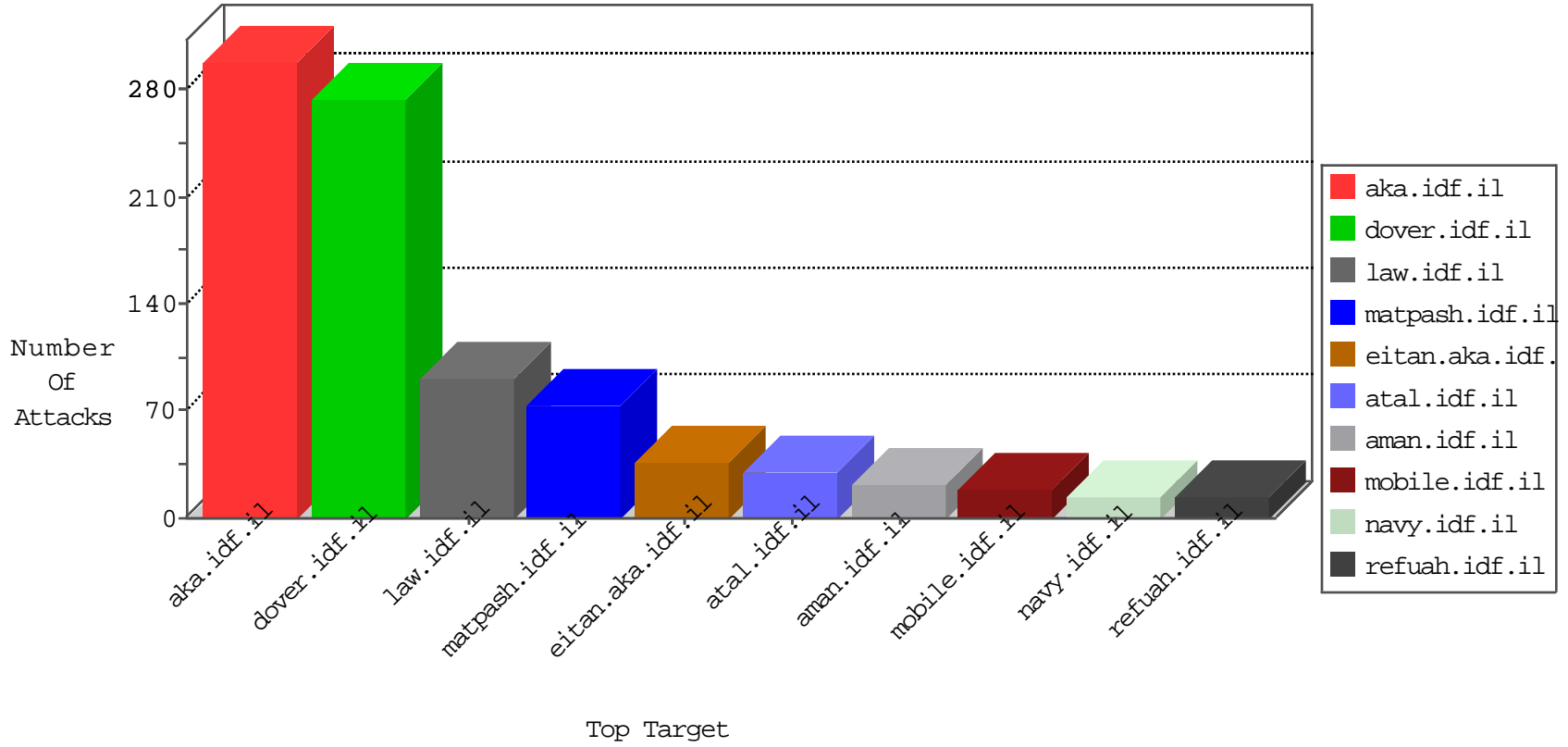


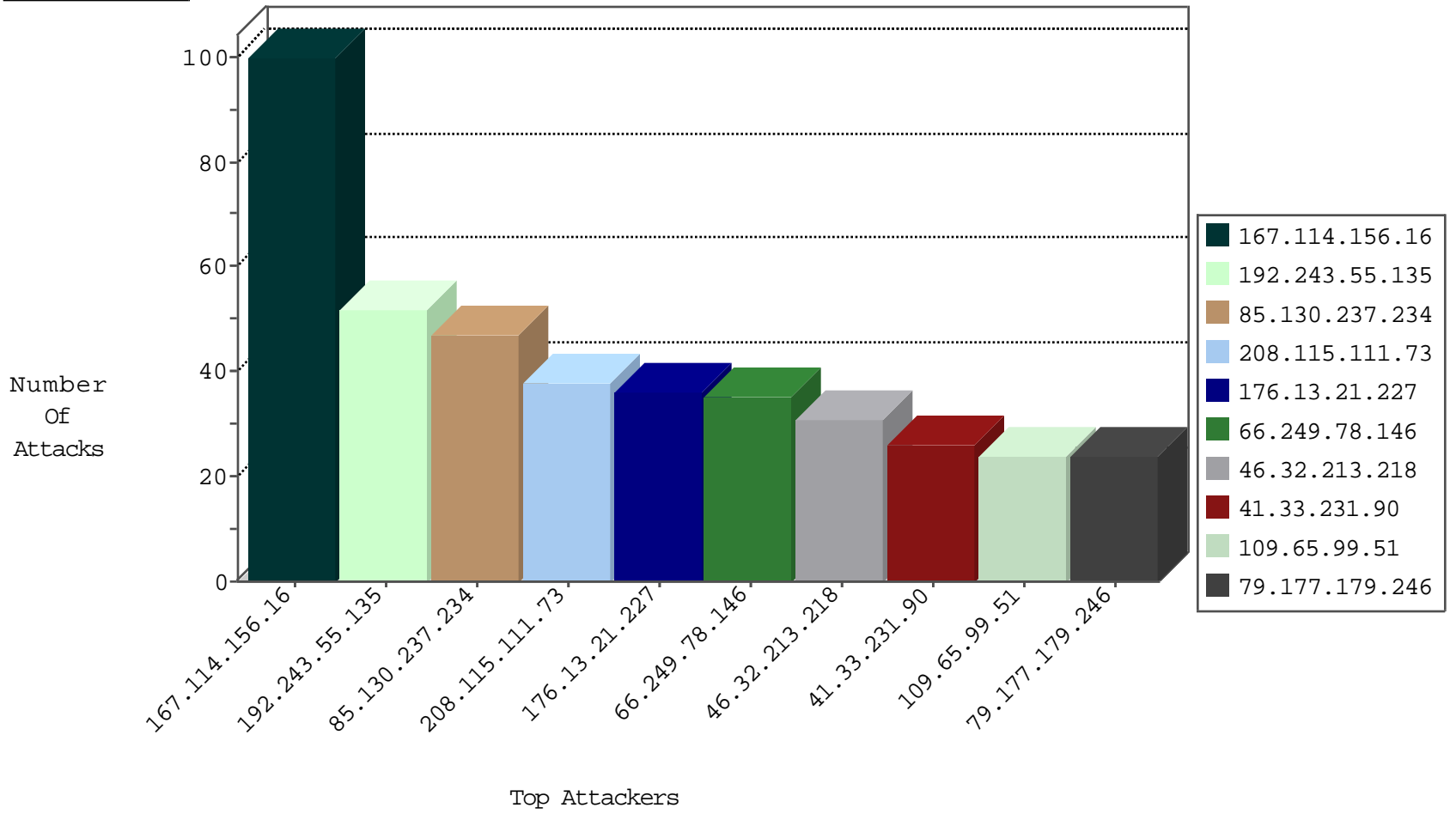
IDF Under Attack Daily Report



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	HTTP-POST-Segmented-DoS	dest-reset	7638
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7561
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	200
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	4
123.59.59.52	China	147.237.76.39	mobile.meitav.idf.il	block-sp-trafl	forward	4
180.153.91.183	China	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3
74.91.17.182	United States	147.237.76.86	navy.idf.il	block-sp-trafl	forward	2
174.59.23.134	United States	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1
104.238.135.152	United States	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.99	Lithuania	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
74.91.23.107	United States	147.237.77.233	atal.idf.il	block-sp-trafl	drop	1
93.174.93.50	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.99	Lithuania	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
173.208.197.254	United States	147.237.77.205	prisha.idf.il	block-sp-trafl	drop	1
94.102.52.10	Netherlands	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.99	Lithuania	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
94.245.88.135	United Kingdom	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3

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	3
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.165	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
198.20.69.98	147.237.76.44	United States	e.refuah.idf.il	ET DROP Dshield Block Listed Source	1
188.14.242.67	147.237.8.14	Italy	e.orchot.idf.il	ET SCAN NMAP -sS window 4096	1
183.61.109.189	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
173.65.154.27	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
109.72.215.18	147.237.8.46	United Kingdom	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
40.114.42.13	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
183.61.109.189	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 4096	1
183.60.48.25	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
162.221.204.132	147.237.77.74	Canada	law.idf.il	ET SCAN NMAP -sS window 4096	1
80.82.78.38	147.237.0.16	Netherlands	my-kosher-kravi.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
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
176.13.21.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
46.32.213.218	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	27
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	26
85.130.237.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
109.65.99.51	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
94.217.189.82	Germany	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	22
