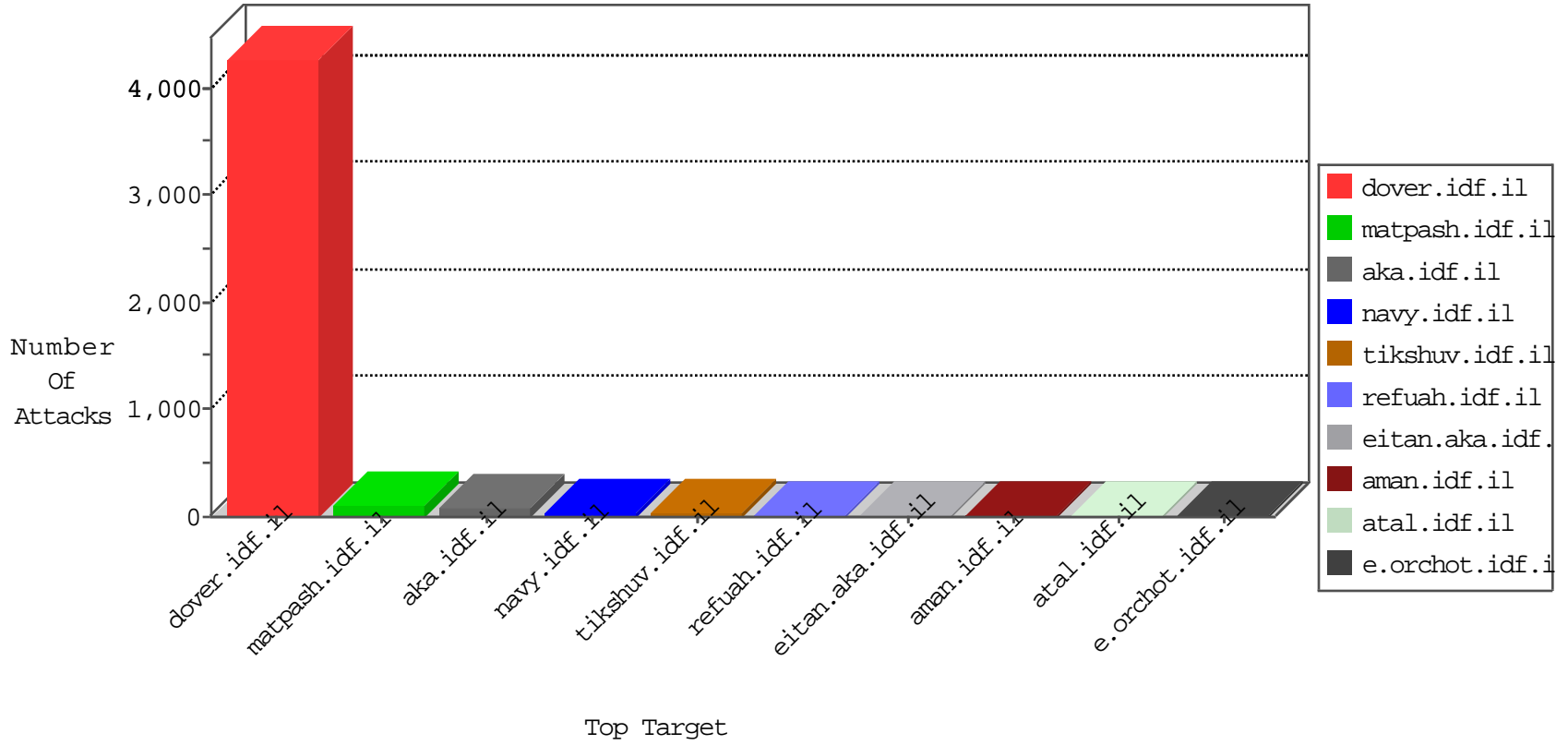


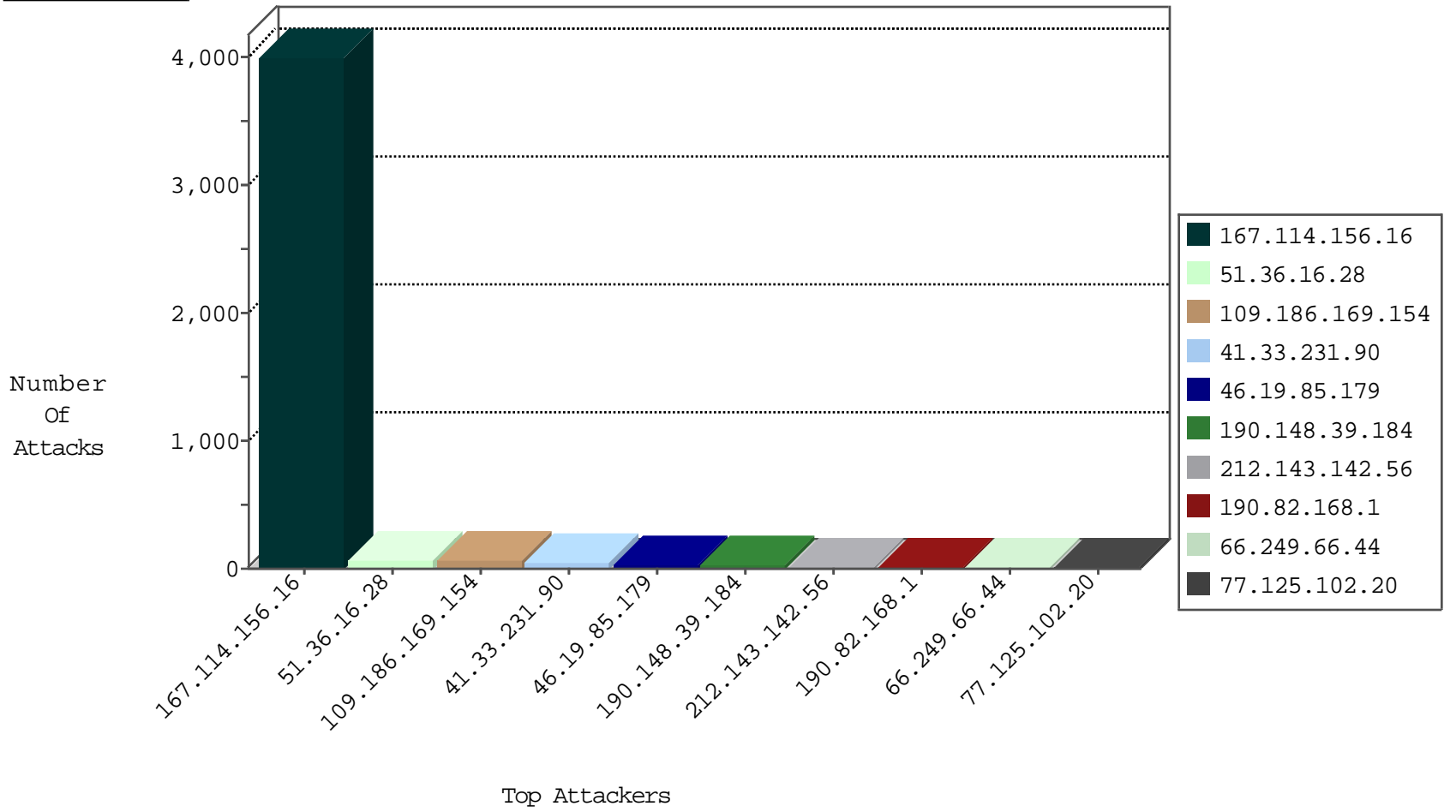
# IDF Under Attack Daily Report



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_Tp_Web_In	drop	4011
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
222.186.58.188	China	147.237.0.15	kosher-kravi.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
185.94.111.1	Russian Federation	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.8.46	e.chinuch.idf.il	Block_Ntp_All_Net	drop	1
69.64.55.124	United States	147.237.77.179	e.mazi.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
81.211.8.238	Europe	147.237.77.243	mobile.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
10.0.0.3		147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
109.65.170.167	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
109.64.102.199	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
61.135.189.114	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	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
87.106.233.202	147.237.72.166	Germany	aka.idf.il	ET SCAN NMAP -sS window 1024	1
84.200.15.174	147.237.77.121	Germany	e.navy.idf.il	ET SCAN NMAP -f -sS	1
59.45.79.103	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.103	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
46.4.79.76	147.237.8.14	Germany	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
40.84.149.32	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
84.200.15.174	147.237.77.121	Germany	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
59.45.79.103	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.103	147.237.8.46	China	e.chimuch.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.103	147.237.0.16	China	ny-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
46.4.79.76	147.237.0.200	Germany	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
40.84.149.32	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -f -sS	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
51.36.16.28	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	70
109.186.169.154	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	68
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
190.148.39.184	Guatemala	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	10
66.249.66.44	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.179	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
77.125.102.20	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.179	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.181.132.4	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.65.62.55	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
176.13.10.91	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
80.246.133.223	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
149.78.49.241	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.64.102.199	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.194	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
190.148.39.184	Guatemala	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
65.55.210.12	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
