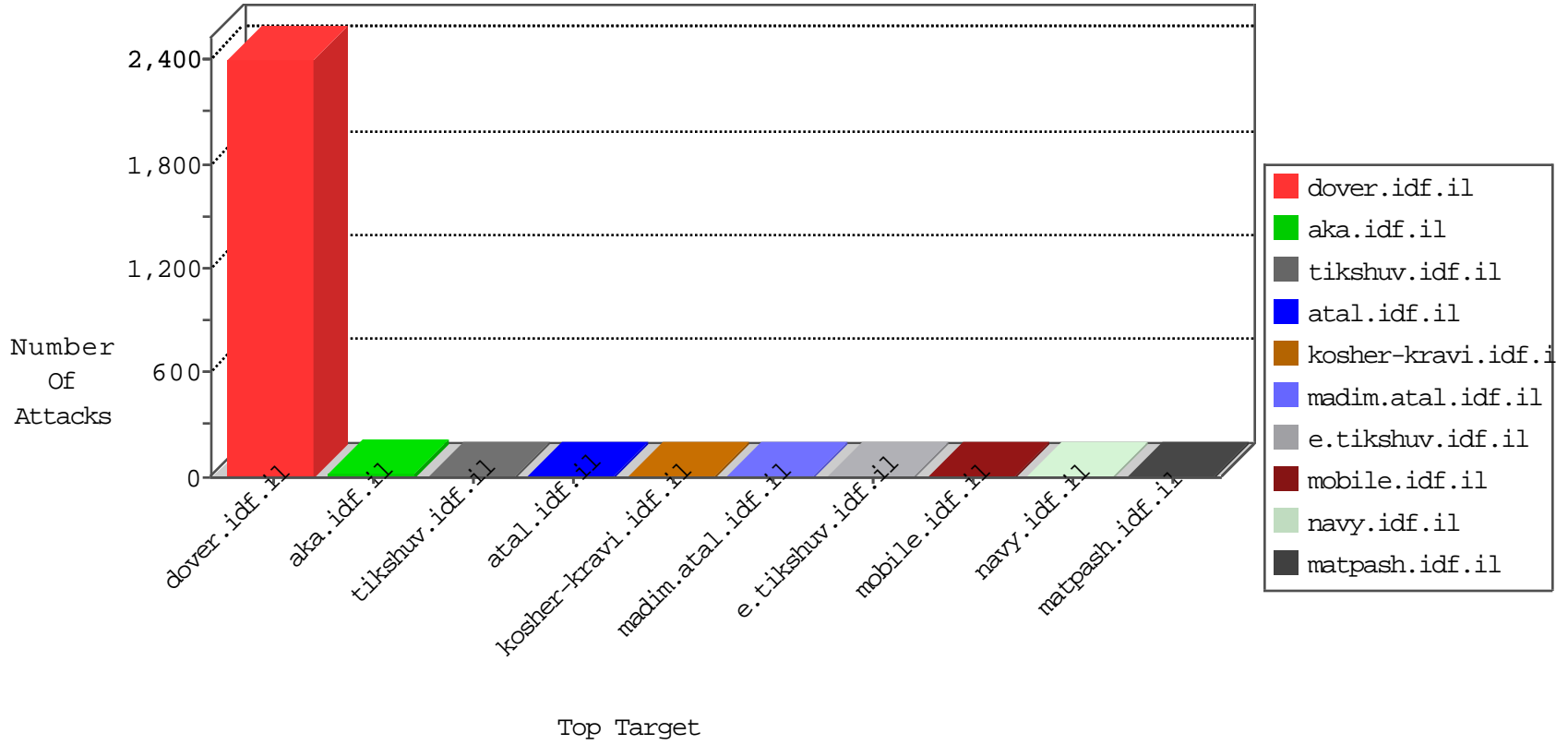




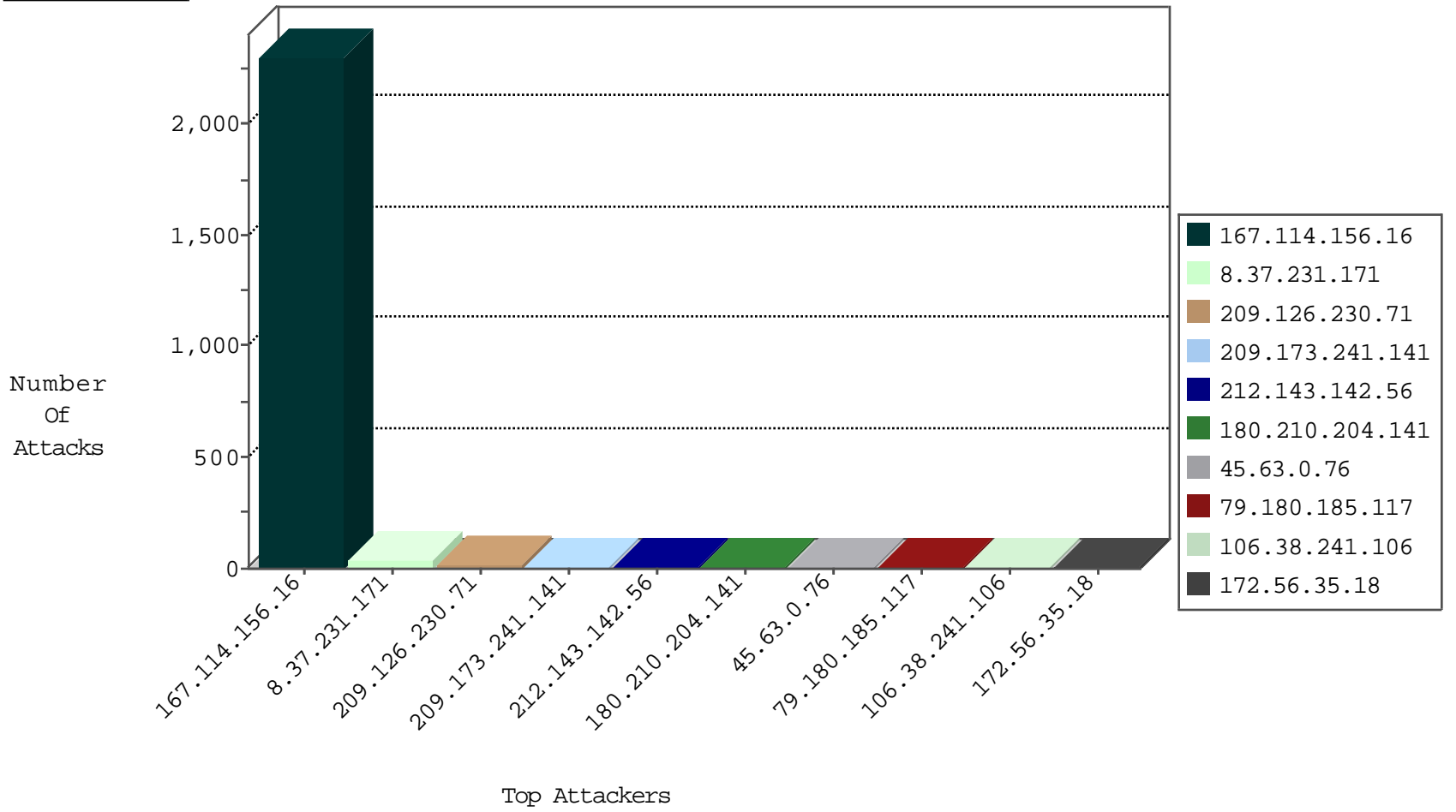
# IDF Under Attack Daily Report



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	3430
8.37.231.171	Anonymous Proxy	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
8.37.231.171	Anonymous Proxy	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
209.173.241.141	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	3
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.69.79	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
156.204.73.173		147.237.77.216	dover.idf.il	2023: HTTP: Cross Site Scripting in GET Request	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
157.55.39.122	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
207.46.13.69	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
209.173.241.141	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
208.109.53.250	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	147.237.77.216	United States	dover.idf.il	ET DROP Dshield Block Listed Source	1
193.105.134.220	147.237.8.14	Sweden	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.76.200	Ukraine	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
208.109.53.250	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential SSH Scan	1
208.109.53.250	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
185.103.252.60	147.237.76.177		ncore.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.198.210	147.237.77.19	Russian Federation	law-forum.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
8.37.231.171	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.180.185.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
172.56.35.18	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.183.207.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.105	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
209.126.230.71	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
209.126.230.71	United States	147.237.0.15	kosher-kravi.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
123.125.71.76	China	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
207.46.13.105	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
62.210.136.206	France	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
45.63.0.76		147.237.0.15	kosher-kravi.idf.il	Web Server Enforcement Violation	Masscan Port Scanner	reject	1
158.58.188.211	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.96	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
131.253.26.248	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
209.126.230.71	United States	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
185.89.217.226		147.237.76.86	navy.idf.il	Directory Traversal	directory traversal overflow	monitor	1
45.63.0.76		147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.114	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
2.53.6.82	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.221	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
209.126.230.71	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
123.125.71.76	China	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
207.46.13.152	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
65.55.218.61	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.228	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
45.63.0.76		147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
159.226.95.66	China	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.110	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
139.162.146.165	Netherlands	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
209.126.230.71	United States	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
195.62.53.168	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.120.97.101	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.139.116	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
