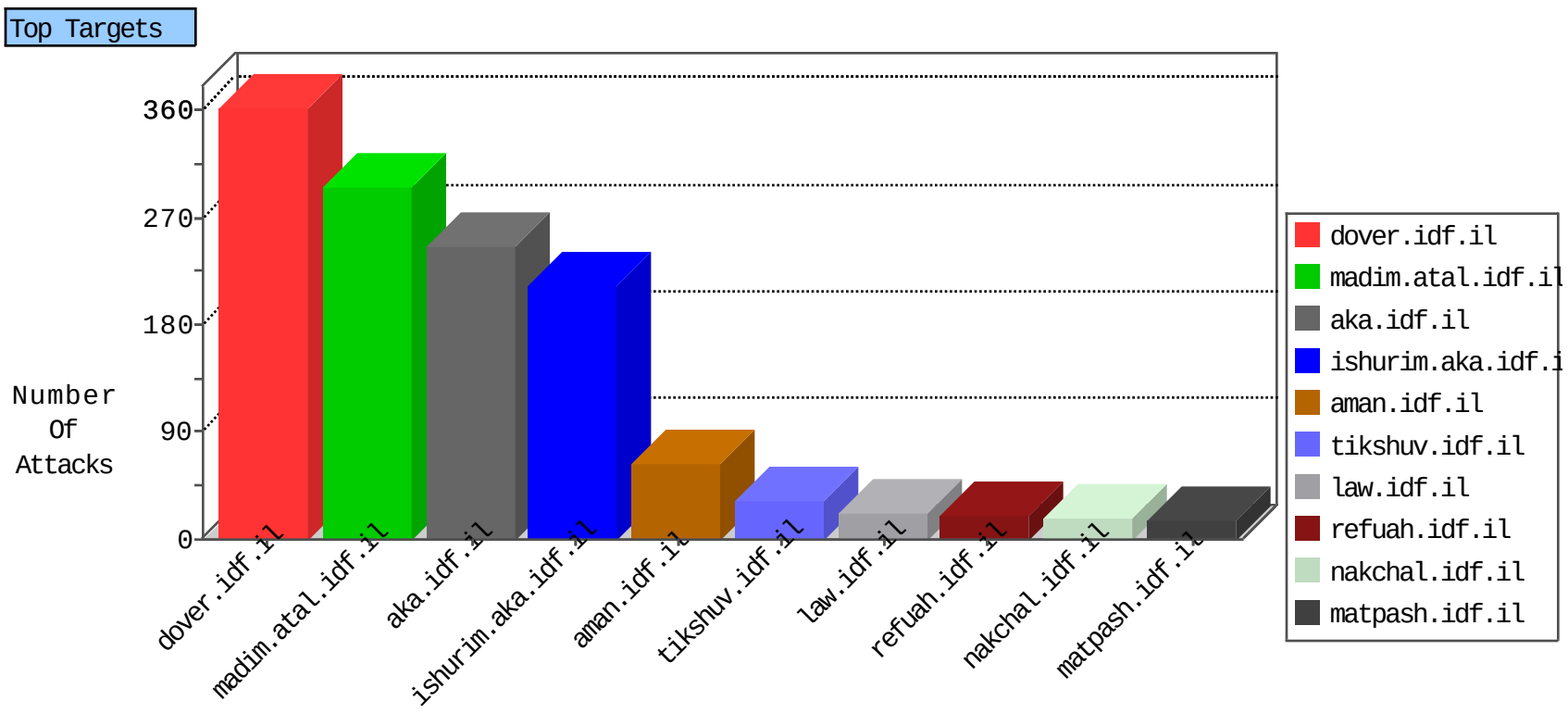
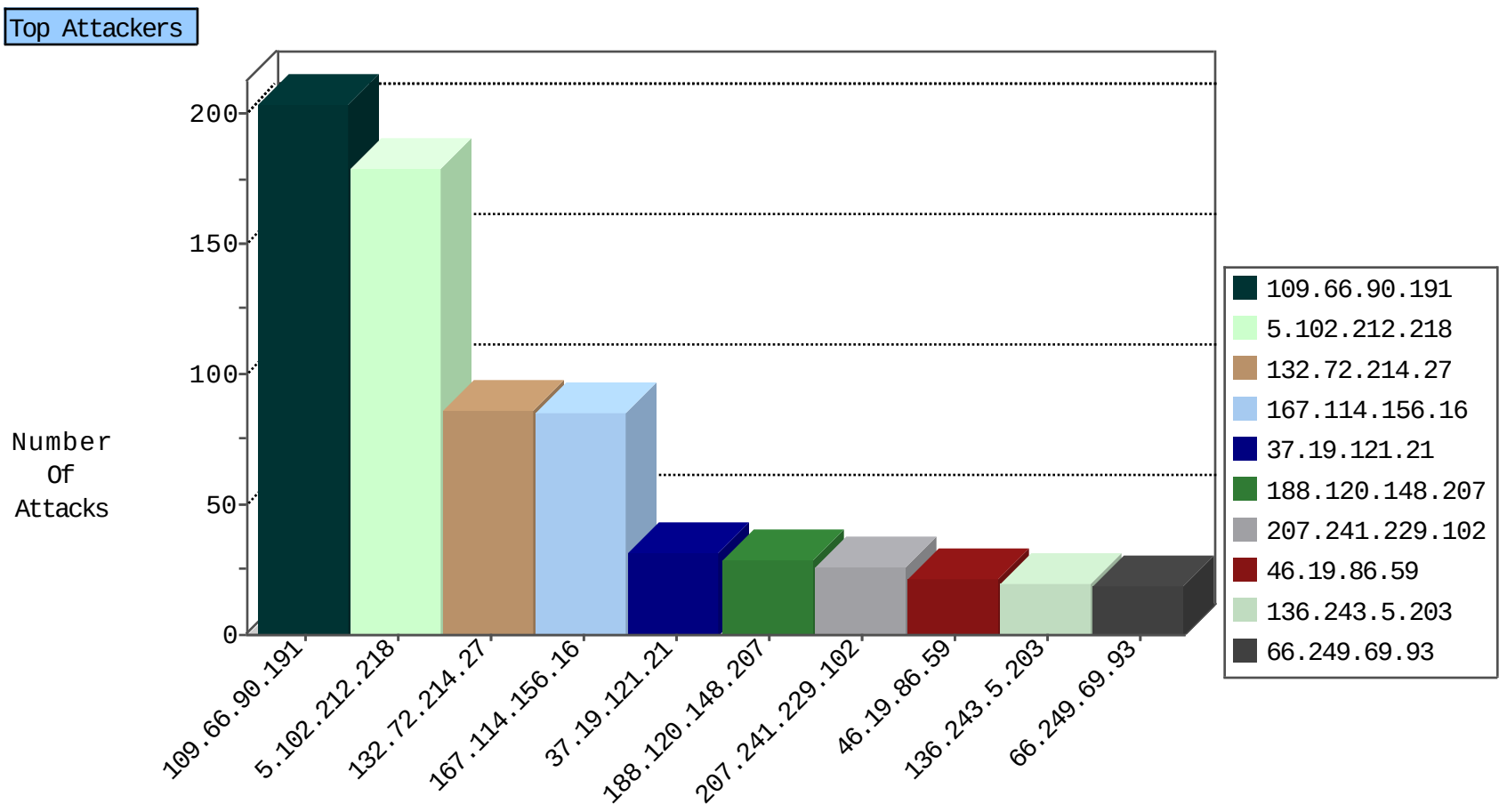
04-21-2016-00:04:08 to 04-21-2016-01:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-21-2016-00:04:08 to 04-21-2016-01:04:08

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	TCP handshake violation, first packet not syn	drop	6401
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	6027
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	23
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
79.178.0.203	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	2
69.30.226.101	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
69.30.226.222	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
185.94.111.1	Russian Federation	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
89.248.160.138	Netherlands	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
69.197.185.18	United States	147.237.72.156	aman.idf.il	block-sp-traf1	drop	1
204.12.196.237	United States	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
107.150.46.34	United States	147.237.77.205	prisha.idf.il	block-sp-traf1	drop	1
74.91.17.180	United States	147.237.77.205	prisha.idf.il	block-sp-traf1	drop	1
69.30.226.101	United States	147.237.77.234	halag.idf.il	block-sp-traf1	drop	1
107.150.46.35	United States	147.237.77.233	atal.idf.il	block-sp-traf1	drop	1
74.91.20.194	United States	147.237.77.19	law-forum.idf.il	block-sp-traf1	drop	1
89.248.160.138	Netherlands	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
74.91.23.110	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	drop	1
69.30.198.147	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1

04-21-2016-00:04:08 to 04-21-2016-01:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-21-2016-00:04:08 to 04-21-2016-01:04:08

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	2
107.158.255.194	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -f -sS	1
78.110.4.98	147.237.76.42	Saudi Arabia	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.214.29.239	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
78.110.4.98	147.237.0.33	Saudi Arabia	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.214.29.239	147.237.76.30	United States	himush.idf.il	ET SCAN Potential SSH Scan	1
13.94.239.168	147.237.8.27	United States	e.madim.atal.idf.i	ET SCAN Potential SSH Scan	1
104.214.29.239	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
93.180.66.29	147.237.72.166	Netherlands	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.82.78.38	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
190.249.121.171	147.237.0.35	Colombia	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
78.110.4.98	147.237.76.198	Saudi Arabia	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
115.29.197.215	147.237.76.31	China	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
78.110.4.98	147.237.76.148	Saudi Arabia	gqcenter.aka.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
107.158.255.194	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
78.110.4.98	147.237.76.86	Saudi Arabia	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.232.98.3	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
78.110.4.98	147.237.76.34	Saudi Arabia	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.214.29.239	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
78.110.4.98	147.237.0.15	Saudi Arabia	kosher-kravi.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
104.214.29.239	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
13.94.239.168	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
