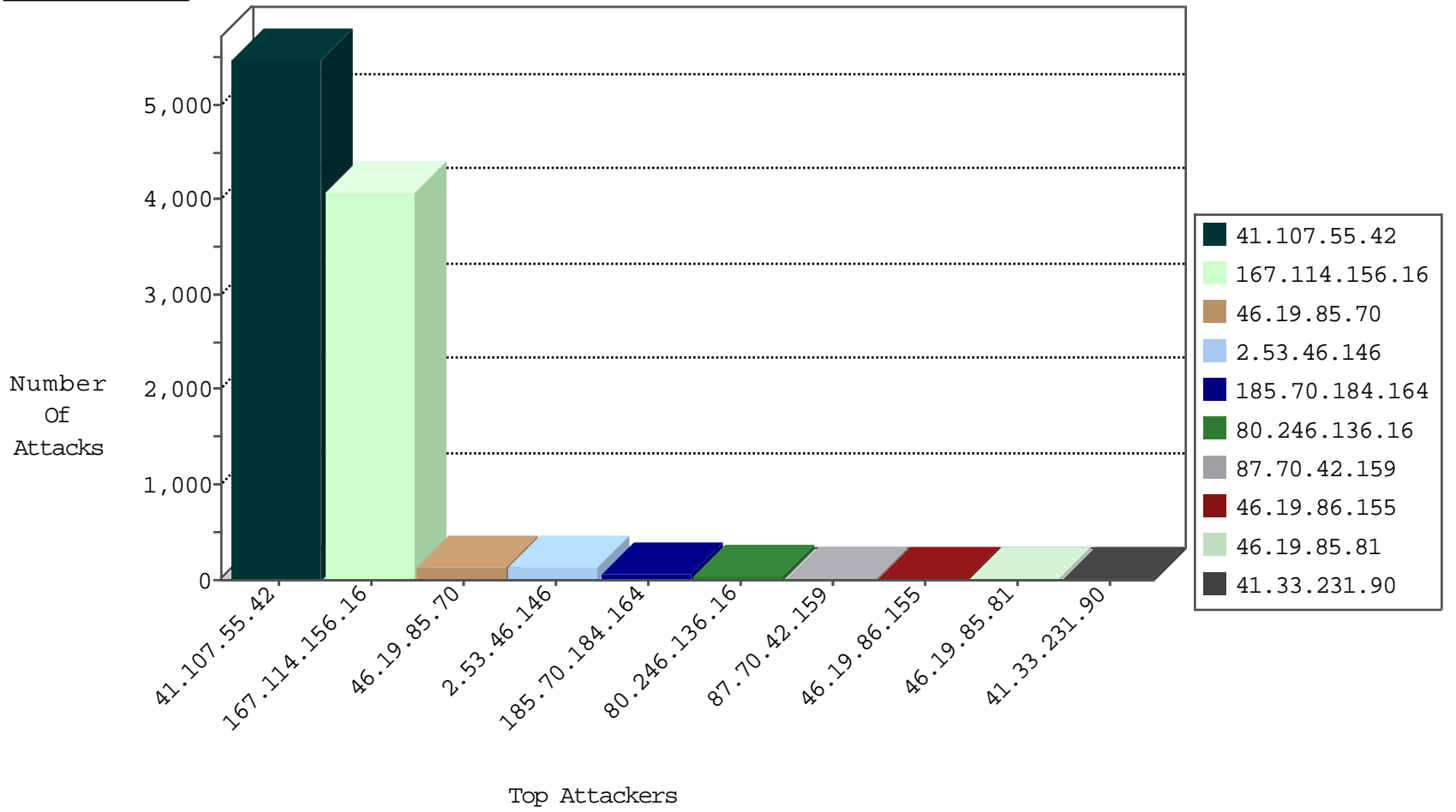
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.107.55.42	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5038
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4069
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
101.201.147.32	China	147.237.76.42	refuah.idf.il	block-sp-trafl	forward	2
45.32.95.13	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.28.156.130	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
109.64.153.33	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
84.108.246.13	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.187	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
52.27.10.0	United States	147.237.72.166	aka.idf.il	C1000016: HTTP: administrator in URI	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
114.199.230.194	147.237.76.201	Korea, Republic of	e.atal.idf.il	ET SCAN NMAP -f -sS	1
89.248.167.131	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.38	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
52.27.10.0	147.237.72.166	United States	aka.idf.il	SERVER-WEBAPP admin.php access	1
185.70.184.178	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN Potential SSH Scan	1
114.199.230.194	147.237.76.201	Korea, Republic of	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
113.240.250.154	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.167.131	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.8	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
46.151.52.139	147.237.76.38	Ukraine	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
114.199.230.194	147.237.76.201	Korea, Republic of	e.atal.idf.il	ET SCAN NMAP -sS window 2048	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.107.55.42	Algeria	147.237.77.216	dover.idf.il	drop		drop	290
41.107.55.42	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	58
41.107.55.42	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
41.107.55.42	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	17
45.59.183.88	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
155.254.239.34	Iraq	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
5.102.201.108	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.65.164.183	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.180.192.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.81	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.130.225.96	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.188.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.161.182.53	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.67.114.131	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
185.3.147.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.81	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.178.232.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.81	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
109.65.112.43	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
87.69.220.99	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.81	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
109.65.112.43	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
85.167.157.83	Norway	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.102.195.128	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
157.55.39.32	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.67.223.247	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
84.228.237.104	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.154.254.160	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.69.220.99	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.179.49.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.5.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.148.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.3.147.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.41.62	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.102.254.101	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.22.131.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.98.249	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.173	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.253.210.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.142	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.70	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.179.171.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.149.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.141	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
2.55.58.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.76.225	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.46.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	127
46.19.85.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	127
80.246.136.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
87.70.42.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
46.19.86.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	9
79.177.21.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
37.26.146.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.181.101.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
149.50.24.121	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	3
46.19.86.248	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	3
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.85.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.44.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
52.27.10.0	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.53.13.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
149.50.24.121	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/894-he/	Block	2
93.173.185.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
95.86.98.46	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 95.86.98.46	Block	1
82.166.240.200	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/general/mobile	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9237-he/refuah.aspx	Block	1
207.46.13.169	United States	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 207.46.13.169	Block	1
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-9903-	Block	1
54.173.113.175	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/news	Block	1
92.103.168.50	France	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
197.116.40.86	Algeria	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
52.27.10.0	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/wp-login.php	Block	1
95.86.98.46	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/9/	Block	1
84.228.237.104	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/giyus/login.aspx	Block	1
37.26.149.213	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/sachar/faq.aspx	None	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
93.86.76.84		147.237.77.216	dover.idf.il	PHP Attempt	Block	1
197.116.40.86	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/admin	Block	1
52.27.10.0	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/admin.php	Block	1
106.186.113.132	Japan	147.237.76.31	nakchal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
85.65.109.18	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.46.41.62	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/1228-he/refuah.aspx	Block	1
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/main/drushim/misrot.aspx	Block	1
149.50.24.121	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 149.50.24.121	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
93.86.76.84		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
81.111.195.163	United Kingdom	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
207.46.13.23	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/links.aspx	Block	1
54.173.9.10	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/checksite/custom-error-page-test	Block	1
109.64.193.137	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
87.69.78.152	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1