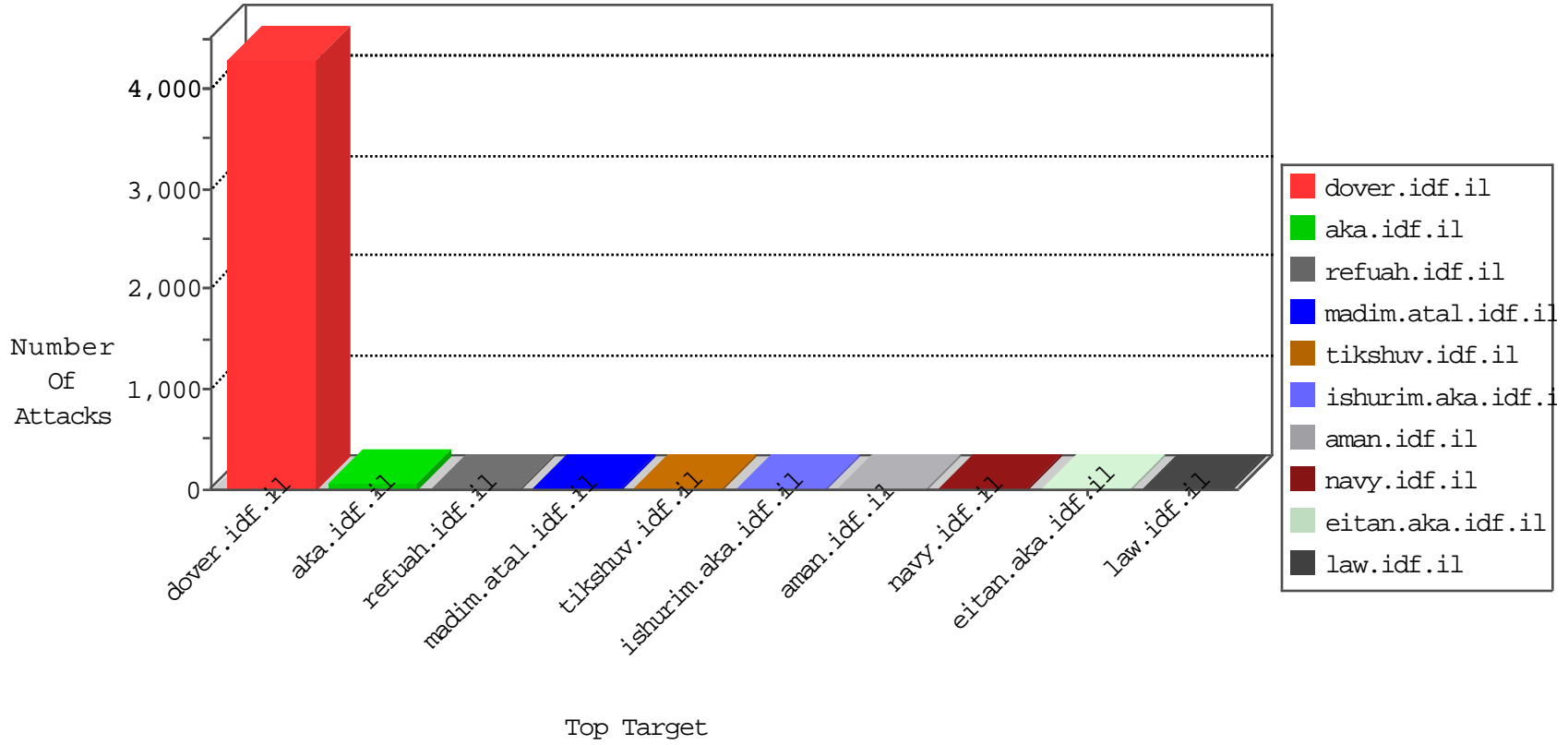


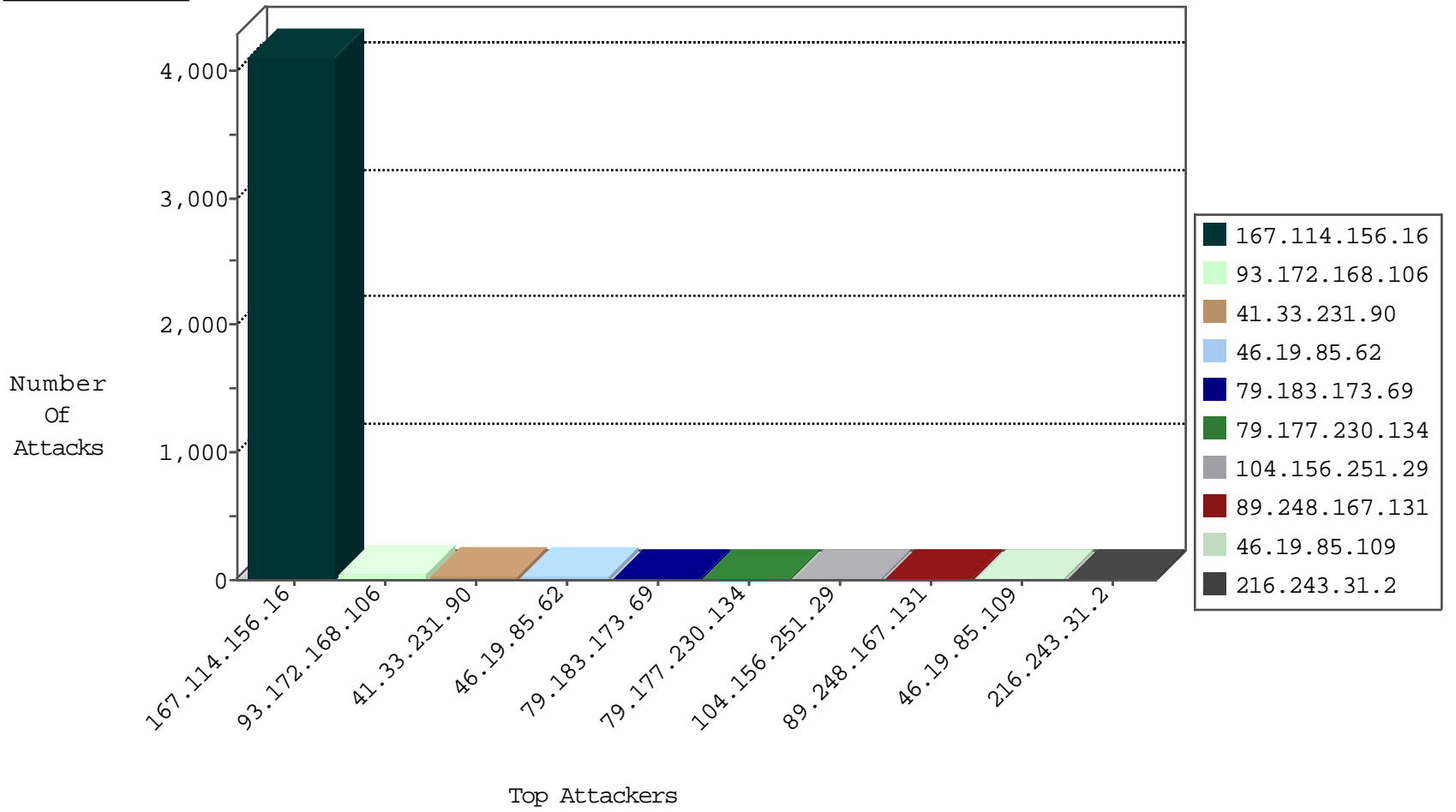
IDF Under Attack Daily Report



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	4112
78.83.111.251	Bulgaria	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	4
79.182.36.215	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
94.102.49.116	Netherlands	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
94.102.52.10	Netherlands	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.229.28.153	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
106.120.173.139	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	8
79.179.113.100	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
123.126.113.19	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.150	Israel	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
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
104.156.251.29	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
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
14.39.145.19	147.237.76.34	Korea, Republic of	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
89.248.167.131	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
87.229.116.42	147.237.0.200	Hungary	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
195.216.176.244	147.237.0.19	Latvia	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
61.182.170.38	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
36.84.76.230	147.237.8.45	Indonesia	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.167.131	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
201.33.34.103	147.237.0.15	Brazil	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
80.82.78.38	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
61.182.170.38	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.77.234	Netherlands	halag.idf.il	ET SCAN Potential SSH Scan	1
36.84.76.230	147.237.76.30	Indonesia	himush.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.167.131	147.237.77.74	Netherlands	law.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
93.172.168.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
46.19.85.62	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
79.183.173.69	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
46.19.85.109	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.93	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	10
37.142.73.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.41.89	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.230.134	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.177.230.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.177.50.57	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
109.60.84.182	Croatia	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	5
79.177.230.134	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
79.180.170.112	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.216.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.19.19	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
2.53.39.108	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
176.13.7.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.29	United States	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.179.241.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.53.144.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.189.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.69.83.74	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
213.57.45.97	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
87.70.126.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.177.83.126	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
207.46.13.183	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
2.53.51.208	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
79.177.3.203	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