69.58.178.59	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.179	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.53.132.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.102.9.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
176.13.2.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.36.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.148.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.47	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
190.148.39.184	Guatemala	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
62.128.48.130	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
87.71.44.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
190.82.168.1	Chile	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.179	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
37.46.39.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
82.205.8.223	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
190.82.168.1	Chile	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
84.94.45.31	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
206.227.136.100	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
5.22.130.246	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
190.106.132.240	Argentina	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
85.114.119.192	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
190.148.39.184	Guatemala	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
62.128.48.130	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
87.70.42.196	Israel	147.237.77.233	atal.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	2
79.176.16.150	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
178.252.150.67	Iran, Islamic Republic of	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
79.177.231.228	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
190.106.132.240	Argentina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
178.252.150.67	Iran, Islamic Republic of	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
82.205.8.223	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
213.151.51.194	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.178.220.8	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationsevice.aspx/getauthuser	Block	3
109.253.202.62	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/894-ar	Block	3
157.55.39.217	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
58.11.113.147	Thailand	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/4/#99	Block	1
190.23.193.158	Paraguay	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/4/#39	Block	1
2.53.30.168	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
120.52.72.19	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/4/#14	Block	1
54.67.87.237	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/4/#36	Block	1
186.203.134.5	Brazil	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/4/#91	Block	1
93.77.110.204	Ukraine	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/eitan/main/	Block	1
79.178.192.192	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
52.26.218.173	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/4/#18	Block	1
169.0.9.247	South Africa	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/4/#89	Block	1