79.179.231.180	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
207.241.231.194	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	19
141.0.14.74	Europe	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	18
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
85.130.237.234	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.243.55.135	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
79.177.179.246	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
68.65.164.38	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
80.246.136.63	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
79.177.179.246	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
79.177.179.246	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
46.19.85.90	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.94.114.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.162.127	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.66.50	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
95.86.104.64	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.64.170.95	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.199	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.106.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.8.165	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
105.208.143.65	South Africa	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.135	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	5
85.130.237.234	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
157.55.39.37	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.34.165.73	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
63.251.215.25	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
85.130.237.234	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
109.64.162.127	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
192.243.55.134	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
85.130.237.234	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
141.0.15.23	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
105.208.143.65	South Africa	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.93.249	Europe	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
5.28.130.244	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 5.28.130.244	Block	5
109.64.170.95	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 109.64.170.95	Block	4
109.64.170.95	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
149.88.55.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
184.94.157.18	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	2
149.78.109.8	United States	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.177.37.254	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatgauntity.aspx	Block	2
84.109.113.216	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	2
84.111.102.209	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam/asp/personalentrance.asp	Block	1
17.142.156.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
184.94.157.18	United States	147.237.77.74	law.idf.il	Admin Blocking	Block	1
123.59.59.52	China	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to www.ctrip.com/1428-he/meitav.aspx	Block	1
79.179.231.180	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1274-he/atal.aspx	Block	1
199.30.24.246	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
51.254.121.188	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman-->	Block	1
157.55.2.151	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
93.158.152.202	Russian Federation	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
66.249.66.185	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/contactus/contactus.aspx	Block	1
37.26.149.173	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
184.94.157.18	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 184.94.157.18	Block	1
128.238.182.61	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;catid in www.aka.idf.il/rights/asp/info.asp	None	1
80.246.133.141	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
208.115.111.73	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kamlar/eur1.axd/fb6bc0383fdbd043abfcf49f14d751c2/	Block	1
54.210.18.124	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Untraceable SSL Sessions from 169.229.3.91 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
105.107.91.38	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip-staro fe/dover	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
40.77.167.89	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 40.77.167.89	Block	1
84.94.169.199	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 84.94.169.199	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
51.254.121.188	France	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/1093-7963-he/.aspx	Block	1
184.94.157.18	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/wp-login.php	Block	1
149.78.132.120	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.64.143	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/userdetails/forgotpassword.aspx	Block	1
5.28.130.244	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/images/shared/active_menu_item.gif"	Block	1
169.229.3.91	United States	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.178.37.197	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1412-he/atal.aspx	Block	1
51.254.121.188	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 51.254.121.188	Block	1
199.30.24.60	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1