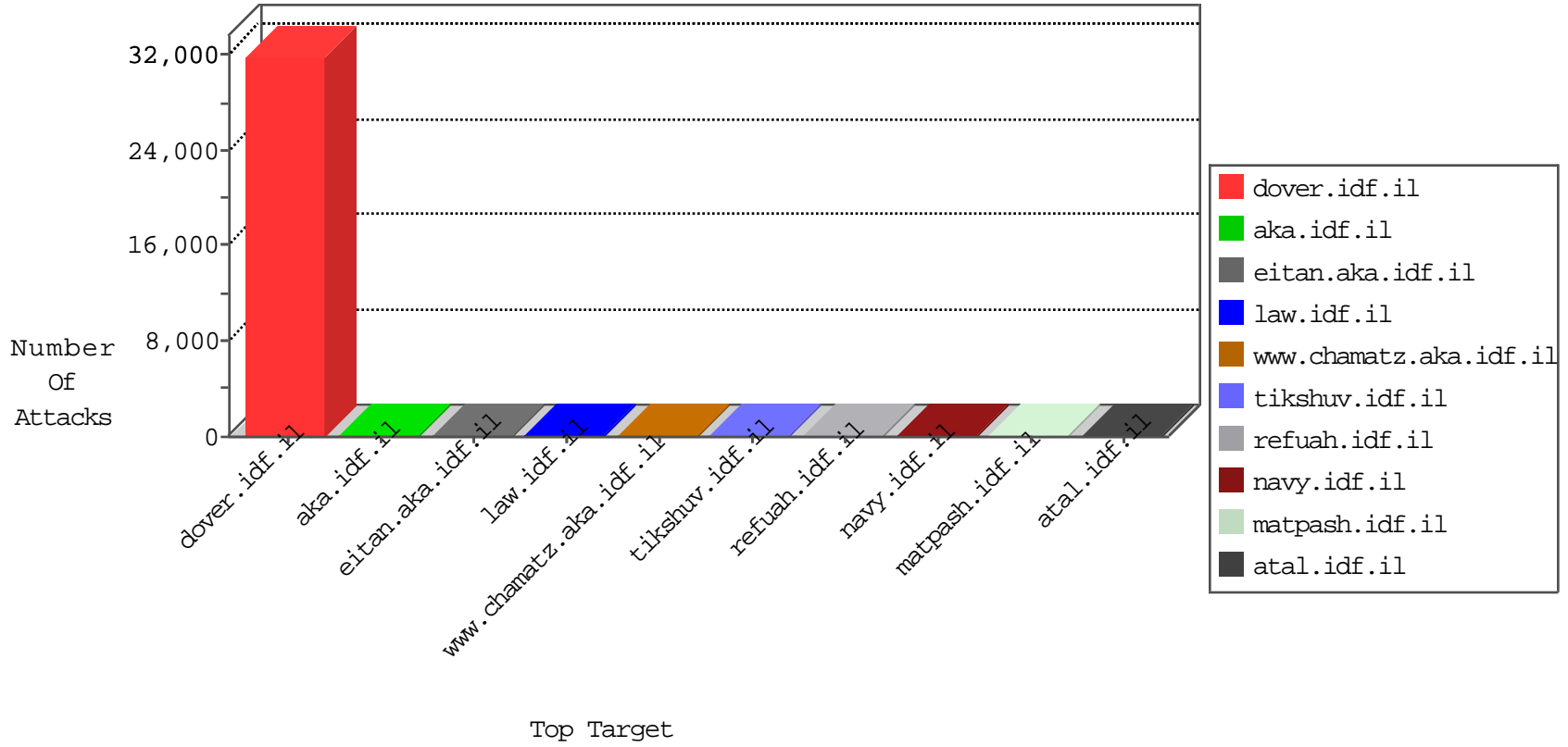


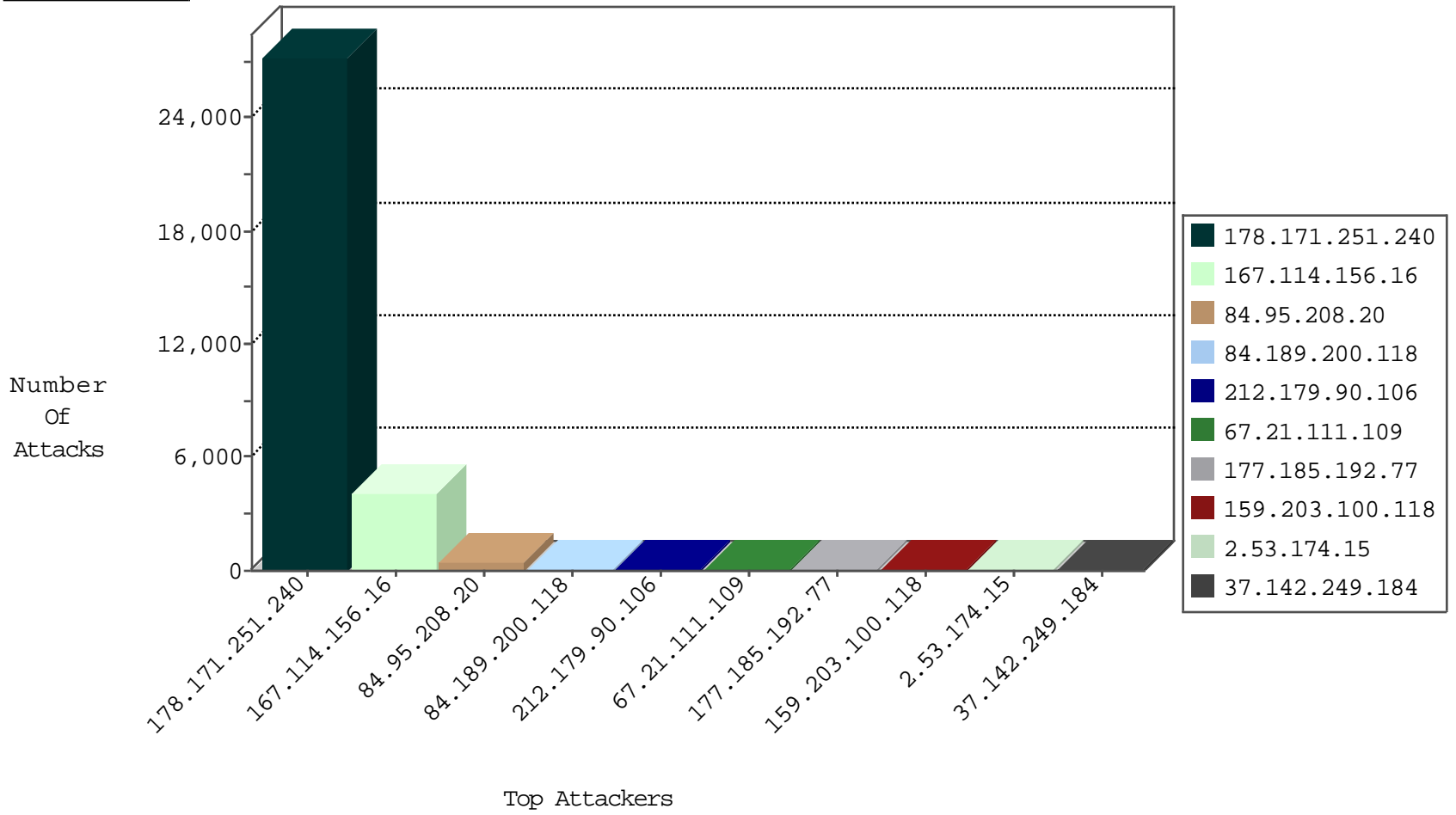
IDF Under Attack Daily Report



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	Block_Ip_Web_In	drop	4088
176.15.192.45	Russian Federation	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
179.43.141.194	Switzerland	147.237.77.235	sviva.idf.il	Block_Ntp_All_Net	drop	1
198.46.138.106	United States	147.237.77.227	e.hamaz.idf.il	Block_Udp_All_Nets	drop	1
176.15.192.45	Russian Federation	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	1
66.240.236.119	United States	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
179.43.141.194	Switzerland	147.237.8.46	e.chinuch.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
177.185.192.77	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
70.89.127.78	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
195.234.228.90	Germany	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
87.70.46.183	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
213.247.63.11	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
87.242.112.35	Russian Federation	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
59.120.255.127	Taiwan	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
66.135.63.82	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
177.185.192.77	Brazil	147.237.0.34	tikshuv.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	3
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.159	France	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
177.185.192.77	Brazil	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
177.185.192.77	147.237.0.34	Brazil	tikshuv.idf.il	SQL Injection - Select From	13
70.89.127.78	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	12
59.120.255.127	147.237.77.74	Taiwan	law.idf.il	SQL Injection - Select From	12
213.247.63.11	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	SQL Injection - Select From	12
177.185.192.77	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	11
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	11
87.242.112.35	147.237.76.42	Russian Federation	refuah.idf.il	SQL Injection - Select From	6
66.135.63.82	147.237.77.74	United States	law.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
195.234.228.90	147.237.77.216	Germany	dover.idf.il	SQL Injection - Select From	4
183.60.48.25	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
177.185.192.77	147.237.0.34	Brazil	tikshuv.idf.il	ET WEB_SERVER SQLi - SELECT and sysobject	1
198.20.69.98	147.237.77.176	United States	matpash.idf.il	ET DROP Dshield Block Listed Source	1
183.60.48.25	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
109.235.254.181	147.237.8.45	Turkey	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
46.4.79.76	147.237.76.201	Germany	e.atal.idf.il	ET SCAN Potential SSH Scan	1