104.214.29.239	147.237.0.15	United States	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
93.180.66.29	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.82.78.38	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
117.196.212.51	147.237.0.34	India	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
78.110.4.98	147.237.76.177	Saudi Arabia	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
113.240.250.154	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
78.110.4.98	147.237.76.147	Saudi Arabia	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

04-21-2016-00:04:08 to 04-21-2016-01:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.66.90.191	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	192
207.241.229.102	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	26
188.120.148.207	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
66.249.69.93	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
41.68.183.223	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
37.19.121.21	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
37.19.121.21	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
109.66.90.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
162.243.126.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
41.68.164.73	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
41.68.139.58	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
176.13.4.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.199.182.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
185.120.126.205	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
45.35.64.142	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
188.120.154.229	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	7
41.33.40.209	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
188.120.148.207	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
149.78.206.98	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.22.135.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.159.148.223	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.148.215	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
149.78.206.98	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
176.13.17.87	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.69.245.123	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.66.47	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.159.148.223	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
41.68.136.52	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.66.187	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
149.78.206.98	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
94.159.148.223	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.228.15.39	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
185.120.126.205	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
84.228.15.39	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.120	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.120	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.76.111.211	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.253.130.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
87.69.245.123	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.13.17.150	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
65.156.61.234	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
149.88.206.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.244.65.130	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.109.126.46	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.102.212.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	179