124.120.165.75	Thailand	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/4/#51	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
198.167.241.26	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
41.44.208.183	Egypt	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/4/#5	Block	1
115.87.239.61	Thailand	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/4/#61	Block	1
54.191.199.253	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 54.191.199.253	Block	1
189.218.120.209	Mexico	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/sip_storage/files/4/	Block	1
54.67.61.145	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/4/#34	Block	1
181.215.107.131	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/4/#96	Block	1
85.114.119.192	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	1
52.11.155.60	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/4/#23	Block	1
124.122.235.48	Thailand	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/4/#11	Block	1
73.97.180.170	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
222.93.156.205	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/4/#57	Block	1
61.90.53.109	Thailand	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/4/#30	Block	1
190.203.216.30	Venezuela	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/4/#70	Block	1
5.135.190.199	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/4/#50	Block	1
120.52.72.56	China	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/sip_storage/files/4/	Block	1
54.67.101.183	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/4/#43	Block	1
186.212.10.124	Brazil	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 186.212.10.124	Block	1
95.31.134.206	Russian Federation	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
52.27.169.101	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/4/#95	Block	1
178.245.190.57	Turkey	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/sip_storage/files/4/	Block	1
41.45.227.140	Egypt	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/4/#93	Block	1
124.120.171.177	Thailand	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/4/#35	Block	1
66.249.78.111	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
201.172.96.35	Mexico	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/sip_storage/files/4/	Block	1
117.135.251.132	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/4/#29	Block	1
54.191.253.135	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/4/#26	Block	1
189.219.96.40	Mexico	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/sip_storage/files/4/	Block	1
54.67.62.186	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/4/#12	Block	1
183.111.169.201	Korea, Republic of	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/4/#67	Block	1
91.121.94.39	France	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 91.121.94.39	Block	1
223.119.2.73	Hong Kong	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 223.119.2.73	Block	1
52.24.229.157	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/4/#45	Block	1
77.125.102.20	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1