198.61.229.62	147.237.0.34	United States	tikshuv.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	19147
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4083
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2637
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1122
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	109
84.189.200.118	Germany	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
84.95.208.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
67.21.111.109	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	28
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	28
159.203.100.118	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
2.53.174.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
37.142.249.184	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	SYN Attack		reject	20
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	13
2.53.159.236	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	11
155.254.215.130	Bahrain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
2.53.171.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.76.127.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.178.187.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.15.192.45	Russian Federation	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.53.160.69	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
109.66.69.18	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
188.120.154.48	Israel	147.237.77.216	dover.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
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	4
46.19.86.75	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.39.163	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
207.46.13.82	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
207.46.13.136	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.105.15.131	Poland	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.87.125.227	United States	147.237.77.176	matpash.idf.il	SYN Attack		reject	3
178.255.215.87	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.10	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
109.186.49.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	3
46.19.85.10	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.126.168.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.186.135	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

04-17-2016-02:04:03 to 04-17-2016-03:04:03

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.73	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	89
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	72
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	23
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	11
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	10
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	8
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	3
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
77.126.168.47	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	3
65.55.210.179	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
181.64.202.15	Peru	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authentication-service.asmx/getauthuser	Block	2
199.30.24.169	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
171.8.167.67	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	2
2.53.25.247	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/general/mobile	Block	2
171.8.167.70	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	2
208.54.85.173	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/main.asp	Block	2
199.30.24.99	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.39.6	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	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
171.8.167.62	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	1
52.23.117.198	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
117.78.13.29	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/894-he	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
185.6.58.20	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/general/mobile	Block	1
157.55.39.125	United States	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on nakchal.idf.il/page.asp	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/2401.jpg	Block	1
207.46.13.9	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/1132-8613-he/navy.aspx.aspx	Block	1
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	PHP Attempt	Block	1
54.210.18.124	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
124.205.8.165	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	1
194.228.13.149	Czech Republic	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/eng	Block	1
157.55.39.145	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakchal.idf.il/page.asp	Block	1
66.249.79.75	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.95.208.20	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
207.46.13.82	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.82	Block	1
54.210.18.124	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18166-	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/div.item	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
198.61.229.62	United States	147.237.0.34	tikshuv.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
157.55.39.163	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.163	Block	1
2.53.160.69	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
101.199.108.119	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	1
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1