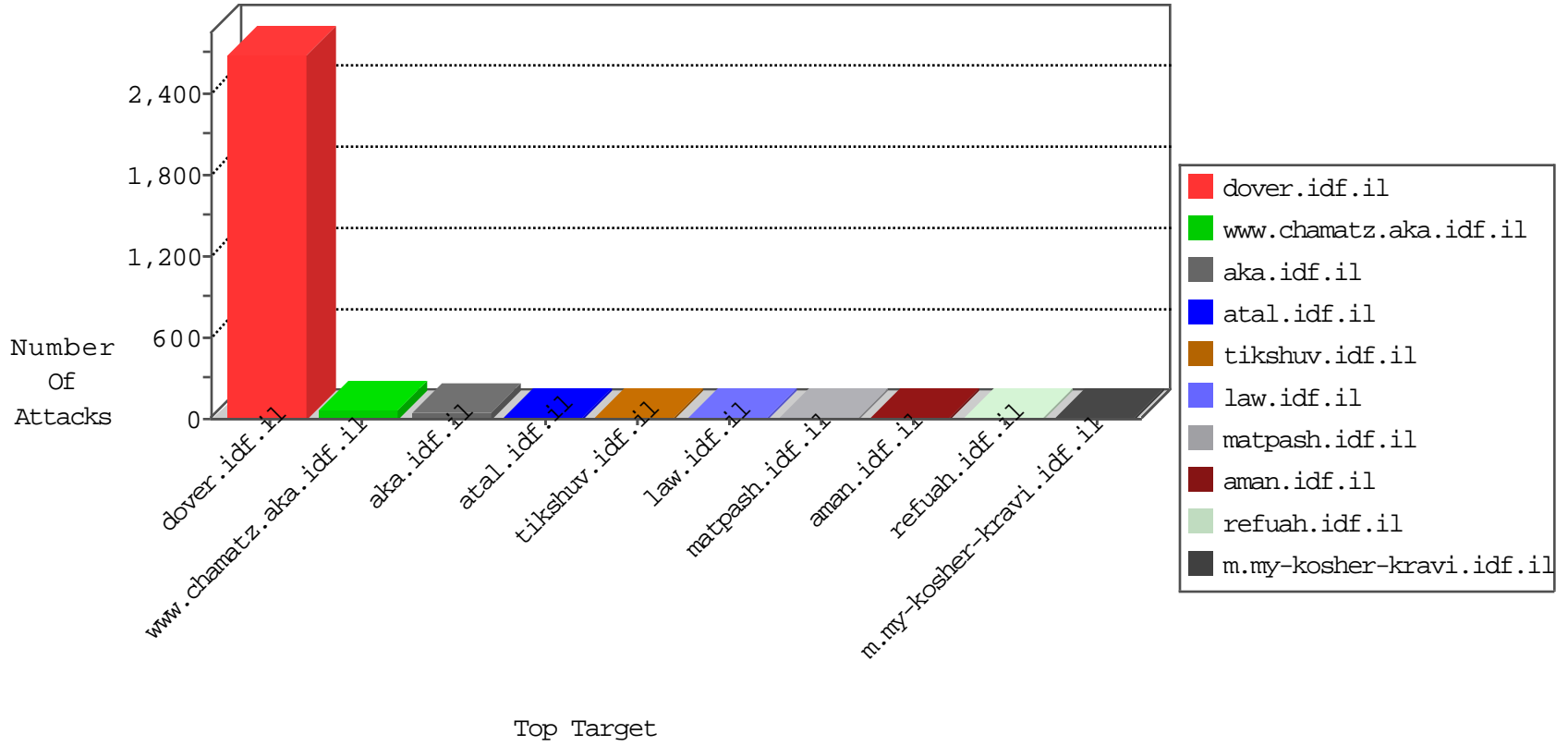


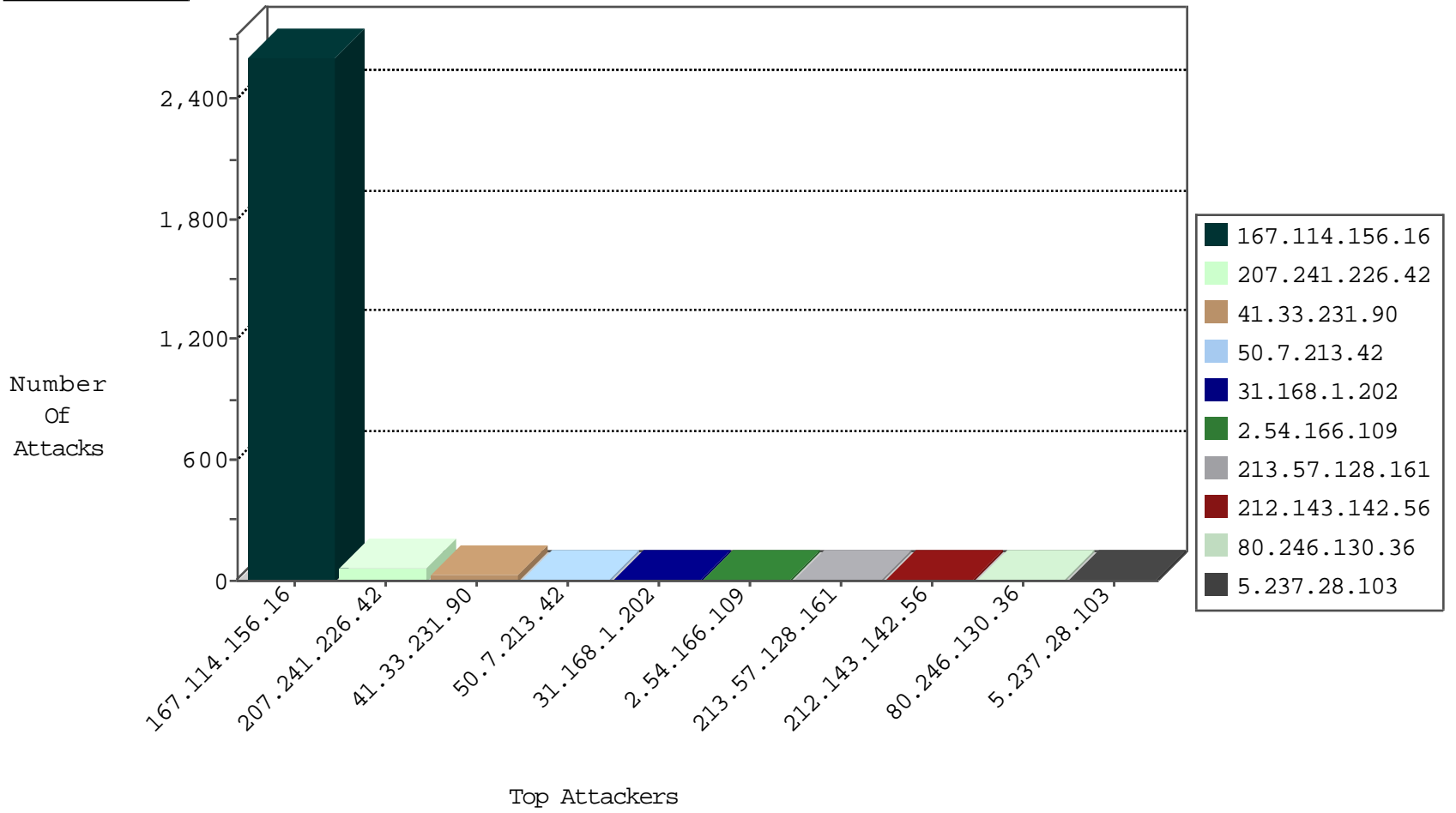
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3377
66.249.66.75	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	78
202.112.51.96	China	147.237.77.233	atal.idf.il	block-sp-traf1	drop	1
118.193.21.98	China	147.237.76.148	ggcenter.aka.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
50.7.213.42	Czech Republic	147.237.77.233	atal.idf.il	C1000196: HTTP: Block admin login to gov.il sites ?q=user	Block	1
165.215.209.15	United States	147.237.77.216	dover.idf.il	14511: HTTP: Win32/Oliga Fake User Agent	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	4
210.211.99.242	147.237.8.14	Vietnam	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
210.211.99.242	147.237.0.17	Vietnam	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.238.82.132	147.237.72.167	Ukraine	ishurim.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
69.250.11.122	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 4096	1
50.7.213.42	147.237.77.233	Czech Republic	atal.idf.il	SERVER-WEBAPP admin.php access	1
210.211.99.242	147.237.0.35	Vietnam	akaws.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
193.105.134.220	147.237.77.179	Sweden	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
91.218.246.103	147.237.8.45	Russian Federation	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
213.57.128.161	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.86.177	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
93.173.242.207	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
80.246.130.36	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
95.108.158.145	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.237.28.103	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
31.168.1.202	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
31.168.1.202	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
31.168.1.202	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
5.237.28.103	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
79.111.185.130	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
37.26.147.137	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
209.126.116.147	United States	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.87	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
195.62.53.168	Russian Federation	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.52.53.196	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.69	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
149.88.23.68	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.86.176	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