2.54.162.127	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.222	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
209.126.230.71	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
123.125.71.76	China	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
209.126.230.71	United States	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.247.235	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
45.63.0.76		147.237.0.35	akaws.idf.il	drop		drop	1
216.218.206.118	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.211	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
85.90.244.226	United Kingdom	147.237.0.33	idf.il	drop		drop	1
197.52.172.34	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
46.120.97.101	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.204	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.86.94.7	Germany	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 80.86.94.7	Block	5
180.210.204.141	Singapore	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 180.210.204.141	Block	5
50.18.86.240	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/163-6958-en/patzar.aspx&amp	Block	2
207.46.13.105	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
183.5.116.72	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
197.52.172.34	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
185.89.216.229		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
173.247.228.10	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
68.180.229.124	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8944-he/refuah.aspx	Block	1
207.46.13.160	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.160	Block	1
197.38.175.202	Egypt	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
183.5.116.72	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 183.5.116.72	Block	1
66.249.64.37	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
197.52.172.34	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
185.89.216.230		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
173.247.228.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
209.126.230.71	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to /	Block	1
68.180.230.189	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
197.38.175.202	Egypt	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
183.5.116.72	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
80.86.94.7	Germany	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
198.20.69.74	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
185.89.216.232		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
209.126.230.71	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to /	Block	1
68.180.230.189	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
197.38.175.202	Egypt	147.237.76.147	chinuch.aka.idf.il	PHP Attempt	Block	1
185.89.216.225		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
94.23.219.182	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
207.46.13.32	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/contactus/contactus.aspx	Block	1
185.89.216.239		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
180.210.204.141	Singapore	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
216.218.206.66	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
68.180.230.189	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1785-he/dover.aspx	Block	1
197.38.175.202	Egypt	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/xmlrpc.php	Block	1
185.89.216.228		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
156.204.73.173		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/	Block	1
68.180.228.167	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-he/cogat.aspx	Block	1
185.89.217.226		147.237.76.86	navy.idf.il	URL is Above Root Directory www.navy.idf.il/./images/shared/home.png	Block	1
216.218.206.66	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
80.82.65.82	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1