132.72.214.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
46.19.86.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
46.19.86.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.117.60.238	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
31.168.186.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
139.129.130.253	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
31.210.188.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
41.33.40.209	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
207.46.13.80	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus×• ×'×—×¨×•	Block	1
58.100.11.222	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 58.100.11.222	Block	1
93.90.33.99	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-en/cogat.aspx	Block	1
66.249.66.114	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/1206	Block	1
149.78.37.96	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	1
93.90.33.99	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/1395-en/dover.aspx	Block	1
69.30.226.222	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to www.369bs.com/	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/unselecatble.aspx	Block	1
66.249.64.108	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
93.90.33.99	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation SortDir in www.cogat.idf.il/901-en/cogat.aspx	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
149.78.37.96	United States	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
109.65.131.116	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
77.75.79.54	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/29/	Block	1
66.249.64.113	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/2/662.pdf	Block	1
139.129.130.253	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 139.129.130.253	Block	1
40.77.167.73	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/klali.aspx	Block	1
93.90.33.99	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation lang in www.cogat.idf.il/901-en/cogat.aspx	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8865-he/refuah.aspx	Block	1
149.78.37.96	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/xmlrpc.php	Block	1
130.185.155.74	Sweden	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
79.178.187.85	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	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
139.129.130.253	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
93.90.33.99	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1395-en/dover.aspx	Block	1
69.30.198.147	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to www.app-softwares.com/	Block	1
58.100.11.222	China	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/miluim/about.aspx	Block	1
176.116.223.94	Russian Federation	147.237.0.34	tikshuv.idf.il	Multiple Admin Blocking from 176.116.223.94	Block	1
130.185.155.74	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
84.228.15.39	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
66.249.65.224	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/contactus/contactus.aspx	Block	1
41.109.232.21	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
149.78.37.96	United States	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
93.90.33.99	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1395-en/dover.aspx	Block	1
69.30.226.101	United States	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on www.369bs.com/	Block	1