31.168.1.202	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
195.62.53.168	Russian Federation	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.18.134.194	Russian Federation	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.71	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
84.211.168.23	Norway	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.19.85.45	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
213.57.74.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
149.88.156.167	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.121.179	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.176	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
202.112.51.96	China	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.18.134.194	Russian Federation	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.72	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
84.211.168.23	Norway	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.45	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
213.57.74.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
31.168.1.202	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
157.55.39.164	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.121.180	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
206.253.226.23	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
146.185.239.102	Russian Federation	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
89.139.8.195	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.81	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
31.168.1.202	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.68	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
207.241.226.42	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 207.241.226.42	Block	57
2.54.166.109	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 2.54.166.109	Block	7
50.7.213.42	Czech Republic	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 50.7.213.42	Block	3
193.201.224.186	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
212.199.53.161	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
93.173.25.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
50.7.213.42	Czech Republic	147.237.77.233	atal.idf.il	Multiple Admin Blocking from 50.7.213.42	Block	2
50.7.213.42	Czech Republic	147.237.77.233	atal.idf.il	PHP Attempt	Block	2
176.228.128.6	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
207.241.226.42	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/a	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
50.7.213.42	Czech Republic	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/wp-login.php	Block	1
197.37.37.121	Egypt	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1
41.44.154.80	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
109.65.74.132	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
93.172.33.206	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	1
66.249.66.72	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/pages/reports.aspx	Block	1
207.46.13.88	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
50.7.213.42	Czech Republic	147.237.77.233	atal.idf.il	Admin Blocking	Block	1
2.54.19.154	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
95.108.158.144	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8853-he/refuah.aspx	Block	1
54.153.32.246	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
198.20.69.74	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
41.44.154.80	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
109.65.74.132	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
207.241.226.42	United States	147.237.77.226	www.chamatz.aka.idf.il	Distributed PHP Attempt	Block	1
66.249.66.75	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/sfgsfdfs.aspx	Block	1
193.201.224.186	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 193.201.224.186	Block	1
105.102.253.64	Algeria	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	1
79.179.125.77	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
54.153.33.233	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
157.55.39.64	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
41.109.132.240	Algeria	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
94.180.164.253	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	1
66.249.66.126	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71850-he/maarachot.aspx	Block	1
193.201.224.186	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
2.54.166.109	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/1048-7488-he/tikshuv.asp	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
80.246.130.36	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
157.55.39.185	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
41.109.132.240	Algeria	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
95.30.58.76	Russian Federation	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/9/	Block	1
207.241.226.42	United States	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/926-he/refuah.aspx	Block	1
197.37.37.121	Egypt	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
5.175.193.164	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1