87.69.83.74	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
23.101.61.176	Ireland	147.237.77.216	dover.idf.il	Instant Messengers	instant messenger pattern found, application: Skype	monitor	1
141.212.122.213	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
79.177.3.203	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
108.61.228.87	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.243.31.2	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.117.212.53	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.91	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
41.216.161.147	Nigeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
84.108.43.112	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
149.88.37.63	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
5.22.131.116	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
79.177.172.190	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
109.253.224.37	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
216.243.31.2	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
79.176.95.15	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
106.186.113.132	Japan	147.237.0.35	akaws.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	1
37.46.41.187	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.214	United States	147.237.72.167	ishurim.aka.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
149.88.37.63	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 149.88.37.63	Block	7
109.64.239.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
104.156.251.29	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 104.156.251.29	Block	5
104.156.251.29	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	4
46.19.85.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.131	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/newsflash/mobile	Block	3
104.156.251.29	United States	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 104.156.251.29	Block	3
46.19.85.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
208.105.66.42	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
219.74.148.111	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
149.88.37.63	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	1
93.196.126.52	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.102.7.226	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
199.30.16.165	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
24.36.51.39	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en	Block	1
104.156.251.29	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
157.55.2.182	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
104.156.251.29	United States	147.237.72.166	aka.idf.il	Admin Blocking	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
207.46.13.11	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in tikshuv.idf.il/site/general.aspx	Block	1
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
46.19.85.238	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/nav.css	Block	1
173.251.20.242	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.146	Block	1
141.212.122.209	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
79.183.173.69	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
62.210.254.52	France	147.237.72.166	aka.idf.il	Unknown Parameter &bc in www.aka.idf.il/main/gyus/captcha.ashx	None	1
173.252.115.8	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gyus/html/newsservice.aspx/js	Block	1
213.57.157.177	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
89.138.198.224	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
65.55.210.96	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
176.13.15.39	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
66.249.78.230	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/apple-app-site-association	Block	1